ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ: ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ: ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΤΙΣ ΕΦΑΡΜΟΓΕΣ ΤΟΥΣ

ΣΠΟΥΔΑΣΤΕΣ: ΡΑΠΤΗ ΚΑΤΕΡΙΝΑ
ΣΦΥΡΑΚΗ ΜΑΡΙΑ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ: ΣΤΑΜΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΠΑΤΡΑ, ΔΕΚΕΜΒΡΙΟΣ 2009

Η παρούσα πτυχιακή εργασία αφιερώνεται:

Στους γονείς μου,

Στα αδέρφια μου,

Στην Σοφία, στην Αναστασία,

Στο φίλο μου Γιάννη.

Ράπτη Κατερίνα

Στους γονείς μου που με υποστηρίζουν σε κάθε μου επιλογή και στην αδερφή μου Ειρήνη.

Σφυράκη Μαρία

Τέλος, ευχαριστούμε θερμά τον επιβλέποντα καθηγητή

Κ. Στάμο Κωνσταντίνο.

Περιεχόμενα

Πρόλογος

Η ανάπτυξη των πληροφοριακών συστημάτων στις μέρες μας είναι ραγδαία. Καθημερινά πλήθος εργασιών πραγματοποιούνται μέσου της χρήσης ηλεκτρονικού υπολογιστή. Από μια απλή ανταλλαγή μηνυμάτων μεταξύ δύο φίλων, την διαχείριση εμπορικών συναλλαγών μιας επιχείρησης μέχρι την πραγματοποίηση μιας χειρουργικής επέμβασης από απόσταση. Η χρήση διαφόρων πληροφοριακών συστημάτων είναι πλέον μέρος της ζωής μας. Όμως, θα πρέπει όλες οι εφαρμογές των πληροφοριακών συστημάτων να διέπονται από ασφάλεια. Αν αυτό δεν συμβαίνει τότε δημιουργούνται σοβαρά προβλήματα. Επιπλέον, έχει αυξηθεί και ο αριθμός αυτών που έχει ουσιαστικό συμφέρον στο να χαρακτηρίζεται ένα πληροφοριακό σύστημα ασφαλές. Στην παρούσα πτυχιακή εργασία παρουσιάζουμε τις κυριότερες προσεγγίσεις του θέματος της ασφάλειας των πληροφοριακών συστημάτων. Δίνουμε επίσης ένα εννοιολογικό πλαίσιο που εμφανίζει το πόσοι διαφορετικοί παράγοντες παίζουν καθοριστικό ρόλο στη διαμόρφωση της ασφάλειας ενός πληροφοριακού συστήματος.

1. Εισαγωγή

Τα Πληροφοριακά Συστήματα είναι πολύπλοκα τεχνουργήματα τα οποία συνήθως δυσκολεύονται να τα ορίσουν οι άνθρωποι. Τις περισσότερες φορές τα ταυτίζουν με την τεχνολογική υποδομή. Ένα πληροφοριακό σύστημα αποτελείται από πέντε συστατικά στοιχεία τα οποία είναι: το υλικό, λογισμικό, οι διαδικασίες, οι άνθρωποι και τα δεδομένα. Ο όρος ασφάλεια πληροφοριακών συστημάτων (information systems security) δίνει έμφαση στην προστασία αυτών των συστατικών στοιχείων ενός ΠΣ αλλά και του ίδιου του ΠΣ στην ολότητά του. Αρκετά συχνά απαντάται ο όρος ασφάλεια στις τεχνολογίες πληροφορικής και επικοινωνιών. Ο όρος αυτός δίνει έμφαση στους τεχνικούς παράγοντες που σχετίζονται με την ασφάλεια.

Όπως ορίζεται στο βιβλίο του Κιουντούζη Ε., “Μοντέλα Ασφάλειας Πληροφοριακών Συστημάτων”, Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά θέματα, Εκδόσεις ΕΠΥ, Αθήνα, 1995 “η Ασφάλεια Πληροφοριακού Συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του Πληροφοριακού Συστήματος, αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.” Ο ορισμός αυτός δίνει έμφαση όχι μόνο στο ΠΣ ως ολότητα αλλά και στα επιμέρους στοιχεία του, ενώ η αναφερόμενη προφύλαξη αφορά κάθε είδους απειλή (τυχαία ή σκόπιμη). Η ασφάλεια του ΠΣ συνδέεται άμεσα τόσο με τις τεχνικές, τις διαδικασίες και τα διοικητικά μέτρα όσο και με ηθικοκοινωνικές αντιλήψεις, αρχές και παραδοχές. Είναι βέβαια προφανές ότι η προφύλαξη δεν θα πρέπει να παρεμποδίζει την απρόσκοπτη λειτουργία του συστήματος και την ελεύθερη διακίνηση των πληροφοριών, έτσι ώστε να μην θέτονται αδικαιολόγητοι φραγμοί στην ανάπτυξη της τεχνολογίας της πληροφορίας.

Η ασφάλεια πληροφοριών αναφέρεται αποκλειστικά στην προστασία των πληροφοριών και είναι στενότερη έννοια από αυτή της ασφάλειας ΠΣ, αφού η πληροφορία εμπεριέχεται σε ένα ΠΣ. Βέβαια η ασφάλεια πληροφοριών δεν μπορεί να αγνοήσει το πληροφοριακό σύστημα, στα πλαίσια του οποίου παράγεται και χρησιμοποιείται η πληροφορία. Αντίθετα, κάθε αναλυτική εργασία, η οποία αποσκοπεί στην ανάπτυξη και διαχείριση της ασφάλειας των πληροφοριών, θα πρέπει να στηρίζεται στην κατανόηση των σχετικών πληροφοριακών συστημάτων.

Συνεπώς, όταν αναφερόμαστε στην ασφάλεια ενός ΠΣ η προστασία όλων των υλικών που μετέχουν σε αυτό έχει ιδιαίτερη σημασία, ενώ όταν αναφερόμαστε στην ασφάλεια πληροφοριών, η ασφάλεια του υλικού μας ενδιαφέρει μόνο στο βαθμό που σχετίζεται με την προστασία των πληροφοριών.

Τα Πληροφοριακά Συστήματα απαιτούν ξεχωριστό τρόπο αντιμετώπισης για τρεις διαφορετικού λόγους. Αυτοί είναι οι παρακάτω:

Πρώτον, σχετίζονται διπλά με τον άνθρωπο, αφού δημιουργούνται από αυτόν και λειτουργούν με τη βοήθεια του, έτσι ώστε να υπηρετήσουν πάλι αυτόν. Ο άνθρωπος όμως έχει συμπεριφορά η οποία δύσκολα μπορεί να εκτιμηθεί και ακόμη πιο δύσκολα να προβλεφθεί. Συνεπώς δεν είναι σίγουρο ότι πάντα οι ίδιοι άνθρωποι, κάτω από τις ίδιες συνθήκες, θα έχουν την ίδια συμπεριφορά.

Δεύτερον, σχετίζονται με την πληροφορία, ένα αγαθό με πάρα πολύ μεγάλη ζήτηση και με μία σειρά από σημαντικές διαφορές έναντι δύο άλλων σημαντικών αγαθών: της ύλης και της ενέργειας. Ενώ οι τελευταίες μπορούν να αποτελέσουν αντικείμενο αποκλειστικών δικαιωμάτων υπέρ κάποιου δικαιούχου, η πληροφορία, σε μερικές περιπτώσεις, θα πρέπει να διαδίδεται και να κυκλοφορεί ελεύθερα. Παράλληλα η πληροφορία είναι ανεξάντλητη, όσο περισσότερο την χρησιμοποιεί ένας Οργανισμός, τόσο περισσότερο έχει την ανάγκη της. Επί πλέον αυξάνει την αξία της όταν συνδυάζεται με άλλες πληροφορίες. Τέλος μια πληροφορία μπορεί να αναπαραχθεί άπειρες φορές, χωρίς να αλλοιωθεί το πρωτότυπό της. Συνεπώς τυχόν «κλοπή» της δεν γίνεται εύκολα αντιληπτή.

Τρίτον, στηρίζονται στην πληροφορική, μια τεχνολογία που χαρακτηρίζεται από μεγάλο ρυθμό ανάπτυξης. Ακόμη, με την πληροφορική, οι διαδικασίες επεξεργασίας πληροφοριών παρουσιάζουν μεγάλα περιθώρια προστιθέμενης αξίας.

Τέλος, το όλο Πληροφοριακό Σύστημα είναι ζωτικής σημασίας για μια επιχείρηση και αποτελεί σημαντική οικονομική επένδυση.

Από τα παραπάνω γίνεται φανερό ότι τα Πληροφοριακά Συστήματα θα πρέπει να προστατεύονται από τις κάθε μορφής απειλές, χωρίς όμως, ταυτόχρονα, η προστασία αυτή να εμποδίζει τη ροή των πληροφοριών.

Μια σειρά από επιστημονικές έρευνες έχουν δείξει ότι διαφορετικοί χρήστες ορίζουν το ίδιο πληροφοριακό σύστημα διαφορετικά, ανάλογα με τις γνώσεις τους, την πείρα τους, τον ρόλο τους κ.λπ.

Όλα τα παραπάνω δικαιολογούν το γιατί η ασφάλεια ενός πληροφοριακού συστήματος παρουσιάζει ιδιαιτερότητες και δυσκολίες ως επιστημονικός ερευνητικός χώρος αλλά και ως επιστημονική πρακτική.

1.1 Ιστορική εξέλιξη

Η ασφάλεια πληροφοριακών συστημάτων μελετήθηκε για πρώτη φορά στις αρχές της δεκαετίας του 1970. Η πρώτη σχετική δημοσίευση, από την Ομάδα Εργασίας του Συμβουλίου Αμυντική Επιστήμης του υπουργείου Άμυνας των ΗΠΑ, εξέτασε το πρόβλημα της χρήσης υπολογιστών εξ αποστάσεως (μέσω τερματικών).

Προηγουμένως, η πρόσβαση στους υπολογιστικούς πόρους προϋπέθετε την φυσική παρουσία και πρόσβαση του χρήστη ή του διαχειριστή στον κεντρικό υπολογιστή. Η προσέγγιση στην λύση των προβλημάτων ασφάλειας μέχρι τότε βασιζόταν στην φυσική απομόνωση και προστασία του κεντρικού υπολογιστή καθώς και στον έλεγχο πρόσβασης σε αυτόν. Ένα από τα συμπεράσματα στην αναφορά της Ομάδας Εργασίας ήταν ότι ο χρήστης δεν θα έπρεπε να δημιουργήσει το δικό του κωδικού πρόσβασης, μια πρόταση που ποτέ δεν υιοθετήθηκε ευρέως. Άλλες καινοτόμες ιδέες που εκφράστηκαν στην ανάλυση είχαν μεγαλύτερη απήχηση. Για παράδειγμα, αναγνωρίστηκε από τους ερευνητές η αρχή της ισορροπίας μεταξύ της ευκολίας της εργασίας του χρήστη και της προστασίας των πληροφοριών και σήμερα έχει καταλήξει θεμέλιος λίθος στη δημιουργία πολιτικών ασφάλειας.

Ο πρώτος ιός, ο Creeper, εμφανίστηκε επίσης στις αρχές της δεκαετίας του 1970 στο ARPANET, και το πρώτο δικτυακό "σκουλήκι" (worm), το σκουλήκι Morris, κυκλοφόρησε το 1998. Εκτιμάται ότι 6.000 συστήματα προσβλήθηκαν από το "σκουλήκι". Το 2007 ανακαλύφθηκαν περισσότεροι από 711.000 καινούργιοι ιοί.

Παρόλο που ο πρώτος υπολογιστής με το λειτουργικό σύστημα Multics εγκαταστάθηκε το 1967 με κωδικό πρόσβασης για χρήστες και με άλλα μέτρα ασφάλειας στο σχεδιασμό του, και δύο από τους δημιουργούς του, ο Ken Thompson και ο Dennis Ritchie, έπαιξαν κρίσιμο ρόλο στην ανάπτυξη του Unix, η πρώτη έκδοση του Unix δεν διέθετε κωδικούς. Η λειτουργία αυτή προστέθηκε αργότερα, το 1973. Σήμερα η χρήση αδύναμων κωδικών πρόσβασης παραμένει μία από τις κυριότερες δυσκολίες που αντιμετωπίζει ο επαγγελματίας στον τομέα. Χρησιμοποιούνται και άλλες μέθοδοι αυθεντικοποίησης, για παράδειγμα οι έξυπνες κάρτες, αλλά μόνο σε συγκεκριμένους τομείς.

1.2 Βασικές αρχές

Η ασφάλεια πληροφοριακών συστημάτων στηρίζεται σε τρεις βασικές αρχές οι οποίες αναλύονται παρακάτω:

Ακεραιότητα (Integrity)

Η ακεραιότητα αναφέρεται στη διατήρηση των δεδομένων ενός πληροφοριακού συστήματος σε μια γνωστή κατάσταση χωρίς ανεπιθύμητες τροποποιήσεις, αφαιρέσεις ή προσθήκες από μη εξουσιοδοτημένα άτομα, καθώς και την αποτροπή της πρόσβασης ή και χρήσης των υπολογιστών και δικτύων του συστήματος από άτομα χωρίς άδεια.

Επομένως, σημαίνει ότι η μετατροπή, διαγραφή και δημιουργία των δεδομένων ενός υπολογιστικού συστήματος, γίνεται μόνο από εξουσιοδοτημένα μέρη.

Για παράδειγμα, μια εφημερίδα που δημοσιεύει τα άρθρα της και στο Διαδίκτυο θα ήθελε αυτά τα άρθρα να είναι ασφαλή από μετατροπές ενός χάκερ που επιθυμεί να εισάγει λανθασμένες πληροφορίες στα κείμενα. Ακριβώς αυτό συνέβη το 1995, όταν άγνωστα άτομα κατάφεραν να εξουδετερώσουν τα μέτρα ασφάλειας της Ελευθεροτυπίας και να εισαγάγουν πρωτοσέλιδο άρθρο για τον πρόωρο θάνατο του Ανδρέα Παπανδρέου, που εκείνη τη στιγμή νοσηλευόταν στο Ωνάσειο.

Διαθεσιμότητα (Availability)

Διαθεσιμότητα ονομάζεται η ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός δικτύου υπολογιστών όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Με τον όρο διαθεσιμότητα εννοούμε ότι τα δεδομένα είναι προσβάσιμα και οι υπηρεσίες λειτουργούν, παρά τις όποιες τυχόν διαταραχές, όπως διακοπή τροφοδοσίας, φυσικές καταστροφές, ατυχήματα ή επιθέσεις. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των υπολογιστών του δικτύου δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν τους πόρους του δικτύου.

Για τους σκοπούς της ασφάλειας, μας απασχολεί βασικά η παρεμπόδιση κακόβουλων επιθέσεων που αποσκοπούν στο να παρακωλύσουν την πρόσβαση των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Αυτές οι επιθέσεις

ονομάζονται επιθέσεις άρνησης παροχής υπηρεσιών. Η άρνηση παροχής υπηρεσιών σημαίνει παρεμπόδιση της εξουσιοδοτημένης προσπέλασης πληροφοριών και πόρων ή πρόκληση καθυστέρησης των λειτουργιών που είναι κρίσιμες στο χρόνο. Η αντιμετώπισή τους αποσκοπεί στο να υπερνικήσει την σκόπιμη, που προκαλείται από κακόβουλα μέρη, παρά τυχαία απώλεια της διαθεσιμότητας. Ένα παράδειγμα επίθεσης άρνησης παροχής υπηρεσιών είναι οι επιθέσεις «πλημμύρας» στο διαδίκτυο, όπου ο επιτιθέμενος κατακλύζει έναν εξυπηρετητή στέλνοντάς του έναν τεράστιο αριθμό αιτήσεων σύνδεσης.

Παρόλο που η διαθεσιμότητα συχνά αναδεικνύεται στο πλέον σημαντικό χαρακτηριστικό της ασφάλειας, εντούτοις λίγοι μηχανισμοί υπάρχουν για να βοηθήσουν στην υποστήριξή της.

Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα σημαίνει ότι ευαίσθητες πληροφορίες δεν θα έπρεπε να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.

Η διαρροή ευαίσθητων πληροφοριών μπορεί να γίνει με πιο παραδοσιακές μεθόδους από την ψηφιακή υποκλοπή, π.χ. με την κλοπή φορητών υπολογιστών από το κατάλληλο τμήμα μιας εταιρίας. Το 2006 μια μελέτη με τη συνεργασία 480 εταιριών έδειχνε ότι 80% των εταιριών είχε πρόβλημα με διαρροή πληροφοριών λόγο κλοπής φορητού.

Σε πολλές περιπτώσεις της καθημερινής ζωής οι έννοιες της ασφάλειας και της εμπιστευτικότητας σχεδόν ταυτίζονται, όπως για παράδειγμα στα στρατιωτικά περιβάλλοντα όπου η ασφάλεια έχει τη σημασία του να κρατούνται μυστικές οι πληροφορίες.

Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κανείς έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε.

Άλλες εκφάνσεις της εμπιστευτικότητας είναι:

- Η ιδιωτικότητα: προστασία των δεδομένων προσωπικού χαρακτήρα, δηλαδή αυτών που αφορούν συγκεκριμένα πρόσωπα και
- Η μυστικότητα: προστασία των δεδομένων που ανήκουν σε έναν οργανισμό ή μια επιχείρηση.

1.3 Ασφάλεια και προστασία ενός Π.Σ. σαν κοινωνική υπόθεση

Πολλοί είναι αυτοί που πιστεύουν ότι άμεσο συμφέρον από την ύπαρξη μέτρων ασφάλειας στο Πληροφοριακό Σύστημα έχουν μόνο οι ιδιοκτήτες και κατ' επέκταση οι σχεδιαστές του. Σήμερα όμως που το Πληροφοριακό Σύστημα παίζει ένα σημαντικό ρόλο μέσα στο "υπερσύστημα", που μπορεί να είναι είτε κάποια επιχείρηση ή οποιοσδήποτε φορέας, αυξήθηκαν και αυτοί που έχουν συμφέρον , άρα και δικαίωμα απαίτησης, το Π.Σ. να ικανοποιεί κάποιους κανόνες ασφάλειας και προστασίας.

Αυτοί που επιδιώκουν να υπάρχουν μηχανισμοί και μέτρα ασφάλειας είναι:

- Ο **Ιδιοκτήτης** του συστήματος, γιατί όλο και περισσότερο η επιχείρησή του εξαρτάται από την απρόσκοπτη λειτουργία του Π.Σ.. Επίσης η δαπάνη που απαιτείται για την δημιουργία του Π.Σ. είναι πολύ μεγάλη.
- Ο **Σχεδιαστής**, ο οποίος προσπαθεί να ικανοποιήσει τις απαιτήσεις που έχει καθορίσει ο αναλυτής για λογαριασμό του ιδιοκτήτη.
- Ο **Χρήστης**, που θέλει να μην εμποδίζονται οι λειτουργίες του συστήματος από οποιαδήποτε παραβίαση.
- Ο **Πελάτης**, γιατί κατά κύριο λόγο αυτός είναι που εξαρτάται από τη σωστή λειτουργία του συστήματος. Παράδειγμα, ο πελάτης μιας τράπεζας, ο ασθενής ενός νοσοκομείου, ο πελάτης μιας αεροπορικής εταιρείας κ.α.

1.4 Επίπεδα προστασίας των πληροφοριακών συστημάτων

Η ασφάλεια και προστασία του Π.Σ. μπορεί να διαχωριστεί σε επιμέρους επίπεδα, έτσι ώστε να είναι δυνατή η παρακολούθηση των αδυναμιών από την μία, και η εύρεση λύσεων αποφυγής των απωλειών από την άλλη.

Έτσι διακρίνονται τα παρακάτω επίπεδα:

α) Φυσική Ασφάλεια του Π.Σ..

β) Ασφάλεια Λειτουργικών Συστημάτων.

γ) Ασφάλεια Δικτύων Υπολογιστικών Συστημάτων.

δ) Ασφάλεια των Συστημάτων Βάσεων Δεδομένων.

1.4.1 Φυσική ασφάλεια του πληροφοριακού συστήματος

Η Φυσική Ασφάλεια του Π.Σ. αναφέρεται κυρίως στην αντιμετώπιση πυρκαγιών, πλημμύρων, σεισμών κ.α. Η σωστή αντιμετώπισή τους εξαρτάται από τον κατάλληλο σχεδιασμό του κτιρίου του Κέντρου Πληροφορικής, την κατάλληλη εκπαίδευση του προσωπικού και των κατάλληλων μηχανισμών προστασίας, όπως συσκευών πυρόσβεσης. Απαραίτητη επίσης είναι η συστηματική συντήρηση των ηλεκτρικών εγκαταστάσεων. Χρήσιμη είναι η ύπαρξη γεννήτριας παροχής ηλεκτρικής ενέργειας ή συστήματος αδιάλειπτης παροχής τάσεως (UPS), για να αποφεύγονται πιθανές απώλειες του λογισμικού και να υποστηρίζεται η καλή λειτουργία του μηχανολογικού εξοπλισμού κατά την πτώση της τάσης του ρεύματος ή διακοπής της παροχής του ηλεκτρικού ρεύματος. Πολλά από τα παραπάνω παραλείπονται λόγω του υψηλού τους κόστους.

1.4.2 Ασφάλεια λειτουργικών συστημάτων

Η κρισιμότερη συνιστώσα ενός Πληροφοριακού Συστήματος είναι το Λειτουργικό Σύστημα (Operating System). Λειτουργικό Σύστημα ενός υπολογιστή ονομάζεται το προϊόν λογισμικού που ελέγχει την εκτέλεση των προγραμμάτων και παρέχει υπηρεσίες χρονοδρομολόγησης (scheduling), σφαλματοθυρίας (debbuging), ελέγχου εισόδου-εξόδου (I-O control), μεταγλώττισης (compilation), διαχείρισης μνήμης (memory management) και άλλες σχετικές.

Ιδιότητες ενός Λ.Σ. - σημεία ευπάθειας ενός Λ.Σ.

Οι ιδιότητες που πρέπει να διαθέτει ένα Λ.Σ. είναι οι εξής :

- Ευχρηστία (Usability). Το σύστημα πρέπει να είναι σχεδιασμένο με στόχο την διευκόλυνση του χρήστη.
- Γενικότητα (Generality). Το σύστημα πρέπει να μπορεί να εκτελέσει ποικίλες διαδικασίες, σύμφωνα με τις ανάγκες του χρήστη.
- Αποδοτικότητα (Effeciency). Το σύστημα πρέπει να λειτουργεί γρήγορα και ορθά, χρησιμοποιώντας κατά βέλτιστο τρόπο τους διατιθέμενους πόρους.

- Ευελιξία (Flexibility). Το σύστημα πρέπει να μπορεί να προσαρμόζεται σε διαρκώς μεταβαλλόμενες καταστάσεις.
- Αδιαφάνεια (Opacity). Ο χρήστης πρέπει να γνωρίζει μόνο ότι είναι απαραίτητο για να διεκπεραιώσει την εργασία του .
- Ασφάλεια (Security). Το σύστημα πρέπει να διαφυλάσσει τα δεδομένα ενός χρήστη από μη εξουσιοδοτημένη χρήση τους από άλλους.
- Ακεραιότητα (Integrity). Οι χρήστες και τα δεδομένα τους πρέπει να διαφυλάσσονται από απρόβλεπτες μετατροπές από μη εξουσιοδοτημένους χρήστες.
- Ευκινησία (Capacity). Οι χρήστες δεν πρέπει να υφίστανται άσκοπους περιορισμούς στις ενέργειές τους.
- Αξιοπιστία (Reliability). Τα συστήματα πρέπει να λειτουργούν σωστά, για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.
- Συντηρησιμότητα (Serviceability). Πιθανά προβλήματα στη λειτουργία του συστήματος πρέπει να μπορούν να ξεπεραστούν εύκολα και γρήγορα.
- Επεκτασιμότητα (Extentability). Το σύστημα πρέπει να μπορεί να αναβαθμισθεί εύκολα, με επέκταση των δυνατοτήτων που διαθέτει.
- Διαθεσιμότητα (Availability). Το σύστημα πρέπει να εξυπηρετεί τους χρήστες όσο το δυνατόν πληρέστερα, για όσο το δυνατόν μεγαλύτερο χρονικό διάστημα.

Από τις παραπάνω ιδιότητες διαφαίνεται ότι το Λ.Σ. αποτελεί το “ακρογωνιαίο λίθο” της σχεδίασης και της ασφαλούς λειτουργίας κάθε Π.Σ. Οποιαδήποτε μη “νόμιμη” παρέμβαση στο Λ.Σ. μπορεί να προκαλέσει σημαντικές συνέπειες στη λειτουργία του Π.Σ. όπως είναι:

- Να υποβαθμισθεί ή και να διακοπεί η λειτουργία του Π.Σ. προσωρινά ή ακόμη και μόνιμα.
- Να επιτραπεί η προσπέλαση κάποιου χρήστη σε διαβαθμισμένα δεδομένα, τα οποία τηρούνται στην προστατευμένη περιοχή.
- Να επιτραπεί η τροποποίηση δεδομένων από χρήστες οι οποίοι δεν έχουν την αντίστοιχη εξουσιοδότηση.

Τα συστατικά ενός υπολογιστικού συστήματος που απαιτούν προστασία είναι μεταξύ άλλων :

- Αρχεία και ευρετήρια αρχείων.
- Εκτελέσιμα προγράμματα.
- Συσκευές υλικού.
- Δομές δεδομένων, όπως είναι ο σωρός.
- Μνήμη άμεσης προσπέλασης (RAM).
- Εντολές του Λ.Σ. οι οποίες καθορίζουν προνόμια στους χρήστες.
- Δεδομένα του Λ.Σ., όπως πίνακες διευθύνσεων διακοπών κ.α.

Σχεδιαστικοί στόχοι - μέθοδοι υλοποίησης ενός Λ.Σ.

Για να είναι δυνατή η προστασία όλων των παραπάνω, πρέπει να έχει προηγηθεί κατάλληλη σχεδίαση του Λ.Σ. Οι στόχοι στους οποίους η σχεδίαση πρέπει να αποβλέπει είναι οι εξής:

- Φυσικός Διαχωρισμός Διαδικασιών. Με τη μέθοδο αυτή κάθε χρήστης διαθέτει συσκευές και χώρο μνήμης τον οποίο χρησιμοποιεί αποκλειστικά ο ίδιος.
- Προσωρινός Διαχωρισμός Διαδικασιών. Με τη μέθοδο αυτή διαδικασίες διαφορετικής διαβάθμισης εκτελούνται σε διαφορετικά χρονικά διαστήματα.
- Λογικός Διαχωρισμός ή Απομόνωση. Με τη μέθοδο αυτή οι χρήστες μπορούν να εργάζονται διαδοχικά, χρησιμοποιώντας τα ίδια μέσα του συστήματος, αλλά δεν είναι δυνατή καμία ανταλλαγή δεδομένων μεταξύ τους.
- Κρυπτογραφικός Διαχωρισμός. Με τη μέθοδο αυτή είναι δυνατόν δυο χρήστες να μοιράζονται τα ίδια μέσα του συστήματος σε διαδοχική βάση, έχοντας δικαίωμα προσπέλασης ο ένας στα δεδομένα του άλλου. Η βασική διαφορά από την προηγούμενη μέθοδο είναι, ότι τα δεδομένα είναι κρυπτογραφημένα, ώστε μόνο ο νόμιμος κάτοχός τους μπορεί να τα αναγνωρίζει.

Προϋποθέσεις σχεδίασης ασφαλών Λ.Σ.

Για τη σχεδίαση ενός ασφαλούς Λ.Σ. απαιτείται η ικανοποίηση των παρακάτω προϋποθέσεων :

- Πολιτική εξασφάλισης (security policy): Πρέπει να υπάρχει μια σαφής δέσμη βασικών αρχών, η οποία περιλαμβάνει τους στόχους των σχεδιαστών του Λ.Σ.
- Ταυτοποίηση (identification): Κάθε αντικείμενο του συστήματος πρέπει να μπορεί να αναγνωρισθεί θετικά.

- Σήμανση (marking): Κάθε αντικείμενο του συστήματος πρέπει να συνοδεύεται από μια ένδειξη του βαθμού εμπιστευτικότητας του.
- Ελεγκτικότητα (accountability): Το Λ.Σ. πρέπει να καταγράφει όλες τις ενέργειες που αφορούν ή μπορούν να επηρεάσουν την ασφάλεια του.
- Διαβεβαίωση (assurance): Το σύστημα πρέπει να παρέχει τεχνικές ρυθμίσεις για την υλοποίηση της πολιτικής εξασφάλισής του, οι οποίες να μπορούν να εκτιμηθούν ως προς την αποτελεσματικότητά τους.
- Συνεχής προστασία (continuous protection): Οι τεχνικές εξασφάλισης του Λ.Σ. πρέπει να προστατεύονται από κάθε ανεπιθύμητη μετατροπή.

2. Κίνδυνοι των πληροφοριακών συστημάτων

2.1 Γιατί οι υπολογιστές δεν είναι ασφαλείς

Ένα εύλογο ερώτημα που απασχολεί τον σύγχρονο άνθρωπο ο οποίος βλέπει την τεχνολογία των ηλεκτρονικών υπολογιστών να καλπάζει και να αναπτύσσεται με τρομακτικούς ρυθμούς, είναι το γιατί οι υπολογιστές είναι τόσο ανασφαλείς. Από όσα βρέθηκαν σε Ελληνική αλλά και ξένη βιβλιογραφία η μεγάλη πλειοψηφία των περιπτώσεων εισβολών σχετίζεται με ένα από τα παρακάτω προβλήματα:

Η ασφάλεια έχει το κόστος της

Οι διαχειριστές συχνά δεν υλοποιούν χαρακτηριστικά ασφαλείας μέσα σε λειτουργικά συστήματα, επειδή αν το κάνουν αυτό δημιουργούν προβλήματα στους χρήστες. Από την άλλη πλευρά οι χρήστες συχνά παρακάμπτουν την ασφάλεια αφού επιλέγουν εύχρηστους κωδικούς πρόσβασης χωρίς να τους αλλάζουν στη συνέχεια και χωρίς να διστάζουν να τους αποκαλύπτουν σε συνεργάτες και άλλους χρήστες. Οι προμηθευτές παραδίδουν το λογισμικό τους, έτσι ώστε να μπορεί να εγκατασταθεί με τα περισσότερα χαρακτηριστικά του και με ανενεργά τα χαρακτηριστικά ασφαλείας του. Με αυτόν τον τρόπο οι άπειροι χρήστες δεν χρειάζεται να κατανοούν και να διαμορφώνουν το λογισμικό σωστά πριν να το χρησιμοποιήσουν με αποτέλεσμα τις περισσότερες φορές οι εγκαταστάσεις των υπολογιστών να μην είναι σωστά ασφαλισμένες.

Τα χαρακτηριστικά παραδίδονται βιαστικά στην αγορά

Οι κατασκευαστές συστημάτων ηλεκτρονικών υπολογιστών επικεντρώνουν την προσοχή τους στην προσθήκη χαρακτηριστικών που κάνουν το λογισμικό τους περισσότερο χρήσιμο και αδιαφορούν για την παράμετρο της ασφάλειας. Ένα τέλειο παράδειγμα είναι η προσθήκη υποστήριξης γλώσσας προγραμματισμού στο Microsoft Outlook και το Outlook Express. Όταν το διαδίκτυο άρχισε να γίνεται ευρέως γνωστό, απειλές περί ‘e-mail ιών’ άρχισαν να κυκλοφορούν μέσω της ηλεκτρονικής αλληλογραφίας. Οι ειδικοί στην πληροφοριακή ασφάλεια τις αγνοούσαν, γνωρίζοντας ότι ένας ιός απαιτούσε κάποιο περιβάλλον εκτέλεσης όπως μια γλώσσα προγραμματισμού για να μπορέσει στην πραγματικότητα να διαδοθεί.

Έτσι γελούσαν με την ιδέα ότι κάποιος θα συνέδεε μια γλώσσα προγραμματισμού με ένα σύστημα ηλεκτρονικής αλληλογραφίας γιατί οποιοσδήποτε είχε στοιχειώδη αίσθηση της πληροφοριακής ασφάλειας δεν θα επιχειρούσε ποτέ κάτι τέτοιο. Παρά τις προειδοποιήσεις, και παρόλο που η γλώσσα προγραμματισμού που ήταν ενσωματωμένη στο Microsoft Office είχε ήδη γίνει αντικείμενο εκμετάλλευσης για την δημιουργία μακροϊών που μόλυναν έγγραφα των εφαρμογών Word και Excel, η Microsoft αγνόησε τις ρητές προειδοποιήσεις των ίδιων των υπαλλήλων της και ενσωμάτωσε μια γλώσσα προγραμματισμού στο λογισμικό της που διαχειριζόταν την ηλεκτρονική αλληλογραφία. Ακόμη χειρότερα, ήταν ρυθμισμένο εξ'ορισμού ώστε να εκτελεί αυτόματα τον κώδικα που βρισκόταν ενσωματωμένος στα αρχεία e-mail, και περιείχε λειτουργίες όπως το "auto-preview", η οποία άνοιγε τα μηνύματα για ανάγνωση μόλις κατέφθαναν και εκτελούσε τυχόν ενσωματωμένο κώδικα. Για να γίνουν τα πράγματα ακόμη πιο στυγερά, η Microsoft ενσωμάτωσε το ανασφαλές αυτό λογισμικό με κάθε αντίγραφο του απανταχού παρόντος λειτουργικού συστήματος Windows, εξασφαλίζοντας έτσι ότι θα διαδοθεί ευρέως.

Συμπεραίνει δηλαδή κανείς από αυτό πως η μόλυνση των e-mail ιών που υπάρχει σήμερα είχε προβλεφθεί, είχαν δοθεί προειδοποιήσεις και είχαν τελείως αγνοηθεί από τον συγκεκριμένο κατασκευαστή προκειμένου να υλοποιηθεί ένα αξεσουάρ λογισμικού που θα το χρησιμοποιούσαν λιγότερο από το 1% των χρηστών. Η Microsoft δεν ενδιαφέρθηκε ούτε καν με μια στοιχειώδη έρευνα των συνεπειών στην ασφάλεια που θα είχε αυτή η προσθήκη στο λογισμικό της. Δεν θα μπορούσε να κάνει καλύτερη δουλειά, ακόμη και αν δούλευε για λογαριασμό των εισβολέων.

Επισκίαση της ασφάλειας από τον ανταγωνισμό

Αυτό που κατευθύνει τις εταιρείες που ασχολούνται με τους υπολογιστές να μην δίνουν ιδιαίτερη προσοχή στην ασφάλεια των συστημάτων που παράγουν, είναι οι ίδιοι οι πελάτες που δεν δίνουν αξία στην ασφάλεια. Αν το έκαναν θα χρησιμοποιούσαν παλιότερο, καλά δοκιμασμένο, αποδεδειγμένα ασφαλές λογισμικό που θα είχε όλα τα χαρακτηριστικά των καινούριων εκδόσεων. Εταιρίες σαν την Microsoft που προσάρμοσαν τα προϊόντα τους ώστε να εργάζονται στο διαδίκτυο, αποδεκάτισαν τον ανταγωνισμό. Αν περίμεναν να τα κάνουν όλα αυτά με ασφάλεια, θα είχαν νικηθεί από κάποια άλλη εταιρεία που δεν θα έδινε σημασία στην ασφάλεια.

Ποιο ήταν το τελικό αποτέλεσμα; Τα λιγότερο ασφαλή προϊόντα φθάνουν πρώτα στην αγορά και γίνονται πρότυπα της αγοράς.

Η ταχύτητα εξέλιξης των υπολογιστών και του λογισμικού

Οι υπολογιστές και η τεχνολογία δικτύωσης εξελίσσονται πολύ γρήγορα και οι εταιρείες δεν είναι σε θέση να προβλέψουν τι θα πάει στραβά. Ο νόμος του Moore αναφέρει ότι το υλικό των υπολογιστών θα διπλασιάζεται σε ισχύ κάθε δύο χρόνια. Η πρόβλεψή του έχει αποδειχθεί ακριβής για πάνω από τρεις δεκαετίες τώρα. Πρωτόκολλα που δεν αναπτύχθηκαν ώστε να είναι ασφαλή υιοθετήθηκαν για άλλες χρήσεις, εκτός αυτών για τις οποίες αναπτύχθηκαν και έγιναν πολύ δημοφιλή σε μεγαλύτερο κοινό από αυτό που είχαν φανταστεί οι δημιουργοί τους.

Η ταχύτητα αυτή της εξέλιξης ευθύνεται ακόμη και για το ότι οι προγραμματιστές δεν μπορούν να προβλέψουν τα προβλήματα με ακρίβεια. Σπάνια σκέφτονται ότι η κατάσταση ενός προγράμματος μπορεί να αλλάξει από εξωτερικό παράγοντα όσο ο κώδικας εκτελείται και έτσι απλά ελέγχουν τον κώδικα με τις τιμές που τροφοδοτούν οι ίδιοι. Μόλις ο κώδικας περάσει τους ελέγχους αποσφαλμάτωσης, συσκευάζεται και διανέμεται, χωρίς να έχει δοκιμαστεί από μια σειρά τυχαίων δεδομένων. Ακόμη και αν προσπαθούσαν να προβλέψουν τις ατέλειες, οι δέκα προγραμματιστές που δημιούργησαν μια εφαρμογή δεν θα μπορούσαν ποτέ να φανταστούν όλες τις πιθανές επιθέσεις που τα εκατομμύρια εισβολέων θα προσπαθούσαν να δοκιμάσουν.

Έλλειψη ποικιλομορφίας στην αγορά λογισμικού

Το μονοπώλιο των λειτουργικών συστημάτων Windows και Unix έχει μειώσει τους στόχους των εισβολέων στις μικρές παραλλαγές αυτών των δύο λειτουργικών συστημάτων. Στις περισσότερες εφαρμογές, το ένα από τα δύο αυτά προϊόντα κατέχει τη μερίδα του λέοντος, οπότε οι εισβολείς αρκεί να σπάσουν μόνο το ένα πρόγραμμα για να αποκτήσουν ευρεία πρόσβαση σε μεγάλο πλήθος υπολογιστών.

Για να αποφύγουν προβλήματα με τους πελάτες τους, οι προμηθευτές προσπαθούν να κρύψουν τα προβλήματα των λειτουργικών συστημάτων τους και έτσι αποθαρρύνουν την συζήτηση για αυτά. Αντίθετα οι εισβολείς κοινοποιούν τα προβλήματα που ανακαλύπτουν αμέσως σε όλο τον κόσμο μέσω του διαδικτύου. Αυτή η διαφορά σημαίνει ότι τα προβλήματα διαδίδονται πολύ περισσότερο απ’ ότι οι λύσεις τους.

Άτακτες διορθώσεις

Όταν βρίσκονται προβλήματα ασφαλείας σε κάποιο λογισμικό, ο προμηθευτής θα διορθώσει το πρόβλημα, θα δημοσιεύσει μια διόρθωση στο διαδίκτυο και θα στείλει μια ειδοποίηση μέσω e-mail σε εγγεγραμμένους πελάτες. Δυστυχώς, δεν παίρνουν όλοι την ειδοποίηση και δεν εγκαθιστούν τη διόρθωση. Στην πραγματικότητα, οι περισσότεροι χρήστες δεν εγκαθιστούν ποτέ διορθώσεις ασφάλειας για λογισμικό, εκτός και αν υποστούν κάποια εισβολή.

Ακόμη χειρότερα, οι προμηθευτές στέλνουν βιαστικά διορθώσεις σε πελάτες για σφάλματα που δεν έχουν βρεθεί ακόμη, οι οποίες μπορούν να προκαλέσουν ακόμη μεγαλύτερα προβλήματα στα μηχανήματα των πελατών τους και ακόμη και στις καλύτερες περιπτώσεις, να απαιτούν πρόσθετη επεξεργασία για να βρεθούν τα προβλήματα, με αποτελέσματα την επιβράδυνση του συστήματος. Σε ορισμένες περιπτώσεις, η θεραπεία είναι χειρότερη από την ασθένεια.

2.2 Τρόποι παραβίασης της ασφάλειας

Στην ασφάλεια, μια αποκάλυψη είναι ένας τρόπος για πιθανή απώλεια ή βλάβη του Πληροφοριακού Συστήματος. Παραδείγματα αποκαλύψεων είναι η μη εξουσιοδοτημένη αποκάλυψη των δεδομένων, τροποποίηση των δεδομένων ή άρνηση του νόμιμου δικαιώματος πρόσβασης στο σύστημα. Η ευπάθεια είναι η αχίλλειος πτέρνα στο σύστημα ασφάλειας που μπορεί να εκμεταλλευτεί από τρίτους για την πρόκληση απωλειών ή ζημιάς. Ένα πρόσωπο που εκμεταλλεύεται την ευπάθεια του συστήματος διαπράττει μια επίθεση στο σύστημα. Ο συνεχής έλεγχος είναι ένα προστατευτικό μέτρο, που μπορεί να είναι είτε μια ενέργεια ή μια συσκευή ή ακόμα και μια διαδικασία ή τεχνική μέθοδος που μειώνει την ευπάθεια του συστήματος.

Τα μεγαλύτερα αντικείμενα του Πληροφοριακού Συστήματος είναι το υλικό, το λογισμικό και τα δεδομένα. Υπάρχουν τέσσερα είδη απειλής στην ασφάλεια του Πληροφοριακού Συστήματος που είναι οι παρακάτω:

- Η διακοπή (interruption). Τα αντικείμενα του συστήματος χάνονται, δεν είναι διαθέσιμα ή είναι μη χρησιμοποιήσιμα. Παράδειγμα αποτελεί η ηθελημένη καταστροφή μιας συσκευής, το σβήσιμο ενός προγράμματος ή ενός αρχείου δεδομένων, ή η δυσλειτουργία του διαχειριστή αρχείων του λειτουργικού

συστήματος, έτσι ώστε να μην μπορεί να βρεθεί ένα συγκεκριμένο αρχείο στο δίσκο.

- Η παρεμπόδιση (Interception). Σημαίνει πως μια μη εξουσιοδοτημένη ομάδα έχει κερδίσει το δικαίωμα πρόσβασης σε ένα αντικείμενο. Αυτή η εξωτερική ομάδα μπορεί να είναι είτε πρόσωπα, είτε προγράμματα ή ακόμα και παρέμβαση ενός άλλου πληροφοριακού συστήματος. Παράδειγμα τέτοιου είδους είναι η παράνομη αντιγραφή των προγραμμάτων ή των αρχείων δεδομένων ή οι υποκλοπές των τηλεφωνημάτων για την απόκτηση δεδομένων από το δίκτυο. Παρόλο που μια απώλεια μπορεί να αποκαλυφθεί σχετικά γρήγορα, ο υποκλοπέας μπορεί να μην αφήσει καθόλου ίχνη για την ανίχνευση της ύπαρξης του.
- Τροποποίηση (Modification). Τροποποίηση έχουμε όταν μια μη εξουσιοδοτημένη ομάδα όχι μόνο προσπελάσει τα δεδομένα, αλλά ανακατευτεί και με κάποια αντικείμενα. Για παράδειγμα κάποιος μπορεί να αλλάξει τις τιμές σε μια βάση δεδομένων ή να μετατρέψει ένα πρόγραμμα έτσι ώστε να εκτελεί επιπλέον υπολογισμούς ή να τροποποιεί τα δεδομένα που μεταφέρονται ηλεκτρονικά. Είναι ακόμα δυνατό να τροποποιηθεί και το υλικό μέρος του συστήματος.
- Κατασκευή (fabricate). Σημαίνει ότι μια μη εξουσιοδοτημένη ομάδα μπορεί να κατασκευάσει πλαστά αντικείμενα σε ένα πληροφοριακό σύστημα. Ο εισβολέας μπορεί να προσθέσει εγγραφές σε μια υπάρχουσα βάση δεδομένων. Μερικές φορές αυτές οι προσθέσεις ανιχνεύονται σαν πλαστές, αλλά εάν έχουν γίνει περίτεχνα τότε είναι αδιαχώριστες από πραγματικά αντικείμενα.

2.3 Hackers

Υπήρχε μια εποχή κατά την οποία οι ειδικοί σε θέματα ασφάλειας της πληροφορικής μάλωναν για το όρο ‘hacker’. Μερικοί από αυτούς νόμιζαν ότι hackers είναι εξαίρετοι και κάπως παθιασμένοι προγραμματιστές και άλλοι υποστήριζαν ότι οι hackers είναι κοινοί εγκληματίες. Ένα γεγονός που έκανε τα πράγματα ακόμη δυσκολότερα στο να ερμηνευτούν ήταν ότι πολλοί ειδικοί σε θέματα πληροφορικής ήταν στο παρελθόν και οι ίδιοι hackers, εντασσόμενοι και στους δύο παραπάνω

ορισμούς. Κάποιοι από αυτούς ήταν ανυπόμονοι να απαλλαγούν από αυτό το προσωνύμιο, ενώ άλλοι ήθελαν να το διατηρήσουν.

Σύμφωνα με την καθαρά τεχνική έννοια του όρου, το hacking πριν την έλευση των υπολογιστών, σήμαινε την επινόηση έξυπνων λύσεων σε δύσκολα τεχνικά προβλήματα. Όταν εμφανίστηκαν για πρώτη φορά υπολογιστές στα πανεπιστήμια και άρχισαν να ασχολούνται με αυτούς οι φοιτητές, το hacking άρχισε να σημαίνει την επινόηση έξυπνων λύσεων σε δύσκολα προγραμματιστικά προβλήματα.

Στην σύγχρονη χρήση της λέξης hacking, σημαίνει την δραστηριότητα με κακόβουλο κίνητρο, όπως οι απόπειρες εισβολής σε υπολογιστικά συστήματα και δίκτυα για την κλοπή ή καταστροφή δεδομένων. Αν και το hacking, μπορεί να έχει πάρα πολλά κίνητρα, όπως απλή περιέργεια, επιθυμία για επίδειξη, κοινωνική διαμαρτυρία κ.α. είναι οι εγκληματικές δραστηριότητες των ‘hackers’ αυτές που κερδίζουν την μεγαλύτερη δημοσιότητα από τα μέσα ενημέρωσης. Αυτοί που έχουν αγνότερα κίνητρα συχνά διαμαρτύρονται για αυτήν την σημασιολογική μετατόπιση στην έννοια της λέξης και προτιμούν να προσδιορίζουν την δραστηριότητα του κακόβουλου hacking με άλλους όρους όπως π.χ. ‘cracking’. Οι αρχές αρέσκονται να χρησιμοποιούν τους όρους cybercrime (κυβερνοέγκλημα) και cyberterrorism (κυβερνοτρομοκρατία) για να περιγράψουν τις εγκληματικές δραστηριότητες των hackers.

Οι hackers συχνά λαμβάνουν περισσότερη προσοχή από τις κοινές και επικίνδυνες απειλές. Το αμερικανικό υπουργείο δικαιοσύνης προτείνει τρεις λόγους γι’ αυτό.

- Πρώτα, η απειλή των hackers είναι η πιο πρόσφατη. Διάφοροι οργανισμοί πάντα έπρεπε να ανησυχούν για τις ενέργειες των υπαλλήλων τους και να λαμβάνουν διάφορα μέτρα πειθαρχίας για να μειώνουν τις απειλές που προέρχονται από αυτούς. Ωστόσο, αυτά τα μέτρα είναι μη αποτελεσματικά γι’ αυτούς που δεν ανήκουν στον οργανισμό αυτόν και δεν υποκύπτουν στους κανόνες που επιβάλλει σε υπαλλήλους.
- Δεύτερον, οι οργανισμοί δεν γνωρίζουν τις προθέσεις του hacker, οπότε, μερικοί hackers απλώς μπαίνουν, άλλοι κλέβουν και άλλοι προκαλούν άλλου είδους ζημιά. Αυτή η αδυναμία του προσδιορισμού των προθέσεων των hackers δείχνει ότι οι επιθέσεις τους δεν έχουν όρια.
- Τρίτον, οι επιθέσεις των hackers κάνουν τους ανθρώπους να νιώθουν αδύναμοι, κυρίως επειδή η ταυτότητα των hackers είναι άγνωστη. Για

παράδειγμα, υποθέστε ότι ένας ελαιοχρωματιστής προσλαμβάνεται για να βάψει ένα σπίτι και μόλις μπει μέσα, κλέβει κάποιο κόσμημα. Οι γείτονες μπορεί να μην νιώσουν ότι απειλούνται και θα προστατεύσουν τον εαυτό τους με το να μην προσλάβουν ποτέ τον συγκεκριμένο ελαιοχρωματιστή. Όμως αν κάποιος διαρρήκτης μπει μέσα στο ίδιο σπίτι τη νύχτα και κλέψει το ίδιο κόσμημα, τότε όλη η γειτονιά μπορεί να νιώσει ευπρόσβλητη.

2.4 Κακόβουλο Λογισμικό

Οι υπολογιστές είναι σχεδιασμένοι να εκτελούν εντολές, την μια μετά την άλλη. Αυτές οι εντολές επιτελούν συνήθως κάτι χρήσιμο, δηλαδή, υπολογίζουν τιμές, διατηρούν βάσεις δεδομένων, επικοινωνούν με άλλους χρήστες και συστήματα. Ωστόσο μερικές φορές οι εκτελούμενες εντολές μπορούν να προκαλούν κάποιο είδος ζημιάς ή να είναι κακόβουλης φύσεως. Όταν κάποια ζημιά γίνεται από ατύχημα συνήθως οφείλεται σε λάθος του λογισμικού. Αυτά τα προγραμματιστικά λάθη είναι πιθανότατα η πιο κοινή αιτία απροσδόκητης συμπεριφοράς των προγραμμάτων.

Όμως όταν ο σκοπός των εντολών είναι αυτή ακριβώς η απροσδόκητη συμπεριφορά τότε αποκαλούμε το λογισμικό που τις περιέχει κακόβουλο ή προγραμματιστική απειλή. Υπάρχουν πολλά είδη προγραμματιστικών απειλών και οι ειδικοί τις κατηγοριοποιούν ανάλογα με τον τρόπο που συμπεριφέρονται, πως ενεργοποιούνται και πως εξαπλώνονται. Τα τελευταία χρόνια, οι περιπτώσεις προγραμματιστικών απειλών που έλαβαν δημοσιότητα, περιγράφηκαν ενιαία από τα μέσα ενημέρωσης σαν ιοί των υπολογιστών. Ωστόσο οι ιοί αποτελούν μόνο ένα μικρό ποσοστό του κακόβουλου λογισμικού που έχει εφευρεθεί.

Οι ειδικοί στον χώρο της ασφάλειας της πληροφορικής έχούν επίσημους ορισμούς για όλους τους τύπους κακόβουλου λογισμικού και ηλεκτρονικής απάτης. Δεν συμφωνούν όλοι όμως στους κοινούς αυτούς ορισμούς. Ακολουθεί μια λίστα με πρακτικούς ορισμούς των περισσότερων τύπων κακόβουλου λογισμικού και μια σύντομη ανάλυση των σημαντικότερων από αυτών.

Εργαλεία ασφάλειας (Security tools and toolkits)

Τα τελευταία χρόνια έχουν γραφτεί πολλά προγράμματα τα οποία μπορούν να ελέγξουν αυτόματα τα πληροφοριακό συστήματα για αδυναμίες ασφάλειας. Αυτού του είδους τα εργαλεία μπορούν να ελέγξουν έναν υπολογιστή ή ένα δίκτυο

υπολογιστών για εκατοντάδες καταχωρημένες αδυναμίες ασφάλειας μέσα σε ένα σύντομο χρονικό διάστημα. Τα περισσότερα από αυτά τα εργαλεία είναι σχεδιασμένα για χρήση από διαχειριστές συστημάτων για να εντοπίζουν προβλήματα ασφάλειας στα δίκτυα στα οποία εργάζονται. Αυτά τα εργαλεία είναι αυτόματα και πολύ αναλυτικά. Φυσικά αυτού του είδους το λογισμικό πρέπει να μπορεί να παράγει αναλυτικές αναφορές των αδυναμιών που βρίσκει έτσι ώστε αυτές να διορθωθούν. Αυτό ακριβώς το χαρακτηριστικό τα κάνει τόσο ελκυστικά σε κάποιον που ψάχνει να βρει αδυναμίες στην ασφάλεια προς εκμετάλλευση. Επειδή αυτά τα εργαλεία είναι ευρέως διαθέσιμα, μερικές φορές χρησιμοποιούνται από μη εξουσιοδοτημένους χρήστες που θέλουν να εισβάλουν σε κάποιο πληροφοριακό σύστημα. Υπάρχουν επίσης και άλλα προγράμματα και εργαλεία που ο μόνος σκοπός τους είναι να επιτίθενται σε υπολογιστές. Αυτού τους είδους το λογισμικό γίνεται συνεχώς αρτιότερο και ευρέως διατιθέμενο στο διαδίκτυο. Συχνά απαιτεί μόνο ελάχιστη τεχνική γνώση για να χρησιμοποιηθεί.

Δούρειοι ίπποι (Trojan Horses)

Είναι αυτόνομα προγράμματα που φαίνεται να κάνουν μια χρήσιμη εργασία για τον χρήστη ενώ στην πραγματικότητα επιτελούν μυστικά κάποια άλλη λειτουργία με απώτερο σκοπό την κατάλυση της ασφάλειας. Ενώ το πρόγραμμα φαίνεται να κάνει αυτό που θέλει ο χρήστης στην πραγματικότητα κάνει και κάτι άλλο άσχετο με τον διαφημιζόμενο σκοπό του όπως η διαγραφή του σκληρού δίσκου, η ενεργοποίηση ενός ιού που κουβαλάει μέσα του, η επιλεκτική διαγραφή αρχείων, η ανεύρεση της λίστας ονομάτων του προγράμματος αποστολής ηλεκτρονικού ταχυδρομείου του χρήστη, η ανεύρεση αριθμών πιστωτικών καρτών και η αποστολή τους στον δημιουργό του Δούρειου ίππου κ.α. Ο συγγραφέας ενός Δούρειου ίππου συχνά προκαλεί τους χρήστες να εκτελέσουν το πρόγραμμά του, τοποθετώντας το σε κάποιο κοινό και πολυσύχναστο σημείο του διαδικτύου και δίνοντάς του ένα ελκυστικό όνομα έτσι ώστε να μοιάζει με κάποιο χρήσιμο πρόγραμμα.

Οι δούρειοι ίπποι βρίσκονται σε περίοδο μεγάλης εξάπλωσης σήμερα, εκμεταλλευόμενοι την αφέλεια των άπειρων χρηστών ηλεκτρονικών υπολογιστών. Οι σύγχρονοι Δούρειοι Ίπποι μεταμφιέζονται τόσο καλά που μπορεί να παραπλανήσουν ακόμη και έναν έμπειρο χρήστη. Η πρώτη δημόσια εμφάνιση Δούρειου ίππου παρατηρήθηκε το 1987 στη Γερμανία.

Ένας Δούρειος ίππος θα μπορούσε να παρακολουθεί και να καταγράφει οτιδήποτε πληκτρολογεί ο χρήστης και να στέλνει τις πληροφορίες στον εισβολέα που τον φύτεψε ή να τις αποθηκεύει σε αρχείο για μετέπειτα ανάκτηση. Πιθανότατα, το χειρότερο είδος Δούρειου ίππου είναι αυτό που επιτρέπει στον εισβολέα να αποκτήσει τον πλήρη έλεγχο του παραβιασμένου συστήματος.

Ένας χειρονακτικός τρόπος εντοπισμού Δούρειων Ίππων σε ένα σύστημα είναι η καταγραφή κάθε εκτελέσιμου αρχείου του συστήματος και η σύγκριση της λίστας με μια προηγούμενη που έχει δημιουργηθεί όταν το σύστημα εγκαταστάθηκε και ρυθμίστηκε σε ‘καθαρές’ συνθήκες (χωρίς δικτυακές συνδέσεις). Οποιοδήποτε ασυνήθιστο αρχείο, ιδίως αν έχει ονομασία παρόμοια με κάποιο νόμιμο αρχείο (π.χ.’service.exe’ αντί για ‘services.exe’) θα μπορούσε να είναι Δούρειος ίππος.

Ιοί (Viruses)

Ο όρος αυτός εμφανίστηκε για πρώτη φορά στο λεξικό των υπολογιστών το 1984. Η λέξη virus είναι λατινική και σημαίνει δηλητήριο. Ένας πραγματικός ιός στην κλασσική του έννοια είναι ένα κομμάτι κώδικα που προσαρτάται σε κάποιο άλλο εκτελέσιμο κώδικα, έτσι ώστε όταν εκτελείται το ‘μολυσμένο’ πρόγραμμα να εκτελείται και ο ιός μαζί του. Αφού εκτελεστεί ο ιός μεταφέρεται στην κύρια μνήμη του ηλεκτρονικού υπολογιστή και μπορεί να έχει τον πλήρη έλεγχο του συστήματος. Συνήθως το πρώτο μέλημά του είναι να προσαρτήσει πανομοιότυπα αντίγραφα του εαυτού του σε άλλα εκτελέσιμα προγράμματα με γεωμετρικό ρυθμό και με αυτόν τον τρόπο να εξαπλωθεί. Κάθε φορά που κάποιος μολυσμένος υπολογιστής έρχεται σε επαφή με ένα μη – μολυσμένο κομμάτι λογισμικού, ένα νέο αντίγραφο του ιού περνά στο νέο πρόγραμμα. Επομένως η μόλυνση μπορεί να μεταφερθεί από υπολογιστή σε υπολογιστή από ανυποψίαστους χρήστες, οι οποίοι είτε εναλλάσσουν δίσκους είτε αποστέλλουν προγράμματα ο ένας στον άλλο μέσω δικτύου. Οι ιοί δεν είναι αυτόνομα προγράμματα – δεν μπορούν να εκτελεστούν από μόνοι τους- και απαιτούν για την ενεργοποίηση τους, την εκτέλεση κάποιου προγράμματος ‘ξενιστή’ που περιέχει τον ιό μέσα στον κώδικά του.

Ένας ιός μπορεί να περιέχει χαρακτηριστικά από άλλα είδη κακόβουλου λογισμικού: δηλαδή, μπορεί να λειτουργεί ταυτόχρονα σαν Δούρειος Ίππος, σκουλήκι και λογική βόμβα η μπορεί ακόμη και να περιέχεται μέσα σε αυτά.

Η πρώτη και πιο κοινή μορφή ιών είναι οι παρασιτικοί (parasitic viruses). Αυτοί προσαρτούν το εαυτό τους στο τέλος του αρχείου αφήνοντας ανέπαφη την βασική

δομή του αρχείου. Η ροή της εκτέλεσης του αρχείου ανακατευθύνεται έτσι ώστε ο κώδικάς του ιού να εκτελείται πάντα πρώτος. Έπειτα ο έλεγχος περνάει στο μολυσμένο πρόγραμμα το οποίο στις περισσότερες περιπτώσεις θα εκτελεστεί κανονικά.

Μια υποκατηγορία των ιών είναι οι μακροϊοί (macro-viruses). Αυτοί οι ιοί βρίσκονται συνήθως κρυμμένοι σε ιστοσελίδες του Διαδικτύου και μπορούν να μολύνουν πολλαπλές πλατφόρμες ηλεκτρονικών υπολογιστών. Αυτό επιτυγχάνεται επειδή στοχεύουν να μολύνουν συγκεκριμένα εμπορικά προγράμματα όπως π.χ. Microsoft Word και όχι λειτουργικά συστήματα.

Τα ενιαία πρωτόκολλα ηλεκτρονικού ταχυδρομείου που διασυνδέουν τους περισσότερους υπολογιστές σήμερα, ανεξαρτήτως κατασκευαστικής πλατφόρμας, αποτελούν ένα εξαιρετικό μέσο μεταφοράς και διάδοσης των μακροϊών. Ο σιγουρότερος τρόπος προστασίας ενάντια στους μακροϊούς είναι η απενεργοποίηση των μακροεντολών, αλλά αυτό συντελεί στην απώλεια λειτουργικότητας που μπορούν να παρέχουν οι μακροεντολές.

Πίσω πόρτες (Back doors ήTrap doors)

Είναι κομμάτια κώδικα που γράφονται μέσα σε εφαρμογές ή λειτουργικά συστήματα έτσι ώστε να δώσουν στους προγραμματιστές πρόσβαση σε προγράμματα χωρίς να χρειάζεται αυτοί να περάσουν από τις συνήθεις, χρονοβόρες διαδικασίες ασφάλειας της πρόσβασης. Στην ουσία είναι ‘τρύπες’ ασφάλειας που δημιουργούνται εσκεμμένα. Μερικές φορές ονομάζονται και trap doors ανάλογα με το ποιος τις δημιουργεί και επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε κάποιο σύστημα. Αρκετά συχνά αποτελούν τροποποίηση νόμιμου λογισμικού με κακόβουλο σκοπό. Επίσης μπορούν να χρησιμοποιηθούν και από ειδικούς ασφαλείας σαν ‘δόλωμα’ για τον εντοπισμό και παγίδευση ιδιαίτερα ταλαντούχων εισβολέων.

Οι περισσότερες πίσω πόρτες γράφονται μέσα σε εφαρμογές που απαιτούν χρονοβόρες διαδικασίες πιστοποίησης. Όταν ο προγραμματιστής διορθώνει τα λάθη του προγράμματος μπορεί να θελήσει να έχει ειδικά προνόμια ή να αποφύγει να περάσει από την διαδικασία πιστοποίησης για να κάνει πιο γρήγορα την δουλειά του. Επίσης αποτελεί και μια εναλλακτική μέθοδο ενεργοποίησης του προγράμματος σε περίπτωση που κάτι πάει στραβά με την διαδικασία πιστοποίησης. Η πίσω πόρτα συνήθως ενεργοποιείται όταν το πρόγραμμα ανιχνεύσει κάποια ειδική ακολουθία εισαγωγής δεδομένων.

Οι πίσω πόρτες μετατρέπονται σε απειλές όταν χρησιμοποιούνται από ασυνείδητους προγραμματιστές που θέλουν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Αποτελούν επίσης πρόβλημα όταν ο αρχικός προγραμματιστής της εφαρμογής ξεχάσει να αφαιρέσει την πίσω πόρτα όταν πια η εφαρμογή έχει διορθωθεί από όλα τα σφάλματα (θεωρητικά φυσικά) και κάποιος άλλος ανακαλύψει την ύπαρξή της.

Μια πίσω πόρτα θα μπορούσε να εισαχθεί σε ένα ηλεκτρονικό καλάθι αγορών έτσι ώστε να επιτρέψει στον κατασκευαστή της να συλλέξει κρυφά πληροφορίες συναλλαγών, συμπεριλαμβανομένων αριθμών πιστωτικών καρτών.

Ο εντοπισμός και το καθάρισμα του υπολογιστικού συστήματος από αυτές τις πίσω πόρτες είναι τις περισσότερες φορές σχεδόν αδύνατο καθότι υπάρχουν αμέτρητοι τρόποι για να δημιουργηθεί μια πίσω πόρτα. Η μόνη πραγματικά έμπιστη επιλογή για την επαναφορά του συστήματος μετά από κάποια επίθεση από τα πρωτότυπα μέσα αποθήκευσης και η έναρξη της χρονοβόρας διαδικασίας της επαναφοράς των δεδομένων των χρηστών και των εφαρμογών από καθαρά αντίγραφα ασφαλείας.

Σκουλήκια (Worms)

Τα σκουλήκια (worms) είναι προγράμματα που εξαπλώνονται μέσω των δικτυωμένων υπολογιστών, αντιγράφοντας τα ίδια ανεξέλεγκτα, αλλά συνήθως δεν προκαλούν άλλου τύπου επιπλοκές. Εξ ορισμού τα “σκουλήκια” δεν τροποποιούν άλλα προγράμματα αλλά μπορεί να κουβαλούν μέσα τους κάποιο ιό που μπορεί να το κάνει. Τα σκουλήκια μοιάζουν πολύ με τους ιούς στο ότι αντιγράφονται από μόνα τους και επιτίθενται σε συστήματα με σκοπό να επιφέρουν βλάβες. Πρόκειται για αυτόνομα προγράμματα τα οποία μολύνουν υπολογιστικά συστήματα μόνο μέσω δικτυακών συνδέσεων. Για τη δημιουργία τους απαιτούνται ιδιαίτερες γνώσεις πρωτοκόλλων επικοινωνίας, ευπαθειών δικτυακών συστημάτων και ειδικών θεμάτων πάνω σε λειτουργικά συστήματα.

Βασική φιλοδοξία ενός «σκουληκιού» είναι η αναπαραγωγή του εαυτού του. Η δημιουργία ενός σκουληκιού απαιτεί την ύπαρξη ενός δικτυακού περιβάλλοντος και έναν συγγραφέα που να είναι βαθύς γνώστης όχι μόνο του δικτυακού περιβάλλοντος μέσω του οποίου θα ταξιδέψει το σκουλήκι αλλά και του υπολογιστικού περιβάλλοντος που είναι ο τελικός προορισμός του. Σε ένα σύστημα πολύ-προγραμματισμού (multitasking), το σκουλήκι μπορεί να αποκρύψει την παρουσία

του παριστάνοντας μια διεργασία συστήματος ή χρησιμοποιώντας κάποιο άλλο όνομα που δεν προσελκύει την προσοχή. Βασική “φιλοδοξία” ενός σκουληκιού είναι να εισχωρήσει σε όσο το δυνατόν περισσότερα δικτυακά συστήματα εκμεταλλευόμενο αδυναμίες ή “τρύπες” του λειτουργικού συστήματος καθώς και ανεπαρκείς μεθόδους διαχείρισης αυτών των συστημάτων. Οι μέθοδοι κλωνοποίησης των σκουληκιών περιλαμβάνουν:

- Ηλεκτρονικό ταχυδρομείο (e-mail): ένα σκουλήκι αποστέλλει ένα αντίγραφο του εαυτού του, μέσω κάποιου μηνύματος, σε άλλα συστήματα.
- Δυνατότητα απομακρυσμένης εκτέλεσης: ένα σκουλήκι εκτελεί ένα αντίγραφο του εαυτού του σε κάποιο άλλο σύστημα.
- Δυνατότητα απομακρυσμένης εισαγωγής σε σύστημα: ένα σκουλήκι εισάγεται σε ένα απομακρυσμένο σύστημα ως χρήστης και στη συνέχεια χρησιμοποιεί εντολές για να αντιγράψει τον εαυτό του από το ένα σύστημα στο άλλο.

Η προστασία από σκουλήκια είναι παρόμοια με την προστασία από εισβολή. Αν ένας εισβολέας μπορεί να εισχωρήσει σε κάποιο πληροφοριακό σύστημα τότε το ίδιο μπορεί να κάνει και ένα σκουλήκι. Φυσικά ισχύει και το αντίθετο.

Λογικές βόμβες (Logic Bombs)

Οι λογικές βόμβες είναι μικρά προγράμματα που προστίθενται σε κάποιο υπάρχον πρόγραμμα ή ακόμα τροποποιούν κάποιον υπάρχοντα κώδικα. Καλούνται έτσι διότι είναι προγραμματισμένες να εκραγούν ηλεκτρονικά όταν συντρέξουν οι κατάλληλες συνθήκες. Οι συνθήκες που μπορούν να ενεργοποιήσουν μια λογική βόμβα μπορεί να είναι η παρουσία ή απουσία συγκεκριμένων αρχείων, μια συγκεκριμένη ημέρα της εβδομάδας, η εκτέλεση μιας συγκεκριμένης εφαρμογής κλπ. Αποτελούν μια από τις αρχαιότερες μορφές προγραμματιστικών απειλών.

Η λογική βόμβα προστίθεται στο πρόγραμμα από κάποιον που έχει το ελεύθερο σε αυτό, δηλαδή εύκολή πρόσβαση στο σύστημα και εννοείται και την απαιτούμενη γνώση για την εγκατάσταση. Η πρόσβαση πάλι μπορεί να αποκτηθεί και με κάποιο μέσο υποκλοπής.

Πολλές φορές οι λογικές βόμβες ενσωματώνονται σε διάσημα εμπορικά προγράμματα από τους προγραμματιστές για τον έλεγχο της πειρατείας λογισμικού ή σαν μέτρο προστασίας των συμφερόντων των προγραμματιστών.

Υποκατηγορία αυτών των προγραμμάτων είναι η ωρολογιακή βόμβα (Time Bomb) που χρησιμοποιεί το εσωτερικό ρολόι του υπολογιστή και είναι ιδιαίτερα χρήσιμη καθώς επιτρέπει να διαπραχθεί το αδίκημα αυτόματα, χωρίς ο ένοχος να είναι παρών.

Προγράμματα λαγοί (Rabbit programs).

Είναι προγράμματα που δεν έχουν σαν βασικό στόχο να προκαλέσουν ζημιά σε αρχεία αλλά να κλωνοποιούν τον εαυτό τους ατέρμονα ή να διατάζουν τον υπολογιστή να εκτελεί χωρίς νόημα ενέργειες επ' άπειρων, με στόχο να κατακλύσουν τους πόρους (κεντρική και περιφερειακή μνήμη, επεξεργαστική ισχύ) του 'μολυσμένου' υπολογιστικού συστήματος, και να προκαλέσουν την κατάρρευσή του. Αυτή η επίθεση είναι από τις αρχαιότερες μορφές προγραμματιζόμενης απειλής.

Προγράμματα ζόμπι (Zombies)

Είναι προγράμματα που καταλαμβάνουν κρυφά κάποιον υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο και μετά χρησιμοποιούν αυτόν τον υπολογιστή για να εκκινήσουν επιθέσεις εναντίον υπολογιστών-στόχων. Συνήθως επιτίθενται και κατακλύζουν τους υπολογιστές – εξυπηρετητές (servers) των διαφόρων τοποθεσιών του Παγκόσμιου Ιστού (Word Wide Web) με χιλιάδες αιτήσεις σύνδεσης, επιβραδύνοντας την λειτουργία αυτών με αποτέλεσμα την αδυναμία εξυπηρέτησης (Denial-of-Service ή Dos). Τα ζόμπι εμφυτεύονται σε εκατοντάδες υπολογιστές ανυποψίαστων χρηστών και ξεκινούν από εκεί τις επιθέσεις τους. Έτσι διατηρούν κρυφή την ταυτότητα του δημιουργού τους.

2.5 Συγγραφείς – προγραμματιστές κακόβουλου λογισμικού(Malicious software authors)

Δεν είναι γνωστά πολλά πράγματα για τους ανθρώπους που γράφουν και εγκαθιστούν προγραμματιζόμενες απειλές καθώς και στους εισβολείς συστημάτων κυρίως γιατί ένα πολύ μικρό ποσοστό από τα σχετικά συμβάντα γίνονται γνωστά στην ευρύτερη κοινότητα. Οι λιγοστές μαρτυρίες αναφέρουν ότι η συγγραφή ιομορφικού λογισμικού είναι ένα είδος διαμαρτυρίας, πιθανότατα ενάντια στην πολιτεία γενικότερα, σχεδόν σίγουρα ενάντια στην έλλειψη ευκαιριών και ελπίδας. Τουλάχιστον για ένα μεγάλο ποσοστό των συγγραφέων κακόβουλου λογισμικού,

αυτή η ενασχόλησή τους είναι μια μορφή εκδήλωσης της ατομικότητας, ένας τρόπος να ξεχωρίσουν από τη μάζα. Είναι επίσης μια ευκαιρία για δόξα.

Εμπειρικές μελέτες στην Γερμανία δείχνουν ότι το 60% των δραστών πληροφοριακών εγκλημάτων δεν έχουν ειδικές γνώσεις ή ικανότητες. Παλιότερες μελέτες όμως έδειξαν υψηλό ποσοστό προγραμματιστών ως εγκληματιών. Προφανώς η διάδοση των ηλεκτρονικών υπολογιστών δημιούργησε την δυνατότητα διάπραξης τέτοιων εγκλημάτων από το ευρύ κοινό. Βασιζόμενοι στους συγγραφείς που είναι γνωστοί στις αρχές και στα γεγονότα που τελικά αναδύθηκαν στην επιφάνεια, αυτοί μπορούν να χωριστούν στις ακόλουθες βασικές κατηγορίες:

Εργαζόμενοι

Τα τρία συστατικά κάθε απάτης είναι η ανάγκη, η ευκαιρία και η γνώση. Με την πρόσληψη ενός υπαλλήλου, δυο από τα τρία στοιχεία, και συγκεκριμένα η ευκαιρία και η γνώση, υπάρχουν ήδη λόγω της φύσης του επαγγέλματος της πληροφορικής.

Μια από τις μεγαλύτερες κατηγορίες ατόμων που προκαλούν προβλήματα ασφάλειας περιλαμβάνει τους δυσαρεστημένους υπαλλήλους ή πρώην υπαλλήλους που νιώθουν ότι αδικήθηκαν ή φέρουν μια βαθιά αντιπάθεια για τους εργοδότες τους (Αυτού του είδους οι εργαζόμενοι ονομάζονται Insiders, αυτοί δηλαδή που κάνουν την ζημιά από μέσα). Οι εργαζόμενοι ή πρώην εργαζόμενοι αποτελούν συνήθως τους πιο επικίνδυνους πληροφοριακούς εγκληματίες αφού γνωρίζουν πολλούς από τους κωδικούς ασφαλείας και μέτρα προστασίας που είναι ήδη εγκατεστημένα. Ξέρουν σε ποιους υπολογιστές να επιτεθούν, ποια αρχεία θα προκαλέσουν την μεγαλύτερη ζημιά αν σβηστούν και που βρίσκονται αποθηκευμένα τα αντίγραφα ασφαλείας. Επίσης λόγω του σημερινού οικονομικού κλίματος, η απειλή της ανεργίας μπορεί να παρακινήσει τους εργαζόμενους να κλέψουν τον εργοδότη τους.

Αυτή η εσωτερική απειλή είναι ο λόγος ύπαρξης πολλαπλών επιπέδων ασφάλειας σε ένα δίκτυο. Είναι ίσως ειρωνική η σκέψη ότι σε πολλές εταιρείες τα άτομα που είναι υπεύθυνα για την ασφάλεια και τον έλεγχο είναι επίσης τα άτομα που μπορούν να προκαλέσουν την μεγαλύτερη ζημιά αν ήθελαν απλά να εκτελέσουν τις κατάλληλες εντολές. Οι περισσότεροι Δούρειοι ίπποι, Λογικές βόμβες και Πίσω πόρτες εμφανίζονται σε ένα σύστημα γιατί απλά δημιουργήθηκαν εκεί.

Μια γνωστή τεχνική που έχει χρησιμοποιηθεί από υπαλλήλους οικονομικών και πιστωτικών οργανισμών είναι η τεχνική του σαλαμιού (salami technique) κατά την οποία η κατάλληλη τροποποίηση ενός ή περισσοτέρων προγραμμάτων, προκαλεί

τον υπολογιστή να στρογγυλοποιεί τις συναλλαγές προς τα κάτω κατά πολύ ασήμαντα χρηματικά ποσά, που μεταφέρονται στους λογαριασμούς των ένοχων υπαλλήλων. Οι παθόντες μπορεί να είναι χιλιάδες, επομένως μη προσδιορίσιμοι (άδηλοι).

Κλέφτες

Μια δεύτερη κατηγορία περιλαμβάνει τους κλέφτες και τους παραχαράκτες. Αυτά τα άτομα θα μπορούσαν να εμποδίσουν την ομαλή λειτουργία ενός υπολογιστικού συστήματος για να εκμεταλλευθούν την κατάσταση που θα προκύψει ή να καλύψουν αποδείξεις της εγκληματικής τους δραστηριότητας. Η κλοπή λογισμικού -φαινόμενο αρκετά πιο συχνό από ότι ίσως πιστεύει το ευρύ κοινό- αποτελεί ισχυρό πλήγμα για κάθε εταιρεία και μπορεί να την θέσει εκτός ανταγωνισμού. Παρόμοιο πλήγμα μπορεί να συμβεί σε κάποια εταιρεία λογισμικού και από την πειρατεία λογισμικού που αποτελεί ένα από τα μεγαλύτερα οικονομικά προβλήματα στον χώρο της πληροφορικής.

Κατάσκοποι

Βιομηχανική, πολιτική και οικονομική κατασκοπία ή σαμποτάζ είναι ένας άλλος λόγος συγγραφής κακόβουλου κώδικα. Η βιομηχανική κατασκοπία είναι η συλλογή ιδιοκτησιακών πληροφοριών (όπως τα σχέδια νέων προϊόντων, μυστικές φόρμουλες, πληροφορίες σχετικές με κέρδη) από ιδιωτικές εταιρείες ή την κυβέρνηση για τον σκοπό της βοήθειας κάποιας άλλης εταιρείας ή εταιρειών. Η βιομηχανική κατασκοπία μπορεί να διαπραχθεί είτε από εταιρίες που επιθυμούν να βελτιώσουν το ανταγωνιστικό τους πλεονέκτημα είτε από κυβερνήσεις που επιθυμούν να βοηθήσουν τις εγχώριες βιομηχανίες τους. Πολλοί sneakers λόγω της φύσης της δουλειάς τους επιδίδονται σε τέτοιου είδους κατασκοπία. Οι προγραμματιζόμενες απειλές είναι ένα πολύ ισχυρό και δύσκολα εντοπίσιμο μέσο απόκτησης απόρρητων ή ευαίσθητων πληροφοριών, ή καθυστέρησης του ανταγωνισμού. Οι εισβολείς που ασχολούνται με την κατασκοπία είναι συνήθως πολύ ικανοί και υποστηρίζονται πολύ καλά οικονομικώς.

Εκβιαστές

Ο εκβιασμός μπορεί επίσης να αποτελέσει κίνητρο για τη συγγραφή τέτοιου είδους λογισμικού. Σε αυτή την περίπτωση οι εκβιαστές απειλούν να ενεργοποιήσουν

καταστροφικό λογισμικό αν δεν πληρωθεί κάποιο ποσό ή αν δεν ικανοποιηθεί κάποια άλλη τους επιθυμία. Επίσης υπάρχουν περιπτώσεις όπου εισβολείς έχουν εισβάλει σε συστήματα ηλεκτρονικών επιχειρήσεων κλέβοντας στοιχεία χιλιάδων πιστωτικών καρτών και εκβιάζοντας την εταιρεία με δημοσιοποίηση τους. Πολλές εταιρείες έχουν πέσει θύματα κάποιας μορφής εκβιασμού στην οποία έχουν συμφωνήσει να μην κινηθούν δικαστικά εναντίον των ατόμων που παραβίασαν την ασφάλεια των υπολογιστικών τους συστημάτων. Δεν είναι λίγες οι περιπτώσεις μάλιστα όπου οι εταιρίες έχουν προσλάβει στο προσωπικό τους τέτοιου είδους άτομα. Σε αντάλλαγμα οι εκβιαστές συμφωνούν να μην φανερώσουν δημόσια τις ατέλειες των δικτύων των εταιριών που τους επέτρεψαν την παράνομη πρόσβαση. Φυσικά ο σημαντικότερος λόγος για τον οποίο οι εταιρίες διστάζουν να οδηγήσουν σε δίκη κάποιο εκβιαστή είναι η δυσφήμιση που θα υποστούν σχετικά με την ασφάλειά τους και επίσης η απειλή περαιτέρω ζημιάς αν δεν ανακαλυφθούν και διορθωθούν οι αδυναμίες στην ασφάλεια.

Πειραματιστές

Αναμφίβολα κάποιες προγραμματιζόμενες απειλές θα γραφτούν από πειραματιστές και περίεργους. Μερικές φορές τα άτομα αυτής της κατηγορίας μπορεί να δημιουργήσουν κάποιο πρόγραμμα που να αποβεί επικίνδυνο λόγω κάποιων προγραμματιστικών λαθών στον κώδικά του ή λόγω αφέλειας ή κακής κρίσης από μέρους τους. Οι άνθρωποι αυτοί μπορούν να αποτολμήσουν την συγγραφή κάποιας προγραμματιζόμενης απειλής σαν ‘ακαδημαϊκή άσκηση’ απλά, για να αποδείξουν κάτι. Με πολλούς τρόπους ο πειραματιστής μπορεί να δει τα πληροφοριακά συστήματα σαν ένα παιχνίδι σκάκι, μια μάχη των μυαλών που συνδυάζει στρατηγική και τακτική σκέψη, υπομονή και πνευματική δύναμη. Οι πειραματιστές που έχουν σαν κίνητρο την πρόκληση είναι συνήθως αδιάφοροι ως προς το πιο σύστημα θα επιτεθούν, είτε αυτό είναι ένα οικογενειακό δίκτυο είτε μια στρατιωτική εγκατάσταση. Οι πειραματιστές είναι απρόβλεπτοι, τόσο ως προς τις ικανότητές τους όσο και προς την αφοσίωσή τους.

Λαγωνικά δημοσιότητας

Άλλο μεγάλο κίνητρο για την συγγραφή κακόβουλου λογισμικού καθώς και την εισβολή σε πληροφοριακά συστήματα μπορεί να είναι το κέρδος, η φήμη ή απλά η ικανοποίηση του εγώ από το κυνηγητό των διωκτικών αρχών. Σε αυτό το συχνό

σενάριο, κάποιος θα συγγράψει έναν ιό, θα τον εξαπολύσει στο διαδίκτυο και μετά θα προσπαθήσει να κερδίσει δημοσιότητα σαν αυτός που τον ανακάλυψε, ή σαν ο πρώτος που θα δημιουργήσει κώδικα που τον απενεργοποιεί, ή απλά να κοκορευτεί για το δημιούργημά του σε κάποιο δημόσιο χώρο συνομιλιών στο διαδίκτυο. Αυτού του είδους το σενάριο εμφανίζεται με αυξημένη συχνότητα τελευταία αφού δίνεται μεγάλη έμφαση από τον δημοσιογραφικό τύπο και την τηλεόραση σε τέτοιου είδους γεγονότα. Οι εισβολείς αυτής της κατηγορίας ψάχνουν να βρουν έναν τρόπο να κερδίσουν την αποδοχή της ηλεκτρονικής κοινότητας των hackers. Έτσι οι επιθέσεις που επιχειρούν είναι πολύ δημόσιες. Ο καλύτερος τρόπος γι' αυτό είναι αυτός που αναφέρθηκε πάνω, η συγγραφή κακόβουλου λογισμικού δηλαδή, αλλά επίσης και η διατάραξη των πολυσύχναστων ιστόχωρων. Παραβιάζοντας το δίκτυο μιας μεγάλης εταιρείας ή κυβερνητικού οργανισμού και παραμορφώνοντας την ιστόχωρό τους, τότε η δημοσιότητα είναι σχεδόν εγγυημένη για τον εισβολέα.

Εισβολείς

Οι εισβολείς που έχουν σαν κύρια ασχολία την εισχώρηση σε πληροφοριακά συστήματα, έχουν μια πληθώρα κινήτρων. Σίγουρα ένα μικρό ποσοστό αποβλέπει σε κάποιο οικονομικό όφελος, ένα μεγαλύτερο ποσοστό για την εμπειρία και την γνώση που θα αποκομίσουν και ένα σεβαστό ποσοστό για την φήμη που θα δημιουργήσουν στον περίγυρο τους. Συνήθως το λογισμικό που δημιουργούν προορίζεται για συγκεκριμένα κάθε φορά πληροφοριακά συστήματα και είναι πολύ ανώτερο σε ποιότητα από αυτό που κυκλοφορεί δημόσια στο διαδίκτυο. Αν και η απειλή των εισβολέων είναι εκτεταμένη και σημαντική για το πληροφοριακό σύστημα κάθε οργανισμού και επιχείρησης, οι ζημιές από εισβολείς είναι σημαντικά μικρότερες από ζημιές που προκαλούνται από εργαζόμενους.

Ακτιβιστές

Ο χακτιβισμός (hacktivism) είναι η online έκφραση του ακτιβισμού και μπορεί να έχει σαν κίνητρο λόγους παρόμοιους με αυτούς για τους οποίους άτομα μπορεί να συμμετάσχουν σε πορείες διαμαρτυρτίας, καθιστικές διαμαρτυρίες κλπ. Ο χακτιβισμός μπορεί να πάρει πολλές μορφές που μπορούν να παρεμποδίσουν επιχειρηματικές και κρατικές λειτουργίες σε διάφορους βαθμούς. Οι χακτιβιστές μπορούν να δημοσιοποιήσουν προϊόντα πνευματικής ιδιοκτησίας που δεν ανήκουν σε αυτούς, όπως πειρατικό λογισμικό και μουσική. Η παραμόρφωση κάποιου

ιστόχωρου (web site defacement) είναι μια μορφή χακτιβισμού παρόμοια με τα συνθήματα στους τοίχους. Οι βόμβες ηλεκτρονικού ταχυδρομείου (e-mail bombs) αποτελούν μια άλλη μορφή και γενικά περιλαμβάνουν την αποστολή μηνυμάτων με συνημμένα αρχεία μεγάλου μεγέθους σε μια προσπάθεια να δεσμευθεί πλήρως η ισχύς ενός εξυπηρετητή ηλεκτρονικού ταχυδρομείου (e-mail server). Το αποτέλεσμα είναι μια επίθεση άρνησης εξυπηρέτησης (Denial of Service attack) κατά την οποία ο εξυπηρετητής δεν μπορεί να διαχειριστεί την ηλεκτρονική αλληλογραφία. Σε αυτήν την περίπτωση οι DoS επιθέσεις ονομάζονται εικονικές καθιστικές διαμαρτυρίες. Άλλες μορφές χακτιβισμού μπορούν να περιλαμβάνουν ηλεκτρονικές αιτήσεις ή παρακλήσεις, ιούς ή σκουλήκια, εισβολές σε υπολογιστικά συστήματα κλπ. Οι γνώμες για το αν αυτές οι πράξεις θεωρούνται ηθικές ποικίλουν. Μερικοί θεωρούν τον χακτιβισμό σαν μια νόμιμη μορφή λαϊκής ανυπακοής, ενώ άλλοι του δίνουν την στάμπα της πληροφορικής τρομοκρατίας ή της εγκληματικής ενέργειας.

Κερδοσκόποι

Πολλές από τις κατηγορίες εισβολέων και συγγραφέων κακόβουλου λογισμικού που αναφέρθηκαν παραπάνω μπορούν να έχουν σαν κίνητρο το οικονομικό κέρδος. Μια ιδιαίτερη κατηγορία εισβολέων είναι αυτοί που έχουν οικονομικά κίνητρα αλλά με έμμεσο τρόπο. Ένας ερευνητής κάποιας εταιρείας πληροφοριακής ασφάλειας, μπορεί να κάνει μια μεγάλη προσπάθεια για να ανακαλύψει ευπάθειες και τρωτότητες σε εμπορικές εφαρμογές και λειτουργικά συστήματα, και μετά να χρησιμοποιήσει αυτήν την ανακάλυψη καθώς και την δημοσιοποίηση των μέχρι πρώτινος άγνωστων ευπαθειών σαν διαφημιστικό μέσο για τις υπηρεσίες ασφάλειας που προσφέρει η δική του εταιρεία. Η δημοσιότητα που μπορεί να κερδίσει μια επιχείρηση ή κάποιος ιδιώτης από την ανακάλυψη μιας σοβαρής αδυναμίας ασφάλειας σε κάποια εμπορική εφαρμογή, ιδιώς κάποια ευρέως χρησιμοποιούμενη εφαρμογή, μπορεί να είναι ανεκτίμητη. Για παράδειγμα, οι περισσότερες σημαντικές αδυναμίες που ανακαλύπτονται σε κάποια διάσημη εμπορική εφαρμογή θα αναφερθούν στην πρώτη σελίδα των μεγαλύτερων ιστόχωρων πληροφόρησης και πληροφοριακής ασφάλειας και επίσης στο τμήμα τεχνολογίας των μεγαλύτερων εφημερίδων. Αυτός που θα έχει ανακαλύψει την αδυναμία μπορεί ακόμη και να εμφανιστεί σε τηλεοπτικό δελτίο ειδήσεων. Για τις περισσότερες μικρές εταιρείες παροχής υπηρεσιών υπολογιστικής και δικτυακής

ασφάλειας, η απόκτηση τέτοιου είδους δημοσιότητας κανονικά αποκλείεται να συμβεί ποτέ.

Στρατιώτες πληροφορίας

Ο πόλεμος της πληροφορίας (information warfare) είναι ένα ακόμη κίνητρο για την εισβολή σε υπολογιστικά δίκτυα το οποίο γίνεται συνεχώς πιο επικίνδυνο καθώς άνθρωποι απ' όλο τον κόσμο στηρίζονται στα δίκτυα αυτά για να διεξάγουν κρίσιμες εργασίες. Μεγάλοι πόλεμοι έχουν χαρακτηριστεί από την εξέλιξη πολεμικών συστημάτων–το οπλοπολυβόλο άλλαξε την φύση της μάχης στον Πρώτο Παγκόσμιο Πόλεμο, το τάνκ άλλαξε την φύση της μάχης στον δεύτερο Παγκόσμιο Πόλεμο και οι δορυφόροι άλλαξαν την φύση της μάχης στον Πόλεμο του Κόλπου. Πίσω από το προσκήνιο, κάθε πόλεμος σημείωσε την εξέλιξη της ηλεκτρονικής μάχης. Από αναχαιτισμένα τηλεγραφικά μηνύματα που αποκρυπτογράφονταν με το χέρι, στην παρεμπόδιση της λειτουργίας των ραντάρ με παράσιτα, στις εκπομπές δορυφόρων που μπορούν να "σπάσουν" μόνο με την υποκλοπή των κλειδιών κρυπτογράφησης (παρά την τεράστια ισχύ πολλών υπερυπολογιστών)–η ηλεκτρονική μάχη και κατασκοπεία έχουν αναχθεί σε αποφασιστικούς παράγοντες στα σύγχρονα σενάρια πολέμου. Αν και δεν έχουν υπάρξει ευρέως διαδεδομένα περιστατικά κυβερνοτρομοκρατίας (cyberterrorism), να είστε σίγουροι ότι έχουν συμβεί. Υπάρχουν αποδείξεις ότι διεξάγεται πληροφοριακός πόλεμος από αρκετές χώρες όπως Η.Π.Α., Κίνα, Ισραήλ, Πακιστάν, Ινδία και πολλές άλλες.

2.6 Κοινές απειλές σε ένα πληροφοριακό σύστημα

Ένα Πληροφοριακό Σύστημα το οποίο διαχειρίζεται δεδομένα και βασίζεται επιπλέον στην αξιοποίηση των δυνατοτήτων του διαδικτύου εκτίθεται σε μία σειρά σημαντικών απειλών, οι οποίες απαιτείται να αντιμετωπισθούν αποτελεσματικά. Ως απειλή ορίζεται μία πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων ιδιοτήτων ασφάλειας ενός πληροφοριακού συστήματος. Οι απειλές αυτές δεν προέρχονται μόνο από κακόβουλες ενέργειες που προκαλούνται από τρίτους με στόχο την κατοχή ή την απαξίωση πολύτιμων δεδομένων. Είναι πιθανό να δημιουργηθούν από το εσωτερικό του συστήματος εξαιτίας σχεδιαστικών λαθών και αδυναμιών. Οι κυριότερες από αυτές περιγράφονται παρακάτω:

Υποκλοπή συνθηματικών (password stealing): Τα συνθηματικά είναι ένας από τους πιο διαδεδομένους τρόπους για να ‘αναγνωρίζεται’ ένας χρήστης από το σύστημα. Παρά την ευρεία τους διάδοση και πολύχρονη χρήση ωστόσο υπάρχει μια σειρά από ζητήματα που σχετίζεται με τη χρήση και αποτελεσματικότητά τους. Ένα συνθηματικό μπορεί να διαρρεύσει σε έναν δυνητικό εισβολέα είτε από αμέλεια του χρήστη του συστήματος είτε μετά από παρακολούθηση των διακινούμενων πακέτων(sniffing) είτε μέσω εξαντλητικής αναζήτησης (δοκιμή όλων των δυνατών συνθηματικών), είτε με χρήση λιστών με συχνά χρησιμοποιούμενα συνθηματικά, καθώς και με πληθώρα άλλων μεθόδων.

Άρνηση παροχής υπηρεσίας (Denial of Service): Σε αυτή την περίπτωση ο εισβολέας επιχειρεί να επηρεάσει αρνητικά τη διαθεσιμότητα μιας υπηρεσίας, αφού έχει παρεισφρήσει στο σύστημα που την παρέχει. Το ίδιο μπορεί να συμβεί όταν ο εισβολέας καταφέρει να εγκαταστήσει λογισμικό που καταναλώνει ανεξέλεγκτα όλους τους διαθέσιμους πόρους του συστήματος ή του δικτύου, με αποτέλεσμα οι υπόλοιπες υπηρεσίες να παραμείνουν ουσιαστικά ανενεργές. Χαρακτηριστικό παράδειγμα αποτελεί το mail spam, η επαναλαμβανόμενη δηλαδή αποστολή μηνυμάτων προκειμένου να φτάσει το σύστημα στα όρια της χωρητικότητάς του. Οι επιθέσεις αυτού του τύπου δεν χρειάζονται αυξημένες γνώσεις, αν και είναι αποτελεσματικότερες, εάν υπάρχει πληροφόρηση για την αρχιτεκτονική του δικτύου που θα δεχθεί επίθεση.

Κατανεμημένη επίθεση άρνησης παροχής υπηρεσίας (Distributed Denial of Service): Η λογική είναι η ίδια με την άρνηση παροχής υπηρεσίας, με τη διαφορά ότι ο εισβολέας έχει εγκαταστήσει το κακόβουλο λογισμικό σε δεκάδες συστήματα αφού έχει παρεισφρήσει σε αυτά και τα χρησιμοποιεί ως μεσάζοντες (agents). Τα συστήματα αυτά με τη σειρά τους επιτίθενται συντονισμένα προς τον τελικό στόχο με δραματικές συνέπειες στους πόρους του συστήματος αυτού, αλλά και στο δίκτυο που οδηγεί προς αυτό.

Παρακολούθηση γραμμών επικοινωνίας (tapping): Παρακολουθώντας τις επικοινωνιακές γραμμές μπορεί κανείς να αποκτήσει μη εξουσιοδοτημένη προσπέλαση σε μετακινούμενα δεδομένα, με πιθανό αποτέλεσμα να παραβιαστεί η ιδιωτικότητά τους.

Ανάλυση κυκλοφορίας (traffic analysis): Για δεδομένες διευθύνσεις πηγής και προορισμού η παρακολούθηση των διακινούμενων δεδομένων μπορεί να οδηγήσει σε ανάπτυξή ενός προτύπου κυκλοφορίας. Η στατιστική και μόνο ανάλυση της επικοινωνίας, χωρίς απαραίτητα να γίνεται ανάγνωση των ίδιων των δεδομένων, μπορεί να οδηγήσει σε χρήσιμα συμπεράσματα για κάποιον τρίτο.

Αξιοποίηση καταπακτών (trapdoors exploiting): Οι καταπακτές είναι γνωστές ή άγνωστες αδυναμίες των υπηρεσιών του συστήματος που επιτρέπουν την υπέρβαση των μηχανισμών ασφάλειας για την προσπέλαση στους πόρους του συστήματος. Μολονότι συνήθως εγκαθίστανται από τους εισβολείς μετά από μια επιτυχημένη επίθεση και για μελλοντική χρήση, δεν είναι σπάνια η περίπτωση να εγκατασταθούν από κατασκευαστές ως ‘δίοδοι ταχείας πρόσβασης’ για την περίπτωση που ‘κάτι πάει στραβά’. Διάσημα προγράμματα αυτής της κατηγορίας είναι παραφθαρμένες εκδόσεις του login που επιτρέπουν είσοδο με δικαιώματα υπερχρήστη σε συγκεκριμένα usernames.

Αποτυχία η καταστροφή υλικού (hardware failure): Σημαντική απειλή στη διαθεσιμότητα ενός υπολογιστικού συστήματος αποτελεί η ενδεχόμενη καταστροφή του χρησιμοποιούμενου υλικού, είτε από κακόβουλη ενέργεια, είτε από αστοχία είτε από φυσική αιτία.

Πλαστογράφηση διευθύνσεων δικτύου (spoofing): Καταργείτε η ιδιότητα της μονοσήμαντης αντιστοίχισης των διευθύνσεων δικτύου σε μια συγκεκριμένη θέση, με αποτέλεσμα τα διακινούμενα δεδομένα να χάνουν την ιδιότητα της αυθεντικότητας προέλευσης.

Μη εξουσιοδοτημένη τροποποίηση (unauthorized modification): Η κακόβουλη τροποποίηση των δεδομένων ενός συστήματος έπεται της παρακολούθησης των γραμμών επικοινωνίας ή της παρείσφρησης στο σύστημα έπειτα από υποκλοπή συνθηματικού ή αξιοποίηση καταπακτών.

Κατάχρηση πόρων (misuse of resources): Μια μη εξουσιοδοτημένη οντότητα είναι πιθανό να υποκλέψει πόρους ενός συστήματος, όπως κύκλους του

επεξεργαστή, εύρος ζώνης δικτύου, χωρητικότητα δίσκων, είτε για να εξυπηρετηθούν διεργασίες του εισβολέα είτε για να προκληθεί άρνηση παροχής υπηρεσίας.

Διάψευση εκτέλεσης ενέργειας (repudiation of action): Μια οντότητα μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε ένα μήνυμα ή ότι τροποποίησε κάποια δεδομένα, εφόσον δεν υπάρχουν επαρκή αποδεικτικά στοιχεία. Ομοίως ο παραλήπτης του μηνύματος μπορεί να διαψεύσει τη παραλαβή του και τη ανάγνωση του περιεχομένου του.

Εσωτερικοί κίνδυνοι (internal threats): Είναι πιθανό μέλη του απασχολούμενου προσωπικού σε μια επιχείρηση να υποκλέψουν χρήσιμες πληροφορίες για παράνομη χρήση. Παράλληλα η έλλειψη ασφάλειας στην φυσική πρόσβαση στο υλικό του συστήματος δημιουργεί επιπλέον κινδύνους.

Πλαστοπροσωπία (masquerade): Στο επίπεδο εφαρμογής είναι πιθανό η προέλευση ενός μηνύματος να φαίνεται διαφορετική από την πραγματική.

Ιομορφικό λογισμικό (viral software): Πρόκειται για κακόβουλο λογισμικό που εκτελείται ή φορτώνεται δυναμικά στο σύστημα και προκαλεί ποικίλα σημαντικά προβλήματα. Συνήθως βρίσκεται ενσωματωμένο σε εκτελέσιμο κώδικα ή αυτόνομο σε μορφή δέσμης εντολών (script). Φροντίζει να προσκολλάται σε άλλα εκτελέσιμα αρχεία ή να διαδίδεται μέσω δικτυακών εφαρμογών, έτσι ώστε να επηρεάζει όσο το δυνατόν περισσότερα συστήματα.

Καταχρηστικά μηνύματα (spamming): Αφορά κυρίως τις υπηρεσίες μηνυμάτων όπως τα νέα και η ηλεκτρονική αλληλογραφία. Πρόκειται για μηνύματα διαφημιστικού και πολλές φορές προσβλητικού περιεχομένου που αποστέλλονται μαζικά σε μεγάλο αριθμό χρηστών, χωρίς να υπάρχει υπαρκτή διεύθυνση αποστολέα και από εξυπηρετητές που έχουν εκτεθεί στους εισβολείς, έτσι ώστε να μην είναι ανιχνεύσιμη η προέλευσή τους ούτε σε επίπεδο εφαρμογής ούτε σε επίπεδο δικτύου.

Μη ηθελημένη καταστροφή (Not wanted destruction): Ένας χρήστης μπορεί να πραγματοποιήσει ατυχείς ενέργειες π.χ. να διαγράψει ένα χρήσιμο αρχείο ή να σβήσει ένα σύνολο εγγραφών από μια βάση δεδομένων. Ως ενέργειες που

υποβαθμίζουν την αξία του συστήματος τα περιστατικά αυτά πρέπει να καλύπτονται από μηχανισμού ασφάλειας. Μολονότι προφανώς δεν είναι δυνατόν να στερήσουμε από τους χρήστες τα βασικά τους προνόμια για να αποτραπούν οι ατυχείς ενέργειες, θα πρέπει στο σχέδιο ασφάλειας να μεριμνούμε για μεθόδους αντιμετώπισης των περιστατικών αυτών.

Παρά την πληθώρα δυνατών επιθέσεων στην ασφάλεια και τις σημαντικές συνέπειες που μπορεί αυτές να έχουν, πολλές φορές οι επιθέσεις αυτές δεν αναφέρονται στους υπεύθυνους, στη διοίκηση ή σε κατάλληλους φορείς στο Internet. Οι λόγοι μη αναφοράς είναι κυρίως οι ακόλουθοι:

- Η αναφορά ενός προβλήματος δίνει ιδέες σε άλλους επίδοξους εισβολείς. Έτσι αν διαρρεύσει μία πληροφορία ότι «ο τάδε υπολογιστής έχει μία αδυναμία σ' αυτή την υπηρεσία», αρκετοί εισβολείς μπορεί να προσπαθήσουν να εκμεταλλευτούν το συγκεκριμένο κενό ή να εντοπίσουν και άλλα.
- Η αρνητική δημοσιότητα διώχνει πελάτες και δυσαρεστεί τους μετόχους. Για παράδειγμα, αν μία τράπεζα ανακοινώσει ότι κάποιος «έσπασε» το διαδυκτιακό σύστημα εξυπηρέτησης πελατών, οι καταθέτες της τράπεζας θα είναι πολύ διστακτικοί στο να αξιοποιήσουν την υπηρεσία αυτή, ενώ και η μετοχή στη Σοφοκλέους πιθανόν να μπει στην κόκκινη ζώνη.
- Πολλές φορές η σημασία ενός συμβάντος υποβαθμίζεται και δεν τίθεται στις πραγματικές της διαστάσεις, πιθανώς λόγω άγνοιας των ενδεχόμενων συνεπειών.

Η μη αναφορά των περιστατικών πάντως δίνει την ψευδαίσθηση ότι «όλα πάνε καλά» και έτσι δεν βοηθά στην δημιουργία (ή αναμόρφωση) και εφαρμογή ενός καλύτερου σχεδίου ασφάλειας.

3. ΑΣΦΑΛΕΙΑ ΔΕΔΟΜΕΝΩΝ – ΕΞΟΠΛΙΣΜΟΥ

3.1 Υποσυστήματα RAID

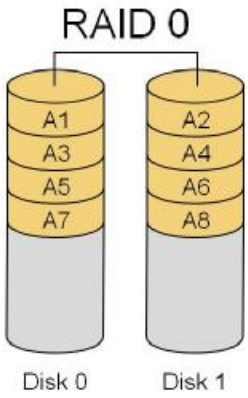
Οι σχεδιαστές των συστημάτων RAID είχαν δύο στόχους: να βελτιώσουν την απόδοση των φθηνών, χαμηλής απόδοσης σκληρών δίσκων (από εκεί προέρχεται και το ακρωνύμιο Redundant Array of Inexpensive Disks - πλεονασματική διάταξη φθηνών δίσκων) και να βελτιώσουν την ανοχή των υποσυστημάτων σκληρών δίσκων σε σφάλματα, έτσι ώστε να μπορούν να συνεχίζουν την λειτουργία τους χωρίς να χάνουν δεδομένα, ακόμη κι αν κάποιος σταματήσει να λειτουργεί κανονικά.

Ενα σύστημα RAID συνδυάζει δύο ή περισσότερους σκληρούς δίσκους με διάφορους τρόπους για να επιτύχει διαφορετικούς στόχους, αντίστοιχα. Εχουν οριστεί έξι κατηγορίες RAID, με αριθμούς από το Ο μέχρι και το 5. Αυτή η αρίθμηση δεν αντιπροσωπεύει κάποια ιεραρχία, και καμία κατηγορία RAID δεν είναι εξ ορισμού καλύτερη από τις άλλες. Απλώς έχουν διαφορετικούς στόχους.

3.1.1 RAID Ο

Η κατηγορία RAID Ο ονομάζεται επίσης και data striping (κατανομής δεδομένων).

Όπως φαίνεται και στην Εικόνα, το RAID Ο κατανέμει τις εγγραφές μεταξύ δύο ή περισσότερων σκληρών δίσκων. Αυτό οδηγεί σε αύξηση της απόδοσης, επειδή όλοι οι δίσκοι μπορούν να εξυπηρετούν ταυτόχρονα αιτήσεις για ανάγνωση/εγγραφή δεδομένων. Μία διάταξη δίσκων RAID Ο μπορεί να έχει πολύ καλύτερη απόδοση σε σχέση με αντίστοιχους μεμονωμένους.

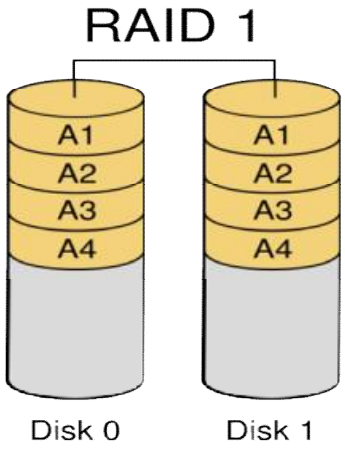


Αυτή η μέθοδος όμως, δεν αυξάνει την ανοχή σε σφάλματα. Στην πραγματικότητα, αν ένας δίσκος χαλάσει, όλα τα δεδομένα του συστήματος θα έχουν πρόβλημα, επειδή οι εγγραφές κατανέμονται στους δίσκους λίγο-πολύ τυχαία.

Το λειτουργικό Σύστημα παρέχει ενσωματωμένη υποστήριξη RAID Ο επειδή δίνει την δυνατότητα στους λογικούς δίσκους (volumes) να εκτείνονται σε πολλαπλούς σκληρούς δίσκους. Μ' αυτό τον τρόπο επιτρέπει στους λογικούς δίσκους να είναι μεγαλύτεροι απ' ότι ένας φυσικός σκληρός δίσκος και βελτιώνει την απόδοση ανάγνωσης/εγγραφής. Μερικές φορές όμως δεν συνιστάται αυτή την πρακτική, διότι οι πιθανότητες βλάβης αυξάνονται με κάθε σκληρό δίσκο που προστίθεται στον λογικό δίσκο.

3.1.2 RAID 1

Η κατηγορία RAID 1 ονομάζεται επίσης και transparent mirroring (διαφανής κατοπτρισμός δίσκων). Το RAID 1 διαμορφώνει δύο σκληρούς δίσκους έτσι ώστε να περιέχουν ακριβή αντίγραφα των ίδιων δεδομένων. Η ανοχή σε σφάλματα βελτιώνεται, επειδή ένας δίσκος μπορεί να πάθει βλάβη χωρίς να χαθούν δεδομένα. Η απόδοση κατά την ανάγνωση αυξάνει σημαντικά, επειδή η διάταξη θα ανακτήσει τα δεδομένα από τον πρώτο δίσκο που θα ικανοποιήσει την αίτηση. Η απόδοση κατά την εγγραφή, όμως, μπορεί να μειωθεί, επειδή τα δεδομένα πρέπει να γραφούν δύο φορές. Συνήθως, ο ελεγκτής των δίσκων περιμένει την επιβεβαίωση ότι τα δεδομένα έχουν ενημερωθεί σωστά από τον ένα δίσκο, πριν γράψει την εγγραφή στον άλλο δίσκο.



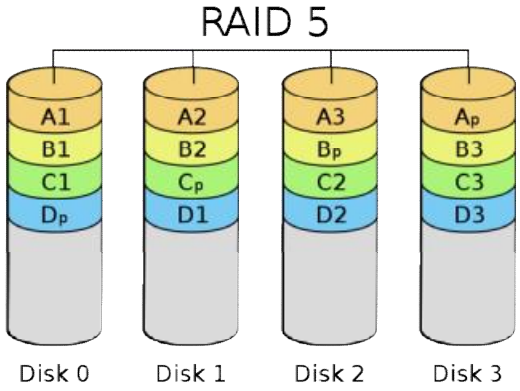
Το μειονέκτημα του RAID 1 είναι ότι απαιτούνται δυο δίσκοι για την χωρητικότητα ενός. Κάποτε, όταν το κόστος των σκληρών δίσκων ήταν εξαιρετικά υψηλό, αυτό ήταν σημαντικό μειονέκτημα. Σήμερα που οι σκληροί δίσκοι κοστίζουν ελάχιστα ανά megabyte, ο κατοπτρισμός δίσκων είναι εφικτός από άποψη κόστους.

Το λειτουργικό σύστημα αυτό υποστηρίζει διαμόρφωση RAID 1 και την ονομάζει κατοπτρισμό δίσκων (disk mirroring). Οι κατοπτρικοί δίσκοι μπορούν να εξυπηρετούνται από την ίδια κάρτα ελεγκτή (οπότε η διαμόρφωση ονομάζεται mirroring), ή από διαφορετικές κάρτες ελεγκτών για πραγματικό κατοπτρισμό (duplexing). Στη διαμόρφωση με έναν ελεγκτή, αν ο ελεγκτής πάθει βλάβη, ολόκληρο το υποσύστημα των δίσκων σταματά να λειτουργεί. Σε διαμόρφωση κατοπτρικών δίσκων με δύο ελεγκτές (duplexing), οποιοσδήποτε από τους ελεγκτές μπορεί να πάθει βλάβη χωρίς να σταματήσει η λειτουργία ολόκληρου του υποσυστήματος των δίσκων.

Ο κατοπτρισμός δίσκων μπορεί να συνδυαστεί με κατανομή δεδομένων ώστε να επαυξηθούν τα πλεονεκτήματα και των δύο. Ο κατοπτρισμός παρέχει μία διαμόρφωση με ανοχή σε σφάλματα, η οποία επιτρέπει την χωρίς κίνδυνο κατανομή των δεδομένων σε πολλαπλούς δίσκους. Ο κατοπτρισμός των δίσκων βελτιώνει την απόδοση κατά την ανάγνωση. Η κατανομή δεδομένων βελτιώνει την απόδοση τόσο κατά την ανάγνωση, όσο και κατά την εγγραφή. Αυτή είναι μία από τις ταχύτερες και περισσότερο αξιόπιστες διαμορφώσεις σκληρών δίσκων που υπάρχουν, και το Λειτουργικό σύστημα την υποστηρίζει χρησιμοποιώντας στάνταρ hardware και software.

3.1.3 RAID 5

Η κατηγορία RAID 5 είναι επίσης δημοφιλής στους servers. Αυτή η μέθοδος συνδυάζει μία μορφή κατανομής δεδομένων με μία λειτουργία αθροιστικού ελέγχου (checksum). Το αποτέλεσμα είναι μία διάταξη δίσκων η οποία μπορεί να αντέξει την βλάβη ενός δίσκου χωρίς να χάσει δεδομένα. Αυτό ακούγεται σαν το RAID 1, αλλά το RAID 5 καταναλώνει πολύ λιγότερη από την συνολική χωρητικότητα των δίσκων για να παρέχει ανοχή σε σφάλματα. Σε μία διαμόρφωση RAID 5 με τέσσερις δίσκους, μόνο το 25 τοις εκατό της συνολικής χωρητικότητας των δίσκων χρησιμοποιείται για την υποστήριξη ανοχής σε σφάλματα.



Οι εγγραφές κατανέμονται στους δίσκους με τρόπο παρόμοιο με αυτόν του RAID 0. Κάθε ομάδα εγγραφών όμως συμπεριλαμβάνει και μία εγγραφή αθροιστικού ελέγχου, η οποία υπολογίζεται από τα δεδομένα που γράφονται στους άλλους δίσκους. Αν οποιοσδήποτε δίσκος πάθει βλάβη, αυτές οι εγγραφές αθροιστικού ελέγχου μαζί με τις υπόλοιπες ακέραιες εγγραφές των δίσκων μπορούν να χρησιμοποιηθούν για τον επαναϋπολογισμό των χαμένων εγγραφών.

Προσέξτε ότι η εγγραφή αθροιστικού ελέγχου εγγράφεται σε διαφορετικό δίσκο από την ομάδα των κανονικών εγγραφών. Αυτό βελτιώνει την απόδοση κατανέμοντας την δραστηριότητα των εγγραφών αθροιστικού ελέγχου σε όλους τους δίσκους, δεδομένου ότι για κάθε λειτουργία εγγραφής θα πρέπει να αποθηκεύεται και μία εγγραφή αθροιστικού ελέγχου.

Το RAID 5 μπορεί να υλοποιηθεί χρησιμοποιώντας software, έναν δίαυλο SCSI και απλούς οδηγούς δίσκων. Τα πλεονεκτήματα του RAID 5 όμως, φαίνονται όταν όλοι οι δίσκοι είναι τοποθετημένοι μέσα σε μία συσκευή η οποία επιτρέπει την αντικατάσταση τους ενώ το σύστημα λειτουργεί. Αφού αντικατασταθεί ο δίσκος με την βλάβη, το υποσύστημα RAID 5 επαναδημιουργεί τις εγγραφές στον νέο δίσκο χωρίς

να απαιτείται το κλείσιμο του συστήματος. Επομένως, τα υποσυστήματα RAID 5 είναι ιδανικά για οργανισμούς οι οποίοι πρέπει να λειτουργούν 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα. Σε ένα συγκεκριμένο επίπεδο, το RAID 5 μπορεί επίσης να είναι οικονομικότερο από τον κατοπτρισμό δίσκων.

3.2 Αντίγραφα ασφαλείας

Δεν μπορεί να δοθεί αρκετή έμφαση στην σπουδαιότητα δημιουργίας αντιγράφων ασφαλείας. Οι περισσότεροι χρήστες δεν τηρούν αντίγραφα ασφαλείας σε τακτική βάση. Πιστεύουν ότι η διαδικασία περιλαμβάνει πολύ μεγάλη προσπάθεια. Δυστυχώς, δεν λαμβάνουν υπ'όψιν τους την απαιτούμενη προσπάθεια για να συλλέξουν και να δημιουργήσουν από την αρχή τα αρχεία τους.

Το σχέδιο τήρησης αντιγράφων ασφαλείας (backup plan) καθορίζει πότε, ποια και πώς θα αποθηκεύονται τα δεδομένα. Η δημιουργία ενός τέτοιου σχεδίου περιλαμβάνει τον καθορισμό απαντήσεων σε αρκετά ερωτήματα όπως τα παρακάτω:

- Ποιος είναι υπεύθυνος για την σωστή εκτέλεση των αντιγράφων ασφαλείας;
- Ποια δεδομένα πρέπει να συμπεριληφθούν στο αντίγραφα ασφαλείας και πόσο συχνά;
- Ποιες τεχνολογίες, εργαλεία, μέσα και μέθοδοι τήρησης αντιγράφων ασφαλείας θα πρέπει να χρησιμοποιηθούν για να είναι βέβαιο ότι τα δεδομένα μπορούν να επαναφερθούν γρήγορα και σωστά μετά από μια καταστροφή;
- Που μπορούν να αποθηκευτούν τα μέσα των αντιγράφων ασφαλείας έτσι ώστε να μην υπάρχει περίπτωση τα σημαντικά δεδομένα της επιχείρησης να χαθούν για πάντα μετά από μια καταστροφή;
- Πως μπορεί να ελεγχθεί αποτελεσματικά αν τα αντίγραφα λειτουργούν όπως θα έπρεπε;
- Πόσο γρήγορα πρέπει να μπορεί να γίνει η επαναφορά του συστήματος μετά από μια ολοκληρωτική/μερική απώλεια αυτού;
- Μπορεί να γίνει η δημιουργία/επαναφορά των αντιγράφων ασφαλείας όσο το σύστημα είναι σε κανονική λειτουργία;
- Ποια δεδομένα πρέπει να επαναφερθούν πρώτα; Μετά; Τελευταία;

- Από όλους τους χρήστες, ποιος θα παραπονεθεί περισσότερο αν τα δεδομένα του δεν είναι διαθέσιμα;
- Τι θα προκαλέσει την μεγαλύτερη απώλεια αν δεν είναι διαθέσιμο;
- Ποιος χάνει δεδομένα συχνότερα από βλάβη του υλικού ή από ανθρώπινα σφάλματα;
- Πόσο χρονικό διάστημα χρειάζεται να κρατηθούν τα αντίγραφα ασφαλείας;
- Τι χρηματικό ποσό μπορεί να δαπανηθεί;

Τα αντίγραφα ασφαλείας παρέχουν την τελευταία γραμμή άμυνας –και πιθανότατα την πιο σημαντική– ενάντια σε προβλήματα ασφάλειας και καταστροφές του πληροφοριακού συστήματος. Μια καλή πολιτική τήρησης αντιγράφων ασφαλείας σχεδόν πάντα επιτρέπει την επαναφορά του συστήματος σε μια κατάσταση πολύ παρόμοια με την κατάσταση που βρισκόταν λίγο πριν συμβεί το κακό. Ένα καλό αντίγραφο ασφαλείας μπορεί επίσης να χρησιμοποιηθεί για να επαναδημιουργηθεί το πληροφοριακό σύστημα πάνω σε καινούργιο υλικό αν υπάρξει κάποια μηχανική βλάβη. Φυσικά αν κάποιος εισβολέας καταφέρει να κλέψει δεδομένα χωρίς να σβήσει ή να τροποποιήσει κομμάτια του πληροφοριακού συστήματος, τα αντίγραφα ασφαλείας σε αυτήν την περίπτωση δεν έχουν σημασία.

Το πόσο συχνά θα πρέπει να γίνεται κάποιο αντίγραφο ασφαλείας εξαρτάται από αρκετούς λόγους που διαφέρουν κατά περίπτωση. Ωστόσο μερικοί από τους πιο σημαντικούς είναι οι εξής:

- Πρωτίστως από την αξία των δεδομένων.
- Κατά δεύτερο λόγο από την ταχύτητα του εξοπλισμού που χρησιμοποιείται για την συγκεκριμένη εργασία, δηλαδή τον χρόνο που θα απαιτηθεί για την εργασία.
- Τέλος από την ποσότητα δεσμευμένου χώρου για την αποθήκευση των αντιγράφων ασφαλείας.

Ο χρόνος που απαιτείται για κάθε προγραμματισμένη δημιουργία αντιγράφων ασφαλείας πρέπει να αντιπαρατεθεί με την μείωση της παραγωγικότητας και την χρονική καθυστέρηση που θα υπάρξει αν τα αρχεία χρειάζονται αλλά δεν είναι διαθέσιμα. Κάποιος χρήστης θα μπορούσε να δημιουργεί αντίγραφα ασφαλείας των δεδομένων του προσωπικού του υπολογιστή κάθε έξι μήνες, ενώ ένας διαχειριστής

συστήματος κάθε εβδομάδα. Επίσης θα ήταν καλό για τους διαχειριστές συστήματος, τουλάχιστον μια φορά τον χρόνο να προσπαθούν να επαναφέρουν το σύστημα τους εξ' ολοκλήρου από αντίγραφα ασφαλείας για να σιγουρευτούν ότι το υποσύστημα που είναι υπεύθυνο για την τήρηση των αντιγράφων ασφαλείας λειτουργεί όπως θα έπρεπε. Αυτή η δοκιμή θα πρέπει να γίνεται σε κάποιο εφεδρικό υπολογιστή και όχι στον κεντρικό. Στην ιδανική περίπτωση, μετά το τέλος της επαναφοράς των αρχείων, ο εφεδρικός υπολογιστής θα πρέπει να είναι πανομοιότυπος όσο αφορά το σύστημα αρχείων με τον κεντρικό. Επίσης θεωρείται καλή τακτική από τον χρήστη ή διαχειριστή να δοκιμάζει την επαναφορά κάποιων τυχαίων αρχείων αμέσως μετά το τέλος της δημιουργίας αντιγράφων ασφαλείας. Είναι καλή ιδέα η επιλογή των αρχείων που θα αντιγραφούν να γίνει με μια δόση υπερβολής και έτσι αν γίνει κάποιο λάθος αυτό να είναι η αντιγραφή περισσότερων αρχείων απ'όσα χρειάζονταν και όχι λιγότερα. Αν παραβλεφθεί κάτι σημαντικό, οι πιθανότητες λένε ότι θα είναι το πρώτο αρχείο που θα χαθεί.

Η γενική απαίτηση για κάθε αντίγραφο ασφαλείας είναι ότι θα πρέπει να επιτρέπει την επαναφορά ολόκληρου του πυρήνα του πληροφοριακού συστήματος μέσα σε ένα αποδεκτό χρονικό όριο σε περίπτωση που υπάρξει βλάβη μεγάλης κλίμακας ενώ παράλληλα να μην θυσιάζει πάρα πολύ όσο αφορά την ευκολία είτε στην διαδικασία παραγωγής του αντιγράφου ασφαλείας ή το πόσο εύκολο είναι να επαναφερθούν ένα ή δύο αρχεία που κάποιος χρήστης έσβησε κατά λάθος.

Καθώς η πρόσβαση ευρείας ζώνης γίνεται συνεχώς και πιο δημοφιλής, τα δικτυακά και απομακρυσμένα αντίγραφα ασφαλείας κερδίζουν δημοτικότητα. Η επιλογή της τήρησης αντιγράφων ασφαλείας μέσω του διαδικτύου σε ενα απομακρυσμένο σημείο, εξαλείφει τα χειρότερα σενάρια, όπως η καταστροφή ενός γραφείου μαζί με όλο τον υπολογιστικό εξοπλισμό και τα μέσα αποθήκευσης των αντιγράφων ασφαλείας. Αρκετές εταιρείες τώρα παρέχουν υπηρεσίες τήρησης κρυπτογραφημένων και συγχρονισμένων αντιγράφων ασφαλείας σε τρίτους.

Τα αντίγραφα ασφαλείας παρέχουν προστασία από απώλεια δεδομένων και ζημιά του συστήματος μόνο σε συνδυασμό με συχνό έλεγχο του συστήματος, που σαν σκοπό έχει τον γρήγορο εντοπισμό προβλημάτων στην ακεραιότητα των δεδομένων. Σε διαφορετική περίπτωση, κάποιο πρόβλημα μπορεί να παραμονεύει για πολύ καιρό. Αν αυτό συμβεί, τότε τα αντίγραφα ασφαλείας απλά θα περιέχουν το "ελαττωματικό" σύστημα αρχείων, έτσι κάνοντας αναγκαστική την ανέτρεξη εβδομάδες ή και μήνες πριν σε μια γνωστή κατάσταση "υγιούς" αντιγράφου

ασφαλείας το οποίο κατά πάσα πιθανότητα θα περιέχει αρκετά παλιές εκδόσεις των αρχείων. Η ασφάλεια μπορεί να καλύψει το κόστος ενός κατεστραμμένου υπολογιστικού συστήματος αλλά τα χαμένα δεδομένα πολλές φορές είναι αδύνατο να αντικατασταθούν.

Ποτέ δεν μπορούν να χαθούν περισσότερα δεδομένα από αυτά που δημιουργήθηκαν μετά το τελευταίο καλό εφεδρικό αντίγραφο τους.

Όμως ακόμη και τα αντίγραφα ασφαλείας δεν έχουν μόνο πλεονεκτήματα. Αντίθετα θέτουν ένα διπλό πρόβλημα ασφάλειας. Από την μια μεριά, τα αντίγραφα ασφαλείας αποτελούν το δίχτυ ασφαλείας για τα δεδομένα του συστήματος· ιδανικά θα πρέπει να φυλάσσονται μακριά από τον χώρο που βρίσκονται οι κεντρικοί υπολογιστές του συστήματος έτσι ώστε μια τοπική φυσική καταστροφή (φωτιά, πλημμύρα, έκρηξη, δομική κατάρρευση) να μην ρημάξει και τα δύο. Από την άλλη, τα αντίγραφα ασφαλείας περιέχουν όλα τα αρχεία του συστήματος, και πρέπει να προστατεύονται πολύ προσεκτικά.

Υπάρχουν τέσσερις βασικοί τύποι αντιγράφων ασφαλείας:

- **Το αρχικό αντίγραφο ασφαλείας (day-zero backup).** Δημιουργεί ένα αντίγραφο του αρχικού συστήματος. Όταν το πληροφοριακό σύστημα εγκαθίσταται για πρώτη φορά, πριν αρχίσουν να το χρησιμοποιούν άνθρωποι, πρέπει να αντιγράφεται κάθε αρχείο και πρόγραμμα του συστήματος. Τέτοια αντίγραφα ασφαλείας είναι ανεκτίμητα, ιδίως μετά από κάποιο περιστατικό εισβολής όπου το σύστημα πρέπει να αναδημιουργηθεί από την αρχή.
- **Το πλήρες αντίγραφο ασφαλείας (full backup).** Δημιουργεί ένα αντίγραφο κάθε αρχείου στο σύστημα ή κάθε αρχείου από ένα προκαθορισμένο σύνολο. Αυτή η μέθοδος είναι παρόμοια με την προηγούμενη, με την διαφορά ότι γίνεται σε τακτική βάση.
- **Το αυξητικό αντίγραφο ασφαλείας (incremental backup).** Δημιουργεί αντίγραφα μόνο από τα αρχεία που έχουν τροποποιηθεί α) μετά από κάποιο συγκεκριμένο γεγονός όπως κάποια σημαντική αλλαγή στο σύστημα ή β) μετά από κάποια συγκεκριμένη ημερομηνία όπως η ημερομηνία που δημιουργήθηκε το προηγούμενο αντίγραφο ασφαλείας.
- **Το καθημερινό αντίγραφο ασφαλείας (daily backup).** Δημιουργεί αντίγραφα από τα αρχεία που τροποποιήθηκαν την ίδια μέρα.

Τα πλήρη και τα αυξητικά αντίγραφα ασφαλείας λειτουργούν μαζί. Μια κοινή στρατηγική τήρησης αντιγράφων ασφαλείας είναι η εξής:

- Δημιουργία πλήρους αντιγράφου ασφαλείας την πρώτη μέρα κάθε δεύτερης εβδομάδας.
- Δημιουργία αυξητικού αντιγράφου ασφαλείας κάθε απόγευμα, που να περιέχει οτιδήποτε τροποποιήθηκε από το τελευταίο πλήρες αντίγραφο ασφαλείας.

Καθώς τα δίκτυα γίνονται όλο και πιο πολύπλοκα και απαιτούν υψηλότερο επίπεδο προστασίας, τα συστήματα αντιγράφων ασφαλείας θα πρέπει να είναι πιο ευέλικτα. Αρχίζουν ήδη να εμφανίζονται αυτόματα έμπειρα συστήματα (expert systems) τα οποία παρέχουν πλήρεις και ευφυείς λύσεις. Ένα τέτοιο σύστημα δεν είναι απλά ένα σύστημα τήρησης αντιγράφων ασφαλείας σε ταινία, αλλά ένα πλήρως αυτοματοποιημένο προϊόν διαχείρισης μαγνητικών μέσων. Παρέχοντας πλήρως αυτόματα προγράμματα περιστροφής ταινιών εντός και εκτός εγκατάστασης, τα συστήματα αυτά απαιτούν υψηλό επίπεδο γνώσεων για την πλήρη κατανόηση της ροής των διεργασιών τους. Τα αντίγραφα ασφαλείας είναι πιθανότατα ο πολυτιμότερος πόρος ενός πληροφοριακού συστήματος. Σε τελική ανάλυση αποτελούν ασφάλεια. Αντιπροσωπεύουν χρόνο και κόπο που αναλώθηκε σε μια προσπάθεια να αποφευχθούν μελλοντικές απώλειες. Τα λειτουργήσιμα, ολοκληρωμένα και ενημερωμένα αντίγραφα ασφαλείας μπορούν να κάνουν την διαφορά ανάμεσα σε ένα δυσάρεστο συμβάν μικρής σημασίας και μια καταστροφή. Ο τρόπος προφύλαξης τους μπορεί να τα καταστήσει ευλογία για τους διαχειριστές του συστήματος και κατάρα για τους εισβολείς αλλά και το αντίθετο.

3.3 Ειδικές περιπτώσεις

Η τήρηση αντιγράφων ασφαλείας από ενεργές βάσεις δεδομένων, δηλαδή βάσεις που λειτουργούν 24 ώρες το 24ωρο, ακόμη και όταν γίνονται αντίγραφα ασφαλείας, απαιτεί ειδικευμένο λογισμικό το οποίο πρέπει να είναι ενσωματωμένο με το σύστημα ελέγχου της βάσης δεδομένων για να αποφευχθεί η απώλεια δεδομένων. Για παράδειγμα, ας πούμε ότι ένας χρήστης προσπελαύνει τον ιστότοπο της τράπεζας του και μεταφέρει ένα χρηματικό ποσό από ένα λογαριασμό του σε έναν άλλο την στιγμή που στις εγκαταστάσεις της τράπεζας δημιουργείται ένα γενικό

αντίγραφο ασφαλείας. Μια τέτοια συναλλαγή θα επηρεάσει πολλαπλά σημεία στους σκληρούς δίσκους των υπολογιστικών συστημάτων της τράπεζας.

Ουσιαστικά, το ποσό της μεταφοράς θα αφαιρεθεί από τον πρώτο λογαριασμό και θα προστεθεί στον δεύτερο. Αν εκείνη την στιγμή συμβεί κάποιο τεχνικό πρόβλημα και γίνει επαναφορά δεδομένων από τα αντίγραφα ασφαλείας, είναι σημαντικό η βάση δεδομένων που κρατάει τα στοιχεία των λογαριασμών του πελάτη να παραμείνει ακέραια και με τις σωστές πληροφορίες. Αν το κομμάτι της συναλλαγής που αφορά την αφαίρεση του ποσού επαναφερθεί σωστά αλλά όχι το κομμάτι της πρόσθεσης στον άλλο λογαριασμό, αυτό σημαίνει απώλειες για τον πελάτη. Από την άλλη, αν το κομμάτι της πρόσθεσης επαναφερθεί σωστά αλλά όχι αυτό της αφαίρεσης, τότε αυτό σημαίνει απώλειες για την τράπεζα.

3.4 Φυσική ασφάλεια

Η φυσική ασφάλεια είναι μια από τις συχνότερα παραμελημένες μορφές ασφάλειας λόγω του ότι τα θέματα που περικλείει –οι απειλές, οι πρακτικές, και οι διαθέσιμες προφυλάξεις– είναι διαφορετικά για κάθε υπολογιστική εγκατάσταση. Η φυσική ασφάλεια αναφέρεται σπάνια σε βιβλία για την υπολογιστική ασφάλεια, καθώς διαφορετικοί οργανισμοί που χρησιμοποιούν πανομοιότυπο λογισμικό μπορούν να έχουν δραματικά διαφορετικές απαιτήσεις όσο αφορά την φυσική ασφάλεια. Επειδή η φυσική ασφάλεια απαιτεί να εγκατασταθεί επί τόπου στην υπολογιστική εγκατάσταση, δεν μπορεί να προ-εγκατασταθεί από τον παροχέα του λογισμικού ή από πωλητές και επίσης δεν μπορεί να βρεθεί έτοιμη στο διαδίκτυο σαν κομμάτι κάποιου συνόλου εργαλείων ασφάλειας. Οτιδήποτε λοιπόν γραφεί για την φυσική ασφάλεια πρέπει αναγκαστικά να είναι γενικό. Επειδή κάθε εγκατάσταση είναι διαφορετική, αυτή η παράγραφος δεν μπορεί να δώσει συγκεκριμένες υποδείξεις αλλά μόνο ένα σημείο εκκίνησης. Λένε πως τα τακτικά γραφεία δείχνουν τακτικά μυαλά. Οι ειδικοί των υπολογιστών είναι συνήθως εξαιρετικά ανοικοκύρευτοι. Οι προγραμματιστές συνηθίζουν να συσσωρεύουν τις εκτυπώσεις επάνω στα γραφεία τους. Οι λίστες με κώδικα, με διαδικασίες ασφάλειας, με προσχέδια νέων προϊόντων βρίσκονται αφύλαχτες σε κάποια γωνία του δωματίου. Όλο αυτό το χαρτομάνι μπορεί να φανεί ανεκτίμητο σε κάποιον ανταγωνιστή. Η εισαγωγή των νέων τεχνολογιών αύξησε την ποσότητα του παραγόμενου στα γραφεία χαρτιού, παρόλες τις αντίθετες αρχικές προβλέψεις. Η ελεγχόμενη και ασφαλής καταστροφή των ανεπιθύμητων ή περιττών αντιγράφων καθώς και του απαρχαιωμένου υλικού δεν πρέπει να

υποτιμάται. Τα ακλείδωτα γραφεία μπορεί να έχουν ταινίες, δίσκους ή κασέτες με πολύτιμα πιθανώς στοιχεία όπως τα αντίγραφα ασφαλείας (δεν θα έπρεπε βέβαια). Η εισαγωγή των υπολογιστών σ'ένα γραφείο δε σημαίνει ότι αχρηστεύει τις κλειδωμένες ντουλάπες. Σήμερα με την τεχνολογία των αποθηκευτικών μέσων να επιτρέπει την αποθήκευση τεράστιων ποσοτήτων δεδομένων μέσα σε ένα μικρό δισκάκι ή κασέτα που μπορεί να χωρέσει άνετα στην τσέπη του πουκαμίσου, τα δεδομένα μιας ολόκληρης επιχείρησης μπορούν εύκολα να περάσουν απαρατήρητα από τις διαδικασίες ασφάλειας του φυσικού της χώρου. Έτσι περισσότερη προσοχή από ποτέ πρέπει να δοθεί στις εγκαταστάσεις που έχουν αφαιρέσιμα αποθηκευτικά μέσα (removable media). Με την αποκεντροποίηση (decentralization) των συστημάτων τα αφαιρέσιμα μέσα είναι πια παντού. Οι προφυλάξεις πρόσβασης του φυσικού χώρου πρέπει να υπάρχουν οπουδήποτε υπάρχουν αφαιρέσιμα μέσα. Πρόσβαση σε αυτά επιτρέπει σε κάποιο εισβολέα να αφαιρέσει πληροφορίες από το σύστημα και την εγκατάσταση χωρίς να χρειαστεί να περάσει από την ασφάλεια δικτύου η οποία πιθανόν να τον εντόπιζε. Η πυκνότητα των δεδομένων και το φυσικό μέγεθος των σύγχρονων μέσων αποθήκευσης των αντιγράφων ασφαλείας ευνοούν την ρήξη της φυσικής ασφάλειας όσο ποτέ άλλοτε.

Από το σημείο όπου κάποιος εισβολέας/κλέφτης θα αφαιρέσει την πληροφορία από την εταιρεία, όλη η ενέργεια, ο χρόνος και το χρήμα που δαπανήθηκαν για την ενίσχυση της ασφάλειας του δικτυακού της συστήματος, δεν παίζουν κανένα ρόλο. Σε αυτήν την περίπτωση το μόνο που μπορεί να σώσει τα δεδομένα από την γνωστοποίηση τους στον εισβολέα είναι η κρυπτογράφηση. Η χρήση της κρυπτογράφησης μπορεί να αυξήσει δραματικά την ασφάλεια των αντιγράφων ασφαλείας. Σε αυτήν την περίπτωση θα πρέπει να χρησιμοποιείται πάντα το ίδιο κλειδί κρυπτογράφησης (η φυσική ασφάλεια των μέσων όπου αποθηκεύονται τα αντίγραφα ασφαλείας θα πρέπει να είναι το πρώτο μέλημα) και να είναι γνωστό σε τουλάχιστον δύο άτομα.

Μερικές γενικές υποδείξεις για το τι θα μπορούσε να περιλαμβάνει η φυσική ασφάλεια μιας εγκατάστασης θα μπορούσαν να είναι οι εξής:

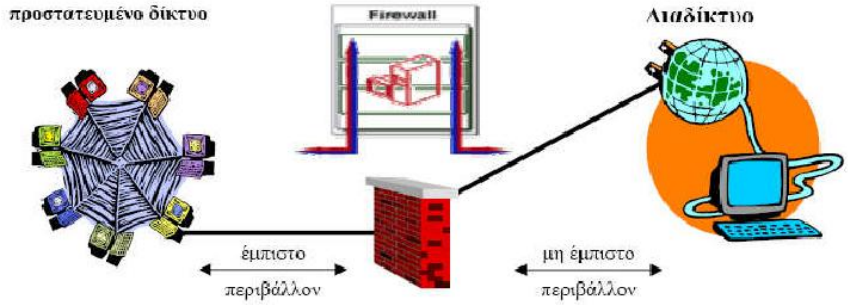
- Τοποθέτηση κρίσιμων υπολογιστικών συστημάτων σε κλειδωμένα δωμάτια και περιορισμός πρόσβασης σε αυτά τα δωμάτια (ακόμη και απόκρυψη του μέρους που αυτά βρίσκονται).

- Χρήση συστημάτων πρόσβασης με ηλεκτρονικές κάρτες-κλειδιά για τα δωμάτια με τους κεντρικούς υπολογιστές έτσι ώστε να καταγράφεται ποίος μπαίνει σε αυτά και πότε.
- Η επιτήρηση των δωματίων με τους κεντρικούς υπολογιστές μέσω βιντεοκαμερών με δυνατότητες απομακρυσμένης καταγραφής για την προστασία των παραγόμενων βιντεοκασετών.
- Απενεργοποίηση ή αφαίρεση υλικού από τους υπολογιστές όπως οι οδηγοί δισκέτας και CD.
- Αποθήκευση των μέσων αντιγράφων ασφαλείας που περιέχουν ευαίσθητα εταιρικά δεδομένα σε ασφαλή τοποθεσία εκτός των γραφείων της εταιρείας.

4. Φράγματα Ασφαλείας

4.1 Τι είναι τα φράγματα ασφαλείας (firewalls)

Ο όρος Firewall προέρχεται από τον χώρο της κατασκευαστικής βιομηχανίας. Πολλά εργαστήρια, γραφεία και εργοστάσια όταν πρωτοφτιάχνονται εξοπλίζονται με Firewalls δηλαδή ειδικά κατασκευασμένους πυρίμαχους τοίχους. Σε περίπτωση που ξεσπάσει μια πυρκαγιά στο κτίριο, είναι πολύ πιθανόν ότι θα είναι εκτός ελέγχου μόνο στο συγκεκριμένο κομμάτι του κτιρίου που ξεκίνησε καθότι τα Firewalls θα σταματήσουν ή θα συγκρατήσουν την εξέλιξη της φωτιάς μέχρι να έρθει βοήθεια. Στην περίπτωση των δικτύων υπολογιστών, τα Firewalls αποτελούν την αναγκαία λύση προστασίας τους, καθώς αυτά συνδέονται ολοένα και περισσότερο σε μεγαλύτερα δίκτυα τα οποία επίσης είναι συνδεδεμένα στο διαδίκτυο.



Από τη στιγμή που ένα δίκτυο αποκτήσει σύνδεση στο Internet, ανοίγει ένα κανάλι αμφίδρομής επικοινωνίας: οι χρήστες του δικτύου, Insiders, αποκτούν επαφή με τον έξω κόσμο, αλλά ταυτόχρονα και οι Outsiders, δηλαδή οι εξωτερικοί χρήστες αποκτούν πλέον δυνατότητα πρόσβασης σε αυτό. Ο τρομακτικός ρυθμός αύξησης του διαδικτύου, προκαλεί ανάλογη αύξηση των πιθανών κινδύνων στα ιδιωτικά δίκτυα που συνδέονται μαζί του. Για την προστασία τους από διάφορους εισβολείς απαιτείται ένας κατάλληλος φράκτης. Ο φράκτης αυτός που καλείται firewall, πρέπει να είναι ικανός να επεξεργάζεται όλη την κυκλοφορία μηνυμάτων ανάμεσα σε ένα συγκεκριμένο τοπικό ή ιδιωτικό δίκτυο και στο Internet. Στην πραγματικότητα ένα σύστημα firewall ανορθώνει ένα εξωτερικό τοίχο ασφαλείας, οριοθετώντας μια περίμετρο προστασίας. Έτσι προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο – εσωτερικό δίκτυο ενός οργανισμού το οποίο θεωρείται ασφαλές και έμπιστο και στο εξωτερικό διαδίκτυο το οποίο θεωρείται μη ασφαλές και μη έμπιστο. Ο πρωταρχικός σκοπός των firewalls, δηλαδή είναι να προστατεύσουν τα δίκτυα από εξωτερικούς εισβολείς, περιορίζοντάς τους τα δικαιώματα προσπέλασης σε αυτό, χωρίς να περιορίζουν την προσπέλαση στο εξωτερικό περιβάλλον.

Ένα firewall μπορεί να ελέγξει την κίνηση (traffic) των πακέτων του Internet από και προς τον υπολογιστή. Μπορεί να εντοπίσει τις πιθανές επιθέσεις στον υπολογιστή, να αναλύσει την κίνηση και τα αρχεία που ανταλλάσσονται, να διακρίνει τις ύποπτες δραστηριότητες και να εμποδίσει την ολοκλήρωσή τους. Ένα firewall προστατεύει ένα δίκτυο από ένα άλλο δίκτυο, υποβάλλοντας τα διερχόμενα πακέτα πληροφοριών (εισερχόμενα και εξερχόμενα) σε μια σειρά από ελέγχους και λαμβάνει την απόφαση να τα αφήσει να διέλθουν ή να τα εμποδίσει, ανάλογα με το αν περνούν κάποια τεστ ή όχι. Στην ουσία πρόκειται για έναν ελεγκτή κυκλοφορίας δεδομένων του Internet.

Μπορεί επίσης να ελέγξεί τα προγράμματα που είναι εγκατεστημένα στον ίδιο τον υπολογιστή μας και συνδέονται στο internet και τα οποία στέλνουν προς τα έξω ευαίσθητα προσωπικά δεδομένα ή αφήνουν ανοιχτή μια πίσω πόρτα (backdoor) για να μπορούν οι πιθανοί hackers να ελέγξουν τον υπολογιστή μας. Ένα firewall μπορεί να κρατήσει κλειστές αυτές τις πόρτες και να μας ενημερώνει για κάθε ύποπτη κίνηση.

Η κάθε σοβαρή εταιρεία και ο κάθε οργανισμός που έχει συναλλαγές μέσω internet, οφείλει να εφαρμόζει μια πολιτική ασφαλείας (security policy) και την καρδιά αυτής της πολιτικής ασφαλείας αποτελεί το firewall. Θα πρέπει να έχουμε υπόψη μας ότι για να μπορεί να θεωρηθεί μια εφαρμογή firewall ως πετυχημένη, θα πρέπει να μπορεί να ελέγχει και τις εσωτερικές αιτήσεις εφαρμογών και υπηρεσιών που γίνονται για πρόσβαση στο Internet και όχι μόνο αυτές που γίνονται από έξω προς τα μέσα.

4.2 Πως λειτουργεί ένα φράγμα ασφαλείας

Ένα firewall μπορεί να είναι ο συνδυασμός δρομολογητών (routers), υποδικτύων (network segments) και υπολογιστών που έχουν ρόλο host.

Ανάλογα με τον τρόπο λειτουργίας της συσκευής υπάρχουν διαφορετικού είδους εγκαταστάσεις. Παρακάτω αναφέρουμε μερικά στοιχεία των firewalls:

Bastion host: Ένας υπολογιστής γενικού σκοπού που χρησιμοποιείται για να ελέγξει την προσπέλαση ανάμεσα στο εσωτερικό (ιδιωτικό) δίκτυο (intranet) και το internet. Συνήθως το λειτουργικό του σύστημα είναι της κατηγορίας Unix που έχει τροποποιηθεί, αφαιρώντας συγκεκριμένες εντολές και υπηρεσίες, ώστε να ελαττωθούν οι δυνατότητές του στις ελάχιστες απαραίτητες για την υποστήριξη των υπηρεσιών που επιτρέπονται.

Δρομολογητής (router): Ένα υπολογιστικό σύστημα ειδικού σκοπού που διασυνδέει δύο δίκτυα. Διαχειρίζεται τα πακέτα που διακινούνται ανάμεσα στα δίκτυα, δρομολογώντας την κυκλοφορία στα κατάλληλα δίκτυα.

Ελεγκτής Λίστας Προσπέλασης (Access Control List-ACL): Πολλοί δρομολογητές έχουν την δυνατότητα να επεξεργάζονται τα πακέτα που δρομολογούν και να επιτρέπουν (ή όχι) την κυκλοφορία τους ανάλογα με το αν πληρούν (ή όχι) ορισμένες συνθήκες. Αυτές συμπεριλαμβάνουν την διεύθυνση του αποστολέα, του παραλήπτη, το port που απαντά η υπηρεσία κλπ. Έτσι μπορούν να δημιουργηθούν λίστες με κανόνες που πρέπει να ικανοποιούνται για να μπορεί να γίνει προσπέλαση ενός εξυπηρετητή ή μιας υπηρεσίας.

Η αποστρατικοποιημένη ζώνη (Demilitarized Zone-DMZ): Είναι ένα κρίσιμο συστατικό του δικτύου που βρίσκεται ανάμεσα στο ιδιωτικό δίκτυο που προφυλάσσει το firewall και το διαδίκτυο. Είναι μία περιοχή που ανήκει μεν στην εσωτερική δομή του δικτύου μας, αλλά οι κόμβοι του δεν απολαμβάνουν την εμπιστοσύνη που έχουν οι κόμβοι του υπόλοιπου δικτύου. Ο σκοπός της ζώνης αυτής είναι στρατηγικής

σημασίας για την ασφάλεια του δικτύου μας και επιτρέπει στην ουσία την προσπέλαση σε κόμβους και υπηρεσίες του εσωτερικού δικτύου. Οι εξωτερικοί χρήστες του διαδικτύου μπορούν να προσπελάσουν μόνο τους κόμβους του εσωτερικού δικτύου. Σε περίπτωση επίθεσης ο hacker θα πρέπει να αντιμετωπίσει και δεύτερο ‘τείχος’ άμυνας.

Proxy: Όταν ένας εξυπηρετητής δρα σαν να ήταν κάποιος άλλος. Για παράδειγμα ένας κόμβος που μπορεί να φέρει μια σελίδα από το διαδίκτυο πρέπει να στηθεί σαν proxy server και ένας κόμβος που ζητά την σελίδα αυτή αλλά βρίσκεται στο εσωτερικό του δικτύου πρέπει να στηθεί σαν proxy client. Με τον τρόπο αυτό όταν ένας κόμβος από το εσωτερικό μας δίκτυο ζητά μία σελίδα από το διαδίκτυο, ο proxy server την ζητά για λογαριασμό του client και την παραδίδει σε αυτόν. Με τον τρόπο αυτό μόνο οι proxy servers έρχονται σε επικοινωνία με το διαδίκτυο, ενισχύοντας την ασφάλεια του εσωτερικού μας δικτύου.

Ένα firewall μπορεί να είναι ένα μηχάνημα (συσκευή) ή και ένα πρόγραμμα (εφαρμογή) υπολογιστή, το οποίο χρησιμοποιείται για να επιβάλλει συγκεκριμένους κανόνες επικοινωνίας και ανταλλαγής πληροφοριών ανάμεσα σε δύο δίκτυα υπολογιστών. Το firewall παρεμβάλλεται ανάμεσα σε δύο διαφορετικά δίκτυα υπολογιστών και φιλτράρει τα διακινούμενα πακέτα πληροφοριών. Το firewall κατά τη λειτουργία του λαμβάνει υπόψη του ένα σύνολο από κανόνες που ορίζονται από το χρήστη (διαχειριστή του firewall) και με βάση αυτούς τους κανόνες επιτρέπει ή απορρίπτει την κυκλοφορία των δεδομένων ανάμεσα στα δύο δίκτυα υπολογιστών.

Θεωρείται ως ένας συνδετικός κρίκος ανάμεσα σε δύο δίκτυα υπολογιστών ή ως ένα φίλτρο δεδομένων. Αν δεν επιτρέψει την κυκλοφορία ενός πακέτου δεδομένων, η ενέργεια αυτή χαρακτηρίζεται ως block traffic, ενώ αν επιτρέψει την κυκλοφορία ενός πακέτου δεδομένων, ή ενέργεια αυτή χαρακτηρίζεται ως permit traffic. Ενώ τα προγράμματα anti-virus, anti-Trojan, anti-Spam κοκ έχουν συγκεκριμένο αντικείμενο απασχόλησης και προστατεύουν από πολύ συγκεκριμένες απειλές, ένα firewall μπορεί να προστατεύσει από κάθε είδους απειλή όσον αφορά τη σχέση του υπολογιστή ή του δικτύου με τον έξω κόσμο.

Ένα firewall θα πρέπει να ρυθμιστεί έτσι ώστε να λειτουργεί σωστά και αποδοτικά γιατί αλλιώς το πιθανότερο είναι να κάνει ζημιά και να μειώσει την απόδοση και την ευελιξία του υπολογιστή. Το firewall είτε πρόκειται για συσκευή είτε για πρόγραμμα είναι ένα ενδιάμεσο ανάμεσα σε δύο δίκτυα υπολογιστών. Ο χρήστης ενός οικιακού υπολογιστή ή ο administrator ενός δικτύου υπολογιστών θα πρέπει να

ορίσει τους κανόνες με βάση του οποίους θα γίνεται η κυκλοφορία των δεδομένων ανάμεσα στα δύο αυτά δίκτυα.

Μετά την εγκατάσταση ενός οποιουδήποτε firewall, ο χρήστης οφείλει να μελετήσει όλες τις επιλογές που έχει το firewall και να τις προσαρμόσει ανάλογα με τις ανάγκες του και τις τεχνικές γνώσεις που έχει. Μπορούμε να χρησιμοποιήσουμε ένα firewall για να προστατεύσουμε το δίκτυό μας από επιθετικά Web sites και πιθανούς hackers. Ένα firewall παρεμβάλλεται ανάμεσα στον υπολογιστή μας ή σε ένα δίκτυο υπολογιστών και σε ένα άλλο δίκτυο, όπως είναι το Internet ή και ένα ενδοδίκτυο (Intranet).

Σε γενικές γραμμές, ένα firewall είναι ένας φράκτης για να μπορεί να κρατάει μακριά οποιονδήποτε θελήσει να κάνει κακό στο σύστημα.

4.3 Τύποι φραγμάτων ασφαλείας

Στον απλούστερο ορισμό τους τα firewalls είναι τα συστήματα ή ο συνδυασμός συστημάτων τα οποία δημιουργούν ένα φράγμα ασφαλείας ανάμεσα σε δύο δίκτυα. Σήμερα έχουν υλοποιηθεί και προσφέρονται διάφοροι τύποι firewalls ανάλογα με τον τρόπο λειτουργίας τους. Αρχικά μπορούμε να θεωρήσουμε δύο τύπους firewalls:

1. Σε επίπεδο δικτύου (NETWORK LEVEL) και
2. Σε επίπεδο εφαρμογής (APPLICATION LEVEL)

Network level firewalls

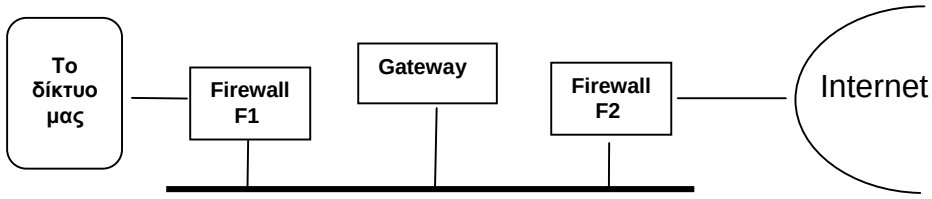
Η απλούστερη μορφή των firewall απορρίπτει επιλεκτικά πακέτα βασισμένα σε κριτήρια όπως η network address και το port. Μπορεί να διαμορφωθεί έτσι ώστε να επιτρέπει σε μερικά μόνο συστήματα του δικτύου μιας εταιρείας να επικοινωνούν με τον έξω κόσμο, ή μερικές διευθύνσεις έξω από το δίκτυο της εταιρείας να επικοινωνούν με αυτό. Για κάθε κατεύθυνση το firewall μπορεί να διαμορφωθεί με ένα σύνολο από νόμιμες διευθύνσεις πηγής και προορισμού (source and destination addresses), και να πετά όποια πακέτα δεν ικανοποιούν το πεδίο της διεύθυνσης. Αυτό είναι γνωστό ως φιλτράρισμα διεύθυνσης(address filtering).

Ένας απλός δρομολογητής είναι το ‘παραδοσιακό’ network level firewall, ενώ τα μοντέρνα διατηρούν εσωτερικές πληροφορίες σχετικά με την κατάσταση των συνδέσεων που περνάνε μέσω αυτών.

Τα network level firewalls είναι πολύ γρήγορα και επιπλέον είναι διάφανα στους χρήστες.

Application level gateway

Μια άλλη στρατηγική για να προστατεύσει το δίκτυο μια εταιρεία ή ένας ιδιώτης είναι το Application level gateway(βλέπε σχήμα)



Τα δύο firewalls είναι routers που αρνιούνται να προωθούν οτιδήποτε εκτός αν είναι από / προς το gateway. Στο gateway τρέχει ένας proxy server που εκτελεί logging και auditing της κίνησης που περνά διαμέσου αυτού. Τα Application level firewalls μπορούν να θεωρηθούν μεταφραστές διεύθυνσης δικτύου (network address translators) καθώς η κίνηση πηγαίνει από τη μια ‘πλευρά’ στην άλλη. Το firewall F2 αρνείται να προωθήσει οτιδήποτε από το σφαιρικό δίκτυο εκτός αν η διεύθυνση προορισμού είναι το gateway, και αρνείται να προωθήσει οτιδήποτε από το σφαιρικό δίκτυο εκτός αν η διεύθυνση πηγής είναι το gateway. Το firewall F1 αρνείται να προωθήσει οτιδήποτε από το δίκτυο εκτός αν η διεύθυνση προορισμού είναι το gateway, και αρνείται να προωθήσει οτιδήποτε προς το δίκτυο, εκτός αν η διεύθυνση πηγής είναι το gateway. Για να μεταφερθεί ένα αρχείο από το δίκτυο στο σφαιρικό δίκτυο, χρειάζεται κάποιος να μεταφέρει το αρχείο στο gateway, και μετά το αρχείο μπορεί να διανεμηθεί στον έξω κόσμο. Όμοια, για να διαβαστεί ένα αρχείο στο δίκτυο, ο χρήστης πρέπει πρώτα να το αντιγράψει στο gateway. Το gateway δεν υποστηρίζει όλες τις εφαρμογές. Μια κοινή στρατηγική είναι να επιτρέπει μόνο e-mail μεταξύ του δικτύου και του έξω κόσμου, και να μην επιτρέπει μεταφορά αρχείων (file transfer) και απομακρυσμένη σύνδεση (remote login). Φυσικά το e-mail μπορεί να χρησιμοποιηθεί για μεταφορά αρχείων. Τα Application level firewalls παρέχουν ποιο λεπτομερείς αναφορές και υποστηρίζουν ποιο συντηρητικά μοντέλα ασφαλείας από τα Network level firewalls.

4.4 Τεχνικές ασφάλειας με firewalls

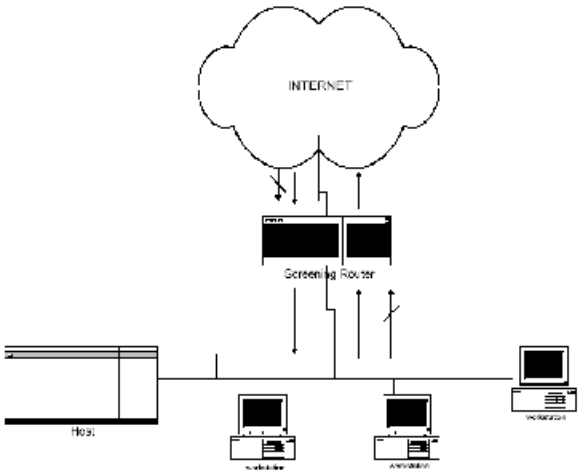
Υπάρχουν τέσσερις βασικές τεχνικές ασφάλειας με firewalls, οι οποίες είναι:

- Πύλες φιλτραρίσματος πακέτων (packet filtering gateways) ή δρομολογητές φιλτραρίσματος (screening routers),
- Πύλες κυκλωμάτων (circuit gateways),
- Πύλες εφαρμογών (application gateways),
- Πύλες μετάφρασης διευθύνσεων Δικτύου

4.4.1 Πύλες φιλτραρίσματος πακέτων

Οι πύλες φιλτραρίσματος πακέτων δρομολογούν επιλεκτικά πακέτα μεταξύ των εσωτερικών και εξωτερικών εξυπηρετητών. Επιτρέπουν ή περιορίζουν τη κυκλοφορία κατηγοριών πακέτων ανάλογα με την πολιτική ασφάλειας που έχει προκαθοριστεί. Αυτό το είδος δρομολογητών ονομάζεται screening router.

Αυτή η τεχνική φιλτραρίσματος είναι η πρώτη που εμφανίστηκε ως συνοδευτικό εργαλείο λογισμικού για την υποστήριξη επιπλέον ρυθμίσεων στον αρχικά απλό εξοπλισμό των διατάξεων ή συσκευών δρομολόγησης που δεν είχαν δυνατότητες φιλτραρίσματος των πακέτων.



Όπως είναι γνωστό κάθε πακέτο περιλαμβάνει επικεφαλίδες που περιέχουν τις ακόλουθες πληροφορίες:

IP διεύθυνση αποστολέα

IP διεύθυνση παραλήπτη

Πρωτόκολλο (TCP, UDP, ICMP)

TCP ή UDP υποδοχέα (port) αποστολέα

TCP ή UDP υποδοχέα (port) προορισμού

Τύπος μηνύματος ICMP

Επιπλέον ένας δρομολογητής γνωρίζει την σύνδεση (interface) στην οποία φθάνει το πακέτο και την σύνδεση από την οποία θα εξέλθει από αυτόν.

Η κύρια λειτουργία ενός απλού δρομολογητή είναι η επιλογή του καλύτερου τρόπου αποστολής των πακέτων στις διευθύνσεις προορισμού. Επιπλέον, οι screening routers εξετάζουν και το αν θα πρέπει να δρομολογηθεί το πακέτο προς τον κόμβο προορισμού με βάση τις πληροφορίες που περιέχονται στις επικεφαλίδες των πακέτων. Μερικά παραδείγματα φίλτρου της κυκλοφορίας είναι τα παρακάτω:

- Απαγόρευση όλων των συνδέσεων από συστήματα του εξωτερικού δικτύου (internet) εκτός αυτών που υλοποιούν SMTP συνδέσεις (ηλεκτρονικό ταχυδρομείο).
- Περιορισμός όλων των συνδέσεων από και προς τα ‘ευαίσθητα συστήματα’ που χρειάζονται ιδιαίτερη προστασία.
- Ελευθερία συνδέσεων που υλοποιούν ηλεκτρονικό ταχυδρομείο (e – mail) και υπηρεσίες FTP, απαγόρευση των συνδέσεων που αφορούν υπηρεσίες όπως TFTP, X – Window system, RPC, και ‘r’ υπηρεσίες (rlogin, rsh, scp κλπ).

4.4.2 Πύλες κυκλωμάτων

Η χρήση των πυλών κυκλωμάτων σε διατάξεις firewalls αναβαθμίζει σημαντικά την ασφάλεια των δικτύων. Επιτρέπουν τη χρήση εφαρμογών που βασίζονται στα πρωτόκολλα επικοινωνίας TCP και UDP, όπως για παράδειγμα WWW και Telnet χωρίς να αφήνουν να γίνονται όλα σε επίπεδο πρωτοκόλλου επικοινωνίας.

Οι πύλες κυκλωμάτων λειτουργούν ως εκπρόσωποι των πρωτοκόλλων επικοινωνίας, μεταβιβάζοντας την δικτυακή κίνηση μεταξύ δυο υπολογιστών που είναι συνδεδεμένοι μεταξύ τους μέσω ενός ιδεατού κυκλώματος του δικτύου. Ένας εσωτερικός χρήστης για παράδειγμα, μπορεί να συνδέεται σε μια θύρα πύλης η οποία στη συνέχεια μπορεί να συνδέεται σε μια άλλη θύρα ενός υπολογιστή που βρίσκεται σε εξωτερικό δίκτυο. Η πύλη απλά αντιγράφει bytes από την μια θύρα στην άλλη. Κανονικά η πύλη μεταβιβάζει τα δεδομένα χωρίς να τα εξετάζει, αλλά συνήθως

διατηρεί μια καταγραφή της ποσότητας των μεταβιβαζόμενων δεδομένων και του προορισμού τους. Σε μερικές διαμορφώνει τελικά ένα ‘κύκλωμα’, λειτουργεί αυτόματα. Άλλες φορές πάλι, χρειάζεται να καθορισθεί στην πύλη η επιθυμητή θύρα προορισμού.

Ένα από τα μειονεκτήματα αυτών των συστημάτων είναι ότι οι εφαρμογές των πελατών πρέπει να μετατραπούν πριν να καταστούν έτοιμες για να λειτουργήσουν σε μια συγκεκριμένη πύλη.

4.4.3 Πύλες Εφαρμογών

Οι πύλες κυκλωμάτων και οι πύλες εφαρμογών αναφέρονται και ως proxy servers, καθώς και οι δυο συμπεριφέρονται ως εκπρόσωποι του υποτιθέμενου πελάτη. Όμως οι πύλες εφαρμογών προχωρούν ακόμη παραπέρα, σε ότι αφορά την ασφάλεια δικτύων. Λειτουργούν στο υψηλότερο στρώμα επικοινωνίας, γνωστό ως το επίπεδο εφαρμογής. Έτσι έχουν πρόσβαση σε περισσότερες πληροφορίες από ότι τα συστήματα με απλό φιλτράρισμα πακέτων και μπορούν να προγραμματιστούν πιο έξυπνα κάνοντάς τα ικανά να υποστηρίξουν σύνθετες πολιτικές ασφάλειας.

Όλα τα IP – πακέτα που φτάνουν ή που πρέπει να φύγουν, εξετάζονται πρώτα ως προς το περιεχόμενό τους και ανάλογα προωθούνται ή απορρίπτονται. Για το σκοπό αυτό χρησιμοποιούνται προγράμματα που εκτελούνται ως εφαρμογές, οι οποίες ονομάζονται proxies. Κάθε TCP / IP υπηρεσία που θέλουμε να ελέγχεται από το firewall, έχει το δικό της proxy, δηλαδή μια υπηρεσία διαμεσολαβητή. Για παράδειγμα, ένας χρήστης προερχόμενος από το Internet, για να αποκτήσει πρόσβαση στη υπηρεσία FTP ενός μηχανήματος του προστατευμένου δικτύου, θα πρέπει πρώτα να συνδεθεί με την αντίστοιχη proxy εφαρμογή, να ακολουθήσει η αναγνώριση – πιστοποίησή του και στη συνέχεια, αν η πολιτική ασφάλειας του firewall περιέχει για το συγκεκριμένο και αναγνωρισμένο χρήστη τις κατάλληλες εξουσιοδοτήσεις, θα προωθηθεί η σύνδεση με την υπηρεσία FTP που ζήτησε.

Κάθε υπηρεσία proxy, είναι ένα λογισμικό δυο κατευθύνσεων που δρα ταυτόχρονα και σαν εξυπηρετητής και σαν πελάτης. Στους εσωτερικούς χρήστες απαντάει σαν να είναι η εξωτερική σύνδεση που ζήτησαν, ενώ στους εξωτερικούς χρήστες αποκρίνεται σαν να είναι η εσωτερική υπηρεσία που θα χρειαστούν.

4.4.4 Πύλες μετάφρασης διευθύνσεων Δικτύου (Network Address Translation – NAT)

Η μετάφραση διευθύνσεων Δικτύου επιτρέπει την πολύπλεξη μιας δημόσιας διεύθυνσης IP επάνω σε ένα ολόκληρο δίκτυο. Πολλές μικρές εταιρείες βασίζονται στις υπηρεσίες ενός παροχέα υπηρεσιών Internet, ο οποίο μπορεί να είναι απρόθυμος να παρέχει μεγάλα μπλοκ διευθύνσεων, επειδή και ο δικός του χώρος διευθύνσεων είναι περιορισμένος. Ίσως να υπάρχει όμως ανάγκη κάποιος χρήστης να μοιραστεί μια μόνο διεύθυνση μέσω τηλεφωνικής κλήσης ή διεύθυνση μέσω καλωδιακού μόντεμ, χωρίς να ενημερώσει για αυτό τον παροχέα υπηρεσιών. Αυτές οι επιλογές είναι δυνατές με τη χρήση Μετάφρασης Διευθύνσεων Δικτύου.

4.5 Σύγχρονες Τεχνολογίες Firewalls

Για μια ολοκληρωμένη προστασία απαιτείται η συνδυασμένη δράση των τεχνολογιών επιπέδου πακέτων και επιπέδου εφαρμογής. Έτσι παρατηρείται μια τάση υιοθέτησης της σύγκλισης αυτών των τεχνολογιών ως ο ιδανικός τρόπος υλοποίησης συστημάτων firewall για περιβάλλοντα μεσαίας έως υψηλής επικινδυνότητας.

Ο όρος υβριδικές ή σύνθετες πύλες χρησιμοποιείται για να περιγράψει τα σύγχρονα συστήματα firewall που συνδυάζοντας τα πλεονεκτήματα των προηγούμενων τεχνολογιών προχωρούν ακόμη ένα βήμα παραπέρα. Δυο είναι οι σύγχρονες εναλλακτικές υλοποιήσεις, ο συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών και η τεχνολογία Stateful Inspection.

Συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών

Έχει ήδη τονιστεί ότι ο σχετικά πρωτόγονος έλεγχος αποκλειστικά των IP επικεφαλίδων, είναι μια λειτουργία που κάθε firewall χρειάζεται, γιατί σε αρκετές περιπτώσεις αυτός είναι ο πιο κατάλληλος και πιο γρήγορος τρόπος ελέγχου. Έτσι ακόμη και τα καθαρά proxy firewalls διαθέτουν λογισμικό που προσομοιώνει έναν δρομολογητή φιλτραρίσματος. Επειδή όμως αυξάνει κατά πολύ η ασφάλεια ενός συστήματος όταν δεν είναι συγκεντρωμένη η άμυνά του σε ένα μοναδικό σημείο, πολλές φορές ένα proxy – based σύστημα firewall συνδυάζεται με μια επιπλέον

διάταξη φίλτρου πακέτων. Το υβριδικό αυτό σύστημα αποκτά παράλληλα ακόμη πιο γρήγορα και πιο αξιόπιστο φιλτράρισμα πακέτων, αφού είναι επιπέδου hardware. Η σύνδεσή τους πρέπει φυσικά να γίνει εν σειρά έτσι ώστε οι επικοινωνίες να διέρχονται και από τα δύο αυτά συστατικά μέρη του firewall.

Τεχνολογία Stateful Inspection

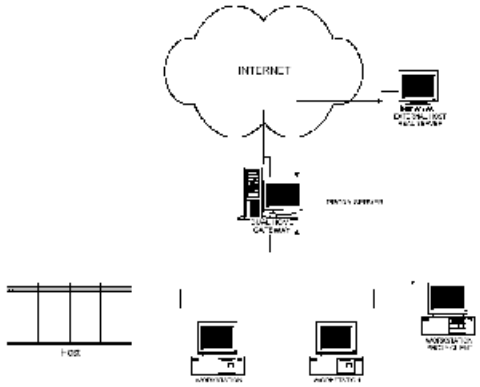
Πρόκειται για μια νέα τεχνολογία, κατηγορίας packet filtering. Όμως εδώ επεκτείνεται το απλό IP φιλτράρισμα δίνοντας δυνατότητα να εξετάζεται το κάθε πακέτο στο εσωτερικό του και μάλιστα όχι το κάθε ένα ξεχωριστά και απομονωμένα αλλά ο έλεγχος να γίνεται σε σχέση με προηγούμενες επικοινωνίες. Δημιουργείται δηλαδή μια εσωτερική βάση δεδομένων με πληροφορίες προηγούμενων πακέτων που συνεχώς ενημερώνεται. Με αυτό τον τρόπο είναι δυνατόν να καταγράφονται πληροφορίες κατάστασης και συναφείς πληροφορίες για κάθε επικοινωνία, οπότε από τον έλεγχό τους και με συνεχή τροφοδοσία από την εξελισσόμενη βάση δεδομένων, επιτρέπεται ή απαγορεύεται μια επικοινωνία με δυναμικό τρόπο.

4.6 Αρχιτεκτονικές firewall

Τα Firewalls μπορούν να διαρθρωθούν ποικιλότροπος, σχηματίζοντας διαφορετικές αρχιτεκτονικές και παρέχοντας διαφορετικά επίπεδα ασφάλειας, με διαφορετικό κόστος εγκατάστασης και λειτουργίας. Η εταιρεία θα πρέπει να επιλέξει την αρχιτεκτονική ανάλογα με τους κινδύνους που θέλει να αντιμετωπίσει. Τρεις είναι οι βασικές αρχιτεκτονικές, οι άλλες είναι συνδυασμοί αυτών. Αυτές είναι οι παρακάτω:

Dual – Homed Gateway

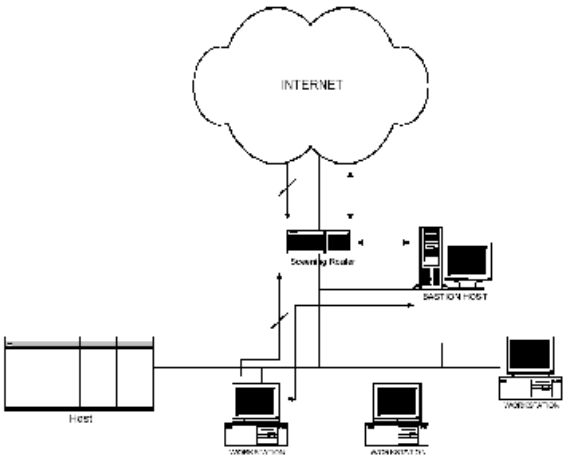
Το Dual – Homed Gateway είναι ένα Firewall που αποτελείται από ένα και μόνο σύστημα με δυο τουλάχιστον interfaces δικτύου (κάρτες). Σε ένα dual – homed firewall, η μια κάρτα είναι συνδεδεμένη στο εξωτερικό και μη έμπιστο διαδίκτυο, ενώ η άλλη κάρτα συνδέεται με το εσωτερικό και θεωρούμενο ασφαλές δίκτυο. Σημείο προσοχής σε αυτήν την αρχιτεκτονική είναι ότι δεν πρέπει να επιτρέπεται η άμεση δρομολόγηση των πακέτων των δεδομένων ανάμεσα στα δύο δίκτυα. Η επικοινωνία τους πρέπει να γίνεται μόνο μέσω του λογισμικού firewall του διακομιστή.



Αρχιτεκτονική Dual – Homed Gateway

Screen – Host Gateway

Το Screen – Host Gateway είναι μια αρχιτεκτονική firewall που αποτελείται από τουλάχιστον ένα δρομολογητή φιλτραρίσματος και ένα διακομιστή που καλείται οχυρό ή bastion host με ένα interface δικτύου. Ο δρομολογητής αυτός είναι έτσι διαμορφωμένος ώστε να περιορίζει όλη την κίνηση προς το εσωτερικό δίκτυο έτσι ώστε το bastion host να είναι το μοναδικό σύστημα που μπορεί να πλησιάσει κάποιος που βρίσκεται εκτός. Σε αντίθεση με το Dual – Homed Gateway, η εν λόγω αρχιτεκτονική δεν υποχρεώνει τη διέλευση όλης της κίνησης από το bastion host.



Αρχιτεκτονική Screen – Host Gateway

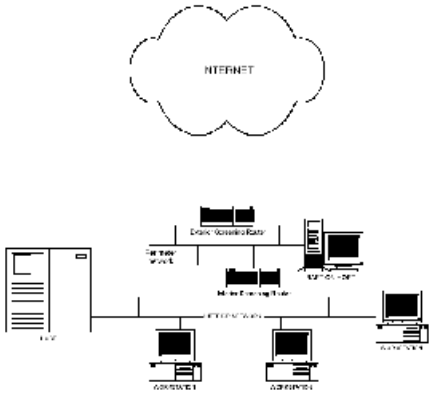
Screened subnet

Η αρχιτεκτονική αυτή παρέχει ένα επιπλέον επίπεδο ασφάλειας με την προσθήκη ενός δεύτερου δρομολογητή φιλτραρίσματος προκειμένου να διαχωρίσει τον bastion host και το δίκτυο που αυτός βρίσκεται, το οποίο καλείται περιμετρικό δίκτυο, από το υπόλοιπο εσωτερικό δίκτυο. Με την απομόνωση του bastion host στο

περιμετρικό δίκτυο περιορίζεται η σοβαρότητα των επιπτώσεων στη περίπτωση που κάποιος εισβολέας εισέλθει στον εξυπηρετητή αυτό. Η απλούστερη μορφή αυτής της τοπολογίας είναι δύο δρομολογητές με δυνατότητα φιλτραρίσματος των πακέτων και ενδιάμεσα ο εξυπηρετητής ‘οχυρό’ (bastion host). Ο ένας δρομολογητής είναι εγκατεστημένος μεταξύ του περιμετρικού και του εσωτερικού δικτύου και ο άλλος μεταξύ του περιμετρικού δικτύου και του Internet. Για να μπορέσει να εισέλθει ο εισβολέας θα πρέπει να περάσει και τους δύο δρομολογητές. Στη περίπτωση που ο εισβολέας εισέλθει στο bastion host τότε πρέπει να διαπεράσει και τον εσωτερικό δρομολογητή.

Στην αρχιτεκτονική αυτή ο εξυπηρετητής ‘οχυρό’ μπορεί να παρέχει τις ακόλουθες υπηρεσίες:

- Παραλαβή εισερχόμενου ηλεκτρονικού ταχυδρομείου
- Δρομολόγηση των εισερχομένων υπηρεσιών ftp στον εξυπηρετητή ανώνυμου ftp.
- Παροχή υπηρεσιών διευθυνσιοδότησης (DNS).



Αρχιτεκτονική Screened subnet

4.7 Πολιτική και χρήσεις των φραγμάτων ασφαλείας

Η θεμελιώδης λειτουργία ενός firewall είναι να περιορίζει την ροή πληροφορίας μεταξύ δύο δικτύων. Για να στηθεί ένα firewall, πρέπει να οριστεί επακριβώς τι είδους δεδομένα θα περνάνε και τι δεδομένα θα μπλοκάρονται. Αυτή η διαδικασία ονομάζεται ορισμός της πολιτικής του φράγματος ασφαλείας. Μετά τον ορισμό μιας πολιτικής, πρέπει να δημιουργηθούν οι μηχανισμοί που θα υλοποιούν αυτήν την πολιτική.

Υπάρχουν δυο βασικές στρατηγικές για τον ορισμό της πολιτικής φράγματος ασφαλείας:

Εξ' ορισμού διέλευση (default permit): με αυτήν την στρατηγική, ο διαχειριστής του firewall ορίζει το σύνολο των συνθηκών που οδηγούν στο μπλοκάρισμα της διέλευσης των δεδομένων. Οποιοσδήποτε διακομιστής (host) ή πρωτόκολλο (protocol) δεν καλύπτεται από την πολιτική θα του επιτρέπεται να επικοινωνεί μέσα από το firewall.

Εξ' ορισμού απαγόρευση (default deny): με αυτήν την στρατηγική, περιγράφονται τα συγκεκριμένα πρωτόκολλα που θα τους επιτρέπεται να επικοινωνούν μέσα από το firewall, και οι συγκεκριμένοι κόμβοι που μπορούν να περάσουν δεδομένα και να προσβαστούν. Σε οτιδήποτε άλλο απαγορεύεται η επικοινωνία.

Τα φράγματα ασφαλείας αποτελούν μέρος μιας στρατηγικής ασφάλειας σε βάθος. Η βασική ιδέα είναι η τοποθέτηση αρκετών στρωμάτων ασφαλείας ανάμεσα στους υπολογιστές του οργανισμού ή της εταιρείας και τις πιθανές απειλές.

Λόγω του ότι το firewall τοποθετείται στην τομή δύο δικτύων, μπορεί να χρησιμοποιηθεί για αρκετούς σκοπούς εκτός από τον έλεγχο πρόσβασης. Για παράδειγμα:

- Μπορούν να χρησιμοποιηθούν για να αποτρέψουν την πρόσβαση σε συγκεκριμένες διευθύνσεις του Διαδικτύου, ή για να απαγορεύσουν σε συγκεκριμένους χρήστες ή μηχανές από το να έχουν πρόσβαση σε συγκεκριμένους υπολογιστές – εξυπηρετητές ή υπηρεσίες.
- Ένα firewall μπορεί να χρησιμοποιηθεί για την παρακολούθηση και καταγραφή όλης της επικοινωνίας μεταξύ του εσωτερικού δικτύου και του έξω κόσμου. Μπορεί να προσφέρει εκτεταμένες αναλύσεις για το είδος και το μέγεθος των μεταφερόμενων δεδομένων, την πηγή και τον τελικό προορισμό τους, ακόμη και το περιεχόμενό τους. Αποτελεί μέσο καταγραφής και δημιουργίας στατιστικών στοιχείων για τη χρήση και κατάχρηση του δικτύου. Πρόκειται για πολύτιμες πληροφορίες που λόγω της θέσης του firewall ως το μοναδικό σημείο σύνδεσης με το έξω δίκτυο, είναι ακριβείς και αξιόπιστες.
- Αν οι εγκαταστάσεις του οργανισμού βρίσκονται σε πολλαπλές τοποθεσίες και κάθε τοποθεσία έχει το δικό της firewall, τότε κάθε ένα από αυτά μπορούν να ρυθμιστούν έτσι ώστε αυτόματα να κρυπτογραφούν τα δεδομένα που μεταφέρονται μεταξύ τους μέσω του Διαδικτύου. Ακόμη και εξωτερικά

συστήματα μπορούν να συνομιλήσουν σε κρυπτογραφημένη μορφή, αρκεί να εγκαταστήσουν το ανάλογο λογισμικό πελάτη και να παρουσιάσουν τα σχετικά διαπιστευτήρια που προέρχονται από το διαχειριστή του firewall. Με αυτόν τον τρόπο ένα κομμάτι του Διαδικτύου μπορεί να χρησιμοποιηθεί σαν ένα ιδιωτικό δίκτυο ευρείας περιοχής. Η διαδικασία αυτή πολλές φορές αναφέρεται σαν δημιουργία ενός εικονικού ιδιωτικού δικτύου.

Παρακολούθηση και Καταγραφή

Η παρακολούθηση είναι μια από τις σημαντικότερες πτυχές της σχεδίασης ενός firewall. Ο διαχειριστής του δικτύου που είναι υπεύθυνος για το firewall, θα πρέπει να γνωρίζει τις προσπάθειες παράκαμψης της ασφάλειας. Αν το firewall δεν αναφέρει τα περιστατικά αυτά, ο διαχειριστής πιθανόν να μην μπορεί να γνωρίζει ότι υπάρχουν προβλήματα.

Η παρακολούθηση μπορεί να είναι ενεργητική ή παθητική. Στην ενεργητική παρακολούθηση, το firewall ενημερώνει το διαχειριστή κάθε φορά που υπάρχει κάποιο περιστατικό. Το κύριο πλεονέκτημα της ενεργητικής παρακολούθησης είναι η ταχύτητα –ο διαχειριστής εντοπίζει αμέσως ένα ενδεχόμενο πρόβλημα. Το κύριο μειονέκτημα είναι ότι η ενεργητική παρακολούθηση συνήθως παράγει τόσο πολλές πληροφορίες που ο διαχειριστής δεν είναι σε θέση να τις κατανοήσει ή να παρατηρήσει τα προβλήματα. Για τον λόγο αυτόν, οι περισσότεροι διαχειριστές προτιμούν την παθητική παρακολούθηση, ή ένα συνδυασμό παθητικής παρακολούθησης με λίγα περιστατικά υψηλού κινδύνου να αναφέρονται από την ενεργητική παρακολούθηση.

Στην παθητική παρακολούθηση, το firewall καταγράφει μια εγγραφή για κάθε περιστατικό σε ένα αρχείο καταγραφής στο δίσκο (log file). Η παθητική παρακολούθηση καταγράφει συνήθως πληροφορίες για τη φυσιολογική κυκλοφορία (π.χ., απλά στατιστικά στοιχεία) καθώς και για πακέτα δεδομένων που φιλτράρονται. Ο διαχειριστής μπορεί να προσπελάσει το αρχείο καταγραφής οποιαδήποτε στιγμή –οι περισσότεροι διαχειριστές χρησιμοποιούν κάποιο ειδικό πρόγραμμα για τον σκοπό αυτόν. Το κύριο πλεονέκτημα της παθητικής παρακολούθησης προέρχεται από την καταγραφή των συμβάντων –ο διαχειριστής μπορεί να συμβουλευτεί το αρχείο καταγραφής, για να παρατηρήσει τις τάσεις και, όταν προκύψει πραγματικά ένα πρόβλημα ασφάλειας, να εξετάσει το ιστορικό των συμβάντων που οδήγησησαν στο πρόβλημα. Ακόμα σημαντικότερο είναι το γεγονός ότι ο διαχειριστής μπορεί να

αναλύει περιοδικά το αρχείο καταγραφής (π.χ. καθημερινά), για να προσδιορίσει αν αυξάνονται ή μειώνονται οι προσπάθειες πρόσβασης στο πληροφοριακό σύστημα με την πάροδο του χρόνου.

4.8 Από τι μπορεί να μας προστατεύσει ένα firewall

Υπάρχουν πολλοί τρόποι που μπορεί να χρησιμοποιήσει κάποιος ασυνείδητος για να κάνει ζημιά σε μη προστατευμένους υπολογιστές, όπως :

- Απομακρυσμένη Πρόσβαση (Remote Login). Συμβαίνει όταν κάποιος έχει τη δυνατότητα να συνδεθεί στον υπολογιστή μας και να τον ελέγξει κατά κάποιον τρόπο. Αυτό μπορεί να κυμαίνεται από το να μπορεί να δει απλά ή να έχει πρόσβαση σε αρχεία έως το να μπορεί να τρέχει προγράμματα στον υπολογιστή μας.
- Κερκόπορτες Εφαρμογής (Application Backdoors). Μερικά προγράμματα έχουν ιδιαίτερα χαρακτηριστικά που επιτρέπουν την απομακρυσμένη πρόσβαση (remote access), ενώ άλλα περιέχουν σφάλματα (bugs) τα οποία δίνουν τη δυνατότητα για την ύπαρξη κερκόπορτας ή πίσω πόρτας (backdoor), δηλ. μιας κρυφής πρόσβασης, με την οποία μπορεί να έχει κάποιος κάποιο επίπεδο ελέγχου του προγράμματος.
- SMTP Session Hijacking. Το SMTP αποτελεί την πιο κοινή μέθοδο αποστολής ηλεκτρονικού ταχυδρομείου (e-mail) στο Internet και αποκτώντας πρόσβαση σε μια λίστα από διευθύνσεις e-mail, κάποιος μπορεί να στείλει αυτόκλητα e-mail (Spam) σε χιλιάδες χρήστες.
- Σφάλματα στο Λειτουργικό Σύστημα. Όπως και οι εφαρμογές, μερικά λειτουργικά συστήματα έχουν backdoors, ενώ άλλα παρέχουν απομακρυσμένη πρόσβαση με ανεπαρκείς ελέγχους ασφαλείας ή έχουν ελαττώματα (bugs) που μπορεί να εκμεταλλευθεί ένας έμπειρος hacker.
- Άρνηση Υπηρεσίας (Denial of Service). Αυτό το είδος επίθεσης είναι σχεδόν αδύνατο να αντιμετωπισθεί. Αυτό που συμβαίνει είναι ότι ο hacker στέλνει μια αίτηση (request) στον server για να συνδεθεί σ’ αυτόν. Όταν ο server απαντήσει με μια αναγνώριση (acknowledgement) και προσπαθήσει να κάνει μια σύνοδο (session), δεν θα μπορεί να βρει το σύστημα που έκανε την αίτηση (request). Κατακλύζοντας έναν server με τέτοιες αναπάντητες αιτήσεις

session, ένας hacker αναγκάζει τον server να δουλεύει πολύ αργά (σέρνεται) έως ότου καταρρεύσει.

- Βόμβες e-mail (e-mail Bombs). Μια βόμβα e-mail είναι συνήθως μια προσωπική επίθεση όπου κάποιος μάς στέλνει το ίδιο e-mail εκατοντάδες ή και χιλιάδες φορές μέχρις ότου το σύστημά μας να μην μπορεί να δεχθεί άλλα μηνύματα.
- Μακροεντολές (Macros). Για να απλοποιήσουν περίπλοκες διαδικασίες ή εργασίες, πολλές εφαρμογές (applications) μάς δίνουν τη δυνατότητα να δημιουργήσουμε ένα μικρό πρόγραμμα (σενάριο εντολών, script) από εντολές που η εφαρμογή μπορεί να εκτελέσει. Αυτό το script είναι γνωστό ως μακροεντολή (macro). Οι hackers μπορούν να εκμεταλλευθούν αυτή τη δυνατότητα και να δημιουργήσουν τα δικά τους macros, τα οποία, ανάλογα με την εφαρμογή, μπορούν να καταστρέψουν τα δεδομένα ή και να προκαλέσουν την κατάρρευση του υπολογιστή μας.
- Ιοί (Viruses). Πιθανώς η πιο γνωστή απειλή είναι οι ιοί των υπολογιστών (computer viruses). Ένας ιός (virus) είναι ένα μικρό πρόγραμμα που μπορεί να αντιγράψει τον εαυτό του σ' άλλους υπολογιστές. Μ' αυτόν τον τρόπο μπορεί να διαδοθεί ταχύτατα από το ένα σύστημα στο άλλο. Το αποτέλεσμα ενός ιού μπορεί να κυμαίνεται από την εμφάνιση ενός αβλαβούς μηνύματος έως και τη διαγραφή όλων των αρχείων του υπολογιστή μας.
- Spam e-mail. Μπορεί να μην κάνει ζημιά αλλά είναι πάντα ενοχλητική, η μη ζητηθείσα ή αυτόκλητη εμπορική αλληλογραφία (spam e-mail), που αποτελεί το ηλεκτρονικό ισοδύναμο της άχρηστης διαφημιστικής αλληλογραφίας (junk mail). Το spam e-mail μπορεί να είναι και επικίνδυνο καθώς αρκετά συχνά περιέχει συνδέσμους (links) σε Web sites, τα οποία ενδέχεται να στέλνουν cookies για να ανοίξουν έτσι μια κερκόπορτα (backdoor) στον υπολογιστή μας.
- Βόμβες Ανακατεύθυνσης (Redirect Bombs). Οι hackers μπορούν να χρησιμοποιήσουν το πρωτόκολλο ICMP για να αλλάξουν (ανακατευθύνουν) τη διαδρομή που ακολουθούν οι πληροφορίες, στέλνοντάς τες σ' έναν διαφορετικό δρομολογητή (router). Αυτός είναι κι ένας από τους τρόπους που γίνεται μια επίθεση άρνησης υπηρεσίας (denial of service attack).
- Source routing. Στις περισσότερες περιπτώσεις, η διαδρομή που ακολουθεί ένα πακέτο στο Internet (ή σ' ένα άλλο δίκτυο) καθορίζεται από τους

δρομολογητές (routers) που υπάρχουν κατά μήκος της διαδρομής. Αλλά η πηγή (source), δηλ. ο αρχικός υπολογιστής, που παρέχει το πακέτο μπορεί αυθαίρετα να καθορίσει τη διαδρομή (route) που θα πρέπει να ακολουθήσει το πακέτο. Οι hackers το εκμεταλλεύονται αυτό μερικές φορές για να κάνουν τις πληροφορίες να φαίνονται ότι προέρχονται από μια έγκυρη πηγή ή ακόμη και μέσα από το ίδιο το δίκτυο. Τα περισσότερα Firewalls μπορούν και εξουδετερώνουν το source routing.

Μερικές από τις παραπάνω επιθέσεις, είναι δύσκολο, αν όχι αδύνατο, να αντιμετωπισθούν με τη χρήση ενός firewall. Ενώ μερικά firewalls προσφέρουν προστασία από ιούς, αξίζει τον κόπο να εγκαταστήσουμε ένα πρόγραμμα anti-virus σε κάθε υπολογιστή του δικτύου μας. Και, αν και είναι ενοχλητικά, πολλά spam e-mails μπορούν να περάσουν μέσα από το firewall όσο εμείς λαμβάνουμε τα e-mails μας. Το επίπεδο ασφάλειας (level of security) που ορίζουμε είναι αυτό που καθορίζει πόσες πολλές απ' αυτές τις απειλές μπορούν να αναχαιτισθούν από ένα firewall. Το υψηλότερο επίπεδο ασφάλειας θα είναι το μπλοκάρισμα των πάντων.

Στην ουσία κάτι τέτοιο καταργεί την ύπαρξη μιας σύνδεσης στο Internet, αλλά ένας κοινός πρακτικός κανόνας είναι να μπλοκάρουμε τα πάντα και μετά να αρχίζουμε να επιλέγουμε τι είδος κυκλοφορίας θα επιτρέψουμε.

Μπορούμε επίσης να περιορίσουμε την κυκλοφορία (traffic) που περνάει μέσα από το firewall έτσι ώστε μόνο συγκεκριμένα είδη πληροφοριών, όπως τα e-mail, να μπορούν να περάσουν. Για τους περισσότερους χρήστες, το καλύτερο είναι να εργάζονται με τις προκαθορισμένες ρυθμίσεις που δίνονται από τον κατασκευαστή του firewall εκτός κι αν υπάρχει κάποιος πολύ συγκεκριμένος λόγος για να γίνουν αλλαγές.

Ένα από τα καλύτερα πράγματα όσον αφορά ένα firewall από την άποψη της ασφάλειας είναι ότι εμποδίζει τον οποιονδήποτε βρίσκεται έξω από το να εισβάλλει σ' έναν υπολογιστή του δικτύου μας. Μπορεί αυτό να ενδιαφέρει κυρίως τις επιχειρήσεις, αλλά και οι οικιακοί χρήστες με τη χρήση ενός firewall μπορούν να έχουν ήσυχο το κεφάλι τους.

4.9 Σε ποιες περιπτώσεις δεν μπορεί να προστατεύσει το Firewall

Τα Firewalls δεν μπορούν να προστατεύσουν από επιδρομές οι οποίες δεν περνούν από αυτά. Πολλές εταιρίες δίνουν βάρος στις διαδικασίες των firewalls,

προσπαθώντας να αποτρέψουν τα δεδομένα τους να διαρρεύσουν έξω από αυτές. Είναι όμως εξαιρετικά εύκολο, όσα firewalls και αν σηκωθούν, οι πληροφορίες να διαρρεύσουν με άλλους τρόπους εξαιρετικά απλούς όπως για παράδειγμα με φυσικό τρόπο με μια μαγνητική ταινία. Το firewall θα πρέπει να είναι μέρος της συνολικής πολιτικής ασφάλειας των δεδομένων και να λαμβάνει υπόψη του και την συνολική αρχιτεκτονική και δομή του συστήματος. Έτσι για παράδειγμα δεδομένα τα οποία είναι απόρρητα δεν χρειάζονται καθόλου firewall. Τα συστήματα τα οποία περιλαμβάνουν τα δεδομένα αυτά θα πρέπει να είναι απόλυτα απομονωμένα από το Internet. Το firewall δεν μπορεί να προστατεύσει από τις κακόβουλες επιδρομές οι οποίες ξεκινούν από το εσωτερικό του τοίχου. Αντίστοιχα όπως κάποιος αφελώς μπορεί να επιτρέψει την διαρροή εμπιστευτικών πληροφοριών μέσα από το τηλέφωνο το ίδιο αφελώς μπορεί να βοηθήσει να αποκτήσουν τρίτοι πρόσβαση στην συλλογή των modems. Τέλος το firewall δεν μπορεί να προστατεύσει από τις διόδους που δημιουργούν τα διάφορα πρωτόκολλα εφαρμογών. Υπάρχει πάνα η δυνατότητα διοχέτευσης ανεξέλεγκτων εφαρμογών μέσα από πρωτόκολλα όπως είναι το HTTP, το SMTP και άλλα πρωτόκολλα τα οποία είναι ευρέως διαδεδομένα.

5. Ασφάλεια Βάσεων Δεδομένων

Με δεδομένο ότι πάνω από το 90% των σύγχρονων συστημάτων χρησιμοποιεί κάποιο είδος βάσης δεδομένων, η ασφάλεια των βάσεων δεδομένων αποκτά ιδιαίτερη σημασία, αν μάλιστα λάβουμε υπ' όψιν ότι η αξία της πληροφορίας είναι το κύριο «περιουσιακό στοιχείο» των πληροφοριακών συστημάτων.

Αντικείμενο της Ασφάλειας Βάσεων Δεδομένων (Database Security) είναι η ικανότητα του συστήματος να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των πληροφοριών της Βάσης Δεδομένων που αφορά τη δυνατότητα προσπέλασης, την διαθεσιμότητα και την δυνατότητα τροποποίησης ή διαγραφής των πληροφοριών.

Με τον όρο ασφάλεια των βάσεων δεδομένων καθορίζουμε τους μηχανισμούς αποφυγής της μη επιθυμητής διαρροής (disclosure), μεταβολής(modification) και καταστροφής(destruction) των αποθηκευμένων πληροφοριών.

Για παράδειγμα, στην περίπτωση ενός ιατρικού πληροφοριακού συστήματος ο ασθενής θα πρέπει να είναι βέβαιος ότι οι προσωπικές του πληροφορίες ή τα ευαίσθητα προσωπικά του δεδομένα που δόθηκαν κατά την είσοδό του στο νοσοκομείο ή αυτά που δημιουργήθηκαν κατά την διάρκεια της θεραπείας του σε αυτό συλλέγονται, αποθηκεύονται και επεξεργάζονται με ένα τρόπο που αποκλείει τυχόν λάθη, διατίθενται μόνο σε εξουσιοδοτημένους χρήστες και χρησιμοποιούνται με νόμιμο τρόπο.

Με την ορολογία “ασφαλές” Σ.Δ.Β.Δ. εννοούμε ότι οι μηχανισμοί ασφάλειας ενεργοποιούνται αυτόματα (χωρίς επιπλέον προγραμματισμό) σε κάθε απόπειρα πρόσβασης στα δεδομένα. Οι μηχανισμοί αυτοί θα πρέπει να εκτελέσουν τους απαραίτητους ελέγχους για την αντιμετώπιση του συνόλου των πιθανών καταστάσεων απειλής, που θα αντιμετωπίσει το σύστημα σε όλη τη διάρκεια του κύκλου ζωής του.

Όταν σε ένα πληροφοριακό σύστημα εισάγεται κάποια βάση δεδομένων, οι συνήθεις διαστάσεις της ασφάλειας (ακεραιότητα, έλεγχος προσπέλασης, εμπιστευτικότητα, διαθεσιμότητα, έλεγχος) επαυξάνονται με μερικές ακόμη και συγκεκριμένα:

1. **Διακριτότητα** (granularity). Στα συνήθη συστήματα ένα υποκείμενο είτε έχει ένα δικαίωμα πάνω σε ένα αντικείμενο είτε δεν το έχει, ενώ το αντικείμενο καθορίζεται από τη φυσική του οντότητα. Για παράδειγμα, ένας εκτυπωτής είναι ένα διακριτό αντικείμενο και ένας χρήστης μπορεί να έχει δικαίωμα να τυπώσει ή όχι, ένα τερματικό είναι επίσης ένα διακριτό αντικείμενο και μπορεί να παρέχει το δικαίωμα σύνδεσης ή να μην το παρέχει. Σε μία βάση δεδομένων ωστόσο, το αντικείμενο που αφορούν οι εξουσιοδοτήσεις μπορεί να είναι μία ολόκληρη βάση δεδομένων, μία σχέση, μία γραμμή ή στήλη σχέσης ή ακόμη και μία μεμονωμένη τιμή. Η έννοια της διακριτότητας σχετίζεται με το πόσο λεπτομερής είναι η διάκριση των αντικειμένων πάνω στα οποία εφαρμόζονται οι εξουσιοδοτήσεις.

2. **Συμπερασμός** ή **έμμεση προσπέλαση** (inference). Υπάρχουν περιπτώσεις κατά τις οποίες κάποιος χρήστης δεν έχει δικαίωμα άμεσης προσπέλασης σε κάποια δεδομένα, μπορεί όμως να τα συνάγει με κατάλληλες εντολές προς τη βάση δεδομένων. Για παράδειγμα, ένα σύστημα βάσεων δεδομένων πιθανόν να μη μας επιτρέπει να ζητήσουμε τον μισθό ενός συγκεκριμένου εργαζόμενου βάσει αριθμού ταυτότητας, αλλά μόνο μέσω φύλου, ηλικίας και ετών προϋπηρεσίας (προκειμένου για εξαγωγή στατιστικών στοιχείων). Αν εμείς γνωρίζουμε ότι υπάρχει ένας μόνο άνδρας σε ηλικία 45 ετών με 16 χρόνια προϋπηρεσίας, τότε μπορούμε χρησιμοποιώντας τα νομότυπα κριτήρια να εξάγουμε πληροφορία που δεν θα έπρεπε.

3. **Συνάθροιση** (aggregation). Με τον όρο συνάθροιση αναφερόμαστε στη συλλογή δεδομένων από διαφορετικές πηγές και τον συνδυασμό τους για την εξαγωγή πρόσθετων πληροφοριών. Το πρόβλημα αυτό έχει ενταθεί με την πρόοδο των τεχνικών εξόρυξης δεδομένων.

4. **Φιλτράρισμα** (filtering). Η απόκρυψη δηλαδή από τον χρήστη δεδομένων που δεν πρέπει να έχει τη δυνατότητα να δει.

5. **Καταγραφή** (journaling). Η τήρηση δηλαδή πλήρους ημερολογίου σχετικά με τις ενέργειες που έχουν γίνει επί των δεδομένων και τους συσχετισμούς τους με τους χρήστες.

5.1 Απαιτήσεις Ασφάλειας των Βάσεων Δεδομένων

Οι βασικές απαιτήσεις για την ασφάλεια των συστημάτων βάσεων δεδομένων δεν διαφέρουν ουσιαστικά από αυτές του υπολοίπου συστήματος. Οι κυριότερες από αυτές είναι :

- **Φυσική ακεραιότητα της βάσης** (physical database integrity). Η φυσική ακεραιότητα της βάσης δεδομένων συσχετίζεται με τη φθορά που μπορούν να υποστούν τα μαγνητικά μέσα αποθήκευσης από διακοπές ρεύματος, βλάβες κυκλωμάτων ή φυσιολογική φθορά. Το σύστημα θα πρέπει να παρέχει μηχανισμούς ώστε κατόπιν εμφανίσεως τέτοιων περιστατικών να είναι δυνατή η ανάκαμψη από το σφάλμα και η ανάκληση των δεδομένων.
- **Λογική ακεραιότητα της βάσης** (logical database integrity). Πρέπει να διατηρείται σε κάθε περίπτωση η λογική ακεραιότητα της βάσης. Για παράδειγμα η διατήρηση της λογικής ακεραιότητας της βάσης εγγυάται ότι η μεταβολή της τιμής ενός από τα πεδία της δεν επηρεάζει τις τιμές των άλλων πεδίων, παρά μόνο εφόσον κάτι τέτοιο έχει προβλεφθεί.
- **Ακεραιότητα των πεδίων της βάσης** (element integrity). Εγγυάται ότι οι τιμές των επί μέρους πεδίων της βάσης είναι ακριβείς (σωστές). Οι εξουσιοδοτημένοι χρήστες είναι υπεύθυνοι για την εισαγωγή σωστών δεδομένων στη βάση. Παρόλα αυτά οι χρήστες κάνουν λάθη στη συλλογή των δεδομένων, στην επεξεργασία των αποτελεσμάτων και στην εισαγωγή των τιμών. Τα Σ.Δ.Β.Δ. μπορούν να βοηθήσουν τον χρήστη να αντιληφθεί τα δεδομένα καθώς αυτά εισέρχονται και να τα διορθώσει. Αυτό γίνεται με τρεις τρόπους: α) Μπορεί να εφαρμοστεί έλεγχος πεδίων (field checks), που κάνει έλεγχο για τις κατάλληλες τιμές σε μια θέση, β) Με τον έλεγχο πρόσβασης (access control), και τέλος γ) Με ένα πρόχειρο αλλαγής για τη βάση (change

log). Το ημερολόγιο αλλαγών είναι μια λίστα για κάθε αλλαγή που συμβαίνει στη βάση και το οποίο περιέχει και τις αυθεντικές και τις τροποποιημένες τιμές.

- **Έλεγχος προσπέλασης** (access control). Εγγυάται ότι οι χρήστες της βάσης μπορούν να προσπελάσουν μόνο τα δεδομένα εκείνα για τα οποία έχουν εξουσιοδοτηθεί. Οι διάφοροι τύποι χρηστών μπορεί έτσι να περιοριστούν σε ορισμένους χώρους και τρόπους προσπέλασης, ανάλογα με τις ανάγκες τους (π.χ. μόνο διάβασμα). Οι βάσεις δεδομένων είναι συνήθως λογικά χωρισμένες από τα προνόμια πρόσβασης του χρήστη. Για παράδειγμα όλοι οι χρήστες μπορεί να είναι εξουσιοδοτημένοι να προσπελάσουν γενικά δεδομένα, αλλά μόνο το τμήμα προσωπικού μπορεί να αποκτάει δεδομένα μισθών και μόνο το τμήμα μάρκετινγκ μπορεί να αποκτά δεδομένα σχετικά με τις πωλήσεις. Οι βάσεις δεδομένων είναι πολύ χρήσιμες, γιατί συγκεντρώνουν την αποθήκευση και διατήρηση των δεδομένων. Η περιορισμένη πρόσβαση είναι και μια ευθύνη και ένα όφελος από αυτή τη συγκέντρωση.
- **Πιστοποίηση των χρηστών** (user authentication). Η διαδικασία πιστοποίησης εγγυάται ότι ο κάθε χρήστης της βάσης αναγνωρίζεται θετικά από τη βάση, πριν του επιτραπεί η προσπέλαση σε αυτήν.
- **Διαθεσιμότητα** (availability). Εγγυάται ότι οι εξουσιοδοτημένοι χρήστες μπορούν γενικά να προσπελάσουν άμεσα την βάση και τα δεδομένα για τα οποία είναι εξουσιοδοτημένοι. Οι απαιτήσεις της διαθεσιμότητας ενός Σ.Δ.Β.Δ είναι πολύ μεγάλες. Ένα πρόβλημα διαθεσιμότητας προέρχεται από την διαδικασία διαιτησίας δυο απαιτήσεων των χρηστών για την ίδια εγγραφή.
- **Εμπιστευτικότητα** (Confidentiality). Μια βάση δεδομένων θα πρέπει να διαφυλάσσει την εμπιστευτικότητα των πληροφοριών επιτρέποντας την προσπέλασή τους μόνο από εξουσιοδοτημένους χρήστες, να προστατεύει την ακεραιότητα και τη διαθεσιμότητα των δεδομένων. Οι στόχοι αυτοί είναι αλληλοσυγκρουόμενοι, έτσι συνήθως βρίσκεται κάποια χρυσή τομή, ανάλογα με τις προτεραιότητες και τις ανάγκες του οργανισμού. Τα συστήματα επιβάλουν την Εμπιστευτικότητα μέσω των μηχανισμών της ταυτοποίησης, αυθεντικοποίησης και των υποχρεωτικών και διακριτικών μηχανισμών ελέγχου πρόσβασης.
- **Ασφάλεια/Πεπίθηση** (Assurance). Παρέχει ένα βαθύτερο επίπεδο εμπιστοσύνης για τη σωστή λειτουργία και αποδοτικότητα των

χαρακτηριστικών της Εμπιστευτικότητας, Ακεραιότητας, και Διαθεσιμότητας του συστήματος. Η ασφάλεια αυτή επιτυγχάνεται με τη χρήση ηχητικών και μηχανικών τεχνικών ασφαλείας.

- **Πληρότητα Δεδομένων** (Data Integrity). Το πληροφοριακό περιεχόμενο της βάσης δεδομένων είναι αποδεκτό μόνο όταν ικανοποιούνται συγκεκριμένες προϋποθέσεις πληρότητας των καταχωρημένων στοιχείων. Όταν συμβεί παραβίαση της συνθήκης πληρότητας των δεδομένων το σύνολο του πληροφοριακού περιεχομένου της βάσης είναι άχρηστο.
- **Εξ' αναφοράς Πληρότητα** (Referential Integrity). Η εξ' αναφοράς Πληρότητα έχει να κάνει με την λογική σύνδεση του περιεχομένου των πινάκων. Δηλαδή, η συνθήκη της εξ' αναφοράς πληρότητας επιβάλλει για την κάθε στιγμή που το ξένο κλειδί παίρνει τιμή, η τελευταία να είναι ήδη καταχωρημένη στον πίνακα που περιέχει το αντίστοιχο κύριο κλειδί.
- **Πληρότητα ΄Υπαρξης**. Έχει να κάνει με την δέσμευση του κάθε πίνακα να έχει ένα κύριο κλειδί, έτσι ώστε να προσδιορίζεται μονοσήμαντα η κάθε εγγραφή. Η τιμή του κύριου κλειδιού πρέπει να μην είναι Null (δηλαδή το πεδίο να είναι κενό).

5.2 Διακρίβωση ταυτότητας χρηστών σε Συστήματα Βάσεων Δεδομένων

Τα συστήματα βάσεων δεδομένων πρέπει να έχουν ένα πρώτο επίπεδο ελέγχου πρόσβασης, όπου διαπιστώνεται αν ένας χρήστης έχει συνολικά το δικαίωμα να χρησιμοποιήσει το σύστημα βάσεων δεδομένων ή όχι. Συνήθως παρέχονται οι εξής δυνατότητες για διακρίβωση της ταυτότητας των χρηστών:

Διακρίβωση ταυτότητας με όνομα χρήστη συνθηματικό

Κατά τρόπο πλήρως αντίστοιχο με τα λειτουργικά συστήματα, μία βάση δεδομένων μπορεί να ζητά από τους χρήστες της ένα όνομα χρήστη και ένα συνθηματικό ως διαπιστευτήρια της σύνδεσης. Το Σ.Δ.Β.Δ. οφείλει να διατηρεί έναν κατάλογο με τις έγκυρες αντιστοιχίες ονομάτων χρηστών και συνθηματικών ώστε να αποφασίζει για το αν τα παρουσιασθέντα διαπιστευτήρια είναι έγκυρα. Δεν είναι απαραίτητο να υπάρχει οποιαδήποτε συσχέτιση ανάμεσα στα διαπιστευτήρια της βάσης δεδομένων και του λειτουργικού συστήματος.

Η τεχνική αυτή είναι χρήσιμη όταν το λειτουργικό σύστημα δεν παρέχει αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας των χρηστών ή όταν πραγματοποιούνται συνδέσεις μέσω δικτύου στη βάση δεδομένων, οπότε η ταυτότητα του χρήστη στο λειτουργικό σύστημα δεν είναι διαθέσιμη (ή αξιόπιστη).

Διακρίβωση ταυτότητας από το λειτουργικό σύστημα

Σ' αυτή την περίπτωση το Σ.Δ.Β.Δ. επαφίεται στους μηχανισμούς του λειτουργικού συστήματος να εκτελέσουν ορθή διακρίβωση ταυτότητας. Από τη στιγμή που ένας χρήστης έχει αναγνωριστεί από το λειτουργικό σύστημα και ο χρήστης λειτουργικού συστήματος είναι εξουσιοδοτημένος να χρησιμοποιεί τη βάση δεδομένων, δεν ζητάτε κανένα πρόσθετο στοιχείο για την προσπέλαση του χρήστη στη βάση δεδομένων. Αυτό είναι βολικό για τους χρήστες καθώς δεν είναι απαραίτητο να γνωρίζουν οποιαδήποτε άλλα συνθηματικά, πέρα από αυτά που χρησιμοποιούν για τη σύνδεσή τους στο σύστημα.

Ο μηχανισμός αυτός δεν μπορεί (ή δεν είναι σκόπιμο) να χρησιμοποιείται ως αποκλειστικός μηχανισμός διακρίβωσης ταυτότητας σε συστήματα όπου επιτρέπεται δικτυακή πρόσβαση στη βάση δεδομένων, καθώς επιτάσσει κάθε χρήστης να έχει λογαριασμό στο λειτουργικό σύστημα (κάτι που μπορεί να μην είναι επιθυμητό). Επίσης, πρέπει να χρησιμοποιείται μόνον όταν το λειτουργικό σύστημα έχει επαρκώς αξιόπιστους μηχανισμούς διακρίβωσης ταυτότητας.

Διακρίβωση ταυτότητας μέσω καθολικών υπηρεσιών καταλόγου

Ο χρήστης εισάγει στο Σ.Δ.Β.Δ. ένα όνομα και ένα συνθηματικό και το Σ.Δ.Β.Δ. διασυνδέεται με καθολικές υπηρεσίες καταλόγου για τη διακρίβωση της ορθότητας των διαπιστευτηρίων του χρήστη. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι προωθεί τη χρήση κεντρικού σημείου φύλαξης των διαπιστευτηρίων σύνδεσης. Έχοντας ένα κεντρικό σημείο φύλαξης, είναι δυνατόν όλες οι ενότητες λογισμικού που απαιτούν πιστοποίηση (λειτουργικό σύστημα, βάση δεδομένων κ.λπ.) να συνδιαλέγονται με το σημείο αυτό, ούτως ώστε κάθε χρήστης να χρησιμοποιεί ένα μόνο ζεύγος διαπιστευτηρίων για προσπέλαση σε όλους τους πόρους.

5.3 Έλεγχος προσπέλασης

Από τη στιγμή που το σύστημα βάσης δεδομένων έχει διακριβώσει την ταυτότητα του χρήστη, αποδίδει σ' αυτόν συγκεκριμένα προνόμια για την εργασία του μέσα στη βάση δεδομένων, όπως καθορίζονται από την πολιτική ασφάλειας. Τα προνόμια χωρίζονται σε δύο κύριες κατηγορίες:

1. Προνόμια επί του συστήματος. Τα προνόμια αυτά καθορίζουν τις γενικές δυνατότητες που έχει ο χρήστης σε σχέση με το σύστημα βάσεων δεδομένων. Τέτοια προνόμια μπορεί να καθορίζουν τη δυνατότητα δημιουργίας συνόδου (create session), τη δυνατότητα χρήσης πόρων (resource), τη δυνατότητα δημιουργίας πινάκων (create table), τη δυνατότητα δημιουργίας δεικτών (create index), τη δυνατότητα δημιουργίας διαδικασιών (create procedure) κ.λπ. Τα προνόμια επί του συστήματος μπορούν επίσης να αφορούν όρια χρήσης αποθηκευτικού χώρου, όρια χρόνου εκτέλεσης, όρια εισόδου-εξόδου κ.λπ.

2. Προνόμια επί συγκεκριμένων αντικειμένων. Τα προνόμια αυτά καθορίζουν τι δικαιώματα έχει ο χρήστης πάνω σε συγκεκριμένα αντικείμενα της βάσης – πίνακες, γραμμές ή στήλες πινάκων ή συγκεκριμένες τιμές. Για τα προνόμια αυτά υπάρχουν δύο βασικές στρατηγικές ορισμού των, ο κατ' επιλογήν έλεγχος προσπέλασης και ο υποχρεωτικός έλεγχος προσπέλασης.

Κατ' επιλογή έλεγχος προσπέλασης

Ο κατ' επιλογήν έλεγχος προσπέλασης είναι το σχήμα δικαιοδοσίας σύμφωνα με το οποίο:

1. δημιουργός ενός αντικειμένου είναι και ο ιδιοκτήτης του αντικειμένου.
2. ο ιδιοκτήτης ενός αντικειμένου έχει όλα τα δικαιώματα επί του αντικειμένου.

Μεταξύ των δικαιωμάτων που έχει ο ιδιοκτήτης του αντικειμένου είναι η παραχώρηση προνομίων σε άλλους χρήστες και η ανάκληση των παραχωρηθέντων δικαιωμάτων.

Τα συγκεκριμένα δικαιώματα που εφαρμόζονται σε ένα αντικείμενο εξαρτώνται από τη φύση του αντικειμένου. Έτσι:

- Για τους πίνακες, τα σχετικά προνόμια είναι η επιλογή, εισαγωγή, διαγραφή, ενημέρωση, τροποποίηση, δημιουργία δεικτών, δημιουργία αναφορών προς τον πίνακα.
- Για τις όψεις, τα σχετικά προνόμια είναι η επιλογή, εισαγωγή, διαγραφή, ενημέρωση, τροποποίηση.
- Για τις αποθηκευμένες διαδικασίες, το σχετικό προνόμιο είναι η εκτέλεσή τους.

- Για τους δείκτες, το σχετικό προνόμιο είναι η αλλαγή δομής αποθήκευσης.

Υποχρεωτικός έλεγχος προσπέλασης

Σε αντίθεση με τον κατ' επιλογήν έλεγχο προσπέλασης όπου κάθε χρήστης-ιδιοκτήτης πινάκων έχει το δικαίωμα να ορίσει ποιος χρήστης έχει ποιο δικαίωμα στα δεδομένα των πινάκων του, στον υποχρεωτικό έλεγχο προσπέλασης το σύστημα επιβάλλει να διενεργούνται έλεγχοι κατά την προσπέλαση των δεδομένων ανεξαρτήτως ιδιοκτησίας των δεδομένων. Στο σχήμα αυτό, κάθε δεδομένο έχει μία διαβάθμιση και κάθε χρήστης ένα επίπεδο εξουσιοδότησης. Οι κανόνες που ακολουθούνται στις προσπελάσεις δεδομένων είναι:

- Η ανάγνωση επιτρέπεται μόνο αν η εξουσιοδότηση του χρήστη είναι μεγαλύτερη ή ίση από τη διαβάθμιση του δεδομένου (no read-up).
- Η εγγραφή επιτρέπεται μόνο αν η εξουσιοδότηση του χρήστη είναι μικρότερη ή ίση από τη διαβάθμιση του δεδομένου (no write-down).

Ως παραδείγματα διαβάθμισης–εξουσιοδότησης μπορούμε να θεωρήσουμε τα (άκρως απόρρητο, απόρρητο, εμπιστευτικό, αδιαβάθμητο).

5.4 Ποια Δεδομένα Χαρακτηρίζονται Ευαίσθητα (Sensitive Data)

Μερικές βάσεις δεδομένων περιέχουν, όπως καλείται 'ευαίσθητα' δεδομένα, και είναι αυτά τα δεδομένα που δεν θα πρέπει να είναι ευρέως γνωστά. Η απόφαση για το ποια δεδομένα χαρακτηρίζονται ευαίσθητα εξαρτάται από την προσωπική βάση δεδομένων και από την υπονοούμενη έννοια των δεδομένων. Προφανώς κάποιες βάσεις δεδομένων δεν περιέχουν ευαίσθητα δεδομένα όπως ο κατάλογος μια δημόσιας βιβλιοθήκης, ενώ κάποιες άλλες είναι εξ' ολοκλήρου ευαίσθητες, όπως αυτές που περιέχουν στοιχεία άμυνας. Η δυσκολία έγκειται στην περίπτωση όπου κάποια, αλλά όχι όλα από τα στοιχεία της βάσης είναι ευαίσθητα. Υπάρχουν διαφορετικοί βαθμοί ευαισθησίας.

Οι παράγοντες που μπορεί να χαρακτηρίσουν τα δεδομένα ευαίσθητα είναι οι εξής:

i. Έμφυτη ευαισθησία (Inherently sensitive). Η τιμή από μόνη της μπορεί να είναι τόσο αποκαλυπτική που χαρακτηρίζεται ευαίσθητη. Παραδείγματα είναι οι

θέσεις των αμυντικών πυραύλων και το μέσο εισόδημα των κουρέων σε μια πόλη με ένα μόνο κουρέα.

ii. Από μια ευαίσθητη πηγή (From a sensitive source). Η πηγή των δεδομένων μπορεί να υποδηλώνει μια ανάγκη για εμπιστευτικότητα. Ως παράδειγμα είναι η πληροφορία από έναν πληροφοριοδότη του οποίου η ταυτότητα θα εκτεθεί αν αποκαλύπτονταν οι πληροφορίες.

iii. Διακηρυσσόμενη ευαισθησία (Declared sensitive). Ο διαχειριστής της βάσης δεδομένων ή ο ιδιοκτήτης των αντικειμένων μπορεί να έχουν δηλώσει τα δεδομένα να είναι ευαίσθητα. Παραδείγματα είναι τα προστατευμένα στρατιωτικά δεδομένα ή το όνομα ενός ανώνυμου δωρητή ενός έργου τέχνης.

iv. Από ένα ευαίσθητο χαρακτηριστικό γνώρισμα ή από μια ευαίσθητη εγγραφή (of a sensitive attribute or a sensitive record). Σε μια βάση δεδομένων, ένα συνολικό γνώρισμα ή μια εγγραφή μπορεί να χαρακτηριστούν ως ευαίσθητα. Σαν παραδείγματα αναφέρονται το χαρακτηριστικό της μισθοδοσίας σε μια προσωπική βάση ή μια εγγραφή που περιγράφει μια μυστική αποστολή στο διάστημα.

v. Ευαισθησία σε σχέση με προηγούμενη αποκάλυψη πληροφορίας (Sensitive in relation to previously disclosed information). Με έμμεσα συμπεράσματα μπορεί να αποκαλυφθούν ευαίσθητα δεδομένα.

5.5 Τι είναι ασφάλεια πολλαπλών επιπέδων

Ο όρος Ασφάλεια Πολλαπλών Επιπέδων (MultiLevel Security/MLS) αναφέρεται στην ικανότητα του συστήματος να επεξεργάζεται ταυτόχρονα δεδομένα με διαφορετική ευαισθησία χωρίς τον κίνδυνο της παραβίασης .

Ο Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control/ MAC), με τον οποίο ο διαχωρισμός των ευαίσθητων δεδομένων και η πρόσβαση σε αυτά επιβάλλεται πάντοτε αυτόματα, είναι το βασικό κλειδί των συστημάτων που υποστηρίζουν την ασφάλεια πολλαπλών επιπέδων.

Η ανάγκη για μια πολιτική ασφάλειας πολλαπλών επιπέδων προκύπτει όταν η βάση δεδομένων περιέχει πληροφορίες με διαφορετικούς βαθμούς εμπιστευτικότητας, π.χ. “εμπιστευτικό’, “πολύ εμπιστευτικό”, “απόρρητο”, και υπάρχουν χρήστες που δεν έχουν εξουσιοδότηση για τον υψηλό βαθμό εμπιστευτικότητας της βάσης. Η πολιτική αυτή ασφάλειας περιορίζει την προσπέλαση

στις εμπιστευτικές πληροφορίες της βάσης μόνο στους αντίστοιχα εξουσιοδοτημένους χρήστες και εξασφαλίζει ότι τα εμπιστευτικά δεδομένα προστατεύονται όχι μόνο από μη εξουσιοδοτημένη άμεση, αλλά και έμμεση προσπέλαση.

Η Ασφάλεια Πολλαπλών Επιπέδων (MLS) προσφέρει πολλά οφέλη στους παρακάτω τομείς:

i. Διαχείριση των χαρακτηριζομένων δεδομένων.
ii. Ελεγχόμενη ροή και διάδοση της πληροφορίας.
iii. Απομάκρυνση των πλεονασματικών και υπερπροστατευτικών συστημάτων.
iv. Περιορισμένη η επιβολή ασφάλειας από τις εφαρμογές.

Διαχείριση των χαρακτηριζομένων δεδομένων

Ένα MLS σύστημα παρέχει ένα σετ από καθαρούς και εκτελέσιμους κανόνες με τους οποίους ελέγχεται η πρόσβαση στα δεδομένα. Επειδή το σύστημα επιβάλει αυτούς τους κανόνες πέρα και πάνω από την διάκριση των χρηστών, δεν μπορούν να καταστρατηγηθούν.

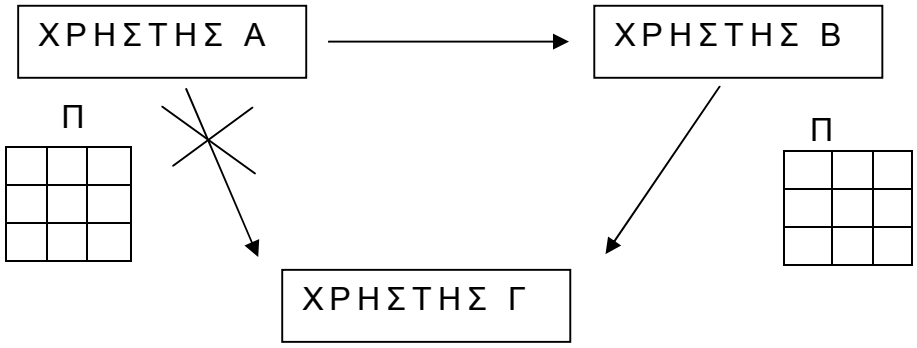
Για να επιβάλει αυτούς τους κανόνες το MLS σύστημα χαρακτηρίζει αυτόματα όλες τις πληροφορίες , κάτω από τον έλεγχό του, με την κατάλληλη ευαισθησία και μετά χρησιμοποιεί αυτές τις ετικέτες για να επιτύχει τον MAC. Ένας χρήστης μπορεί να κερδίσει πρόσβαση στις πληροφορίες εάν η ετικέτα ευαισθησίας του ταιριάζει με το κριτήριο που ορίζεται από το σύστημα, απαραίτητο κριτήριο για να πετύχει την πρόσβαση στην πληροφορία που τον ενδιαφέρει. Το σύστημα που υποστηρίζει την Ασφάλεια Πολλαπλών Επιπέδων εγγυάται ότι η πολιτική του συστήματος δεν μπορεί να καταστρατηγηθεί όσο τα δεδομένα βρίσκονται μέσα στο σύστημα.

Ελεγχόμενη ροή και διάδοση της πληροφορίας

Οι περισσότεροι server βάσεων δεδομένων παρέχουν την ικανότητα στους χρήστες να παραχωρήσουν το δικαίωμα πρόσβασης μέρους των δεδομένων της Β.Δ. που αυτοί ελέγχουν σε άλλους χρήστες που έχουν ανάγκη κάποιο κομμάτι της πληροφορίας για τη δική τους εργασία. Αυτό καλείται Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control/DAC) και ελέγχεται από τις εντολές της SQL GRANT(χορηγώ το δικαίωμα), REVOKE (αφαιρώ την άδεια).

Μπορεί ο DAC να είναι ένας σημαντικός μηχανισμός ασφάλειας και να ελέγχει την αρχική πρόσβαση στην πληροφορία, έχει όμως και κάποιους περιορισμούς στον έλεγχο της περαιτέρω διάδοσης της πληροφορίας .

Για παράδειγμα, έστω ότι ο χρήστης Α χορηγεί στο χρήστη Β τη δυνατότητα να χρησιμοποιεί τις πληροφορίες που βρίσκονται καταχωρημένες στο πίνακα Π1 (με το δικαίωμα SELECT). Ο Γ είναι ένας άλλος χρήστης του συστήματος που όμως δεν ανήκει στην ομάδα του χρήστη Α και συνεπώς δεν θα πρέπει να έχει πρόσβαση σε πληροφορίες του πίνακα Π1. Ο μηχανισμός DAC επιτρέπει στον χρήστη Β να βλέπει τα δεδομένα και εμποδίζει τον χρήστη Γ να τα δει (βλέπε εικόνα).



Εντούτοις, ο χρήστης Β μπορεί να καταπατήσει το δικαίωμα που του χορηγήθηκε και να επιτρέψει στον χρήστη Γ να προσπελάσει την πληροφορία. Αυτό μπορεί να γίνει αν ο Β αντιγράψει τις γραμμές του πίνακα Π1 σε κάποιο άλλο πίνακα Π2 και χορηγήσει το δικαίωμα πρόσβασης στις πληροφορίες του πίνακα στον Γ. Αυτή η δυνατότητα καταπάτησης της πολιτικής ασφάλειας του συστήματος είναι ένα έμφυτο εμπόδιο του μηχανισμού DAC.

Σε πολλά περιβάλλοντα ο DAC από μόνος του δεν είναι ένας επαρκής μηχανισμός να διαβεβαιώσει ότι οι ομαδικές “ευαίσθητες” πληροφορίες προστατεύονται από ακούσιες ή κακόβουλες αποκαλύψεις.

Αντιθέτως οι ετικέτες του μηχανισμού MAC είναι αναπόσπαστο κομμάτι των συστημάτων MLS και πάντα σχετίζονται με την πληροφορία σε ένα αντικείμενο(πίνακας, φόρμα, ερώτηση, αναφορά) και αυτό δεν μπορεί να αλλάξει κατά την κρίση του χρήστη. Όποτε ένα αντικείμενο αντιγράφεται σε ένα MLS σύστημα, οι ετικέτες του μηχανισμού MAC πάντα συνοδεύουν τα δεδομένα. Τα αντίγραφα έχουν τους ίδιους

χαρακτηρισμούς/ετικέτες όπως τα γνήσια δεδομένα και υπόκεινται στους ίδιους περιορισμούς ασφάλειας.

Στο προηγούμενο παράδειγμα, ο χρήστης Γ δεν θα μπορούσε να δει καθόλου τα δεδομένα όχι μόνο του πίνακα Π1, αλλά και του αντίγραφού του Π2.

Απομάκρυνση των πλεονασματικών και υπερπροστατευτικών συστημάτων

Σήμερα, πολλοί οργανισμοί χειρίζονται τις δικές τους συλλογικές "ευαίσθητες" πληροφορίες απομονώνοντας αυτές σε φυσικά ξεχωριστά συστήματα. Στην πραγματικότητα, ένα τυπικό μέρος μπορεί να έχει ένα σύστημα που χειρίζεται σημαντικές πληροφορίες και να υπάρχουν και κάποια άλλα για λιγότερο σημαντικά δεδομένα.

Ένας εμπορικός οργανισμός, για παράδειγμα, μπορεί να έχει ξεχωριστά συστήματα για την έρευνα, την ανάπτυξη και τα οικονομικά του και ξεχωριστό σύστημα για την επεξεργασία γενικών πληροφοριών. Επιπροσθέτως, αυτά τα συστήματα μπορεί να είναι τοποθετημένα σε ξεχωριστά δωμάτια, και για κάθε ένα από αυτά να υπάρχει και το δικό του προσωπικό διαχείρισης.

Σε αντίθεση με το διαχωρισμό των δεδομένων, κατανέμοντάς τα σε ξεχωριστές μηχανές, μερικές εγκαταστάσεις αποθηκεύουν όλες τις πληροφορίες που διαχειρίζονται σε ένα μόνο σύστημα, χαρακτηρίζοντας το ως "υψηλής εμπιστοσύνης" σύστημα. Αυτό σημαίνει ότι οι χρήστες του συστήματος έχουν την απόλυτη εμπιστοσύνη και μπορούν να προσπελάσουν και την πιο απόρρητη πληροφορία.

Έχει αποδειχθεί ότι ο φυσικός διαχωρισμός των δεδομένων, για να επιτευχθεί η ασφάλεια, είναι ακριβός από πλευράς κόστους, τα αποτελέσματα δεν είναι στην ώρα τους, τα δεδομένα που αποθηκεύονται είναι υπεράριθμα και οι πληροφορίες δεν είναι διαθέσιμες όταν τις χρειάζεται ο χρήστης.

Περιορισμένη η επιβολή ασφάλειας από τις εφαρμογές

Πολλοί οργανισμοί διευθετούν την ασφάλεια των δεδομένων με το να γράφουν επιπλέον λογισμικό για να επιβάλουν τις δικές τους πολιτικές ασφάλειας στην αρχή και στο τέλος των εφαρμογών.

Μπορεί κάποιος επιπρόσθετος κώδικας σε επίπεδο εφαρμογής να είναι χρήσιμος ή ακόμα και απαραίτητος για συγκεκριμένα ζητήματα μιας εφαρμογής, αυτή όμως η προσέγγιση έχει πολλά μειονεκτήματα.

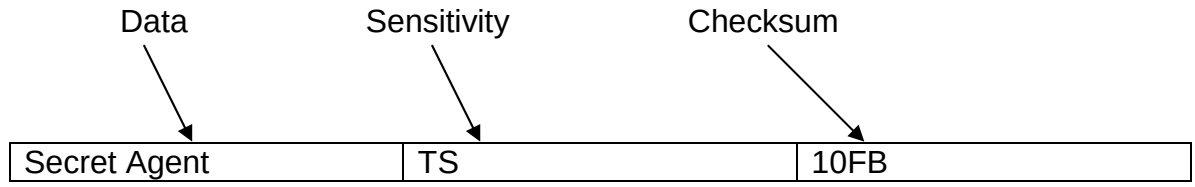
Ένα μειονέκτημα είναι ότι αυτό το είδος του λογισμικού είναι συχνά πολύπλοκο, δύσκολο να γραφεί και ακριβό στο να διατηρήσει πολλές εφαρμογές με συνέπεια. Επιπλέον οι χρήστες μπορούν να προσπελάσουν ή να καταπατήσουν τον κώδικα αρχής-τέλους της εφαρμογής μέσω άλλων εργαλείων του συστήματος.

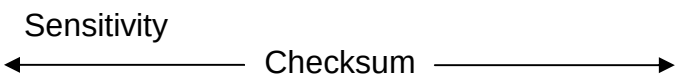
5.6 Προτάσεις για την ασφάλεια πολλαπλών επιπέδων

Η εφαρμογή της ασφάλειας πολλαπλών επιπέδων στις βάσεις δεδομένων είναι πολύ δύσκολη, πιθανόν περισσότερο από ότι σε ένα λειτουργικό σύστημα, εξαιτίας των μικρών στοιχείων που πρέπει να ελεγχθούν. Στην παράγραφο αυτή μελετούνται κάποιες προσεγγίσεις για την ασφάλεια πολλαπλών επιπέδων στις βάσεις δεδομένων.

5.6.1 Μηχανισμός ‘κλειδώματος’ της ακεραιότητας (integrity lock)

Το κλείδωμα είναι ένας τρόπος για να πετύχει κανείς και την ακεραιότητα και την περιορισμένη πρόσβαση σε μια βάση δεδομένων. Αυτή η λειτουργία ονομάζεται διάσπαρτος χαρακτηρισμός, γιατί κάθε στοιχείο χαρακτηρίζεται από την ευαισθησία του. Ο χαρακτηρισμός φυλάσσεται μαζί με τα δεδομένα και όχι σε κάποιο ξεχωριστό πίνακα της βάσης.





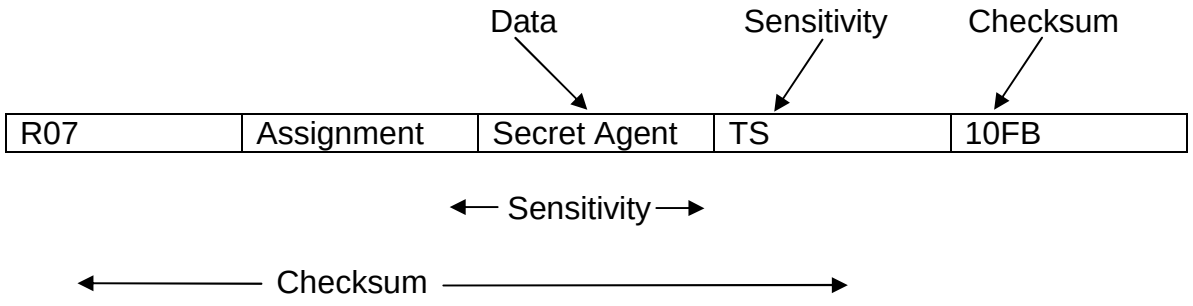
Ένα μοντέλο που παριστάνει τον βασικό μηχανισμό “κλειδώματος” της ακεραιότητας φαίνεται στο παραπάνω σχήμα. Όπως φαίνεται και από το σχήμα κάθε στοιχείο δεδομένου αποτελείται από τρία κομμάτια: τα δεδομένα καθ’ εαυτά (data), την ετικέτα ευαισθησίας (sensitivity) και ένα άθροισμα ελέγχου (checksum). Η ετικέτα ευαισθησίας ορίζει την ευαισθησία του δεδομένου και το άθροισμα ελέγχου υπολογίζεται και από τα δεδομένα και από την ετικέτα ευαισθησίας, για να εμποδίσει μη εξουσιοδοτημένη τροποποίηση των δεδομένων ή της ετικέτας του.

Τα δεδομένα αποθηκεύονται σε μορφή καθαρού κειμένου για καλύτερη απόδοση, γιατί το Σ.Δ.Β.Δ. χρειάζεται να εξετάσει πολλά πεδία όταν επιλέγει τις εγγραφές που ικανοποιούν την ερώτηση. Η ετικέτα ευαισθησίας πρέπει να έχει τα ακόλουθα χαρακτηριστικά:

- Μη πλαστογραφήσιμη, έτσι ώστε ένα κακόβουλο πρόσωπο να μην μπορεί να δημιουργήσει ένα νέο επίπεδο ευαισθησίας για ένα στοιχείο.
- Μοναδική, έτσι ώστε κανένας να μη μπορεί να αντιγράψει ένα επίπεδο ευαισθησίας από άλλο στοιχείο.
- Απόκρυφη, έτσι ώστε κανένας να μην μπορεί καν να αποφασίσει για το επίπεδο ευαισθησίας ενός αυθαίρετου στοιχείο.

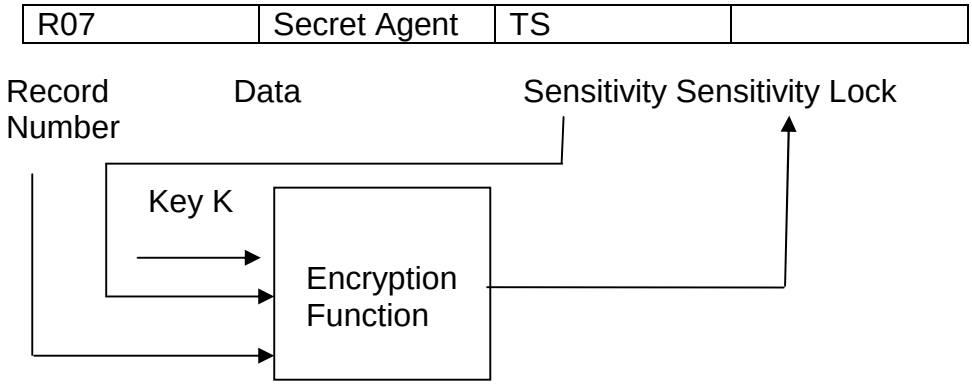
Το τρίτο κομμάτι του μηχανισμού “κλειδώματος” της ακεραιότητας είναι ένας κώδικας ανίχνευσης λαθών για ένα πεδίο. Με σκοπό να εγγυηθεί ότι η τιμή των δεδομένων και το επίπεδο της ευαισθησίας τους δεν έχει αλλάξει, αυτός ο έλεγχος αθροίσματος πρέπει να είναι μοναδικός για το συγκεκριμένο στοιχείο και πρέπει να περιέχει και τα δεδομένα του πεδίου και κάτι που να μπορεί να συνδέσει αυτά τα δεδομένα με μια συγκεκριμένη θέση μέσα στη βάση δεδομένων.

Όπως φαίνεται στο παρακάτω σχήμα, ένας κατάλληλος κρυπτογραφικός έλεγχος αθροίσματος περιλαμβάνει κάτι μοναδικό στην εγγραφή, όπως είναι ο αριθμός εγγραφής, κάτι μοναδικό για τη στήλη μέσα στην εγγραφή, όπως είναι το χαρακτηριστικό όνομα της στήλης, τα δεδομένα του πεδίου και το επίπεδο ευαισθησίας του πεδίου. Αυτά τα τέσσερα κομμάτια προστατεύουν ενάντια στην αλλαγή, στην αντιγραφή ή στην μετατροπή των δεδομένων. Ο έλεγχος αθροίσματος μπορεί να υπολογιστεί χρησιμοποιώντας έναν ισχυρό αλγόριθμο κρυπτογράφησης, όπως είναι ο DES.



5.6.2 Μηχανισμός ‘κλειδώματος’ της ευαισθησίας (Sensitivity lock)

Ο μηχανισμός “κλειδώματος” ευαισθησίας περιγράφεται στο παρακάτω σχήμα και σχεδιάστηκε από τους Graubert και Krammer. Ο μηχανισμός “κλειδώματος” ευαισθησίας είναι ένας συνδυασμός από έναν μοναδικό προσδιοριστή , όπως είναι ο αριθμός εγγραφής, και του επιπέδου ευαισθησίας. Επειδή ο προσδιοριστής είναι μοναδικός κάθε “κλείδωμα” ακεραιότητας σχετίζεται με μια συγκεκριμένη εγγραφή. Πολλά διαφορετικά στοιχεία θα ανήκουν στο ίδιο επίπεδο ευαισθησίας. Κάποιος που θέλει να πειράξει κακόβουλα την βάση δεδομένων δεν θα πρέπει να μπορεί να ταυτοποιήσει δυο στοιχεία γνωρίζοντας τα επίπεδα ευαισθησίας ή τις τιμές των δεδομένων απλά κοιτάζοντας στο κομμάτι που αντιστοιχεί στο επίπεδο ευαισθησίας. Λόγω της κρυπτογράφησης τα στοιχεία του “κλειδώματος” και ειδικότερα το επίπεδο ευαισθησίας είναι απόκρυφα από μια σαφή εικόνα. Έτσι ο μηχανισμός συνδέεται με μια συγκεκριμένη εγγραφή και προστατεύει την μυστικότητα του επιπέδου ευαισθησίας από αυτή την εγγραφή.



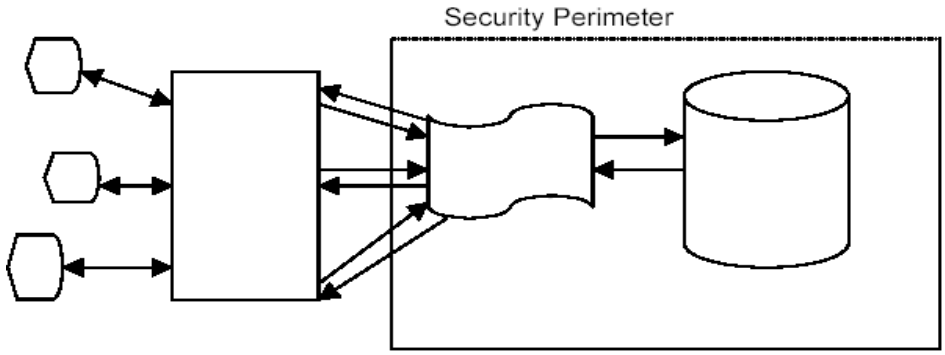
5.6.3 Μηχανισμός ‘κλειδώματος’ της ακεραιότητας του Σ.Δ.Β.Δ.(Integrity lock DBMS)

Ο μηχανισμός “κλειδώματος” της ακεραιότητας επινοήθηκε σαν μια βραχυπρόθεσμη λύση στα προβλήματα ασφάλειας που αντιμετωπίζουν οι πολλαπλών επιπέδων ευαισθησίας βάσεις δεδομένων. Ο σκοπός ήταν να μπορεί να χρησιμοποιηθεί οποιοδήποτε μη έμπιστο Σ.Δ.Β.Δ. με μια έμπιστη διαδικασία που χειρίζεται τον έλεγχο πρόσβασης. Αυτή η προσέγγιση ονομάστηκε διάσπαρτος χαρακτηρισμός, γιατί τα ευαίσθητα δεδομένα εξαφανίστηκαν ως δια μαγείας με την κρυπτογράφηση που προστατεύει και τα δεδομένα και την ευαισθησία τους. Με αυτό τον τρόπο μόνο η διαδικασία πρόσβασης θα χρειάζεται να είναι έμπιστη, γιατί μόνο

αυτή θα μπορεί να πετύχει ή να παραχωρήσει το δικαίωμα πρόσβασης στα ευαίσθητα δεδομένα. Η δομή του μηχανισμού περιγράφεται στο σχήμα.

Η απόδοση του μηχανισμού “κλειδώματος “ της ακεραιότητας έχει ένα μειονέκτημα. Ο χώρος για να αποθηκευτεί ένα πεδίο πρέπει να είναι μεγάλο για να καλύψει και την ετικέτα ευαισθησίας. Λόγω του ότι υπάρχουν αρκετά μερίδια σε αυτή την ετικέτα και του ότι υπάρχει μία ετικέτα σε κάθε πεδίο, ο χώρος που απαιτείται δεν είναι καθόλου ασήμαντος.

Ο χρόνος επεξεργασίας αυτού του μηχανισμού είναι άλλο ένα μειονέκτημα. Η ετικέτα ευαισθησίας πρέπει να αποκωδικοποιείται κάθε φορά που τα δεδομένα φτάνουν στον χρήστη, έτσι ώστε να εξακριβωθεί ότι η πρόσβαση του χρήστη είναι επιτρεπτή. Επίσης κάθε φορά που μια τιμή εισάγεται ή τροποποιείται, η ετικέτα πρέπει να ξαναυπολογιστεί. Έτσι, σημαντικός χρόνος καταναλώνεται κατά την επεξεργασία. Εάν το αρχείο της βάσης δεδομένων μπορεί να προστατευτεί επαρκώς, τότε οι τιμές των δεδομένων για ξεχωριστά πεδία μπορεί να βρίσκονται με μορφή καθαρού κειμένου.

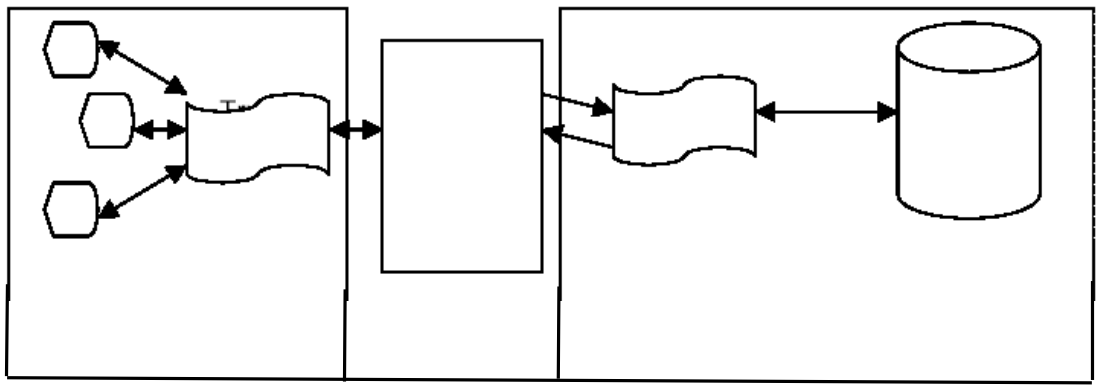


5.6.4 Μηχανισμός Trust Font-End

Το μοντέλο της διαδικασίας του μηχανισμού “έμπιστη βιτρίνα τέλους” (Trusted front-end) είναι γνωστό σαν φύλακας και περιγράφεται στο παρακάτω σχήμα. Το κίνητρο για αυτή την προσέγγιση είναι το γεγονός ότι πολλά Σ.Δ.Β.Δ. έχουν δημιουργηθεί και τεθεί σε λειτουργία χωρίς να εξετάσουν τη ανάγκη ασφάλειας πολλαπλών επιπέδων. Η γενική ιδέα του μηχανισμού αυτού αυξάνει την ασφάλεια ενός τέτοιου συστήματος με μικρές αλλαγές στο σύστημα. Η επικοινωνία μεταξύ του

χρήστη, τον μηχανισμό “έμπιστη βιτρίνα τέλους” και ένα Σ.Δ.Β.Δ. περιλαμβάνει τα εξής βήματα:

- Ο χρήστης δίνει την ταυτότητά του στον μηχανισμό και αναγνωρίζεται σαν εξουσιοδοτημένος ή μη χρήστης.
- Ο χρήστης θέτει την ερώτηση (αίτημα).
- Ο μηχανισμός εξακριβώνει το δικαίωμα πρόσβασης του χρήστη στα δεδομένα.
- Ο μηχανισμός μεταφέρει το αίτημα στο διαχειριστή της βάσης δεδομένων.
- Ο διαχειριστής της βάσης δεδομένων εκτελεί το δικαίωμα I/O πρόσβασης, επικοινωνώντας με χαμηλού επιπέδου ελέγχους πρόσβασης για να επιτευχθεί η πρόσβαση στα πραγματικά δεδομένα.
- Ο διαχειριστής της βάσης δεδομένων επιστρέφει τα αποτελέσματα της ερώτησης στο μηχανισμό.
- Ο μηχανισμός εξακριβώνει την ορθότητα των δεδομένων μέσα από ελέγχους προστασίας των δεδομένων έναντι του επιπέδου ασφάλειας του χρήστη.
- Η “έμπιστη βιτρίνα τέλους” μεταφέρει τα δεδομένα στην μη έμπιστη πρόσοψη για μορφοποίηση.
- Τα μορφοποιημένα δεδομένα μεταφέρονται στον χρήστη.



5.6.5 Μηχανισμός Commutative Filters

Η έννοια του εναλλακτικού φίλτρου (Commutative filter) προτάθηκε από τον Denninig, ως μια απλούστευση του έμπιστου μέσου επικοινωνίας στον διαχειριστή της βάσης δεδομένων. Βασικά το φίλτρο εξετάζει την αίτηση του χρήστη, την ανασχηματίζει αν αυτό είναι απαραίτητο, έτσι ώστε μόνο δεδομένα του κατάλληλου επιπέδου ασφάλειας να επιστρέφονται στον χρήστη.

Το εναλλακτικό φίλτρο είναι μια διαδικασία που αντικατοπτρίζεται και στον χρήστη και στον διαχειριστή της βάσης δεδομένων. Το φίλτρο προσπαθεί να επωφεληθεί από την απόδοση των περισσότερων Σ.Δ.Β.Δ. Το φίλτρο ανασχηματίζει την ερώτηση, έτσι ώστε ο διαχειριστής βάσης δεδομένων να κάνει τόση δουλεία όση είναι δυνατόν, προστατεύοντας πολλές μη προσπελάσιμες εγγραφές. Μετά το φίλτρο παρέχει μια δεύτερη εξέταση για να συλλέξει μόνο τα δεδομένα για τα οποία ο χρήστης έχει πρόσβαση. Τα φίλτρα μπορεί να χρησιμοποιηθούν για την ασφάλεια σε επίπεδο εγγραφής, στήλης, και πεδίου.

- Όταν χρησιμοποιείται σε επίπεδο εγγραφής, το φίλτρο απαιτεί τα επιθυμητά δεδομένα μαζί με τις πληροφορίες του κρυπτογραφικού αθροίσματος ελέγχου και τότε εξακριβώνει την ακρίβεια και το δικαίωμα πρόσβασης στα δεδομένα, έτσι ώστε αυτά να περάσουν στην κατοχή του χρήστη.
- Στο επίπεδο στήλης, το φίλτρο ελέγχει εάν όλες οι στήλες που σχετίζονται με την ερώτηση του χρήστη είναι προσιτές στον χρήστη, και εάν είναι έτσι παραχωρεί την ερώτηση στον διαχειριστή της βάσης δεδομένων. Στην επιστροφή της απάντησης το φίλτρο διαγράφει όλα τα πεδία στα οποία ο χρήστης δεν έχει κανένα δικαίωμα πρόσβασης.
- Στο επίπεδο πεδίου, το σύστημα απαιτεί τα επιθυμητά δεδομένα μαζί με τις πληροφορίες του κρυπτογραφικού αθροίσματος ελέγχου. Όταν αυτό επιστραφεί το φίλτρο ελέγχει το επίπεδο προστασίας για κάθε πεδίο κάθε εγγραφής που ανακτήθηκε έναντι του επιπέδου ασφάλειας του χρήστη .

Τα φίλτρα λειτουργούν περιορίζοντας πρώτα την ερώτηση στον διαχειριστή της βάσης δεδομένων και μετά περιορίζοντας τα αποτελέσματα της ερώτησης πριν αυτά επιστραφούν στον χρήστη.

5.7 Πολιτική Ασφάλειας (Security Policy)

Οι τεχνικές ασφάλειας της βάσης δεδομένων προσπαθούν να αντιμετωπίσουν τα προβλήματα που προκαλούνται από τον άνθρωπο, ενώ οι τεχνικές επανόρθωσης

της βάσης δεδομένων και του ελέγχου κοινής πρόσβασης στα δεδομένα προσπαθούν να λύσουν τα προβλήματα που προκαλούνται από το λογισμικό και το υλικό. Ο καθορισμός μιας αποδοτικής πολιτικής ασφάλειας είναι πολύ σημαντική σε κάθε περιβάλλον που ενδιαφέρεται για τη διαρροή των δεδομένων από μη εξουσιοδοτημένα πρόσωπα.

Η πολιτική ασφάλειας είναι ένα σετ από νόμους, κανόνες και πρακτικές που καθορίζουν πως ένας οργανισμός διαχειρίζεται, προστατεύει και κατανέμει τις πληροφορίες και ειδικότερα αυτές που χαρακτηρίζονται ως “ευαίσθητες”.

Τα περισσότερα συστήματα διαχείρισης βάσεων δεδομένων προσφέρουν πολύ μικρή προστασία ασφάλειας με το σκεπτικό ότι αυτή παρέχεται από το υπάρχον λειτουργικό σύστημα.

Η πολιτική ασφάλειας ενός περιβάλλοντος πρέπει να λαμβάνει υπόψιν τα παρακάτω:

- Εάν η ασφάλεια θα ελέγχεται κεντρικά από ένα διαχειριστή δεδομένων ή από διαφορετικούς διαχειριστές.
- Τις διαδικασίες για τον τρόπο αλλαγής των ελέγχων ασφάλειας και την προσθήκη νέων χρηστών και πόρων δεδομένων στο σύστημα.
- Τις μικρότερες απαιτήσεις για τις δυνατότητες προστασίας ενός συστήματος διαχείρισης βάσεων δεδομένων που θα χρησιμοποιηθεί σε ένα οργανισμό.
- Τις διαδικασίες για την επιβολή ελέγχου ασφάλειας.
- Ποιος είναι υπεύθυνος για κάθε τύπο δεδομένων στο σύστημα.
- Ποια είδη πρόσβασης θα διακρίνονται με την παροχή ελέγχου ασφάλειας.

Κάποιες επιπλέον ερωτήσεις θα πρέπει να ληφθούν σοβαρά υπόψιν με σκοπό τον καθορισμό των απαιτήσεων για την πολιτική ασφάλειας. Μερικές από αυτές είναι:

- Πόσο ‘ευαίσθητα’ είναι τα δεδομένα ;
- Πόσο δύσκολο θα είναι για κάποιον κακόβουλο χρήστη να παραβιάσει την προστασία ασφάλειας ;
- Τι επίπεδο ελέγχου ασφάλειας απαιτείται ;
- Υπάρχουν κάποιες αποδεκτές απαιτήσεις για την ασφάλεια ;

Κάθε οργανισμός έχει τις δικές του απαιτήσεις και προτεραιότητες και ανάλογα με αυτές ορίζει και διαφορετική πολιτική ασφάλειας και φυσικά δίνει διαφορετική βαρύτητα στα χαρακτηριστικά γνωρίσματα ασφάλειας.

Για παράδειγμα, τα στρατιωτικά περιβάλλοντα που απαιτούν αυστηρή προστασία στην “ευαίσθητη” πληροφορία υπολογίζουν το χαρακτηριστικό της Εμπιστευτικότητας πολύ παραπάνω από αυτό της Ακεραιότητας ή της Διαθεσιμότητας, ενώ σε ένα οικονομικό σύστημα ή συνέχεια στη χορήγηση της υπηρεσίας, δηλαδή η Διαθεσιμότητα, είναι το βασικό στοιχείο. Από την άλλη στις βιομηχανίες φαρμάκων και η Εμπιστευτικότητα και η Ακεραιότητα είναι ζωτικά χαρακτηριστικά γνωρίσματα στη δοκιμή κλινικών δεδομένων.

5.8 Αναγνώριση και αυθεντικοποιήση των χρηστών

Πριν επιτραπεί στο χρήστη η πρόσβαση στη βάση δεδομένων πρέπει να καθοριστεί η ταυτότητά του (identity) με ένα αξιόπιστο τρόπο και μετά να ελεγχθεί αν ο συγκεκριμένος είναι εξουσιοδοτημένος χρήστης για την βάση δεδομένων. Υπάρχουν δυο επιλογές μηχανισμών για την αναγνώριση και αυθεντικοποιήση των χρηστών που είναι οι εξής:

- Από το μηχανισμό αυθεντικοποίησης του server της βάσης δεδομένων.
- Από το σύστημα ασφάλειας του λειτουργικού συστήματος.

Αυθεντικοποίηση μέσω της βάσης δεδομένων

Κάθε χρήστης έχει ένα όνομα (username) και ένα συνθηματικό (password). Αυτό το συνθηματικό αποθηκεύεται μέσα στην βάση δεδομένων χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης DES (Data Encryption Standard). Για να συνδεθεί με τη βάση δεδομένων ένας εξουσιοδοτημένος χρήστης του λειτουργικού συστήματος πρέπει να την τροφοδοτήσει με το δικό του username και password της βάσης.

Στα κατανεμημένα συστήματα, ένα συνθηματικό που περνάει από το ένα μηχάνημα στο άλλο μπορεί να θέσει την ασφάλεια σε κίνδυνο. Εάν το συνθηματικό περνάει σε καθαρό κείμενο, δηλαδή δεν έχει κρυπτογραφηθεί, οποιοσδήποτε που παραφυλάει να κρυφακούσει τα δεδομένα μπορεί να διαβάσει και το συνθηματικό και έτσι να γίνει εξουσιοδοτημένος χρήστης.

Για το λόγο αυτό κάποια συστήματα χρησιμοποιούν ένα κλειδί για να κρυπτογραφήσουν το συνθηματικό του χρήστη πριν αυτό διέλθει στο server. Κάθε προσπάθεια σύνδεσης χρησιμοποιεί ένα ξεχωριστό κλειδί για την κρυπτογράφηση, κάνοντας την κρυπτογράφηση πιο δύσκολα να αποκρυπτογραφηθεί. Αφού το κρυπτογραφημένο με το κλειδί συνθηματικό περάσει στον server, τότε αυτός το αποκρυπτογραφεί και το επανακρυπτογραφεί χρησιμοποιώντας τον αλγόριθμο DES και συγκρίνει αυτό με το συνθηματικό που είναι ήδη καταχωρημένο στη βάση. Εάν αυτά ταιριάζουν τότε ο χρήστης συνδέεται επιτυχώς με τη βάση.

Αυθεντικοποίηση μέσω του Λειτουργικού Συστήματος

Κάθε χρήστης έχει ένα όνομα (username) για τη βάση δεδομένων, αλλά δεν έχει συνθηματικό. Για να συνδεθεί στη βάση δεδομένων ένας κατάλληλα εξουσιοδοτημένος χρήστης του λειτουργικού συστήματος δεν είναι απαραίτητο να διευκρινίσει το username και password της βάσης. Αντί για αυτό, όταν ο χρήστης προσπαθεί να συνδεθεί στην βάση, το εξουσιοδοτημένο username του λειτουργικού συστήματος μεταβιβάζεται από το ασφαλές λειτουργικό σύστημα στο σύστημα της βάσης δεδομένων. Το σύστημα της βάσης επαληθεύει ότι το username που δόθηκε είναι εξουσιοδοτημένο να συνδεθεί στην βάση.

Ένα από τα πλεονεκτήματα της χρήσης της αυθεντικοποίησης μέσω του Λ.Σ. αντί αυτής μέσω της βάσης δεδομένων είναι ότι το username που έχει ο χρήστης είναι το ίδιο και στο λειτουργικό σύστημα και στη βάση δεδομένων. Αυτό απομακρύνει την ανάγκη να διατηρούνται ξεχωριστά οι πληροφορίες αναγνώρισης και αυθεντικοποίησης του χρήστη και στο Λ.Σ. και στον server της βάσης και είναι πιο εύκολο στον χρήστη να λογοδοτεί για τις ενέργειες του μέσα στο σύστημα.

5.9 Κρυπτογράφηση της Βάσης Δεδομένων

Η κρυπτογράφηση της βάσης μπορεί να διευθετήσει απειλές κατά της Εμπιστευτικότητας και της Ακεραιότητας τόσο στα δεδομένα που χειρίζονται on- line όσο και σε αυτά που αποθηκεύονται off-line. Η κρυπτογράφηση μπορεί να υλοποιηθεί είτε σε ολόκληρη τη βάση ή σε μέρος αυτής.

Ένας οργανισμός οδηγείται στην κρυπτογράφηση ολόκληρης της βάσης για να περιορίσει την αναγνωσιμότητα των αρχείων της βάσης στο λειτουργικό σύστημα. Δηλαδή, να είναι δυσανάγνωστα τα αρχεία αυτά σε άτομα που έχουν τα νόμιμα

δικαιώματα να προσπελάσουν τα αρχεία της βάσης, αλλά δεν έχουν κανένα προνόμιο πάνω στη βάση, όπως π.χ. είναι ο διαχειριστής του συστήματος.

Η κρυπτογράφηση σε ολόκληρη την βάση είναι προβληματική. Σε ένα λειτουργικό περιβάλλον η κρυπτογράφηση δεν πρέπει να εμποδίζει άλλους ελέγχους πρόσβασης και το κυριότερο να μην εμποδίζει τους χρήστες από το να δουν κάποιο αντικείμενο που έτσι και αλλιώς είναι εξουσιοδοτημένοι να προσπελάσουν, σε διαφορετική περίπτωση η δυνατότητα να εκτελέσουν τις εργασίες τους παραβιάζεται. Επίσης η διαδικασία αυτή προσθέτει ένα πονοκέφαλο στην αποκρυπτογράφηση των δεδομένων πριν οι χρήστες τα διαβάσουν.

Για παράδειγμα, αν τα δεδομένα στους πίνακες της βάσης είναι κρυπτογραφημένα για να παρέχουν επιπρόσθετη ασφάλεια, τότε και οι δείκτες που έχουν πρόσβαση σε αυτούς τους πίνακες πρέπει να κρυπτογραφηθούν, μιας και μπορεί να έχουν ευαίσθητα δεδομένα και έτσι προκαλείται μεγάλη καθυστέρηση στην εκτέλεση της εφαρμογής. Ένας χρήστης που ρωτάει κάτι από τον πίνακα Π πρέπει να περιμένει να αποκρυπτογραφηθούν οι δείκτες, τα δεδομένα στον πίνακα και μετά να ικανοποιηθεί η ερώτηση. Τα αποτελέσματα από άλλες λειτουργίες, όπως είναι οι UPDATE και INSERT, και που επηρεάζουν τα δεδομένα πρέπει επίσης να κρυπτογραφηθούν. Άλλο ένα μειονέκτημα, είναι η απαίτηση της περιοδικής αλλαγής του κλειδιού που χρησιμοποιείται στην κρυπτογράφηση. Αλλαγή του κλειδιού σημαίνει πως πρέπει να αποκρυπτογραφηθεί ολόκληρη η βάση και να ξανακρυπτογραφηθεί με το νέο κλειδί. Αυτή η διαδικασία είναι χρονοβόρα και πρέπει να γίνει όταν δεν υπάρχει καμία πρόσβαση στα δεδομένα.

Μερικοί οργανισμοί αποθηκεύουν τα backups μιας χρονικής περιόδου, συνήθως από έξι μήνες ως ένα χρόνο, σε έναν απομακρυσμένο χώρο. Επιπρόσθετα μπορεί αυτά να κρυπτογραφηθούν πριν την αποθήκευσή τους. Άλλοι πάλι οργανισμοί επιθυμούν να κρυπτογραφήσουν μόνο τα ευαίσθητα δεδομένα, που δεν θα πρέπει να τα δουν ούτε οι διαχειριστές της βάσης δεδομένων.

6. Πιστοποίηση (Authentication)

6.1 Τι είναι πιστοποίηση

Πιστοποίηση (ή επαλήθευση ταυτότητας) ονομάζουμε τη διαδικασία της επιβεβαίωσης και του καθορισμού κάποιου ατόμου ή αντικειμένου σαν αυθεντικού , δηλαδή ότι αυτό που ισχυρίζεται είναι αλήθεια. Στην εποχή μας, όπου ένας προσωπικός υπολογιστής μπορεί να έχει πρόσβαση στο δίκτυο, ή όταν ο υπολογιστής περιέχει ευαίσθητες ή προσωπικές πληροφορίες που ίσως μοιράζονται από μια ομάδα προσώπων, τότε είναι απαραίτητη η χρήση αναγνώρισης ταυτότητας των χρηστών για να αποκτήσουν το δικαίωμα των υπηρεσιών του υπολογιστή.Η απόλυτη πιστοποίηση δεν αποτελεί προαπαίτηση των περισσοτέρων πληροφοριακών συστημάτων. Ένας υπολογιστής σε κάποιο τοπικό δίκτυο δεν χρειάζεται να ξέρει το πραγματικό ονοματεπώνυμο κάποιου χρήστη.

6.2 Βασικές μορφές πιστοποίησης

Η πιστοποίηση είναι η βασικότερη υπηρεσία ασφάλειας που μπορεί να προσφέρει ένα δίκτυο υπολογιστών καθώς αυτή παρέχει προστασία έναντι μη εξουσιοδοτημένων δοσοληψιών εξασφαλίζοντας τη γνησιότητα ενός μηνύματος, τη νομιμότητα ενός χρήστη ή αποστολέα και την εγκυρότητα ενός τερματικού ή υπολογιστή.

Η πιστοποίηση μπορεί να γίνει με τους εξής τρόπους:

Δημιουργία κωδικού πρόσβασης

Οι κωδικοί είναι η απλούστερη μορφή πιστοποίησης: αποτελούν ένα μυστικό που μοιράζεται ο χρήστης με τον υπολογιστή. Όταν ο χρήστης θέλει να αποκτήσει πρόσβαση στο σύστημα, πληκτρολογεί τον κωδικό του για να αποδείξει στον υπολογιστή ότι είναι αυτός που διατείνεται ότι είναι. Ο υπολογιστής με την σειρά του ελέγχει αν ο κωδικός που πληκτρολογήθηκε είναι ίδιος με τον κωδικό του λογαριασμού του χρήστη. Αν όντως είναι ταυτόσημος, τότε επιτρέπεται η πρόσβαση στον χρήστη.

Η αρχική δημιουργία του κωδικού γίνεται συνήθως από τον χρήστη που θα τον χρησιμοποιήσει αλλά αυτό δεν ισχύει πάντοτε. Σε μερικά υπολογιστικά συστήματα ο κωδικός πρόσβασης του χρήστη δημιουργείται από τον υπολογιστή για λογαριασμό του χρήστη, σε μια προσπάθεια να αποφευχθούν κοινά ανθρώπινα λάθη κατά την επιλογή του κωδικού. Σε αυτήν την περίπτωση ο υπολογιστής είναι εξοπλισμένος με ένα ειδικό πρόγραμμα που κατασκευάζει τυχαίους ή σχεδόν τυχαίους κωδικούς οι οποίοι ωστόσο συμμορφώνονται με κάποιους ειδικούς περιορισμούς τέτοιους έτσι ώστε οι παραγόμενοι κωδικοί πρόσβασης να είναι δύσκολοι στο να παραβιαστούν. Οι κωδικοί θα πρέπει να είναι εύκολοι στην θύμηση τους, αλλά δύσκολοι στο να ανακαλυφθούν (από άνθρωπο ή από υπολογιστή) και να μαντευτούν.

Πλεονεκτήματα

- Το κύριο πλεονέκτημα των κωδικών είναι ότι δεν χρειάζεται κάποιος ειδικός εξοπλισμός για την χρήση τους.
- Είναι ένας απλός στη χρήση.
- Είναι φθηνός και εύκολος τρόπος πιστοποίησης της ταυτότητας του χρήστη.

Μειονεκτήματα

Οι άνθρωποι διαλέγουν απλούς κωδικούς για έναν απλό λόγο: Πρέπει να τους θυμούνται. Η χρήση κάποιου ασυνήθιστου συνδυασμού χαρακτήρων αυξάνει την πιθανότητα ο χρήστης να ξεχάσει τον κωδικό του την στιγμή που το ζητάει ο υπολογιστής. Και αν το γράψει σε ένα κομμάτι χαρτί ή σε κάποιο μήνυμα ηλεκτρονικού ταχυδρομείου τότε αυτόματα μειώνεται η ασφάλεια.

Χρήση μαγνητικής κάρτας

Οι μαγνητικές κάρτες και οι “έξυπνες” κάρτες ή smart cards έχουν συνήθως το μέγεθος πιστωτικής κάρτας αλλά το μέγεθος τους ποικίλοι. Διαθέτουν μνήμη μερικών χιλιάδων χαρακτήρων η οποία μπορεί να έχει πρόσβαση μόνο από ειδικό υλικό.

Πλεονεκτήματα

- Οι χρήστες δεν χρειάζεται να θυμούνται τους κωδικούς τους, απλά διαβάζουν τον κωδικό κάθε φορά από την κάρτα. Αυτό αφαιρεί την ανάγκη αλλαγής του

κωδικού από τον χρήστη σε τακτά χρονικά διαστήματα, γιατί γίνεται αυτόματα από την κάρτα.

- Είναι πολύ λιγότερο πιθανό ο χρήστης να δώσει τον κωδικό του σε κάποιον άλλο, επειδή η κάρτα είναι μια φυσική συσκευή που είναι απαραίτητη για κάθε διαδικασία αυθεντικοποίησης.
- Αν ο χρήστης δώσει τον κωδικό του σε κάποιον άλλο, ή αν ο κωδικός μαθευτεί με κάποιον άλλο τρόπο, οι συνέπειες ελαχιστοποιούνται γιατί ο κωδικός έχει περιορισμένη διάρκεια ζωής.

Οι μαγνητικές και οι έξυπνες κάρτες είναι κάτι που ο χρήστης έχει, ωστόσο η ασφάλεια που παρέχουν μπορεί να αυξηθεί και με την χρήση κάποιου κωδικού που ο χρήστης γνωρίζει, δηλαδή μια κάρτα μπορεί να απαιτεί από τον χρήστη της να εισαγάγει έναν προσωπικό αριθμό αναγνώρισης (Personal Identification Number – PIN) πρίν λειτουργήσει, παρέχοντας έτσι κάποιο βαθμό προστασίας σε περίπτωση που η ίδια η κάρτα χαθεί ή κλαπεί.(π.χ. αυτόματες ταμειολογιστικές μηχανές, ATMs - Automated Teller Machines).

Μειονεκτήματα

- Απαιτείται ειδική συσκευή ανάγνωσης της κάρτας.
- Αυξημένο κόστος.
- Κίνδυνος απώλειας κάρτας.

Βιομετρική

Άλλη μια μορφή πιστοποίησης είναι η Βιομετρική. Είναι η στατιστική ανάλυση των βιολογικών χαρακτηριστικών του ανθρώπου, τα τελευταία χρόνια ο όρος τείνει να ταυτιστεί με την επιστήμη που χρησιμοποιεί ψηφιακή τεχνολογία για να αναγνωρίσει την ταυτότητα ατόμων, βάση κάποιων ιδιαίτερων και μοναδικών φυσικών ή βιολογικών χαρακτηριστικών τους.

6.3 Η σημασία των κωδικών πρόσβασης (password)

Στις μέρες μας το διαδίκτυο κυριαρχεί στην καθημερινότητα των ανθρώπων. Έτσι, η ανάγκη για προστασία είναι επιτακτική. Ο κίνδυνος για παραβίαση

προσωπικών δεδομένων και αρχείων είναι τεράστιος. Εισβολείς μπορούν να εισέλθουν μέσου δικτύου στον υπολογιστή και να προκαλέσουν χάος. Αυτό θα ήταν καταστροφικό, κυρίως αν πρόκειται για επιχειρήσεις, μεγάλους οργανισμούς, κυβερνήσεις ,στρατό, ερευνητικά ιδρύματα κλπ. με οτιδήποτε αυτό συνεπάγεται. Γι' αυτό είναι αναγκαίο να λαμβάνονται μέτρα ασφάλειας.

Οι κωδικοί είναι ιδιαίτερα χρήσιμοι σε κοινόχρηστους υπολογιστές όπως οι υπολογιστές ενός ακαδημαϊκού ιδρύματος ή κάποιου οργανισμού. Όμως σε τέτοιες περιπτώσεις, η παραβίασης της ασφάλειας ενός και μόνο λογαριασμού χρήστη μπορεί να διακινδυνεύσει την ασφάλεια ολόκληρης της εγκατάστασης.

Αρκετές από τις αποτελεσματικότερες τεχνικές διείσδυσης σε υπολογιστικά συστήματα ελάχιστη σχέση έχουν με τεχνικές λεπτομέρειες. Αντίθετα βασίζονται στην ανθρώπινη εμπιστοσύνη και άγνοια. Είναι γεγονός ότι πολύ λίγες περιπτώσεις εισβολής σε κάποιο σύστημα αποτελούν ένδειξη ανώτερης ευφυΐας και ταλέντου. Στην πλειοψηφία των περιπτώσεων οι εισβολείς (crackers) στηρίζονται στις παρακάτω κακές συνήθειες των χρηστών:

- Η προθυμία τους να μοιράζονται τους κωδικούς πρόσβασης τους.
- Να μιμούνται τους συναδέλφους τους στην επιλογή κωδικών.
- Να χρησιμοποιούν συνεχώς τους ίδιους εύκολους κωδικούς σε διαφορετικά συστήματα (συνήθως κωδικούς συναφείς με το πρόσωπο τους ή τον επαγγελματικό τους χώρο όπως όνομα, ημερομηνία γέννησης, αριθμό ταυτότητας).
- Να χρησιμοποιούν λίστες κωδικών.
- Να περιγράφουν απλόχερα τα μέτρα ασφάλειας που παίρνουν.
- Να εμπιστεύονται ανθρώπους που ελάχιστα γνωρίζουν.

6.3.1 Κριτήρια δημιουργίας κωδικού

Για την αύξηση της ασφάλειας που παρέχουν οι κωδικοί, οι σχεδιαστές των σύγχρονων πληροφοριακών συστημάτων έχουν ενσωματώσει στα συστήματα τους κάποιους περιορισμούς στην επιλογή κωδικών από τους χρήστες. Έτσι σύμφωνα με αυτούς τους περιορισμούς οι κωδικοί πρέπει να έχουν όσο το δυνατόν περισσότερα από τα εξής χαρακτηριστικά:

- Πρέπει να αλλάζουν από τον χρήστη υποχρεωτικά, ανά τακτά χρονικά διαστήματα.
- Ο νέος κωδικός πρέπει να έχει ένα ελάχιστο πλήθος διαφορετικών χαρακτήρων από τον κωδικό που αντικαθιστά.
- Πρέπει να έχουν ένα ελάχιστο, συνήθως 5 χαρακτήρες καθώς και μέγιστο μήκος.
- Το ιδανικό στις περισσότερες περιπτώσεις είναι 7 ή 8 χαρακτήρες. Μερικά συστήματα υποστηρίζουν μέχρι και 256 χαρακτήρες, δηλαδή ολόκληρες φράσεις (passphrases).
- Πρέπει να περιέχουν τουλάχιστον έναν αριθμό.
- Πρέπει να περιέχουν τουλάχιστον ένα μη-αλφαβητικό σύμβολο.
- Πρέπει να περιέχουν συνδυασμό κεφαλαίων και μικρών χαρακτήρων.
- Παλιοί κωδικοί δεν πρέπει να χρησιμοποιούνται ξανά.
- Δεν πρέπει να είναι συνδυασμοί χαρακτήρων από το πληκτρολόγιο π.χ. asdfgh.
- Κλείδωμα του λογαριασμού μετά από συγκεκριμένο πλήθος εισαγωγών λανθασμένου κωδικού.

6.3.2 Τι πρέπει να έχουν υπ' όψιν οι χρήστες για την δημιουργία ενός καλού κωδικού

- Πρέπει να είναι εύκολοι στην απομνημόνευση τους, έτσι ώστε να μην χρειάζεται να σημειώνονται.
- Δεν πρέπει να είναι κοινές λέξεις που μπορούν να βρεθούν εύκολα σε ένα οποιοδήποτε λεξικό.
- Δεν πρέπει να είναι ονόματα προσώπων, τοποθεσιών, τηλεφωνικά νούμερα, ημερομηνίες γεννήσεως και ονόματα που έχουν σχέση με την επαγγελματική απασχόληση του χρήστη.
- Δεν πρέπει να είναι το όνομα κάποιου πράγματος που είναι σημαντικό για τον χρήστη, όπως αγαπημένο φαγητό, ταινία, όνομα ηθοποιού, μέρος, χόμπι, όνομα καλλιτέχνη κλπ.
- Πρέπει να μπορούν να πληκτρολογούνται γρήγορα έτσι ώστε κανείς να μην μπορεί να τους αναγνωρίσει βλέποντας τα πλήκτρα που πατιούνται.

- Δεν πρέπει να χρησιμοποιούνται οι ίδιοι κωδικοί σε διαφορετικά συστήματα.
- Εισαγωγή μιας λέξης μέσα σε μια άλλη.
- Διαστρωμάτωση δύο ή περισσοτέρων λέξεων: για παράδειγμα, το “cdaotg”, διαστρωματώνει τις λέξεις “dog” και “cat”. Με λίγη προσπάθεια, κάποιοι άνθρωποι μπορούν να το κάνουν αυτό εύκολα στο μυαλό τους· άλλοι δεν μπορούν. Αν ο χρήστης καθυστερεί μεταξύ γραμμάτων καθώς πληκτρολογεί τέτοιου είδους κωδικούς, δεν θα πρέπει να τους χρησιμοποιεί.

Για παράδειγμα, στο λειτουργικό σύστημα Microsoft Windows 2000, η πολιτική για τους κωδικούς μπορεί να ρυθμιστεί με τις ακόλουθες επιλογές:

- Ελάχιστο επιτρεπόμενο μέγεθος κωδικών.
- Αν οι κωδικοί μπορούν να είναι απλοί (π.χ. password) ή σύνθετοι (π.χ. paSS4321).
- Αν το ιστορικό κωδικών (μια λίστα με παλιούς κωδικούς) θα διατηρείται ή όχι, και το πλήθος των κωδικών που θα διατηρούνται.
- Ελάχιστη ηλικία κωδικού (χρονικό διάστημα μέχρι ο κωδικός να πρέπει να αλλαχθεί).
- Μέγιστη ηλικία κωδικού (χρονικό διάστημα μέχρι ο κωδικός να λήξει εκτός και αν έχει αλλάξει).
- Αν οι κωδικοί αποθηκεύονται εσωτερικά χρησιμοποιώντας αντιστρέψιμη ή μη αντιστρέψιμη κρυπτογράφηση.

6.3.3 Κωδικοί πρόσβασης και οι διαχειριστές του συστήματος

Στόχοι εισβολέα

- Να καταστρέψει τις αποδείξεις της επιτυχημένης εισβολής,
- Να αποκτήσει κωδικούς πρόσβασης για άλλους λογαριασμούς του συστήματος,
- Να αποκτήσει πρόσβαση σε διαχειριστικούς λογαριασμούς οι οποίοι θα του δώσουν πλήρη έλεγχο του συστήματος,
- Να ανοίξει νέες “τρύπες” ασφάλειας ή πίσω-πόρτες στο παραβιασμένο σύστημα, σε περίπτωση που το αρχικό σημείο εισβολής ανακαλυφθεί και διορθωθεί,

- Να βρει άλλα συστήματα που επικοινωνούν με το πληροφοριακό σύστημα που παραβίασε.

Οι δύο τελευταίοι στόχοι είναι οι πιο σημαντικοί αφού θα επιτρέψουν στον εισβολέα να εξαπλωθεί σε πλήθος συστημάτων από μια μεμονωμένη αδυναμία ασφάλειας.

Οι διαχειριστές συστήματος οφείλουν σε τακτά χρονικά διαστήματα να επιχειρούν να “σπάσουν” οι ίδιοι τους κωδικούς των χρηστών τους. Η διαδικασία μπορεί να υλοποιηθεί πολύ εύκολα με την χρήση κάποιου από τα ειδικά προγράμματα που κυκλοφορούν για αυτόν ακριβώς τον σκοπό. Αυτά τα προγράμματα ονομάζονται “password crackers” ή ανιχνευτές κωδικών, και είναι (δυστυχώς;) παρόμοια με τα προγράμματα που χρησιμοποιούν οι επίδοξοι εισβολείς συστημάτων. Αν ο διαχειριστής συστήματος ανακαλύψει στο σύστημα του κάποιο κωδικό ασφάλειας που πιστεύει ότι δεν αξίζει να ονομάζεται έτσι τότε θα πρέπει να τον απενεργοποιήσει άμεσα διότι ένας εισβολέας θα μπορούσε να τον βρει επίσης. Αν ο ανιχνευτής κωδικών δεν μπορέσει να ανακαλύψει κάποιο κωδικό αυτό σε καμία περίπτωση δεν πρέπει να σημαίνει για τον διαχειριστή ότι το σύστημα του είναι ασφαλές όσο αφορά τους κωδικούς πρόσβασης.

6.3.4 Πότε πρέπει να αλλάζουν οι κωδικοί

- Οποτεδήποτε κάποιος εκτός από τον ιδιοκτήτη του, τον μαθαίνει, ο κωδικός πρέπει να αλλάζει όσο το δυνατόν γρηγορότερα.
- Όταν ένας διαχειριστής συστήματος αφήνει την θέση του, όλοι οι διαχειριστικοί κωδικοί που γνώριζε πρέπει να αλλαχθούν. Το αν οι χρήστες θα αναγκαστούν να αλλάξουν τους κωδικούς τους επαφίεται στην διακριτικότητα των διαχειριστών, αλλά δεν πρέπει να παραβλέπεται το γεγονός ότι ο πρώην διαχειριστής είχε πρόσβαση στην βάση δεδομένων των λογαριασμών των χρηστών. Έτσι, όταν ένας διαχειριστής παραιτείται ή απολύεται, κάθε κωδικός στο σύστημα πρέπει να αλλαχθεί, αφού ο πρώην διαχειριστής είχε πρόσβαση στο αρχείο με τους κρυπτογραφημένους κωδικούς και μπορεί ενδεχομένως να τους “σπάσει”.
- Αν υπάρχει οποιαδήποτε υποψία ότι τα αρχεία της βάσης δεδομένων των λογαριασμών των χρηστών έχουν αντιγραφεί από κάποιον χωρίς κατάλληλη

εξουσιοδότηση.

- Είναι συνετό για τους διαχειριστές να μην χρησιμοποιούν τους διαχειριστικούς λογαριασμούς τους για να εκτελέσουν απλές εργασίες όπως π.χ. η περιήγηση στο διαδίκτυο. Μια τέτοια δουλειά μπορεί να γίνει κάλλιστα με την χρήση ενός βοηθητικού λογαριασμού με περιορισμένα προνόμια.
- Οι περισσότερες υπολογιστικές πλατφόρμες όπως το Microsoft Windows και το UNIX περιλαμβάνουν έναν τυπικό βοηθητικό λογαριασμό, το guest account. Αυτός ο λογαριασμός χρησιμοποιείται για να παρέχει σε ανώνυμους χρήστες πρόσβαση στο σύστημα. Γενικά τα guest accounts θα πρέπει να απενεργοποιούνται από τους διαχειριστές μια και συχνά μπορεί να προσφέρουν πρόσβαση στους πόρους του συστήματος ακόμη και σε χρήστες των οποίων η ταυτότητα δεν έχει πιστοποιηθεί. Τα guest accounts θα πρέπει να διαθέτουν ισχυρούς κωδικούς ασφάλειας, και στα συστήματα UNIX θα πρέπει να έχουν περιορισμένο κέλυφος (restricted shell).

6.3.5 Αυτόματο κλείδωμα λογαριασμού

Ένα άλλο μέτρο ασφάλειας στα υπολογίστηκα συστήματα είναι το αυτόματο κλείδωμα λογαριασμού. Αν κάποιος προσπαθήσει να εισβάλει στον λογαριασμό ενός χρήστη και δώσει λάθος κωδικό αρκετές συνεχόμενες φορές, τότε ο λογαριασμός του χρήστη κλειδώνεται. Ένας κλειδωμένος λογαριασμός μπορεί να ξεκλειδωθεί μόνο από τον διαχειριστή του συστήματος.

Το αυτόματο κλείδωμα λογαριασμού βοηθάει στο:

- Να προστατεύει το σύστημα από κάποιον που επιμένει να μαντέψει έναν κωδικό, πριν προλάβει να μαντέψει τον σωστό κωδικό, ο λογαριασμός απενεργοποιείται.
- Ειδοποιεί τον νόμιμο χρήστη ότι κάποιος προσπαθούσε να παραβιάσει τον λογαριασμό του.

6.3.6 Ψάρεμα κωδικών πρόσβασης (Password Sniffing)

Υπάρχουν προγράμματα ευρέως διαθέσιμα στο διαδίκτυο τα οποία ελέγχουν όλη την δικτυακή κίνηση, ψάχνοντας για πληροφορίες από ανθρώπους που έχουν

πληκτρολογήσει τα ονόματα χρήστη (usernames) και τους κωδικούς τους. Αυτά τα προγράμματα λέγονται “password sniffers” γιατί “μυρίζονται” ονόματα και κωδικούς πρόσβασης από το δίκτυο. Τα ζευγάρια ονόματος χρήστη/κωδικού έπειτα αποθηκεύονται για μελλοντική χρήση ή στέλνονται μέσω του διαδικτύου στον υπολογιστή του εισβολέα (ή κάποιο άλλο υπολογιστικό σύστημα το οποίο βρίσκεται υπό τον έλεγχο του εισβολέα). Επειδή οι κωδικοί είναι επαναχρησιμοποιήσιμοι, ο εισβολέας μπορεί να τους χρησιμοποιήσει κάποια στιγμή στο μέλλον για να εισβάλει στον λογαριασμό του χρήστη. Μόλις ο εισβολέας καταφέρει να εγκαταστήσει ένα πρόγραμμα password sniffer, αυτό μπορεί να καταγράψει γρήγορα τα ονόματα χρηστών και τους κωδικούς δεκάδων ή και εκατοντάδων χρηστών στο συγκεκριμένο υπολογιστικό σύστημα. Ο εισβολέας μπορεί επίσης να αποκτήσει και τους κωδικούς χρηστών που συνδέονται στο συγκεκριμένο σύστημα από άλλα εξωτερικά συστήματα. Μόλις τα ονόματα χρηστών και οι κωδικοί για κάποιο άλλο σύστημα ανακαλυφθούν, ο εισβολέας μπορεί να μεταβεί σε αυτό και να συνεχίσει την δουλειά του.

6.3.7 Σπάσιμο κωδικών (Password cracking)

Όπως αναφέρθηκε και παραπάνω, οι κωδικοί πρόσβασης είναι ένας από τους σημαντικότερους και ποιο διαδεδομένους τρόπους για την επίτευξη της ασφάλειας στα πληροφοριακά συστήματα και δίκτυα. Αυτό έχει σαν αποτέλεσμα οι εισβολής να προσπαθούν να τους μαντέψουν και να τους ‘’σπάσουν’’. Το σπάσιμο των κωδικών μπορεί να προσεγγιστεί με δύο τρόπους σύμφωνα με τον Mitch Tulloch, στο βιβλίο του “Microsoft Encyclopedia of Security”:

- **Online cracking:** Αυτή η προσέγγιση γενικά περιλαμβάνει την παγίδευση (“sniffing”) της δικτυακής κίνησης και την προσπάθεια εξαγωγής κωδικών από την παγιδευμένη πληροφορία. Αυτή η διαδικασία είναι γενικά αργή και δύσκολη στην υλοποίηση της, αλλά στο διαδίκτυο κυκλοφορούν εργαλεία ειδικά σχεδιασμένα για τον εντοπισμό κωδικών από την δικτυακή πληροφορία.
- **Offline cracking:** Αυτή είναι η συχνότερη μέθοδος και περιλαμβάνει την εισβολή σε κάποιο σύστημα μέσω κάποιας αδυναμίας του για να αποκτηθεί πρόσβαση στο αρχείο κωδικών (password file) ή στην βάση δεδομένων με τους κωδικούς, και μετά την εκτέλεση ενός κατάλληλου εργαλείου (password

cracker) που θα προσπαθήσει να μαντέψει έγκυρους κωδικούς για τους λογαριασμούς των χρηστών. Το offline cracking μπορεί να γίνει επί τόπου, στο σύστημα στο οποίο έχει εισβάλει ο επιτιθέμενος ή το αρχείο με τους κωδικούς μπορεί να αντιγραφεί έξω απο το παραβιασμένο σύστημα έτσι ώστε ο εισβολέας α προσπαθήσει να σπάσει τους κωδικούς με την ησυχία του. Υπάρχουν ακόμη και σκουλήκια όπως το DoubleTap και li0n που μπορούν αυτόματα να υποκλέψουν το αρχείο με τους κωδικούς από παραβιασμένα συστήματα.

6.3.8 Βασικές αρχές σπάσιμου κωδικών πρόσβασης

Επίθεση ωμής βίας (Brute-force attack): Ο απλούστερος αλλά λιγότερο αποτελεσματικός και πιο αργός τρόπος εύρεσης,"σπάσιμου" κωδικών πρόσβασης είναι η επίθεση ωμής δύναμης (brute-force attack), η οποία δοκιμάζει συστηματικά όλους τους πιθανούς συνδυασμούς γραμμάτων, ψηφίων και ειδικών χαρακτήρων κάθε δυνατού μήκους μέχρι να βρεθεί κάποιος κωδικός ή μέχρι να κολλήσει το πρόγραμμα ή να τα παρατήσει ο εισβολέας. Ένας τυπικός προσωπικός υπολογιστής μπορεί να να ελέγξει περίπου 5 κλειδιά ανά δευτερόλεπτο. Μια συσκευή ειδικά σχεδιασμένη να σπάει κρυπτογραφικούς κλειδιά μπορεί να είναι ικανή να ελέγξει 200 κλειδιά το δευτερόλεπτο. Φυσικά, γρηγορότερα αποτελέσματα μπορούν να επιτευχθούν με τον συνδυασμό πολλαπλών συστημάτων. Το πλήθος των δυνατών συνδυασμών του κλειδιού εξαρτάται άμεσα από το μέγεθος του κλειδιού. Όσο μεγαλύτερο είναι το μήκος του κλειδιού, τόσο περισσότεροι συνδυασμοί κλειδιών μπορούν να γίνουν.

Επίθεση λεξικού (Dictionary attack): Η επίθεση λεξικού (dictionary attack), αποτελεί μια βελτιστοποίηση της επίθεσης ωμής δύναμης. Χρησιμοποιεί ένα λεξικό (μια λίστα λέξεων που χρησιμοποιούνται συχνά σαν κωδικοί) κοινών κωδικών το οποίο έχει δημιουργηθεί από τις συνδυασμένες εμπειρίες των εισβολέων όσο αφορά τους περισσότερο κοινούς κωδικούς.

Υβριδική επίθεση (Hybrid attack): Ο συνδυασμός επίθεσης λεξικού και επίθεσης ωμής δύναμης λέγεται υβριδική επίθεση (hybrid attack). Οι χρήστες που προσθέτουν απλές δοκιμασμένες τεχνικές επιλογής κωδικών ασφάλειας όπως το να

προσθέτουν αριθμούς στο τέλος του κωδικού τους μπορούν συχνά να παρακάμψουν τον κίνδυνο μιας επίθεσης λεξικού. Η καλύτερη προσέγγιση λοιπόν για την εύρεση κωδικών είναι γενικά η υβριδική επίθεση που χρησιμοποιεί επίθεση λεξικού αλλά εφαρμόζοντας παράλληλα και κάποιους κανόνες. Τυπικά, ένα πρόγραμμα που υλοποιεί αυτήν την επίθεση, μπορεί να εναλλάσσει συστηματικά τους πεζούς με τους κεφαλαίους χαρακτήρες όπως επίσης και να δημιουργεί μικρά κομμάτια χαρακτήρων και τα προσθέτει στην αρχή και στο τέλος των λέξεων από το λεξικό. Για παράδειγμα, ο κωδικός ασφαλείας “marina123” πιθανότατα θα εντοπιζόταν πολύ γρήγορα από μια υβριδική επίθεση, η οποία θα δοκίμαζε την λέξη “marina” προσθέτοντας διάφορους χαρακτήρες πριν και μετά από αυτήν.

6.4 Κωδικοφράσεις (Passphrases)

Οι κωδικοφράσεις σπάνια χρησιμοποιούνται για έλεγχο πρόσβασης. Όμως μερικές εφαρμογές όπως τα εργαλεία κρυπτογράφησης χρησιμοποιούν κωδικοφράσεις (passphrases) αντί για κωδικούς. Οι κωδικοφράσεις έχουν μέγεθος συνήθως 50 με 100 χαρακτήρες για να διασφαλίσουν ότι τα κλειδιά που θα δημιουργηθούν θα είναι αρκετά δυνατά για να αντέξουν επιθέσεις ωμής δύναμης. Οι κωδικοφράσεις για την κρυπτογράφηση μηνυμάτων θα πρέπει να είναι εύκολες στην θύμηση τους από τον χρήστη αλλά δύσκολες στο να μαντευθούν από άλλους, ακριβώς ότι ισχύει και για τους κωδικούς. Οι ασφαλέστερες κωδικοφράσεις είναι φυσικά οι τυχαίες σειρές χαρακτήρων, αλλά τα ανθρώπινα όντα γενικά δεν είναι πολύ καλά στο να θυμούνται σειρές με 50 ή 100 χαρακτήρες.

6.5 Εξασφάλιση γνησιότητας οντοτήτων

Γνησιότητα σημαίνει ασφαλής αμφότερη πιστοποίηση της ταυτότητας των επικοινωνούντων οντοτήτων. Στα κεντρόμορφα συστήματα η λειτουργία αυτή γίνεται με την χρήση διαδικασιών ταυτοποίησης και συνθηματικών. Επέκταση της μεθόδου αυτής στα κατανεμημένα συστήματα δεν είναι αποδοτική. Για παράδειγμα, όταν ο πομπός θέλει να ταυτοποιηθεί στον αποδέκτη ή το αντίστροφο, αποστέλλει την ταυτότητα και το συνθηματικό του, ο αποδέκτης όμως πιθανά να είναι 'εισβολέας'. Στα κατανεμημένα συστήματα θα πρέπει να υπάρχουν κατάλληλες αμφίδρομες μυστικές - ασφαλείς διεργασίες ταυτοποίησης και εξακρίβωσης της γνησιότητας. Η

μυστικότητα θα πρέπει να εξασφαλίζεται απαραίτητα με την χρήση μεθόδων κρυπτογράφησης. Υπάρχουν αρκετά επίπεδα και τύποι μηχανισμών εξασφάλισης της γνησιότητας. Σε μερικά περιβάλλοντα είναι αρκετή η εξασφάλιση γνησιότητας των μηνυμάτων που ανταλλάσσονται, ενώ σε άλλα υπάρχει επιπρόσθετη ανάγκη μηχανισμών μυστικότητας. Η χρήση των μεθόδων αυτών εξαρτάται από τους πιθανούς κινδύνους, την ευαισθησία των πληροφοριών και το υπολογιστικό κόστος.

Οι μέθοδοι αυτοί είναι οι ακόλουθοι:

Η απλή μέθοδος, που βασίζεται στην ταυτοποίηση με συνθηματικά των συμμετεχόντων οντοτήτων και στην χρήση κόμβου αναφοράς, ο οποίος ελέγχει, συγκεντρωτικά, την ακρίβεια των συνθηματικών.

Η ισχυρή μέθοδος, που βασίζεται στην χρήση κρυπτογραφικών μεθόδων, στην οποία διακρίνουμε τους επόμενους μηχανισμούς :

- Εξασφάλιση γνησιότητας των συμμετεχόντων οντοτήτων με χρήση συμμετρικών και ασύμμετρων κρυπτογραφικών μεθόδων. Η μέθοδος αυτή συνδυάζει την απλή μέθοδο με την χρήση των κρυπτογραφικών συστημάτων.
- Μέθοδοι εξασφάλισης γνησιότητας, που χρησιμοποιούν αποκλειστικούς-εξειδικευμένους εξυπηρετητές-κέντρα γνησιότητας (authentication servers). Ένας εξυπηρετητής γνησιότητας αναλαμβάνει τη διαχείριση των μυστικών κλειδιών των χρηστών. Η βάση δεδομένων, που χρησιμοποιείται για το σκοπό αυτό, είναι ταξινομημένη ως προς τα ονόματα των χρηστών. Η διαχείριση των χρηστών, συνεπώς, ανάγεται στην οικουμενική ονοματολογία του συστήματος (global naming), που είναι απαραίτητη προϋπόθεση για τη λειτουργία ενός ή περισσοτέρων (συνεργαζόμενων μεταξύ τους) εξυπηρετητών γνησιότητας, στη δομή ενός εκτεταμένου κατανεμημένου συστήματος.
- Μέθοδοι εξασφάλισης γνησιότητας με χρήση πρωτοκόλλων ελάχιστης-μηδενικής διαρροής πληροφοριών σχετικά με τα χρησιμοποιούμενα από τους χρήστες κλειδιά (minimum-zero knowledge protocols). Με την ανταλλαγή κλειδιού οι δύο ή περισσότερες οντότητες, που επικοινωνούν, αποκτούν ένα κοινό κλειδί (συνήθως βασισμένο σε τυχαίους αριθμούς) γνωστό μόνο σε αυτές και το οποίο μπορεί να χρησιμοποιηθεί μόνο για ένα συγκεκριμένο χρονικό διάστημα.

Πολλά από τα πρωτόκολλα, τα οποία έχουν προταθεί χαρακτηρίζονται από σοβαρά προβλήματα ασφάλειας, μικρή αποδοτικότητα σχετικά με την υπολογιστική και επικοινωνιακή πολυπλοκότητά τους, καθώς και από πλεονασμούς αναφορικά με το πλήθος και το είδος των πεδίων που απαιτούνται στα μηνύματα επικοινωνίας. Σε μερικές περιπτώσεις (στρατιωτικές, τραπεζικές, ιατρικές εφαρμογές) είναι επιθυμητό ο συγγραφέας ενός κειμένου να 'υπογράψει' σε αυτό, μεταφορικά με τις χειρόγραφες μεθόδους. Η εξακρίβωση της γνησιότητας της ψηφιακής υπογραφής (digital signature), μπορεί να γίνει από τον αποδέκτη του μηνύματος (με βάση προηγούμενη αναφορά) ή με παραπομπή της εξακρίβωσης της γνησιότητας σε τρίτο κόμβο (εγγυητή γνησιότητας). Πρέπει να σημειωθεί ότι οι υπογραφές αυτές μπορούν να χρησιμοποιηθούν επίσης σαν κλειδιά γνησιότητας, για την εξακρίβωση της ταυτότητας του αποστολέα στον αποδέκτη. Βελτιστοποίηση της αποδοτικότητας των μεθόδων αυτών μπορεί να επιτευχθεί με την χρήση έξυπνων καρτών, στις οποίες είναι ήδη ψηφιοποιημένη η ταυτότητα - υπογραφή του χρήστη, καθώς και με την χρήση Τρίτων Εμπίστων Πλευρών (Trusted Third Parties).

6.6 Υπηρεσία εξακρίβωσης γνησιότητας Kerberos

Η υπηρεσία εξακρίβωσης γνησιότητας Kerberos βασίζεται στο πρόγραμμα ATHENA του M.I.T. το οποίο προσφέρει ένα κατανεμημένο περιβάλλον λειτουργίας συστημάτων η/υ. Οι απαιτήσεις ασφάλειας του συστήματος αυτού μετά τη διαδικασία της ταυτοποίησης καλύπτονται από την υπηρεσία εξακρίβωσης γνησιότητας, που ονομάζεται Kerberos. Η υπηρεσία αυτή διασφαλίζει στις οντότητες του συστήματος, την ταυτότητα των αντίστοιχων οντοτήτων, με τις οποίες επικοινωνούν, καθώς και την ασφάλεια των εκπεμπόμενων μηνυμάτων. Βασίζεται στο μοντέλο που προτάθηκε από τους Needham και Schroeder. Χρονικές σφραγίδες (timestamps), οι οποίες αποτελούνται από συμβολοσειρές, που περιέχουν την ημερομηνία και την ώρα χρησιμοποιούνται για την αποτροπή επανάληψης, ήδη σταλμένων μηνυμάτων. Το σύστημα διατηρεί βάση δεδομένων, που περιέχει τους χρήστες και τα προσωπικά τους κλειδιά-συνθηματικά, τα οποία γνωρίζουν μόνον οι ίδιοι. Η βάση αυτή βρίσκεται στον κεντρικό εξυπηρετητή γνησιότητας και αντίγραφα αυτής (τα οποία ενημερώνονται τακτικά) βρίσκονται σε περιφερειακούς εξυπηρετητές. Με τη βάση αυτή σαν κόμβο αναφοράς υπάρχει δυνατότητα εξακρίβωσης της γνησιότητας του χρήστη προς το σύστημα, ή μεταξύ δύο χρηστών που εγκαθιστούν μία σύνοδο.

Επιπλέον ο εκδίδονται 'ιδιωτικά κλειδιά συνόδου' (private session keys), που χρησιμοποιούνται για την κρυπτογράφηση των μηνυμάτων που ανταλλάσσονται. Το σύστημα προσφέρει τρία επίπεδα ασφάλειας.

- Το πρώτο επίπεδο βασίζεται σε αρχική μόνο εξακρίβωση της γνησιότητας. Συγκεκριμένα οι οντότητες που δημιουργούν μία σύνοδο εξακριβώνουν την ταυτότητα αλλήλων μόνο στη διαδικασία της εγκαινίασης της συνόδου. Κατόπιν, δε λαμβάνεται κανένα επιπλέον μέτρο ασφάλειας.
- Το δεύτερο επιπρόσθετο επίπεδο ασφάλειας προβλέπει την εξακρίβωση της γνησιότητας των ανταλλασσόμενων μηνυμάτων, χωρίς όμως να λαμβάνονται μέτρα για την αποτροπή διαρροής του περιεχομένου των μηνυμάτων αυτών.
- Στο τρίτο υψηλότερο επίπεδο με την χρήση ιδιωτικών κλειδιών κρυπτογραφούνται τα μηνύματα που ανταλλάσσονται.

Υπάρχουν δύο τύποι διαπιστευτικών (credentials), που χρησιμοποιούνται στο σύστημα Kerberos, τα 'εισιτήρια' (tickets) και οι 'αυθεντικοποιητές' (authenticators). Και τα δύο βασίζονται στην χρήση διαφορετικών κρυπτογραφημένων μηνυμάτων 'ιδιωτικού κλειδιού'. Το 'εισιτήριο' χρησιμοποιείται για την ταυτοποίηση του χρήστη στον εξυπηρετητή, του οποίου ζητείται η υπηρεσία, μέσω του εξυπηρετητή γνησιότητας. Επίσης διαβεβαιώνει, ότι ο χρήστης, που το χρησιμοποιεί, ταυτίζεται με τον χρήστη για τον οποίο εκδόθηκε. Ο 'αυθεντικοποιητής' παρέχει τις απαραίτητες πληροφορίες για τη διαβεβαίωση της χρήσης του 'εισιτηρίου' από τον κόμβο για τον οποίο εκδόθηκε. Το 'εισιτήριο' περιέχει το όνομα του εξυπηρετητή, το όνομα του 'πελάτη', τη διεύθυνση δικτύου του, ημερολογιακά στοιχεία, τον χρόνο ζωής του εισιτηρίου και το κλειδί συνόδου. Μπορεί να χρησιμοποιηθεί πολλαπλά κατά τη σύνοδο του συγκεκριμένου 'πελάτη' με το συγκεκριμένο εξυπηρετητή. Σε αντίθεση ο 'αυθεντικοποιητής', που περιέχει το όνομα του 'πελάτη', τη διεύθυνση του σταθμού εργασίας και την ημερομηνία-ώρα του σταθμού εργασίας, δημιουργείται κάθε φορά, που ο 'πελάτης' ζητά την χρήση μίας υπηρεσίας.

Μειονεκτήματα

- Η χρήση εξειδικευμένων εξυπηρετητών εξακρίβωσης γνησιότητας και κυρίως του κεντρικού εξυπηρετητή, ο οποίος αν δε λειτουργεί, είναι αδύνατη κάθε διαδικασία διαχείρισης (νέος χρήστης, μεταβολή χρήστη).

- Η υπερφόρτωση της επικοινωνιακής κυκλοφορίας λόγω των διεργασιών των πρωτοκόλλων εξακρίβωσης γνησιότητας.
- Οι απαιτήσεις χρονικού συγχρονισμού μεταξύ των κόμβων.
- Οι περιορισμοί που τίθενται λόγω ύπαρξης δρομολογητών δικτύων (απαίτηση νέου εξυπηρετητή μετά το δρομολογητή).
- Η έλλειψη διαδικασιών αντίστροφης ταυτοποίησης. Να ταυτοποιείται δηλαδή ο εξυπηρετητής και ο σταθμός εργασίας στον χρήστη για την αποφυγή υφαρπαγής συνθηματικών, μέσω ειδικού λογισμικού.
- Η χρονική διάρκεια του 'εισιτηρίου' πρέπει να διατηρεί τη λεπτή ισορροπία μεταξύ ενός ασφαλούς συστήματος (μικρή διάρκεια) με επανειλημμένες καταχωρήσεις συνθηματικού και ενός εύχρηστου πιθανά μη ασφαλούς συστήματος (μεγάλη διάρκεια).

7. Βιομετρική αναγνώριση (Biometric identification)

7.1 Τι είναι η βιομετρική

Βιομετρική είναι η επιστήμη που χρησιμοποιεί ψηφιακή τεχνολογία για να αναγνωρίσει την ταυτότητα ατόμων, βάση κάποιων ιδιαίτερων και μοναδικών φυσικών ή βιολογικών χαρακτηριστικών τους.

Φυσικά χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για βιομετρική αναγνώριση περιλαμβάνουν φυσικά τα δακτυλικά αποτυπώματα, η γεωμετρία της παλάμης, η ίριδα του ματιού ή ο αμφιβληστροειδής, χαρακτηριστικά προσώπου, χαρακτηριστικά φωνής ακόμη και μυρωδιά σώματος. Μπορεί να χρησιμοποιηθεί ακόμη και το ανθρώπινο DNA, αλλά αυτή είναι μια περισσότερο παραβιαστική διαδικασία και απαιτεί δείγμα από δέρμα, ιστό ή αίμα.

Η Βιομετρία είναι πιο ασφαλής από τους κωδικούς πρόσβασης, αλλά μπορεί επίσης να ‘ξεγελαστεί’.

7.2 Αρχές βιομετρικής τεχνολογίας

Οι αρχές της βιομετρικής τεχνολογίας είναι απλές. Σε πρώτο στάδιο, μία κάμερα ή ένας σαρωτής καταγράφει μερικά μοναδικά φυσικά χαρακτηριστικά και τα μετατρέπει σε ηλεκτρονικό κώδικα. Στη συνέχεια ο κώδικας συσχετίζεται με το συγκεκριμένο άτομο και τα δύο δεδομένα αποθηκεύονται σε μία βάση δεδομένων ή σε μία smart card. Για να ελεγχθεί μία ταυτότητα, η σάρωση επαναλαμβάνεται (acquisition) και ο νέος κώδικας συγκρίνεται με αυτόν που είναι αποθηκευμένος (matching).

Η ταυτοποίηση μέσω του DNA είναι πολύ ακριβής, αλλά προς το παρόν είναι εξαιρετικά χρονοβόρα διαδικασία και αρκετά ακριβή. Η σάρωση ίριδας είναι ιδανική για εφαρμογές υψηλής ασφάλειας, στις οποίες η παρεισφρητική φύση της διαδικασίας είναι αποδεκτή. Η σάρωση αποτυπωμάτων, αν και είναι λιγότερο ασφαλής, είναι ιδανική για απλές εφαρμογές ρουτίνας.

7.3 Τύποι βιομετρικής

7.3.1 Δακτυλικά αποτυπώματα (Fingerprints)

Η σταθερότητα και η μοναδικότητα των δακτυλικών αποτυπωμάτων είναι αδιαμφισβήτητη. Σύμφωνα με προσεκτικές εξετάσεις έχει διαπιστωθεί ότι η πιθανότητα δύο ανθρώπων, συμπεριλαμβανομένων και των διδύμων, να έχουν το ίδιο δακτυλικό αποτύπωμα είναι μικρότερη από μια στο ένα δισεκατομμύριο. Πολλές συσκευές στην αγορά σήμερα αναλύουν τη θέση πολύ μικρών σημείων, που ονομάζονται λεπτομέρειες (minutiae). Οι συσκευές προσδιορίζουν τη θέση των λεπτομερειών χρησιμοποιώντας x, y και κατευθυντικές μεταβλητές. Άλλες συσκευές προσεγγίζουν το δάκτυλο ως ένα πρόβλημα επεξεργασίας εικόνας. Τα δακτυλικά αποτυπώματα απαιτούν ένα από τα μεγαλύτερα περιγράμματα δεδομένων στο πεδίο της βιομετρικής, που μπορεί να πάρει από μερικά bytes έως και πάνω από 1.000 bytes, ανάλογα με την προσέγγιση και το επίπεδο ασφάλειας που απαιτείται.

Σήμερα η μεγαλύτερη εφαρμογή με τεχνολογία δακτυλικών αποτυπωμάτων είναι στο αυτοματοποιημένο σύστημα αναγνώρισής δακτυλικών αποτυπωμάτων (AFIS) που χρησιμοποιείται από τις αστυνομικές δυνάμεις σ’ όλη την Αμερική και σε πάνω από 30 ακόμα χώρες.

Οι τεχνολογίες που χρησιμοποιούνται σήμερα είναι η οπτική, με πυρίτιο και με υπέρηχο.

Η οπτική τεχνολογία είναι η παλιότερη και η πιο ευρέως χρησιμοποιημένη. Το δάκτυλο τοποθετείται πάνω σε μια επικαλυμμένη πλάκα, συνήθως από σκληρό πλαστικό. Στις περισσότερες συσκευές μια φορτισμένη ζευγαρωτή συσκευή (CCD) μετατρέπει την εικόνα του δακτυλικού αποτυπώματος σε ψηφιακό σήμα. Η φωτεινότητα είτε αυξομειώνεται αυτόματα, είτε χειροκίνητα, δημιουργώντας μια πιο εύχρηστη εικόνα.

Οι οπτικές συσκευές έχουν πολλά πλεονεκτήματα: είναι πιο ανθεκτικές στο χρόνο, μπορούν να αντέξουν στις διακυμάνσεις τι θερμοκρασίας, είναι αρκετά φθηνές, μπορούν να πετύχουν ανάλυση πάνω από 500 dpi. Στα μειονεκτήματα των συσκευών αυτών περιλαμβάνονται: το μέγεθος, η πλάκα πρέπει να έχει ένα επαρκή μέγεθος για να επιτύχει μια ποιοτική εικόνα. Άλλο ένα μειονέκτημα είναι ότι μπορεί να διατηρήσει απομεινάρια δακτυλικών αποτυπωμάτων από προηγούμενους χρήστες (Latent prints). Αυτό μπορεί να προκαλέσει μια παραμόρφωση στην εικόνα.

Η τεχνολογία πυριτίου (silicon) έχει κερδίσει αξιοσημείωτη αποδοχή μετά την εισαγωγή της προς στο τέλος της δεκαετίας του ’90. Αυτού του είδους η τεχνολογία γενικά παράγει εικόνα καλύτερης ποιότητας, με μικρότερη επιφάνεια, απ’ ότι στην οπτική τεχνολογία.

Η τεχνολογία υπέρηχου (ultrasound) αν και είναι η πιο ακριβής από τις τεχνολογίες σάρωσης δακτύλου, δεν είναι ακόμα ευρέως χρησιμοποιημένη. Μ’ αυτή την τεχνολογία εκπέμπονται ακουστικά κύματα και μετρούνται οι αποστάσεις βάση της σύνθετης αντίστασης του δάκτυλου, τις πλάκας και του αέρα. Ο υπέρηχος είναι ικανός να διαπεράσει τη βρομιά και τα υπολείμματα στην πλάκα, εκμηδενίζοντας το βασικό μειονέκτημα της οπτικής τεχνολογίας.

Figure 1

Τοπογραφία δακτυλικού αποτυπώματος

Πλεονεκτήματα

- Δεν απαιτούν χρήση κλειδιών, κάρτας ή άλλης συσκευής από τον χρήστη.
- Δεν απαιτούν την απομνημόνευση συνθηματικού πρόσβασης.
- Δεν απαιτούν τη διαχείριση σχετικά με την τροποποίηση στοιχείων συνθηματικών για την πρόσβαση κλπ.
- Η πιθανότητα ορθής αναγνώρισης βασίζεται σε μοναδικά χαρακτηριστικά.
- Τα κριτήρια είναι μόνιμα και δεν απαιτούν ανανέωση (εξαίρεση αποτελεί η αναγνώριση φωνής, η σύγκριση υπογραφής και η αναγνώριση πληκτρολόγησης, που απαιτούν ανανέωση με το γήρας του χρήστη).

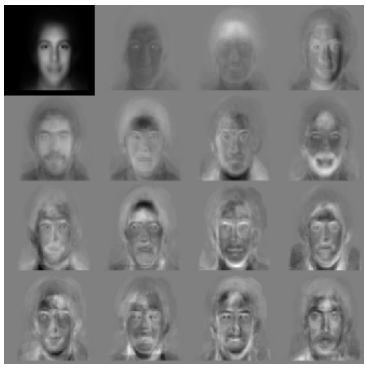
Μειονεκτήματα

- Υψηλό κόστος.
- Αργοί χρόνοι απόκρισης.
- Απαιτήσεις για μεγάλες βάσεις δεδομένων.
- Υψηλά ποσοστά απόρριψης, απαίτηση για εφαρμογή τεχνικών λήψης αντιγράφων ασφαλείας για την αυθεντικοποιήση με έμμεσο αποτέλεσμα τη δυσαρέσκεια του χρήστη.

- Υψηλές απαιτήσεις συντήρησης.
- Μακροσκελείς διαδικασίες καταχώρισης.
- Η κοινωνική αντίληψη ότι η λήψη δακτυλικών αποτυπωμάτων συνδυάζεται με εγκληματική δραστηριότητα.
- Η κοινωνική αντίληψη ότι η χρήση ακτινοβολίας βλάπτει την υγεία
- Η αντίσταση των χρηστών.

7.3.2 Χαρακτηριστικά προσώπου (Facial features)

Στη σάρωση προσώπου δίνεται έμφαση σε σημεία του προσώπου που είναι λιγότερο ευάλωτα στην αλλαγή, όπως τα πάνω περιγράμματα του ματιού, τις περιοχές που περιβάλλουν τα ζυγωματικά και την όψη του στόματος. Τα περισσότερα συστήματα δεν αντιμετωπίζουν πρόβλημα σε αλλαγές κόμμωσης, όπως επίσης δεν χρησιμοποιούν περιοχές του προσώπου κοντά στα μαλλιά. Όλα τα βασικά συστήματα είναι σχεδιασμένα ώστε να είναι αρκετά δυνατά για να διεξάγουν αναζητήσεις 1-προς-πολλά, δηλαδή να μπορούν να βρίσκουν ένα πρόσωπο, μέσα σε μια βάση δεδομένων χιλιάδων ή ακόμα και εκατοντάδων χιλιάδων προσώπων. Όμως τα περισσότερα συστήματα αντιμετωπίζουν δυσκολίες στο να πετύχουν μεγάλα επίπεδα απόδοσης όταν το μέγεθος της βάσης δεδομένων αυξάνεται σε δεκάδες χιλιάδες ή και περισσότερο.



Αποτέλεσμα σάρωσης προσώπου

Πλεονεκτήματα

- Μικρό κόστος λειτουργίας. Το κόστος μιας κάμερας είναι μικρό και εκδόσεις demo των κυριοτέρων εφαρμογών διατίθενται δωρεάν download.

- Είναι η μέθοδος που βρίσκεται πιο κοντά στον τρόπο που εμείς ως άνθρωποι θα αναγνωρίζαμε ένα άτομο.
- Η εικόνα του προσώπου μπορεί να παρθεί από αρκετά μέτρα απόσταση με το σημερινό εξοπλισμό.

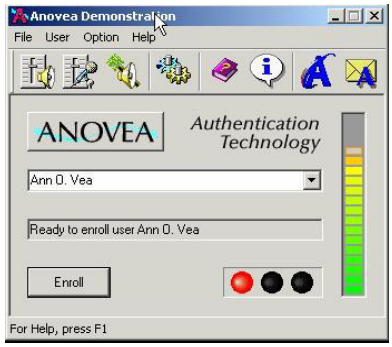
Μειονεκτήματα

- Δυσπιστία των ανθρώπων σε τέτοιου είδους μεθόδους.
- Η κοινωνική αντίληψη ότι η χρήση ακτινοβολίας βλάπτει την υγεία.
- Μακροσκελείς διαδικασίες καταχώρισης.
- Η κοινωνική αντίληψη ότι η λήψη των χαρακτηριστικών του προσώπου συνδυάζεται με εγκληματική δραστηριότητα.

Η σάρωση προσώπου απαιτεί ανάλυση 320x240 και τουλάχιστον 3 – 4 frames το δευτερόλεπτο. Περισσότερα frames το δευτερόλεπτο μαζί με μεγαλύτερη ανάλυση θα οδηγήσουν σε καλύτερη λειτουργία της αναγνώρισης. Το κόστος μιας κάμερας είναι μικρό και εκδόσεις demo των κυριοτέρων εφαρμογών διατίθενται δωρεάν download.

7.3.3 Σάρωση φωνής (Voice scan)

Η σάρωση φωνής χρησιμοποιεί φωνητικά χαρακτηριστικά για να αναγνωρίσει άτομα. Είναι πολύ ελκυστική τεχνολογία λόγω της αποδοχής που έχει από τους χρήστες. Τα συστήματα σάρωσης φωνής αναγνωρίζουν το μοναδικό ηχητικό σήμα που παράγει ο χρήστης λέγοντας μια συγκεκριμένη φράση κλειδί (pass-phrase).



Λογισμικό αναγνώρισης φωνής

Πλεονεκτήματα

- Δυνατότητα για εξ’ αποστάσεως πιστοποίηση.

- Ο χρήστης να βρίσκεται μπροστά σε κάποιο μηχάνημα ή συσκευή του συστήματος.
- Η φράση κλειδί δεν χρειάζεται να περιέχει κανενός είδους μυστικές πληροφορίες ή ειδικές λέξεις.
- Μικρό κόστος λειτουργίας. Ο χρήστης μπορεί να μπει από μακριά χρησιμοποιώντας το τηλέφωνό του ή να βρίσκεται στο σπίτι του και να χρησιμοποιήσει ένα κοινό μικρόφωνο.

Μειονεκτήματα

- Απομιμήσεις φωνής.
- Η κλωνοποίηση της φωνής (αυτός ο φόβος είναι μηδαμινός αν υπολογίσει κανείς ότι για να δημιουργηθεί ένας κλώνος φωνής χρειάζονται 10-40 ώρες ομιλίας του αυθεντικού χρήση και ότι το κόστος πλησιάζει τα 200.000 δολάρια).
- Η φράση-κλειδί συνήθως πρέπει να είναι διάρκειας ενός έως τριών δευτερολέπτων.
- Μαζί με τη φράση-κλειδί περνάνε και θόρυβοι που προκαλούνται άθελα μας, όπως θόρυβος με τα χείλη, θόρυβος αναπνοής, βήχας, άσχετες συλλαβές όπως ‘αα’ ή ‘αχ’ κλπ.

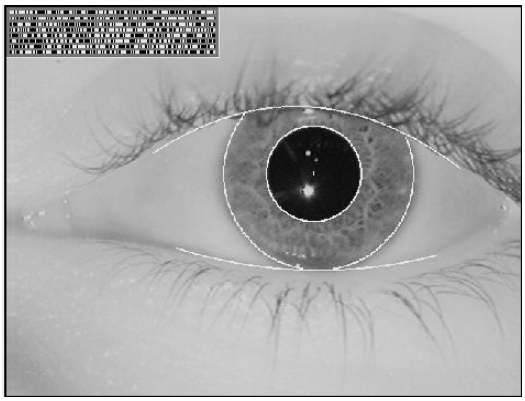
7.3.4 Σάρωση Ίριδας (Iris-scan)

Η αναγνώριση ίριδας ματιού βασίζεταί στα ορατά (μέσο κανονικού ή /και υπέρυθρού φωτός) στοιχεία της ίριδας. Η ίριδα είναι ένα προστατευμένο εσωτερικό όργανο του ματιού, τοποθετημένο πίσω από τον κερατοειδή χιτώνα, όμως μπροστά από τον κρυσταλλοειδή χιτώνα του ματιού. Είναι το μόνο εσωτερικό όργανο του σώματος πού είναι κανονικά ορατό εξωτερικά. Στην ουσία η ίριδα είναι το έγχρωμο μέρος που περιβάλλει την κόρη του ματιού. Αρχίζει να σχηματίζεται κατά τη διάρκεια του 3ου μήνα της κυοφορίας και ολοκληρώνεται στον 8ο μήνα, όμως ο χρωματισμός συνεχίζει και μέσα στα πρώτα χρόνια μετά τη γέννηση.

Η ίριδα έχει πλούσια και μοναδικά χαρακτηριστικά, όπως ραβδώσεις, νεύρα, δακτύλιοι, ιστοί, αυλάκια, αγγεία και το δίκτυο κυττάρων. Σύμφωνα με μελέτες που έχουν γίνει η ανθρώπινη ίριδα έχει σχεδόν 250 χαρακτηριστικά και καθένα από αυτά

είναι μοναδικά σε κάθε άτομο. Ο αριθμός αυτών των χαρακτηριστικών είναι δέκα φορές πάνω από τον αριθμό των γνωρισμάτων που διαθέτουν τα δακτυλικά αποτυπώματα. Αυτό σημαίνει ότι η πιθανότητα ο γενετικός κώδικας τις ίριδας ενός ατόμου να ταιριάζει απόλυτα με το γενετικό κώδικα τις ίριδας κάποιου άλλου ατόμου είναι τόσο απίθανη, σαν να είναι σχεδόν αδύνατο.

Η αναγνώριση ίριδας είναι ακόμα πιο αξιόπιστη και από εξέταση DNA.



Σάρωση ίριδας

Πλεονεκτήματα

- Μπορεί να δημιουργηθεί μια εικόνα από μακριά, χωρίς φυσική επαφή,
- Τα χαρακτηριστικά της παραμένουν ίδια για όλη τη ζωή του ανθρώπου,
- Η έμφυτη απομόνωση και προστασία από το εξωτερικό περιβάλλον,
- Η αδυναμία χειρουργικής αλλαγής της, χωρίς ανεπιθύμητου κινδύνου στην όραση,
- Η φυσιολογική αντίδραση στο φως, η οποία εξασφαλίζει έναν από τους πολλούς φυσικούς ελέγχους,
- Δεν υπάρχει καμία γενετική διείσδυση στην παρατήρηση αυτού του οργάνου πέραν της ανατομικής μορφής, της φυσιολογίας, του χρώματος και γενικά της εμφάνισης, η σύσταση της ίριδας είναι τυχαία ή πιθανώς χαοτική,
- Κάθε ίριδα μπορεί να έχει μοναδικές λεπτομέρειες, ακόμα και σε δίδυμους ή και στο ίδιο άτομο η ίριδα του δεξιού ματιού διαφέρει από αυτή του αριστερού ματιού.

Μειονεκτήματα

- Δεν μπορεί να εφαρμοστεί σε άτομα με προβλήματα όρασης,
- Χρειάζεται μεγάλος χώρος αποθήκευσης για μελλοντική προσπάθεια εξακρίβωσης του ατόμου.
- Δύσκολο στη χρήση.
- Διστακτικότητα των χρηστών.

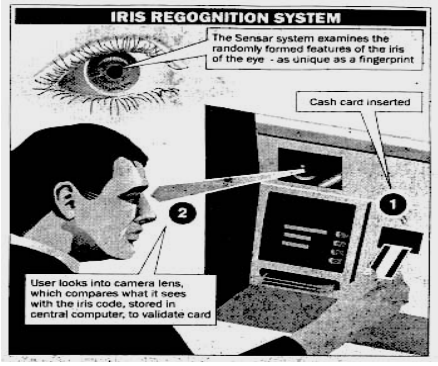
Μια ιδιότητα που η ίριδα έχει από κοινού με τα δακτυλικά αποτυπώματα είναι η τυχαία μορφογένεση των λεπτομερειών τους.

Η σάρωση ίριδας γίνεται από μια συσκευή, η οποία περιέχει μια μικρή κάμερα και φακούς κοντινής λήψης, που παίρνουν μια στατική εικόνα του ματιού. Το σύστημα αναλύει την εικόνα και παράγει έναν κώδικα 512 bytes που ονομάζεται κώδικας ίριδας (IrisCode). Ένα πρότυπο αποθηκεύεται για μελλοντική προσπάθεια εξακρίβωσης του ατόμου. 512 bytes είναι αρκετά συμπαγές μέγεθος για ένα βιομετρικό πρότυπο, όμως η ποσότητα της πληροφορίας που προέρχεται από μια ίριδα είναι μεγάλη. Για μια ίριδα διαμέτρου 11 χιλιοστών, χρειάζονται 3,4 bits ανά χιλιοστό.

Διαδικασία αναγνώρισης μέσου ίριδας

Το πρώτο βήμα στην αναγνώριση μέσο ίριδας είναι να τοποθετηθεί το άτομο μπροστά στην κάμερα σε απόσταση 2-18 ίντσες, ανάλογα με τη συσκευή. Στη συνέχεια εστιάζει το μάτι στη συσκευή, ώστε να μπορεί να δει την αντανάκλαση του ματιού. Η διαδικασία της αναγνώρισης γίνεται πολύ σύντομα. Η εικόνα του ματιού παράγεται σε ένα τέταρτο (1/4) του δευτερολέπτου, ο κώδικας ίριδος δημιουργείται μέσα σ’ ένα δευτερόλεπτο, η αναζήτηση στη βάση δεδομένων είναι άμεση, με εκατοντάδες χιλιάδες εγγραφών να αναλύονται το δευτερόλεπτο. Παρόλα αυτά υπάρχουν κάποιες διαφωνίες, κατά πόσον η αναζήτηση σ’ ένα πραγματικά μεγάλο αριθμό εγγραφών (δεκάδες εκατομμύρια) θα μπορούσε να διεξάγεται τόσο γρήγορα όσο απαιτείται.

Η σάρωση ίριδας είναι μία τρομακτικά ακριβής βιομετρική τεχνολογία. Μόνο η σάρωση του αμφιβληστροειδούς χιτώνα μπορεί να προσφέρει σχεδόν τόσο καλή ασφάλεια από αυτή που προσφέρει η ίριδα. Τα περισσότερα κοινά βιομετρικά προσφέρουν λογικά αποτελέσματα, αλλά δεν μπορούν να χρησιμοποιηθούν σε μεγάλης κλίμακας υλοποιήσεις αναγνώρισης όπως η αναγνώριση ίριδας.



Διαδικασία σάρωσης ίριδας

Κανένα βιομετρικό σύστημα δεν είναι τέλειο. Η αξιοπιστία εξαρτάται από τα χαρακτηριστικά τα οποία σαρώνονται, την τεχνολογία, τη μέθοδο κωδικοποίησης και τον αποδεκτό βαθμό σφαλμάτων: όσο πιο αυστηρό είναι το σύστημα στην απόρριψη όλων των ταυτοτήτων που δεν ταιριάζουν, τόσο πιθανό είναι να απορρίψει μια ταυτότητα η οποία είναι αληθής.

Με εξαίρεση την ταυτοποίηση μέσω του DNA, κάθε βιομετρική τεχνολογία αποκλείει ένα μικρό, αλλά σημαντικό, ποσοστό του πληθυσμού: για παράδειγμα πολλοί τυφλοί δεν μπορούν να περάσουν από σαρωτή ίριδας. Και, παραδόξως, ενδέχεται να κάνουν τις πλαστές ταυτότητες πιο ασφαλείς σε περίπτωση που τα πλαστά έγγραφα γίνουν αποδεκτά στη διαδικασία εγγραφής.

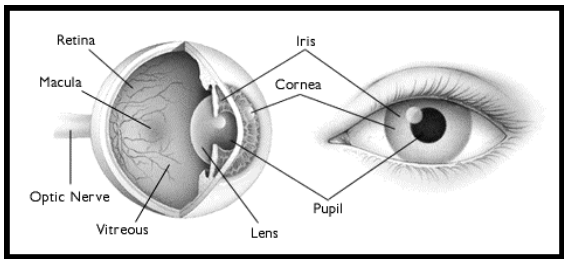
Επιπλέον των μειονεκτημάτων που εμφανίζουν τα βιομετρικά συστήματα ασφαλείας στην περίπτωση ατόμων με αλλοίωση της ίριδας, υπάρχει και η περίπτωση αλλοίωσης του δακτυλικού αποτυπώματος από βαθιά τραύματα, ή και εγκαύματα.

Αν τα βιομετρικά συστήματα χρησιμοποιηθούν σωστά, μπορεί να κάνουν τη ζωή μας ευκολότερη. Εάν, όμως δε χρησιμοποιηθούν σωστά μπορεί να εκθέσουν τις πολιτικές μας ελευθερίες, αλλά όχι σε τέτοιο βαθμό όπως άλλα συστήματα.

Σάρωση αμφιβληστροειδούς χιτώνα ματιού (Retina Scan)

Μαζί με τη σάρωση ίριδας, η σάρωση αμφιβληστροειδούς είναι ίσως οι πιο ακριβής και αξιόπιστη βιομετρική τεχνολογία, όμως είναι και μεταξύ των πιο δύσκολων στη χρήση. Η σάρωση αμφιβληστροειδούς είναι ένα από τα παλαιότερα βιομετρικά. Από το 1930 έρευνες έδειξαν ότι η μορφή των αγγείων αίματος στο πίσω μέρος του ανθρώπινου ματιού είναι διαφορετική από άτομο σε άτομο, ακόμα και σε

δίδυμα αδέρφια. Επίσης ο αμφιβληστροειδής παραμένει ίδιος σε όλη τη ζωή του ανθρώπου, με την εξαίρεση ορισμένων τύπων από εκφυλιστικές ασθένειες του ματιού, ή περιπτώσεις σοβαρών τραυμάτων στο κεφάλι.



Ανατομία οφθαλμού

Ο αμφιβληστροειδής χιτώνας του ματιού είναι ένα μικρό νεύρο (1/50ο της ίντσας) στο πίσω μέρος του ματιού, είναι το μέρος του ματιού το οποίο αισθάνεται το φως και μεταδίδει παλμούς δια μέσου του οπτικού νεύρου προς τον εγκέφαλο. Τα αιμοφόρα αγγεία που χρησιμοποιούνται για τη βιομετρική αναγνώριση βρίσκονται κατά μήκος του νωτιαίου αμφιβληστροειδούς, το έσχατο από τα τέσσερα επίπεδα του αμφιβληστροειδούς.

Οι συσκευές σάρωσης αμφιβληστροειδούς διαβάζουν δια μέσου της κόρης του ματιού, γι' αυτό απαιτείται ο χρήστης να τοποθετήσει το μάτι του εντός μισής ίντσας από τη συσκευή και να μείνει ακίνητος μέχρις ότου η συσκευή ανάγνωσης εξακριβώσει την ταυτότητα του. Ο χρήστης κοιτάει σ' ένα περιστρεφόμενο πράσινο φως. Παίρνονται 350 – 400 σημεία αναφοράς και αποθηκεύονται σ' ένα πεδίο 96 bytes, εξασφαλίζοντας ότι το μέτρημα είναι σωστό, με ένα αμελητέο βαθμό σφάλματος. Σε σύγκριση με το δακτυλικό αποτύπωμα που χρειάζονται 30-70 διακριτά σημεία, γίνεται φανερό το πολύ υψηλό επίπεδο ακρίβειας της τεχνολογίας αυτής.

Πλεονεκτήματα

- Μηδαμινή πιθανότητα να κάποιος χρήστης να διεκδικήσει λάθος ταυτότητα και να γίνει αποδεκτός (μόλις μία πιθανότητα στο ένα εκατομμύριο),
- Σταθερότητα στο βιομετρικό δείγμα,
- Ανθεκτική στην απάτη. Θα ήταν πολύ δύσκολο και χρονοβόρο να δημιουργηθεί ένα ψεύτικο δείγμα αμφιβληστροειδούς,

- Μικρή ποσότητα δεδομένων (μόλις 96 bytes).

Μειονεκτήματα

- Δυσκολία στη χρήση,
- Διστακτικότητα των χρηστών. Το μάτι και ειδικά το εσωτερικό του ματιού είναι πολύ ευαίσθητο και γι' αυτό πολύ χρήστες είναι διστακτικοί στο να χρησιμοποιήσουν τέτοιες συσκευές,
- Στατικός σχεδιασμός. Σε αντίθεση με τις άλλες τεχνολογίες, οι οποίες μπορούν να εκμεταλλευτούν τα πλεονεκτήματα των νέων τεχνολογιών, όπως καλύτερης ποιότητας κάμερες ή αξιοποίηση πυριτίου, ή σάρωση αμφιβληστροειδούς είναι περιορισμένη σε συγκεκριμένους μηχανισμούς σύλληψης του δείγματος και συγκεκριμένα πρωτοκόλλα,
- Υψηλό κόστος συσκευής σάρωσης αμφιβληστροειδούς.

7.3.5 Σάρωση Χεριού (Hand Scan)

Η σάρωση χεριού είναι γνωστή και ως γεωμετρία χεριού (hand geometry). Είναι μια αυτοματοποιημένη μέτρηση πολλών μεγεθών του χεριού και των δακτύλων. Η τεχνολογία αυτή χρησιμοποιεί το ύψος των δακτύλων, την απόσταση μεταξύ των κλειδώσεων και το σχήμα των αρθρώσεων για να πιστοποιήσει την ταυτότητα του χρήστη. Παρόλο που δεν είναι η πιο ακριβής τεχνολογία, η σάρωση χεριού έχει αποδειχτεί ως η ιδανική λύση για χαμηλού επιπέδου εφαρμογές ασφάλειας.

Η μέθοδος απόκτησης του βιομετρικού δείγματος είναι αρκετά απλό. Ο χρήστης τοποθετεί το χέρι του στην ειδική συσκευή ακουμπώντας την παλάμη του σε μία μεταλλική επιφάνεια διαστάσεων 8x10. (Όπως φαίνεται στις παρακάτω εικόνες).

Τοποθέτηση παλάμης

Στη συνέχεια ο χρήστης ευθυγραμμίζει το χέρι του σύμφωνα με τα πέντε ειδικά καρφιά, που είναι σχεδιασμένα ώστε να υποδείξουν την κατάλληλη θέση του αντίχειρα, του δείκτη και του μεσαίου.

Το σύστημα χρησιμοποιεί μια 32.000 pixel CCD (charged coupled device) ψηφιακή κάμερα, εξάγοντας συμπεράσματα για το μήκος, το πλάτος, το πάχος και την επιφάνεια του χεριού από τις εικόνες των περιγραμμάτων που σχεδιάζονται μέσα στον σαρωτή. Γίνονται πάνω από 90 μετρήσεις και τα χαρακτηριστικά του χεριού αναπαριστούνται σ' ένα πρότυπο 9 bytes.

Η σάρωση χεριού ενίοτε παρεξηγείται με τη σάρωση παλάμης που είναι μια εντελώς ξεχωριστή τεχνολογία.

Πλεονεκτήματα

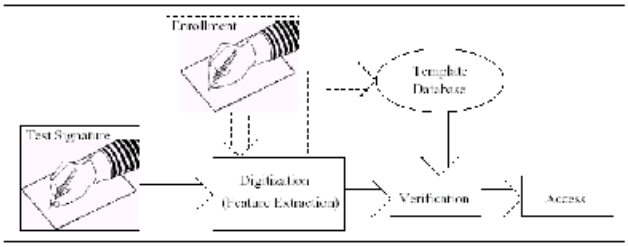
- Ευκολία στη χρήση. Απλή διαδικασία και με κατάλληλη εκπαίδευση μπορούν να μειωθούν και τα λάθη στην τοποθέτηση του χεριού. Με μια μικρή εξαίρεση στα άτομα μεγάλης ηλικίας ή σε άτομα με αρθριτικά προβλήματα στα χέρια, που ίσως να μη μπορούν να ανοίξουν τα δάκτυλα και να τοποθετήσουν το χέρι τους στην συσκευή,
- Ανθεκτική στην απάτη,
- Μικρό μέγεθος προτύπου. Μόλις 9 Bytes,
- Αντίληψη του χρήστη. Σε αντίθεση με τη σάρωση προσώπου ή τις τεχνολογίες βασισμένες στο μάτι, οι οποίες μπορεί να συναντούν κάποιες αντιδράσεις, η σάρωση χεριού είναι αποδεκτή από τη συντριπτική πλειοψηφία των χρηστών.

Μειονεκτήματα

- Στατικός σχεδιασμός. Η τεχνολογία της σάρωσης χεριού παραμένει σε μεγάλο βαθμό αμετάβλητη για χρόνια,
- Οι σαρωτές χεριού έχουν υψηλό κόστος,
- Κακώσεις στο χέρι. Όπως σε όλα τα βιομετρικά φυσικές αλλαγές μπορεί να προκαλέσουν εσφαλμένη απόρριψη των χρηστών,
- Ακρίβεια. Παρόλο που είναι πιο αξιόπιστη από τα βιολογικά βιομετρικά, όπως η φωνή και η υπογραφή, η σάρωση χεριού δεν μπορεί να πραγματοποιήσει αναζητήσεις ένα -προς- πολλά.

7.3.6 Σάρωση υπογραφής (Signature Scan)

Η σάρωση υπογραφής είναι επίσης γνωστή και ως δυναμική εξακρίβωση υπογραφής (Dynamic Signature Verification). Είναι η βιομετρική τεχνολογία η οποία δεν έχει ευρεία χρήση, όμως ίσως σύντομα βοηθήσει στην αντιμετώπιση της πιστοποίησης επίσημων εγγράφων. Μετρώντας τον τρόπο με τον οποίο ένας χρήστης γράφει το όνομα του, ένα συνθηματικό, ή μια φράση κλειδί, η σάρωση υπογραφής ερευνά τον τρόπο, την ταχύτητα, την πίεση και άλλους παράγοντες οι οποίοι συνδέονται με τη διαδικασία της υπογραφής.



Ένα τυπικό σύστημα επαλήθευσης υπογραφής

Πλεονεκτήματα

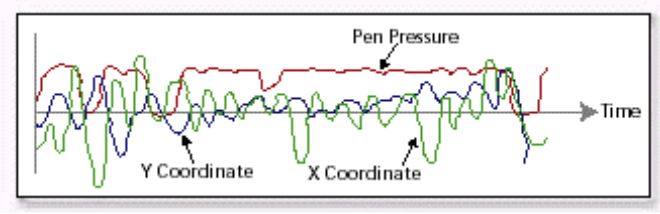
- Η σάρωση υπογραφής εξασφαλίζει αξιόπιστη αναγνώριση ατόμων, με βάση την υπογραφή τους,
- Χρησιμοποιεί μετρήσεις του μοναδικού τρόπου με τον οποίο δημιουργείται μια χειρόγραφη υπογραφή, ώστε να επιβεβαιώσει την ταυτότητα του χρήστη,
- Σε μεγάλες επιχειρήσεις ή μέσο του internet μια ψηφιακή υπογραφή καθιστά ικανές τις εφαρμογές να παρέχουν αυξημένη μυστικότητα και αξιόπιστη ηλεκτρονική εξουσιοδότηση, σε αντίθεση με ένα συνθηματικό, ένα PIN ή μια keycard, που μπορεί να ξεχαστούν, να χαθούν, ή να κλαπούν,
- Τα συστήματα αυτά αναλύουν και τα δυναμικά και τα ”του χώρου” χαρακτηριστικά γνωρίσματα της χειρόγραφης υπογραφής για να ελέγξουν την ταυτότητα του υπογράφοντος. Επειδή κάθε άτομο έχει τον προσωπικό του γραφικό χαρακτήρα, το σύστημα παίρνει τα χαρακτηριστικά του τρόπου γραφής και αναλύουν τη δυναμική του χτυπήματος, της ταχύτητας και της πίεσης. Ενώ με εξάσκηση κάποιος ίσως μπορέσει να αντιγράψει την οπτική εικόνα της υπογραφής κάποιου άλλου, είναι πολύ δύσκολο, έως αδύνατο, να αντιγράψει τον τρόπο με τον οποίο το άτομο αυτό υπογράφει. Ακόμα και αν η

υπογραφή είναι τέλεια σχεδιασμένη, η ταχύτητα, η δύναμη και η πίεση θα διαφέρουν.

Μειονεκτήματα

- Χρειάζεται ειδικό εξοπλισμό,
- Αυξημένο κόστος χρήσης,
- Διστακτικότητα χρηστών.

Αρκετά συστήματα σάρωσης υπογραφής ενσωματώνουν μια συνάρτηση μάθησης, η οποία μπορεί αυτομάτως να απορροφά και να απεικονίζει κάθε φυσική αλλαγή στην υπογραφή κατά τη διάρκεια του χρόνου. Αυτά τα συστήματα χρησιμοποιούν τις αλλαγές στην πίεση, στη μορφή, στην κατεύθυνση και στην ταχύτητα σε συνάρτηση με το χρόνο. Έτσι τα δεδομένα αναλύονται σε τέσσερις διαστάσεις – x (οριζόντια ταχύτητα), y (κάθετη ταχύτητα), z (πίεση) και t (χρόνος).



Γραφική παράσταση συνάρτησης μάθησης

Δυναμική πατήματος πλήκτρου (Keystroke Dynamic)

Η δυναμική πατήματος πλήκτρου είναι γνωστή και ως ρυθμός δακτυλογράφησης. Η μέθοδος εξετάζει τον τρόπο με τον οποίο ένα άτομο δακτυλογραφεί ή πιέζει τα πλήκτρα σ' ένα πληκτρολόγιο.

Αυτή η τεχνολογία αναλύει χαρακτηριστικά όπως η ταχύτητα, η δύναμη, η συχνότητα λάθους, ο συνολικός χρόνος δακτυλογράφησης ενός συγκεκριμένου συνθηματικού και ο χρόνος που μεσολαβεί από το πάτημα ενός συγκεκριμένου πλήκτρου έως το πάτημα ενός άλλου συγκεκριμένου πλήκτρου.

Πλεονεκτήματα

- Η επιβεβαίωση βασίζεται στην παραδοχή ότι ο τρόπος που δακτυλογραφεί ένα άτομο είναι ξεχωριστός, ειδικά ο ρυθμός του. Ακόμα και αν κάποιος

μαντέψει το σωστό συνθηματικό, δεν θα μπορέσει να το δακτυλογραφήσει με τον κατάλληλο ρυθμό,

- Η συσκευή εισόδου μπορεί να είναι το υπάρχον πληκτρολόγιο. Έτσι μειώνεται δραστικά το κόστος.

Μειονεκτήματα

- Υπάρχουν πολλές τεχνικές δυσκολίες που κάνουν την συγκεκριμένη τεχνολογία να μην αποδίδει τα αναμενόμενα αποτελέσματα,
- Οι μισές προσπάθειες σε εμπορικές τεχνολογίες έχουν αποτύχει,
- Διαφορές στα πληκτρολόγια, ακόμα και της ίδιας εταιρίας, και στα πρωτόκολλα επικοινωνίας προκαλούν εμπόδια στις εταιρίες ανάπτυξης αυτής της τεχνολογίας.

7.3.7 DNA

Το DNA είναι ένας τύπος βιομετρικής αφού χρησιμοποιείται ως φυσικό χαρακτηριστικό στην επαλήθευση και τον προσδιορισμό ενός χρήστη.

Διαφορά DNA από τα τυπικά Βιομετρικά συστήματα

- Το DNA απαιτεί ένα χειροπιαστό φυσικό δείγμα, σε αντίθεση με μια εικόνα, ένα αποτύπωμα, ή μια εγγραφή,
- Το ταίριασμα του DNA και δεν γίνεται σε πραγματικό χρόνο και συγχρόνως δεν είναι όλα τα στάδια της σύγκρισης αυτοματοποιημένα,
- Το ταίριασμα του DNA δεν δημιουργεί πρότυπα ή εξαγωγή χαρακτηριστικών, αλλά αντιθέτως αναπαριστά τη σύγκριση με πραγματικά δείγματα.

Πλεονεκτήματα

- Αξιόπιστα και ακριβή αποτελέσματα,
- Τα χαρακτηριστικά του παραμένουν ίδια για όλη τη ζωή του ανθρώπου,
- Δεν μπορεί να αντιγραφεί ή να κλαπεί.

Μειονεκτήματα

- Το ταίριασμα του DNA και δεν γίνεται σε πραγματικό χρόνο και συγχρόνως δεν είναι όλα τα στάδια της σύγκρισης αυτοματοποιημένα,
- Αντίσταση των χρηστών,
- Υψηλό κόστος.

7.4 Ηθικά ζητήματα βιομετρικής

Όταν οι αυτόματες βιομετρικές τεχνολογίες άρχιζαν να εμφανίζονται την δεκαετία του 1970, πολλοί εξέφρασαν την ανησυχία τους για την παραβίαση της ιδιωτικότητας με την ψηφιοποίηση των φυσικών τους χαρακτηριστικών και την αποθήκευση σε κρατικές βάσεις δεδομένων. Άλλοι υποστηρίζουν ότι η βιομετρική στην πραγματικότητα προστατεύουν τους ανθρώπους ενάντια στο αυξανόμενο έγκλημα της κλοπής ταυτότητας. Τα βιομετρικά συστήματα δεν είναι αλάνθαστα, και ενώ τώρα λίγοι είναι αυτοί που διαφωνούν με την χρήση της βιομετρικής για σκοπούς αναγνώρισης, οι υποστηρικτές των πολιτικών δικαιωμάτων συχνά υποστηρίζουν ότι τα συστήματα αναγνώρισης προσώπου σε δημόσια μέρη όπως τα αεροδρόμια είναι μια παραβίαση της ιδιωτικότητας και ότι οι λανθασμένες ταυτίσεις μπορεί να οδηγήσουν σε παρενόχληση αθώων από τις δυνάμεις ασφαλείας του αεροδρομίου.

Κατά καιρούς όμως, οι παραβιάσεις έχουν καταστροφικές συνέπειες, όπως έγινε στις Η.Π.Α στις 11/9, έχει ως αποτέλεσμα την ανάγκη για αύξηση της βιομετρικής παρακολούθησης.

7.5 Το μέλλον της βιομετρικής αναγνώρισης

Αν και οι περισσότερες μέθοδοι βιομετρικής αναγνώρισης είναι πρόσφατες, ήδη γίνεται έρευνα σε πιο εξωτικές μεθόδους, όπως η αναγνώριση της σωματικής οσμής, η αναγνώριση της φλεβικής δομής του επάνω μέρους της παλάμης, η αναγνώριση της παλάμης μέσω των γραμμώσεων, η αναγνώριση της γεωμετρίας τους αυτιού κλπ.,

Μέτρηση Απόδοσης

Δεν υπάρχει ένα τέλειο σύστημα στην βιομετρική τεχνολογία για κάθε εφαρμογή. Τα τέσσερα βασικά κριτήρια για κάθε βιομετρικό σύστημα αναγνώρισης είναι αυτά που περιγράφουν οι χρήστες και αυτά που επιβάλει η τεχνολογία.

Κριτήρια χρηστών

- Προσπάθεια – Πόσος χρόνος και προσπάθεια χρειάζεται να καταβάλει ο χρήστης.
- Διακριτικότητα – Πόσο διακριτικό πιστεύει ο χρήστης πως είναι το σύστημα.

Κριτήρια τεχνολογίας

- Κόστος – Το κόστος του συστήματος αναγνώρισης.
- Ακρίβεια – Πόσο καλά το σύστημα αναγνωρίζει τα άτομα.

Κριτήρια χρηστών:

Για να απαντήσουμε στην ερώτηση ποιό είναι το καλύτερο βιομετρικό σύστημα, πρέπει να έχουμε στο μυαλό μας την εφαρμογή. Για παράδειγμα, δεν είναι υπερβολικό αν πρόκειται να προσπελάσει ο χρήστης μια εγκατάσταση πυρηνικού αντιδραστήρα, να θεωρήσει ανεκτό να περάσει από μία διαδικασία αναγνώρισης 30’’, χωρίς να θεωρήσει ενοχλητική την όλη διαδικασία. Αντίθετα αν πρόκειται να εφαρμοστεί ένα βιομετρικό σύστημα για τον έλεγχο ταυτότητας στον κάτοχο εισιτηρίου διαρκείας σε ένα πάρκο αναψυχής, τότε μπορεί να αισθανθεί άβολα και προσβλημένος.

Κριτήρια τεχνολογίας:

Οι απαιτήσεις ασφάλειας εξαρτώνται πάλι από την εφαρμογή. Η ακρίβεια του συστήματος μετράται με τους ακόλουθους δείκτες:

- FAR (False Acceptance Rate) – Μετράει πόσο συχνά ένα μη εγγραμμένο άτομο ή ακόμα και ένας απατεώνας μπορεί να αναγνωριστεί από το σύστημα ως εξουσιοδοτημένος χρήστης. Αυτό είναι και το χειρότερο σενάριο σ’ ένα ασφαλές περιβάλλον.

- FRR (False Rejection Rate) – Μετράει πόσο συχνά το σύστημα απορρίπτει έναν εξουσιοδοτημένο χρήστη, μια κατάσταση που μπορεί να ενοχλήσει τους χρήστες, όμως δεν προκαλεί κανένα πρόβλημα στην ασφάλεια του συστήματος. Πρακτικά το FRR διαφέρει ανάλογα με τις συνθήκες του περιβάλλοντος ή την ποιότητα του βιομετρικού δείγματος.
- FER (Failure to Enroll Rate) – Υποδηλώνει την πιθανότητα ένας δεδομένος χρήστης να είναι αδύνατο να εγγραφεί σ' ένα βιομετρικό σύστημα, λόγω του ότι είναι ανεπαρκής. Παραδείγματος χάρη ένα άτομο χωρίς χέρια είναι αδύνατο να χρησιμοποιήσει ένα σύστημα αναγνώρισης δακτυλικού αποτυπώματος. Όμως αυτός ο τύπος προβλήματος μπορεί να είναι ακόμα πιο περίπλοκος. Για παράδειγμα μια γενειάδα μπορεί να εμποδίζει ένα χρήστη στο να χρησιμοποιήσει ένα σύστημα αναγνώρισης προσώπου, μια εξαιρετικά ξηρή επιδερμίδα μπορεί να μπερδέψει ένα σύστημα σάρωσης δακτύλου, ένα σύστημα αναγνώρισης φωνής μπορεί να αποδειχτεί ανώφελο σε περίπτωση ενός προβλήματος στην ομιλία.

7.6 Εγγραφή χρήστη

Η εγγραφή είναι το κρίσιμο πρώτο στάδιο για τη βιομετρική πιστοποίηση, επειδή η εγγραφή δημιουργεί ένα πρότυπο το οποίο θα χρησιμοποιηθεί για όλα τα επακολουθούντα ταιριάσματα. Είναι η διαδικασία κατά την οποία ο χρήστης παρέχει ένα φυσικό ή βιολογικό δείγμα και προσδιορίζει την ταυτότητα του στη βάση δεδομένων. Συνήθως η συσκευή κτήσης παίρνει τρία δείγματα του ίδιου βιομετρικού και τα υπολογίζει κατά μέσον όρο ώστε να δημιουργήσει ένα πρότυπο εγγραφής. Η συσκευή κτήσης διαφέρει ανάλογα με τη βιομετρική τεχνολογία. Στον παρακάτω πίνακα φαίνεται η σχέση συσκευής και βιομετρικού.

ΤΕΧΝΟΛΟΓΙΑ	ΣΥΣΚΕΥΗ ΚΤΗΣΗΣ
Σάρωση δακτύλου	Επιτραπέζιο περιφερειακό, PCMCIA card, ποντίκι, chip ή αναγνώστης ενσωματωμένος στο πληκτρολόγιο
Σάρωση φωνής	Μικρόφωνο, τηλέφωνο
Σάρωση προσώπου	Βιντεοκάμερα, κάμερα υπολογιστή
Σάρωση ίριδας	Υπέρυθρη βιντεοκάμερα ή κάμερα υπολογιστή
Σάρωση αμφιβληστροειδούς χιτώνα	Ειδική συσκευή (επιτραπέζια ή στηριγμένη στον τοίχο)
Σάρωση χεριού	Ειδική συσκευή (στηριγμένη στον τοίχο)
Σάρωση υπογραφής	Πλάκα υπογραφής, ευαίσθητο στην κίνηση στυλό
Σάρωση πατήματος πλήκτρου	Πληκτρολόγιο, keypad

Πίνακας: Συσκευές σάρωσης δειγμάτων

Βιομετρικό δείγμα : η αναγνωρίσιμη, μη-επεξεργάσιμη εικόνα ή εγγραφή του φυσικού ή βιολογικού χαρακτηριστικού, που αποκτιέται κατά τη διάρκεια της εγγραφής και χρησιμοποιείται για να παραχθεί το βιομετρικό πρότυπο. Αναφέρεται επίσης και ως βιομετρικά δεδομένα. Ο ακόλουθος πίνακας συνδέει κάθε βιομετρική τεχνολογία με το αντίστοιχο βιομετρικό δείγμα.

ΤΕΧΝΟΛΟΓΙΑ	ΒΙΟΜΕΤΡΙΚΟ ΔΕΙΓΜΑ
Σάρωση δακτύλου	Εικόνα δακτυλικού αποτυπώματος
Σάρωση φωνής	Εγγραφή φωνής
Σάρωση προσώπου	Εικόνα προσώπου
Σάρωση ίριδας	Εικόνα ίριδας
Σάρωση αμφιβληστροειδούς χιτώνα	Εικόνα αμφιβληστροειδούς χιτώνα
Σάρωση χεριού	3-D εικόνα της πάνω και της πλάγιας όψης του χεριού
Σάρωση υπογραφής	Εικόνα της υπογραφής και εγγραφή των σχετικών μετρήσεων
Σάρωση πατήματος πλήκτρου	Εγγραφή των χαρακτήρων που δακτυλογραφήθηκαν και εγγραφή των σχετικών μετρήσεων δυναμικής

Πίνακας: Βιομετρικά δείγματα

7.7 Πρότυπα (template)

Είναι ένα συγκριτικά μικρό, αλλά πολύ ξεχωριστό αρχείο, που παράγεται από τη βιομετρική συσκευή με βάση τα ιδιαίτερα χαρακτηριστικά του βιομετρικού δείγματος του χρήστη και χρησιμοποιείται για την πραγματοποίηση των βιομετρικών ταιριασμάτων. Πρότυπα δεν χρησιμοποιούν όλα τα βιομετρικά συστήματα. Ορισμένα συστήματα σάρωσης φωνής χρησιμοποιούν την αυθεντική φωνή για να πραγματοποιήσουν μια σύγκριση.

Η συσκευή χρησιμοποιεί έναν ιδιαίτερο αλγόριθμο για να εξάγει χαρακτηριστικά κατάλληλα από το βιομετρικό δείγμα. Το πρότυπο είναι απλώς μια εγγραφή των πιο ευδιάκριτων χαρακτηριστικών του βιομετρικού δείγματος του χρήστη. Για παράδειγμα πρότυπο δεν είναι μια εικόνα ή μια ολόκληρη εγγραφή του πραγματικού δακτυλικού αποτυπώματος ή της φωνής. Σε βασικές γραμμές τα πρότυπα είναι αριθμητικές απεικονίσεις βασικών σημείων που παίρνονται από το ανθρώπινο σώμα.

Τα πρότυπα είναι συνήθως μικρά σε μέγεθος και επιτρέπουν γρήγορη επεξεργασία, πράγμα το οποίο αποτελεί ξεχωριστό χαρακτηριστικό της βιομετρικής πιστοποίησης. Το μικρό μέγεθος των προτύπων επιτρέπει την αποθήκευσή τους σε μαγνητικές ταινίες ή σε ραβδωτό κώδικα πάνω σε πλαστικές κάρτες ή έξυπνες κάρτες (smart cards).

7.7.1 Είδη προτύπων

Ανάλογα με το πότε παράγονται τα πρότυπα, μπορούν να αναφέρονται ως πρότυπα εγγραφής ή πρότυπα εξακρίβωσης. Τα πρότυπα εγγραφής (Enrollment template) δημιουργούνται κατά την αρχική αλληλεπίδραση του χρήστη με το βιομετρικό σύστημα και αποθηκεύονται για χρήση σε μελλοντικά βιομετρικά ταιριάσματα. Τα πρότυπα εξακρίβωσης (Verification template) παράγονται κατά τη διάρκεια των επακόλουθων προσπαθειών εξακρίβωσης της ταυτότητας του χρήστη, συγκρίνονται με το αποθηκευμένο πρότυπο και συνήθως αποβάλλεται μετά τη σύγκριση. Πολλαπλά δείγματα μπορεί να χρησιμοποιηθούν για να παραχθεί ένα πρότυπο εγγραφής. Για παράδειγμα στη σάρωση προσώπου θα χρησιμοποιηθούν αρκετές εικόνες του προσώπου του χρήστη, ώστε να παραχθεί το πρότυπο εγγραφής. Τα πρότυπα εξακρίβωσης κανονικά δημιουργούνται από ένα και μοναδικό

δείγμα. Για παράδειγμα το πρότυπο που παράγεται από μια μονή εικόνα προσώπου μπορεί να συγκριθεί με το πρότυπο εγγραφής για να καθοριστεί ο βαθμός ομοιότητας.

Ταίριασμα

Ταίριασμα είναι η σύγκριση βιομετρικών προτύπων για να προσδιοριστεί ο βαθμός ομοιότητας ή συσχέτισης τους. Από μια προσπάθεια ταιριάσματος προκύπτει μια βαθμολογία, που στα περισσότερα συστήματα συγκρίνεται με ένα όριο. Εάν η βαθμολογία υπερβεί το όριο, το αποτέλεσμα είναι ένα ταίριασμα. Εάν η βαθμολογία πέσει κάτω από το όριο, το αποτέλεσμα είναι η αποτυχία ταιριάσματος.

Η διαδικασία ταιριάσματος περιλαμβάνει τη σύγκριση του προτύπου εξακρίβωσης, που παράγεται πάνω στην παράδοση δείγματος, με το πρότυπο εγγραφής, που βρίσκεται ήδη αποθηκευμένο σ' ένα αρχείο. Στα ένα προς ένα (1:1) συστήματα εξακρίβωσης, γενικά υπάρχει ένα απλό πρότυπο εξακρίβωσης να συγκρίνεται απέναντι σ' ένα πρότυπο εγγραφής. Στα ένα προς πολλά (1:N) συστήματα αναγνώρισης, ένα πρότυπο εξακρίβωσης μπορεί να συγκρίνεται με χιλιάδες ή και εκατομμύρια πρότυπα εγγραφής.

Στα περισσότερα συστήματα το πρότυπο εγγραφής και το πρότυπο εξακρίβωσης δεν θα έπρεπε να είναι πανομοιότυπα. Ένα πανομοιότυπο ταίριασμα είναι μια ένδειξη ότι κάποιο είδος απάτης συντελείται.

7.7.2 Βαθμολογία (score)

Βαθμολογία είναι ένας αριθμός που δείχνει τον βαθμό ομοιότητας ή συσχέτισης του βιομετρικού ταιριάσματος. Παραδοσιακές μέθοδοι πιστοποίησης (συνθηματικά, PIN, κλειδιά) είναι δυαδικές και προσφέρουν μόνο μια αυστηρή απάντηση ναι ή όχι. Σχεδόν όλα τα βιομετρικά συστήματα βασίζονται σ' έναν αλγόριθμο ταιριάσματος, ο οποίος παράγει μια βαθμολογία για κάθε προσπάθεια ταιριάσματος. Αυτή η βαθμολογία αντιπροσωπεύει το βαθμό συσχέτισης μεταξύ του προτύπου εξακρίβωσης και του προτύπου εγγραφής. Δεν υπάρχει καθιερωμένη κλίμακα για βιομετρική βαθμολόγηση. Ενδέχεται για κάποιες εταιρίες να χρησιμοποιείται μια κλίμακα 1-100, άλλες μπορεί να χρησιμοποιούν μια κλίμακα από –1 ως 1, μερικές εταιρίες μπορεί να χρησιμοποιούν μια λογαριθμική κλίμακα, ενώ άλλες μια γραμμική κλίμακα. Ανεξάρτητα από την κλίμακα που χρησιμοποιείται, αυτή

η βαθμολογία εξακρίβωσης συγκρίνεται με το όριο του συστήματος για να προσδιοριστεί πόσο επιτυχής ήταν η προσπάθεια εξακρίβωσης.

Παρενθετικά αναφέρεται ότι πολλά συστήματα επιστρέφουν μια βαθμολογία κατά τη διάρκεια της εγγραφής, που αναφέρεται ως βαθμολογία εγγραφής ή βαθμολογία ποιότητας. Αυτή η βαθμολογία αναφέρεται στο πόσο επιτυχής ήταν η διαδικασία εξαγωγής, στο να βρει ιδιαίτερα χαρακτηριστικά στο βιομετρικό δείγμα. Εάν το δείγμα ήταν πλούσιο σε πληροφορία, θα υπήρχε πιθανότατα μια υψηλή βαθμολογία εγγραφής. Αυτή η βαθμολογία δεν χρησιμοποιείται στην διαδικασία ταιριάσματος, αλλά ενδεχομένως χρειάζεται ώστε να προσδιορίσει κατά πόσον ένας χρήστης μπορεί να εγγραφεί με επιτυχία. Μια χαμηλή βαθμολογία ποιότητας δηλώνει ότι δεν θα είναι αξιόπιστη η εξακρίβωση της ταυτότητας του χρήστης.

7.7.3 Όριο (Threshold)

Όριο είναι ένας προκαθορισμένος αριθμός, συχνά ελεγχόμενος από το διαχειριστή του βιομετρικού συστήματος, ο οποίος δηλώνει έναν βαθμό συσχέτισης απαραίτητο ώστε να κριθεί ένα ταίριασμα. Εάν η βαθμολογία που προκύπτει από μια σύγκρισή προτύπων υπερβεί το όριο, τότε το πρότυπο είναι ταιριαστό, ωστόσο δεν είναι πανομοιότυπο.

Όταν ένα βιομετρικό σύστημα είναι χαμηλής ασφάλειας, το όριο για επιτυχές ταίριασμα είναι χαμηλότερο σε σχέση με ένα σύστημα υψηλής ασφάλειας.

7.7.4 Απόφαση (Decision)

Απόφαση είναι το αποτέλεσμα της σύγκρισης μεταξύ της βαθμολογίας και του ορίου. Η απόφαση που μπορεί να λάβει ένα βιομετρικό σύστημα είναι το ταίριασμα, το μη-ταίριασμα ή ακόμα μπορεί να μη βγάλει κανένα συμπέρασμα. Ανάλογα με τον τύπο του βιομετρικού συστήματος ένα ταίριασμα μπορεί να παραχωρεί πρόσβαση στους πόρους του συστήματος, ένα μη-ταίριασμα μπορεί να περιορίζει την πρόσβαση στους πόρους, ενώ αν δεν βγάλει συμπέρασμα μπορεί να προτρέπει το χρήστη να δώσει άλλο δείγμα.

7.8 Οφέλη Από Τη Χρήση Βιομετρικών Συστημάτων

Για τους εργοδότες

- Μειωμένο κόστος – διαχείριση συνθηματικών,
- Αυξημένη ασφάλεια – όχι διαμοιρασμένα ή παραχωρημένα συνθηματικά,
- Αυξημένη ασφάλεια – αποτροπή και εντοπισμός πρόσβασης ψεύτικων λογαριασμών,
- Ανταγωνιστικό όφελος – εξοικείωση με προηγμένες τεχνολογίες.

Για τους υπαλλήλους

- Ευκολία – δεν χρειάζεται να θυμούνται συνθηματικά,
- Ευκολία – γρηγορότερο login,
- Ασφάλεια – εμπιστευτικά αρχεία μπορούν να αποθηκευτούν με ασφάλεια.

Για τον καταναλωτή

- Ευκολία – δεν χρειάζεται να θυμάται συνθηματικά,
- Ασφάλεια – Οι online αγορές είναι ασφαλέστερες όταν εξουσιοδοτούνται με βιομετρική,
- Ασφάλεια – προσωπικά αρχεία και emails μπορούν να είναι ασφαλή,
- Αυξημένη εμπιστοσύνη - μειώνει το αίσθημα εξαπάτησης.

7.9 Προβλήματα Στην Απόκτηση Του Βιομετρικού Δείγματος

Η επίδοση των βιομετρικών συστημάτων διαφέρει ανάλογα με την ποιότητα του δείγματος και το περιβάλλον, μέσα στο οποίο παίρνεται το δείγμα αυτό. Έτσι γίνεται κατανοητό ότι ένα κακό δείγμα αναμένεται να επιδράσει αρνητικά στη σωστή αναγνώριση του χρήστη.

Οι κυριότεροι παράγοντες που ενδέχεται να προκαλέσουν πλήγμα στην διαδικασία λήψης του δείγματος είναι οι εξής:

Σάρωση δακτυλικού αποτυπώματος

- Κρύο δάκτυλο,
- Ξηρό ή λιπαρό δάκτυλο,

- Υψηλή ή χαμηλή υγρασία,
- Γωνία τοποθέτησης,
- Ασκούμενη πίεση,
- Θέση του δάκτυλου στην πλάκα,
- Κοψίματα στο δάκτυλο,
- Χειρονακτική εργασία που ενδεχομένως θα κατάστρεφε ή θα επηρέαζε το δακτυλικό αποτύπωμα (οικοδόμος, κηπουρός).

Σάρωση φωνής

- Κρύωμα ή ασθένεια, η οποία θα επηρέαζε τη φωνή,
- Διαφορετική συσκευή εγγραφής από αυτήν της εξακρίβωσης,
- Διαφορετικά περιβάλλοντα κατά την εγγραφή από αυτά της εξακρίβωσης,
- Χαμηλόφωνη ομιλία,
- Θόρυβος,
- Κακή τοποθέτηση του μικροφώνου ή της συσκευής εισόδου,
- Ποιότητα της συσκευής εισόδου.

Σάρωση προσώπου

- Αλλαγή στην κόμμωση,
- Αλλαγή στα τριχωτά χαρακτηριστικά του προσώπου (γενειάδα, μουστάκι),
- Συνθήκες φωτισμού.
- Προσθήκη καπέλου
- Προσθήκη ή αφαίρεση γυαλιών,
- Αλλαγή στο βάρος,
- Αλλαγή στη γωνία λήψης της φωτογραφίας του προσώπου,
- Μετακίνηση κεφαλιού,
- Ποιότητα της συσκευής εισόδου,
- Αλλαγή μεταξύ της κάμερας εγγραφής από αυτή της εξακρίβωσης (ποιότητα και τοποθέτηση).

Σάρωση ίριδας ματιού

- Μετακίνηση του κεφαλιού ή του ματιού,
- Γυαλιά,

- Χρωματιστοί φακοί επαφής.

Σάρωση αμφιβληστροειδή χιτώνα ματιού

- Μετακίνηση του κεφαλιού ή του ματιού,
- Γυαλιά.

Σάρωση χεριού

- Κοσμήματα,
- Αλλαγή στο βάρος,
- Επίδεσμος,
- Πρήξιμο στις αρθρώσεις.

Σάρωση υπογραφής

- Πολύ γρήγορη υπογραφή,
- Διαφορετικές θέσης υπογραφής (καθιστός, όρθιος).

8. Έξυπνες κάρτες (smart card)

8.1 Εισαγωγή

Την δεκαετία του '50 η εταιρεία Diners Club δημιούργησε ουσιαστικά τις πρώτες πιστωτικές κάρτες. Επρόκειτο για κάρτες που απλώς ανέγραφαν στην εμπρόσθια όψη τους τα στοιχεία του κατόχου για να υποδηλώσουν ότι το πρόσωπο που έφερε τη κάρτα ανήκε στην λέσχη προνομίων που η εταιρεία είχε συστήσει, αρχικώς για υψηλά ιστάμενα πρόσωπα. Σε μεταγενέστερες εκδόσεις τα στοιχεία του κατόχου εμφανίζονται σε ανάγλυφη μορφή για μεγαλύτερη κομψότητα και ασφάλεια, ενώ η μαγνητική λωρίδα στην οπίσθια όψη επιτρέπει την μαγνητική αποτύπωσή τους. Άλλες λέσχες υιοθέτησαν στη συνέχεια ανάλογες τακτικές, ωστόσο, κάρτες αυτού του είδους μπορούσαν ακόμα και εκείνη την εποχή να πλαστογραφηθούν με ευκολία.

8.2 Ιστορική αναδρομή

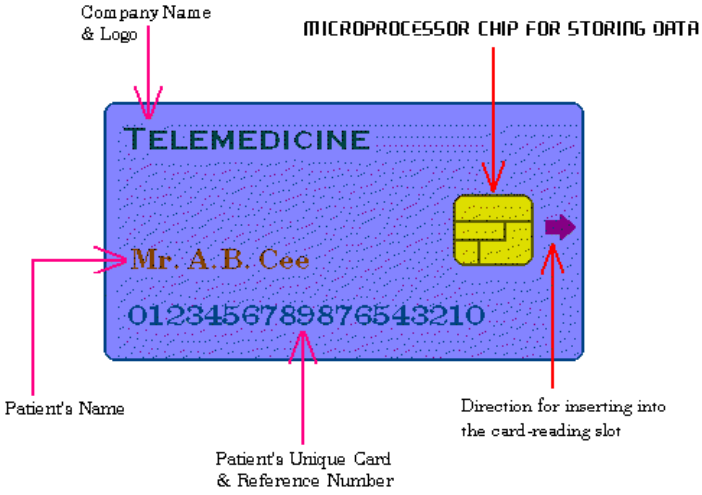
Οι έξυπνες κάρτες αναπτύχθηκαν ανεξάρτητα στη Γερμανία (1967), στην Ιαπωνία (1970) και στις ΗΠΑ (1972). Τα πρώτα χρόνια της δεκαετίας του '80, η Cartes Bancaire ανέπτυξε στη Γαλλία το δικό της ειδικό σύστημα ανάληψης μετρητών από τράπεζα που αξιοποιούσε μια πλαστική κάρτα. Το σύστημα, το οποίο αναπτύχθηκε σε συνεργασία με εταιρείες-κολοσσούς της εποχής στον χώρο της πληροφορικής, όπως οι Bull, Philips και Schumberger, ήταν σύστημα κάρτας με κύκλωμα, όπως είναι οι σημερινές έξυπνες κάρτες νέας γενιάς. Ωστόσο, το πιλοτικό πρόγραμμα ανέδειξε μοναδική αξιόπιστη λύση της εποχής την υιοθέτηση της μαγνητικής λωρίδας ως διεθνούς προτύπου. Ήταν το πλέον ασφαλές και οικονομικά συμφέρον για τα χρηματοπιστωτικά ιδρύματα, διασφαλίζοντας δύο σημαντικές απαιτήσεις: τη συμβατότητα και την αναγνωρισιμότητα της κάρτας. Οι γαλλικές τράπεζες διέθεσαν τις νεόκοπες κάρτες τόσο εντός της γαλλικής επικράτειας όσο και εκτός αυτής μέσω των τραπεζικών ιδρυμάτων στα οποία συμμετείχαν, ενώ πολύ σύντομα οι αμερικάνικες τράπεζες τις μιμήθηκαν. Αυτό είχε αποτέλεσμα η πιστωτική κάρτα και η κάρτα αναλήψεων να γίνει μέχρι τα μέσα της δεκαετίας του '80 μία καθημερινή πραγματικότητα για εκατομμύρια πολίτες σε δεκάδες χώρες.

8.3 Τι είναι έξυπνες κάρτες

Η Κοινωνία της Πληροφορίας συνεχώς εισάγει ζητήματα ασφάλειας και προστασίας των προσωπικών δεδομένων, καθιστώντας απαραίτητη τη χρήση τεχνολογικά προηγμένων και ασφαλών εφαρμογών έξυπνων καρτών. Οι έξυπνες κάρτες, που παρέχουν τη δυνατότητα συνδυασμού πολλαπλών εφαρμογών και αποτελούν αντικείμενο μελέτης και ανάπτυξης σε παγκόσμιο επίπεδο, ήδη εφαρμόζονται σε πλήθος δραστηριοτήτων της καθημερινής μας ζωής, όπως η πληρωμή εισιτηρίων, η ηλεκτρονική ταυτοποίηση, το ιατρικό αρχείο. Οι έξυπνες κάρτες διαχωρίζονται στις memory και microprocessor cards. Η memory card, που απλά αποθηκεύει δεδομένα, θεωρείται ένα είδος μικρής δισκέτας, με προαιρετική ασφάλεια. Η microprocessor card έχει την πρόσθετη ικανότητα να εμπλουτίζει, να διαγράφει και να διαχειρίζεται την πληροφορία που περιέχεται στη μνήμη της. Μοιάζει με μικροσκοπικό υπολογιστή, που περιλαμβάνει input και output port, λειτουργικό σύστημα και σκληρό δίσκο με ενσωματωμένα στοιχεία ασφάλειας. Οι έξυπνες κάρτες έχουν δύο διαφορετικούς τύπους διεπαφής, contact και contactless. Η contact card εισάγεται σε κατάλληλο reader προκειμένου να «διαβαστεί», ενώ η contactless έχει ενσωματωμένη κεραία, για επικοινωνία με το reader εξ αποστάσεως.

Σε επίπεδο εφαρμογών, οι κάρτες χωρίζονται σε τραπεζικές και μη τραπεζικές, αν και ουσιαστικά υπάρχουν κάποιες μικτές μορφές. Με βάση τον επίσημο διαχωρισμό τραπεζικές κάρτες θεωρούνται όσες έχουν πιστωτική (credit) ή χρεωστική (debit) εφαρμογή και μη τραπεζικές όλες οι υπόλοιπες (access cards, prepaid cards, gift cards, loyalty cards, multi merchandise cards κλπ).

Οι "έξυπνες" κάρτες, είναι πλαστικές κάρτες στο μέγεθος μιας πιστωτικής κάρτας με ολοκληρωμένο κύκλωμα ενσωματωμένο σε αυτήν και αποτελούν τη σημερινή ισχυρότερη τάση. Είναι το αποτέλεσμα της ταυτόχρονης βελτίωσης των πλαστικών καρτών και των microchip.



8.4 Από τις μαγνητικές στις "έξυπνες" κάρτες

Με τον όρο **μαγνητική κάρτα** εννοούμε μια πλαστική κάρτα συνήθως από πλαστικό υλικό (PVC ή ABS), με μια λωρίδα από μαγνητικό υλικό επικολλημένη στην οπίσθια όψη της. Αυτή η μαγνητική επίστρωση φέρει όλες τις πληροφορίες της κάρτας και χωρίζεται σε τρία τμήματα που ονομάζονται tracks. Στις τραπεζικές εφαρμογές το δεύτερο track περιέχει τον αριθμό της κάρτας, την ημερομηνία λήξης, και κάποια πληροφορία σχετικά με τον τρόπο που πρέπει να χειριστεί την κάρτα το τερματικό. Στο track 1 βρίσκεται το όνομα του κατόχου της κάρτας, ενώ το τρίτο track, που ονομάζεται watermark track, χρησιμοποιείται από τους χρηματοπιστωτικούς οργανισμούς ορισμένων χωρών σε μια προσπάθεια να αυξηθεί η ασφάλεια των παρεχομένων υπηρεσιών. Για τον ίδιο σκοπό, έχουν αναπτυχθεί και εφαρμόζονται διάφορες τεχνικές σήμανσης (holomagnetics, magnetic signatures κλπ), αλλά καμία από αυτές δεν έχει τύχει ευρείας αποδοχής έως τώρα.

Τα δεδομένα που βρίσκονται στο δεύτερο track (όνομα κατόχου, ημερομηνία λήξης, αριθμός κάρτας), βρίσκονται τυπωμένα -σε κάποιες περιπτώσεις με ανάγλυφα γράμματα- στην πρόσθια όψη της κάρτας. Όσον αφορά στα τεχνικά χαρακτηριστικά της κάρτας, όπως μέγεθος και ύψος γραμμάτων, τρόπος εγγραφής κλπ, αυτά καθορίζονται από διεθνή standards (ISO 7810-7811).

Η δεύτερη μεγάλη κατηγορία καρτών είναι οι λεγόμενες **κάρτες IC** (Integrated Circuit cards, ή κάρτες ολοκληρωμένου κυκλώματος), οι οποίες είναι πιο γνωστές εμπορικά ως **smart cards** ("έξυπνες κάρτες"). Πρόκειται για μια πλαστική κάρτα στο

μέγεθος μιας συμβατικής αντίστοιχης, η οποία ωστόσο φέρει ένα μικροκύκλωμα ενσωματωμένο στην πρόσθια όψη της. Το μικροκύκλωμα αυτό μπορεί να είναι μια απλή μνήμη, ή μπορεί να περιλαμβάνει έναν πλήρη μικροελεγκτή με κεντρική μονάδα επεξεργασίας (CPU), μνήμη, μονάδες εισόδου-εξόδου.

Πολλές έξυπνες κάρτες διαθέτουν ένα μικρό πληκτρολόγιο (όχι απαραίτητα όμως) και μια μικροσκοπική οθόνη στην οποία εμφανίζεται μια μοναδική τιμή, π.χ. ένας οκταψήφιος αριθμός. Αυτή η τιμή αλλάζει περιοδικά (π.χ. κάθε λεπτό) από μια δυναμική γεννήτρια κωδικών μέσα στην κάρτα. Μερικές κάρτες δείχνουν και τον εναπομείναντα χρόνο μέχρι την επόμενη αλλαγή του κωδικού. Ο χρήστης για να αποκτήσει πρόσβαση στο πληροφοριακό σύστημα πρέπει να εισαγάγει τον αριθμό που εμφανίζεται στην κάρτα όπως επίσης και τον προσωπικό του κωδικό πρόσβασης.

Άλλες δυνατότητες

Πέρα από την "ευφυΐα" τους, οι πλαστικές κάρτες έχουν εξελιχθεί και σε άλλους τομείς εξίσου σημαντικούς, για την ενίσχυση της πιστότητας των πελατών μιας επιχείρησης. Μεγάλο ρόλο στην υιοθέτηση καρτών από τους καταναλωτές παίζουν οι υπηρεσίες προσωποποίησης και γενικά της εικαστικής εμφάνισης της κάρτας, που μπορούν πλέον να προσφέρονται άμεσα, εύκολα και αξιόπιστα, ακόμα και από το ίδιο το κατάστημα που τις εκδίδει. Μια συνέπεια της παρεχόμενης ευκολίας στην εξατομικευμένη προσαρμογή κάθε εκδιδόμενης κάρτας είναι η επιχείρηση που υιοθετεί μια τέτοια πρακτική να χρησιμοποιεί την εφαρμογή και εσωτερικά. Μπορεί δηλαδή να δώσει "κάρτες-ταυτότητες", με ή χωρίς έγχρωμη φωτογραφία, στο προσωπικό, προσθέτοντας έτσι έναν περισσότερο προσωπικό τόνο στην εταιρική τους εμφάνιση (στολή) αλλά και στις συναλλαγές τους με τους πελάτες. Η ίδια κάρτα-ταυτότητα μπορεί να χρησιμοποιηθεί για χρονοσήμανση της παρουσίας (με συνακόλουθη αποφυγή του χειροκίνητου υπολογισμού ωρών και υπερωριών εργασίας), για έλεγχο πρόσβασης (άνοιγμα θυρών) και τέλος για ασφαλή πρόσβαση στο εταιρικό δίκτυο και τους σταθμούς εργασίας ή τις ηλεκτρονικές ταμειακές μηχανές. Έτσι, μία κάρτα μετατρέπεται σε πολυχρηστική, μειώνοντας σημαντικά το κόστος απόσβεσης της σχετικής επένδυσης (ROI).

8.5 Το μέλλον

Το μέλλον στο θέμα των πλαστικών καρτών συνίσταται όχι μόνο στην μετάβαση της τεχνολογίας από τις κοινές πλαστικές και μαγνητικές κάρτες σε έξυπνες κάρτες, αλλά και στην δημιουργία νέων επιχειρηματικών μοντέλων και εφαρμογών που θα εξυπηρετούν με τον καλύτερο τρόπο πολλαπλούς εμπλεκόμενους. Χαρακτηριστικό είναι το παράδειγμα της Visa Europe η οποία, σε συνεργασία με τις Barlaycard και την Transport for London, επιλέχτηκε για να παρέχει την τεχνολογία της πρώτης κάρτας ανέπαφων συναλλαγών για μετακινήσεις και πληρωμές στο Ηνωμένο Βασίλειο. Σε λιγότερο από ένα δευτερόλεπτο, η νέα Visa Barclaycard θα επιτρέπει την πραγματοποίηση ασφαλών καθημερινών συναλλαγών αξίας μικρότερης των 10 λιρών, όπως η αγορά καφέ και σάντουιτς, ενώ ταυτόχρονα θα λειτουργεί ως passo για πρόσβαση στο μετρό και στο δίκτυο των λεωφορείων του Λονδίνου. Η πληρωμή πραγματοποιείται απλά κρατώντας την κάρτα μπροστά στο τερματικό για ανέπαφες συναλλαγές (contactless card reader) και όχι με το πέρασμα της κάρτας από ένα POS τερματικό, όπως γίνεται συνήθως. Η νέα κάρτα προσφέρει ευκολία και ταχύτητα στις συναλλαγές, ενώ μειώνει τον όγκο του πλαστικού χρήματος που κάποιος μεταφέρει στο πορτοφόλι του.

8.6 Περιοχές εφαρμογών έξυπνων καρτών

Οι περιοχές εφαρμογών των έξυπνων καρτών αυξάνονται με ταχύτατους ρυθμούς. Ωστόσο, τα κυριότερα πεδία εφαρμογής είναι:

8.6.1 Διαχείριση πληροφοριών

Ο ιδιωτικός και ο δημόσιος τομέας προχωρούν μαζικά σε λύσεις που προϋποθέτουν διαχείριση πληροφοριών μέσω δικτύων (intranets, extranets, internet). Η άμεση και ασφαλής πρόσβαση στην πληροφορία διασφαλίζει ακεραιότητα και προστασία σε ευαίσθητα πληροφοριακά δεδομένα. Οι έξυπνες κάρτες αποτελούν την ενδεδειγμένη λύση, επιτρέποντας την ασφαλή πρόσβαση και εξουσιοδότηση των χρηστών σε υπηρεσίες, την αποθήκευση ψηφιακών πιστοποιητικών, τη δημιουργία credentials και passwords και την κρυπτογράφηση ευαίσθητων δεδομένων.

8.6.2 Εμπορικές Εφαρμογές

Οι έξυπνες κάρτες αποτελούν τη βάση για νέες υπηρεσίες B2B και B2C, αποθηκεύοντας πληροφορία, χρηματικά ποσά και λειτουργίες για χρήση σε εφαρμογές όπως η πιστοποίηση, ο έλεγχος πρόσβασης, οι οικονομικές συναλλαγές, η έκδοση εισιτηρίων, οι χώροι στάθμευσης και οι εισπράξεις. Η δυνατότητα αποθήκευσης και συνδυασμού πολλαπλών εφαρμογών σε μια κάρτα επιτρέπει εταιρικές συνεργασίες, που σκοπό έχουν την παροχή προηγμένων υπηρεσιών.

8.6.3 Ασύρματες Επικοινωνίες

Οι έξυπνες κάρτες χρησιμοποιούνται στα GSM συστήματα των κινητών τηλεφώνων, καθώς και στα κινητά τηλέφωνα τρίτης γενιάς, για την αποθήκευση των προσωπικών στοιχείων και προτιμήσεων των χρηστών. Επιτρέπουν την ασφαλή ταυτοποίηση του χρήστη, την περιαγωγή μεταξύ δικτύων και την παροχή ασφαλών εφαρμογών προστιθέμενης αξίας (mobile commerce, location-based information services).

Πλεονεκτήματα

- Οι έξυπνες κάρτες μπορούν να κρυπτογραφούν τα δεδομένα που εμπεριέχονται στο chip τους, παρέχοντας ένα ιδιαίτερα σημαντικό επίπεδο ασφάλειας συγκριτικά με τις παραδοσιακές κάρτες.
- Η πρόσβαση με τις έξυπνες κάρτες είναι εφικτή και σε γεωγραφικές τοποθεσίες όπου η on-line επικοινωνία δεν είναι διαθέσιμη.
- Η σωστή χρήση των έξυπνων καρτών μειώνει την πιθανότητα εξαπάτησης ή υποκλοπής.
- Η έξυπνη κάρτα μπορεί να προσφέρει αυθεντικοποίηση στον κάτοχο της.
- Στις έξυπνες κάρτες μπορεί να συνυπάρχουν πολλαπλές εφαρμογές. Κάθε αλλαγή των στοιχείων κάποιας εφαρμογής μπορεί να γίνεται ηλεκτρονικά και μετά την έκδοση της κάρτας, χωρίς να χρειάζεται να ακυρωθεί η κάρτα και να εκδοθεί νέα.

Μειονεκτήματα

- Το κόστος της έξυπνης κάρτας είναι σαφώς υψηλότερο από το αντίστοιχο των απλών μαγνητικών καρτών. Επιπλέον για τη χρησιμοποίηση των έξυπνων καρτών, ένα σημαντικό κόστος προστίθεται λόγω της αναγκαίας αγοράς αναγνώστη καρτών.
- Έλλειψη εξοπλισμού από πολίτες και μικρές εταιρείες.
- Το πλήθος των χρηστών αισθάνονται ότι οι τεχνολογίες έξυπνων καρτών δεν είναι αρκετά ώριμες και υπάρχει πιθανότητα να αλλάξουν στο κοντινό μέλλον.
- Μερικές κατηγορίες εργαζομένων-χρηστών θεωρούν ότι η χρήση των έξυπνων καρτών επιφέρει αλλαγές συνηθειών στην εργασία και υπάρχει φόβος επιβολής πρόσθετων ελέγχων με την εφαρμογή έξυπνων καρτών.
- Οι έξυπνες κάρτες μπορούν να μειώσουν την πρόσβαση και τους πόρους σε εκείνους που είναι τεχνολογικά αναλφάβητοι ή αδιάφοροι.
- Υπάρχει έλλειψη ενημέρωσης του κοινού και προκατάληψη στην αξιοποίηση και στην εμπορική εφαρμογή νέων τεχνολογιών.

Σύναψη

Η Κοινωνία της Πληροφορίας καθιστά απαραίτητη τη χρήση τεχνολογικά προηγμένων και ασφαλών εφαρμογών έξυπνων καρτών. Οι έξυπνες κάρτες παρέχουν τη δυνατότητα συνδυασμού πολλαπλών εφαρμογών και αποτελούν αντικείμενο μελέτης και ανάπτυξης σε παγκόσμιο επίπεδο.

9. Κρυπτογραφία

9.1 Βασικές έννοιες

Η κρυπτογράφηση είναι μια διαδικασία με την οποία ένα μήνυμα (plaintext) μετατρέπεται σε ένα άλλο μήνυμα (ciphertext ή cryptogram) χρησιμοποιώντας μια μαθηματική συνάρτηση (αλγόριθμος) και ένα ειδικό κωδικό κρυπτογράφησης που λέγεται κλειδί (key).

Η κρυπτογράφηση έρχεται να εξασφαλίσει το απόρρητο των προσωπικών πληροφοριών. Πρόκειται για μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων. Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι. Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών. Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext), ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext).

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου. Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική, όταν μόνο τα άτομα που συμμετέχουν σε αυτήν μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος. Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση, που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς τη χρήση του αντίστροφου αλγόριθμού κρυπτογράφησης.

Σε ορισμένους κρυπτογραφικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί τόσο για τη διαδικασία της κρυπτογράφησης, όσο και της αποκρυπτογράφησης, ενώ σε άλλους έχουμε διαφορετικά κλειδιά.

Η διαδικασία της κρυπτογράφησης συμβολίζεται ως εξής:

C = EK (P), όπου

P είναι το προς κρυπτογράφηση κείμενο

K είναι το κλειδί και

C είναι το κρυπτογράφημα.

Η αντίστροφη διαδικασία, δηλαδή η αποκρυπτογράφηση συμβολίζεται ως εξής:

DK (EK (P)) = P, όπου

Ε και D είναι μαθηματικές συναρτήσεις.

Η κρυπτογράφηση δεν είναι νέα υπόθεση. Ακόμη και στην αρχαιότητα χρησιμοποιούνταν διάφορες μέθοδοι κρυπτογράφησης, με χαρακτηριστικότερη αυτή του Ιουλίου Καίσαρα, ο οποίος επινόησε έναν απλό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί, π.χ. το 3. Η κρυπτογράφηση δηλαδή του μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται τρεις θέσεις δεξιότερά του στο αλφάβητο. Διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί, παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Παλαιότερα χρησιμοποιούσαν την κρυπτογράφηση αποκλειστικά για στρατιωτικούς σκοπούς. Στη σημερινή κοινωνία της πληροφορίας, η κρυπτογράφηση είναι ένα από τα βασικά εργαλεία διατήρησης του απορρήτου των μηνυμάτων με όλα τα προφανή πλεονεκτήματα. Ως αποτέλεσμα, η σύγχρονη κρυπτογραφία αποτελεί κάτι περισσότερο από απλή κρυπτογράφηση και αποκρυπτογράφηση δεδομένων. Για παράδειγμα, η πιστοποίηση αποτελεί μια εξίσου θεμελιώδη έννοια που συνδέεται άμεσα με την κρυπτογραφία. Όταν υπογράφεται ένα έγγραφο, είναι απαραίτητο να υπάρχουν μηχανισμοί με τους οποίους να μπορούμε να πιστοποιήσουμε τον κάτοχο του εγγράφου. Η κρυπτογραφία μας παρέχει μηχανισμούς για τέτοιες διαδικασίες. Η ψηφιακή υπογραφή (digital signature) «συνδέει» ένα έγγραφο με τον κάτοχο ενός συγκεκριμένου κλειδιού, ενώ η ψηφιακή χρονοσφραγίδα «συνδέει» ένα έγγραφο με το χρόνο της δημιουργίας του.

9.2 Στοιχεία Κρυπτογράφησης

Υπάρχουν πολλοί διάφοροι τρόποι με τους οποίους μπορούμε να κρυπτογραφήσουμε και να αποκρυπτογραφήσουμε μια πληροφορία σε έναν

υπολογιστή. Όλα τα συστήματα κρυπτογράφησης μοιράζονται κοινά στοιχεία τα οποία είναι:

Plaintext: Η πληροφορία την οποία επιθυμούμε να κρυπτογραφήσουμε.

Ciphertext: Η πληροφορία αφού αυτή κρυπτογραφήθηκε.

Αλγόριθμος κρυπτογράφησης: Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών. Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγορίθμου, τόσο μειώνεται η πιθανότητα να τον διαβάλλει κάποιος. Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με το κλειδί για την κρυπτογράφηση του απλού κειμένου. Το ίδιο απλό κείμενο κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά.

Κλειδιά κρυπτογράφησης: Τα κλειδιά κρυπτογράφησης χρησιμοποιούνται από τον αλγόριθμό κρυπτογράφησης για να ορίσουν πως τα δεδομένα είναι κρυπτογραφημένα ή αποκρυπτογραφημένα. Είναι μία σειρά ψηφίων (bits) που χρησιμοποιείται ως είσοδος στην συνάρτηση κρυπτογράφησης και διαδραματίζει καθοριστικό ρόλο στην όλη διαδικασία. Καθορίζει τις ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που εκτελούνται από τον αλγόριθμο κρυπτογράφησης.

Μήκος κλειδιών: Όπως και με τα password, τα κλειδιά κρυπτογράφησης έχουν ένα προκαθορισμένο μήκος. Τα μακρύτερα κλειδιά είναι πιο δύσκολο να τα μαντέψει κάποιος από τα μικρότερα γιατί υπάρχουν περισσότερα πιθανά κλειδιά που πρέπει να δοκιμάσει κάποιος επιτιθέμενος, για να βρει το σωστό. Μερικά συστήματα κρυπτογράφησης μας επιτρέπουν να χρησιμοποιούμε διαφορετικό μήκος κλειδιών και μερικά μας επιτρέπουν μεταβλητού μήκους κλειδιών.

9.3 Τεχνικές Κρυπτογράφησης

Υπάρχουν διάφοροι μέθοδοι κρυπτογραφίας. Όμως, γενικά ταξινομούνται σε κατηγορίες ανάλογα με τα κλειδιά και τον τρόπο κρυπτογράφησης των μηνυμάτων.

Με βάση τα κλειδιά:

Μυστικού ή Συμμετρικού Κλειδιού (Symmetric-Key): Χρησιμοποιούν το ίδιο μυστικό κλειδί για κρυπτογράφηση και για αποκρυπτογράφηση.

Δημοσίου ή Ασύμμετρου Κλειδιού (Public or Asymmetric-Key): Χρησιμοποιούν διαφορετικό κλειδί για κρυπτογράφηση (δημόσιο κλειδί αποστολέα) και διαφορετικό για αποκρυπτογράφηση (προσωπικό κλειδί παραλήπτη).

Με βάση τον τρόπο κρυπτογράφησης των μηνυμάτων:

Δέσμης (Block ciphers): Μετατρέπουν το αναγνώσιμο μήνυμα σε δέσμες, Π.χ. των 64 bits ή πολλαπλασίων τους, τις οποίες στη συνέχεια κρυπτογραφούν με μια περίπλοκη συνάρτηση κρυπτογράφησης. Σε μια σύνοδο, όλες οι ομάδες δεδομένων από το ίδιο αρχείο κρυπτογραφούνται με το ίδιο κλειδί.

Ροής (Stream ciphers): Κρυπτογραφούν το αναγνώσιμο μήνυμα ανά bit/byte κάθε φορά, με μια απλή κρυπτογραφική συνάρτηση. Η κρυπτογράφηση για μια ροή γίνεται με ένα σταθερά εναλλασσόμενο κλειδί, οπότε το κατά πόσον είναι ανθεκτική η παρεχόμενη κρυπτογράφηση εξαρτάται από την γεννήτρια κλειδιών της ροής.

9.3.1 Συμμετρική Κρυπτογραφία (Κρυπτογραφία ιδιωτικού κλειδιού)

Στη συμμετρική κρυπτογραφία οι αλγόριθμοι που χρησιμοποιούνται ονομάζονται αλγόριθμοι μυστικού κλειδιού (secret key algorithms) ή συμμετρικοί αλγόριθμοι (symmetric algorithms). Οι αλγόριθμοι αυτοί χρησιμοποιούν το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση το οποίο ονομάζεται ιδιωτικό κλειδί. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέλη και, κατά συνέπεια απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Η παραγωγή, μετάδοση και αποθήκευση των κλειδιών ονομάζεται διαχείριση κλειδιού. Επειδή όλα τα κλειδιά στα συμμετρικά κρυπτοσυστήματα πρέπει να είναι απόρρητα, η συμμετρική κρυπτογραφία αντιμετωπίζει δυσκολία στο να παρέχει ασφαλή διαχείριση κλειδιού, ιδιαίτερα σε ανοικτά συστήματα με μεγάλο αριθμό χρηστών. Το πλέον δημοφιλές κρυπτοσύστημα ιδιωτικού κλειδιού είναι το DES (Data Encryption Standard).

Τα συστήματα συμμετρικής κρυπτογράφησης προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών. Τέτοια συστήματα έχουν αναπτυχθεί και ήδη χρησιμοποιούνται, με πιο διαδεδομένο το σύστημα Kerberos, του MIT (Massachusetts Institute of Technology).

Αλγόριθμοι Συμμετρικής Κρυπτογράφησης

Οι αλγόριθμοι αυτοί χρησιμοποιούνται για μεγάλο όγκο δεδομένων ή επίσης για δεδομένα με συνεχόμενη ροή. Είναι σχεδιασμένοι να εκτελούνται με ταχύτητα και έχουν μεγάλο αριθμό πιθανόν κλειδιών. Οι πιο συνηθισμένοι αλγόριθμοι συμμετρικού κλειδιού είναι οι παρακάτω:

DES (Data Encryption Standard): Είναι ο πιο γνωστός αλγόριθμος. Αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών. Κρυπτογραφεί ανά τμήματα (blocks) των 64 bits (8 bytes) με 16 επαναλήψεις για κάθε τμήμα, χρησιμοποιώντας ένα κλειδί των 56 bits. Αυτό σημαίνει ότι αν κάποιος θέλει να σπάσει την κωδικοποίηση πρέπει να δοκιμάσει 2^{56} διαφορετικά κλειδιά. Μια παραλλαγή του DES η οποία χρησιμοποιείται σήμερα είναι ο Triple-DES ο οποίος κρυπτογραφεί τρεις φορές το ίδιο κείμενο με τον αλγόριθμο DES, αλλά χρησιμοποιώντας διαφορετικό κλειδί για κάθε κρυπτογράφηση.

DESX: Είναι μια απλή μετατροπή του DES αλγορίθμου για να βελτιώσει την ασφάλεια και να κάνει την αναζήτηση κλειδιού δυσκολότερη.

IDEA (International Data Encryption Algorithm): Αναπτύχθηκε στην Ζυρίχη της Ελβετίας, από τους James L. Massey και τον Xuejia Lai και δημοσιεύτηκε το 1990. Είναι δομημένος όπως ο αλγόριθμος DES, κρυπτογραφεί τμήματα των 64 bits (με 8 επαναλήψεις για κάθε τμήμα) χρησιμοποιώντας ένα κλειδί μήκους 128 bits το οποίο τον κάνει και πιο ασφαλή σε σχέση με τον DES.

RC2 και RC4: Οι αλγόριθμοι RC2 και RC4 αναπτύχθηκαν από τον Ronald Rivest. Είναι γρηγορότεροι από τον DES και χρησιμοποιούν κλειδιά μήκους 1-bit έως 2048- bit. Συχνά το μήκος τους όμως φτάνει τα 40-bit.

RC5: Κι αυτός ο αλγόριθμος αναπτύχθηκε από τον Ronald Rivest και δημοσιεύτηκε το 1994. Ο RC5 επιτρέπει από τον χρήστη να ορίζει το μήκος του κλειδιού, το μέγεθος των δεδομένων και το πόσες φορές να γίνει η κρυπτογράφηση.

9.3.2 Ασύμμετρη Κρυπτογραφία (Κρυπτογραφία Δημοσίου Κλειδιού)

Η ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημόσιου κλειδιού παρουσιάστηκε για πρώτη φορά το 1976 από τους Whitfield Diffie και Martin Hellman, προκειμένου να επιλυθεί το πρόβλημα διαχείρισης κλειδιού που υπήρχε με

την κρυπτογραφία ιδιωτικού κλειδιού. Το 1977 οι Rivest, Shamir και Adleman δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

Στην ασύμμετρη κρυπτογράφηση, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση: το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα. Τα κλειδιά αυτά δημιουργούνται με τρόπο ώστε να έχουν τις εξής ιδιότητες:

- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.
- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

Προκειμένου να επιτευχθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία, συνεπώς μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δεν μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκωδικοποιήσει το μήνυμα, γι' αυτό και η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογράφηση παρέχει μεγαλύτερη ασφάλεια από ό,τι η συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι που χρησιμοποιεί είναι πολύ βραδύτεροι από τους αντίστοιχους της συμμετρικής.

Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας

Οι αλγόριθμοι δημοσίου κλειδιού στηρίζονται στα μαθηματικά. Αναπτύσσοντας έναν τέτοιο αλγόριθμο απαιτείται να λυθεί ένα μαθηματικό πρόβλημα με πολλές ιδιότητες. Γι’ αυτό το λόγο υπάρχουν λιγότερα ασύμμετρα κρυπτογραφικά συστήματα από ότι συμμετρικά. Για να αναπτύξουμε ένα καινούργιο αλγόριθμο συμμετρικού

κλειδιού θα πρέπει να βρούμε έναν νέο ασφαλή τρόπο να αλλάζουμε την είσοδο. Οι πιο γνωστοί αλγόριθμοι δημόσιου κλειδιού είναι οι παρακάτω:

RSA: Ο RSA είναι ένας αλγόριθμος δημοσίου κλειδιού που αναπτύχθηκε το 1977. Είναι ένας από τους πιο δημοφιλείς αλγορίθμους δημοσίου κλειδιού και προσφέρει τη δυνατότητα κρυπτογράφησης και πιστοποίησης. Αναπτύχθηκε από τους καθηγητές του MIT, τους Ronald Rivest, Adi Shamir και Leonard Adleman. Τα δημόσια και ιδιωτικά κλειδιά που χρησιμοποιεί κατασκευάζονται με τη χρήση δυο πολύ μεγάλων πρώτων αριθμών και ο αλγόριθμος στηρίζει τη δύναμή του στη δυσκολία που υπάρχει όσον αφορά στο να παραγοντοποιηθούν πολύ μεγάλοι αριθμοί. Ο RSA μπορεί να χρησιμοποιηθεί και για ψηφιακή υπογραφή αντιστρέφοντας απλά τον τρόπο με τον οποίο χρησιμοποιούνται τα κλειδιά (το ιδιωτικό για αποκρυπτογράφηση και υπογραφή, το δημόσιο για κρυπτογράφηση και πιστοποίηση υπογραφής).

Diffie-Hellman: Ο Diffie-Hellman αλγόριθμος αναπτύχθηκε το 1976 και επιτρέπει σε δύο άτομα να ανταλλάξουν με ασφαλή τρόπο ένα μυστικό κλειδί σε ένα μη ασφαλές μέσο. Είναι ένα σύστημα για ανταλλαγή κρυπτογραφικών κλειδιών ανάμεσα σε ενεργά μέρη. Το Diffie-Hellman δεν είναι ακριβώς μια μέθοδος κρυπτογράφησης και αποκρυπτογράφησης, αλλά μια μέθοδος ανάπτυξης και ανταλλαγής ενός μοιρασμένου μυστικού κλειδιού σε ένα δημόσιο κανάλι επικοινωνίας. Στην πραγματικότητα, τα δύο μέρη συμφωνούν σε μερικές κοινές αριθμητικές τιμές, και τότε το κάθε μέρος δημιουργεί ένα κλειδί. Οι μαθηματικοί μετασχηματισμοί των κλειδιών ανταλλάσσονται. Κάθε μέρος μπορεί τότε να υπολογίσει ένα τρίτο κλειδί συνόδου (session key) το οποίο δεν μπορεί εύκολα να παραχθεί από έναν επιτιθέμενο που γνωρίζει και των δύο τις αριθμητικές τιμές.

ElGamal: Ο δημιουργός αυτού του αλγόριθμου είναι ο Taher ElGamal, είναι ένα κρυπτογραφικό σύστημα δημόσιου κλειδιού που είναι βασισμένο στο πρωτόκολλο ανταλλαγής κλειδιών των Diffie-Hellman. Ο ElGamal χρησιμοποιείται για κρυπτογράφηση και για ψηφιακές υπογραφές με τον ίδιο τρόπο όπως ο RSA.

DSS (Digital Signature Standard): Αναπτύχθηκε από την National Security Agency (NSA) και εφαρμόστηκε σαν ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών FIPS (Federal Information Processing Standard) από την NIST (National Institute for Standards and Technology). Ο DSS είναι βασισμένος στον αλγόριθμο ψηφιακών υπογραφών (DSA). Αν και ο DSA επιτρέπει κλειδιά οποιουδήποτε μήκους, μόνο κλειδιά ανάμεσα σε 512 και 1024 bits επιτρέπονται στον

DSS. Όπως αναφέρθηκε, ο DSS μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές, αν και είναι πιθανό να χρησιμοποιήσει DSA εφαρμογές για την κρυπτογράφηση επίσης.

9.3.3 Υβριδική Κρυπτογραφία δημοσίου/ιδιωτικού κλειδιού

Η υβριδική κρυπτογραφία δημοσίου/ιδιωτικού κλειδιού δεν είναι μια διαφορετική μέθοδος καθότι αποτελεί συνδυασμό των δύο παραπάνω μεθόδων. Οι δύο βασικές μέθοδοι κρυπτογραφίας χρησιμοποιούνται συμπληρωματικά, με την κάθε μια να εκτελεί διαφορετικές λειτουργίες.

Αν και είναι πολύ βραδύτερη από τα συμμετρικά συστήματα, το σύστημα δημόσιου κλειδιού/ιδιωτκού κλειδιού επιλύει έξυπνα το πρόβλημα που ταλανίζει τα συμμετρικά κρυπτοσυστήματα δηλαδή την ανταλλαγή μυστικών κλειδιών.

Δεν υπάρχει όμως ανάγκη να χάσουμε την ταχύτητα των κρυπτοσυστημάτων μυστικού κλειδιού, απλώς επειδή τα μυστικά κλειδιά δεν μπορούν να ανταλλαγούν με ασφάλεια. Τα υβριδικά κρυπτοσυστήματα χρησιμοποιούν κρυπτογράφηση δημόσιου κλειδιού για να ανταλλάσσουν μυστικά κλειδιά και μετά χρησιμοποιούν τα μυστικά κλειδιά για να καθορίσουν ένα κανάλι επικοινωνίας. Σχεδόν όλα τα σύγχρονα κρυπτοσυστήματα λειτουργούν με αυτόν τον τρόπο.

Όταν δύο άνθρωποι ή συσκευές πρέπει να καθορίσουν ένα ασφαλές κανάλι για επικοινωνία, ο ένας τους πρέπει να παράγει ένα τυχαίο μυστικό κλειδί και μετά να κρυπτογραφήσει το μυστικό κλειδί χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Το κρυπτογραφημένο κλειδί στέλνεται κατόπιν στον παραλήπτη. Ακόμη και αν υποκλαπεί το κλειδί, μόνο ο πραγματικός παραλήπτης, χρησιμοποιώντας το δικό του ιδιωτικό κλειδί, μπορεί να αποκρυπτογραφήσει το μήνυμα που περιέχει το μυστικό κλειδί. Όταν και τα δύο μέρη έχουν το μυστικό κλειδί, μπορούν να αρχίσουν να χρησιμοποιούν ένα ταχύτερο κρυπτοσύστημα μυστικού κλειδιού για να ανταλλάσσουν μυστικά μηνύματα.

9.4 Πλεονεκτήματα και Μειονεκτήματα της Συμμετρικής και Ασύμμετρης Κρυπτογραφίας

Η κρυπτογράφηση ιδιωτικού κλειδιού είναι γενικά γρηγορότερη από την κρυπτογράφηση δημοσίου κλειδιού και ευκολότερη στην εφαρμογή. Αντίστοιχες υλοποιήσεις της συμμετρικής κρυπτογραφίας μπορούν να εκτελούνται 1000 έως και 10000 φορές ταχύτερα από την κρυπτογράφηση δημόσιου κλειδιού και γι' αυτόν τον λόγο χρησιμοποιείται συνήθως για την κρυπτογράφηση μεγάλου όγκου δεδομένων. Αυτό ισχύει επειδή τα μεγέθη των κλειδιών που χρησιμοποιούνται είναι πολύ μικρότερα απ' ότι με την κρυπτογραφία δημόσιου κλειδιού.

Το βασικό πλεονέκτημα της κρυπτογραφίας δημόσιου κλειδιού είναι η αυξημένη ασφάλεια που παρέχει. Το πλεονέκτημα αυτό απορρέει από το γεγονός ότι το ιδιωτικό κλειδί, στην ασύμμετρη κρυπτογραφία, δε χρειάζεται ποτέ να μεταδοθεί ή να αποκαλυφθεί σε οποιονδήποτε. Αντίθετα, στα συστήματα κρυπτογράφησης ιδιωτικού κλειδιού, το ιδιωτικό κλειδί πρέπει είτε να μεταδοθεί με κάποιο συμβατικό τρόπο, είτε να μεταδοθεί ηλεκτρονικά μέσω ενός καναλιού μετάδοσης. Κατά τη μετάδοση του ιδιωτικού κλειδιού, υπάρχει πάντα ο κίνδυνος να ανακαλυφθεί το κλειδί από μη εξουσιοδοτημένα άτομα και κατά συνέπεια να 'σπάσει' (όπως λέγεται) η κρυπτογράφηση. Για το λόγο αυτό, η μετάδοση του ιδιωτικού κλειδιού στα συμμετρικά συστήματα αποτελεί βασικό μειονέκτημα τους.

Ένα άλλο σημαντικό πλεονέκτημα των συστημάτων δημοσίου κλειδιού είναι ότι παρέχουν επιπρόσθετα μια μέθοδο για ψηφιακές υπογραφές. Η πιστοποίηση μέσω των συστημάτων ιδιωτικού κλειδιού προϋποθέτει το 'μοίρασμα κάποιου μυστικού' και μερικές φορές απαιτείται και η εμπιστοσύνη από κάποιο τρίτο πρόσωπο. Αυτό δίνει εν δυνάμει τη δυνατότητα στον αποδέκτη να 'αρνείται' προηγούμενες πιστοποιήσεις μηνυμάτων, ισχυριζόμενος ότι το 'κοινό μυστικό' διέρρευσε από ένα από τα πρόσωπα που το γνώριζαν. Για παράδειγμα, το σύστημα πιστοποίησης ταυτότητας Κέρβερος (KAS-Kerberos Authentication System) χρησιμοποιεί μια κεντρική Βάση Δεδομένων στην οποία κρατάει αντίγραφα των ιδιωτικών κλειδιών όλων των χρηστών της. Είναι προφανές πως μια πιθανή προσβολή της βάσης δεδομένων θα προκαλέσει αστοχία του συστήματος. Από την άλλη πλευρά, στα συστήματα δημόσιου κλειδιού, ο κάθε χρήστης έχει ο ίδιος την ευθύνη προστασίας του προσωπικού του ιδιωτικού κλειδιού.

9.5 Ασφάλεια Κρυπτογραφικού Συστήματος

Η ασφάλεια ενός κρυπτογραφικού συστήματος βρίσκεται στο κλειδί του αλγόριθμου (στους αλγόριθμους δημοσίου κλειδιού βρίσκετε στο ιδιωτικό κλειδί). Γι' αυτό το λόγο, οι αλγόριθμοι καθ' αυτοί δε χρειάζεται να μένουν κρυφοί. Υπάρχει μεγάλη ποικιλία αλγόριθμων που διατίθενται στο διαδίκτυο, και μπορούν να επιλεχθούν ασφαλώς, αρκεί τα κλειδιά που χρησιμοποιούνται να παραμένουν μυστικά. Εάν ένα μυστικό κλειδί γίνει γνωστό, μόνο τα μηνύματα που είναι κρυπτογραφημένα με αυτό το κλειδί μπορούν να αποκρυπτογραφηθούν (συμμετρικός αλγόριθμος) ή τα μηνύματα που είναι κρυπτογραφημένα με το δημόσιο κλειδί που αντιστοιχεί στο κλειδί αυτό (αλγόριθμος δημόσιου κλειδιού). Έτσι, είναι δυνατό σε ένα δίκτυο να χρησιμοποιείται ο ίδιος αλγόριθμος από όλους τους χρήστες του, αλλά διαφορετικά κλειδιά για κάθε χρήστη.

Μήκος Κλειδιού

Ο μόνος τρόπος για να παραβιαστεί ένα κρυπτοσύστημα που χρησιμοποιεί «ισχυρό» κρυπτογραφικό αλγόριθμο, είναι η «κατά μέτωπο επίθεση» (brute-force attack). Σε αυτή την επίθεση, κάποιος δοκιμάζει όλα τα πιθανά κλειδιά ώστε να βρει κάποιο που ταιριάζει με το κλειδί που χρησιμοποιήθηκε στην κρυπτογράφηση.

Η πολυπλοκότητα της παραπάνω επίθεσης υπολογίζεται εύκολα. Εάν το κλειδί έχει μήκος 8 bits, τότε υπάρχουν 2^8, ή 256 πιθανά κλειδιά. Επομένως χρειάζονται 256 προσπάθειες προκειμένου να βρεθεί το σωστό κλειδί, με πιθανότητα 50% να βρεθεί το σωστό κλειδί μετά τις μισές προσπάθειες. Εάν το κλειδί έχει μήκος 56 bits, τότε υπάρχουν 2^{56} πιθανά κλειδιά. Υποθέτοντας ότι ένας υπερυπολογιστής μπορεί να δοκιμάζει ένα εκατομμύριο κλειδιά το δευτερόλεπτο, θα χρειαστεί 2285 χρόνια να βρει το σωστό κλειδί. Σήμερα όμως, η τεχνολογία επιτρέπει την υλοποίηση τέτοιων επιθέσεων, από πολλούς υπολογιστές που δουλεύουν παράλληλα. Για το λόγο αυτό το μήκος κλειδιού πρέπει να είναι όσο το δυνατό μεγαλύτερο.

Διαχείριση Κλειδιού

Η διαχείριση κλειδιών αποτελεί ίσως τη δυσκολότερη εργασία στον τομέα της κρυπτογραφίας. Η κακή διαχείριση είναι συνήθως η αιτία που καταρρέουν τα περισσότερα συστήματα, ακόμα και αν βασίζονται στους ισχυρότερους αλγόριθμους.

Δημιουργία Κλειδιού: Ένα κλειδί δεν πρέπει να είναι κοινότυπο. Εάν ναι, τότε είναι ευάλωτο σε επιθέσεις λεξικού (dictionary attack), όπου ο επιτιθέμενος χρησιμοποιεί ένα λεξικό με κοινές λέξεις. Τα «καλά» κλειδιά είναι αλφαριθμητικά τυχαίων bits, τα οποία δημιουργούνται από κάποια αυτόματη επεξεργασία.

Μεταφορά Κλειδιού: Ιδίως στα μεγάλα δίκτυα, ο τρόπος με τον οποίο τα κλειδιά μεταφέρονται μεταξύ χρηστών, πρέπει να είναι ασφαλής. Έχουν προταθεί πολλά πρωτόκολλα ανταλλαγής κλειδιών (π.χ. Diffie Hellman), η επιλογή ενός εκ των οποίων πρέπει να γίνεται με μεγάλη προσοχή.

Αποθήκευση και Ενημέρωση του Κλειδιού: Τα κλειδιά πρέπει να αποθηκεύονται με ασφάλεια. Η καλύτερη λύση είναι η αποθήκευση τους σε μια έξυπνη κάρτα. Επίσης, πρέπει να έχουν μια περίοδο ζωής, δηλαδή να αλλάζουν συχνά, ώστε να μη δίνεται η ευκαιρία στους κρυπταναλυτές να δοκιμάζουν τυχαία κλειδιά (π.χ. με brute-force επίθεση) για μεγάλο χρονικό διάστημα.

9.6 Τύποι ‘επιθέσεων’ σε κρυπτογραφικά συστήματα

Η κρυπτανάλυση, όπως αναφέρθηκε και προηγουμένως, έχει ως στόχο την ανάπτυξη τεχνικών και μεθόδων για την παραβίαση κρυπτογραφημένων μηνυμάτων ή κρυπτογραφικών συστημάτων. Μία επιτυχής κρυπτανάλυση μπορεί να αποκαλύψει το αρχικό από το κρυπτογραφημένο μήνυμα. Μπορεί συγχρόνως να εντοπίσει αδυναμίες σε ένα κρυπτογραφικό σύστημα, οι οποίες οδηγούν τελικά στα παραπάνω αποτελέσματα.

Μία επιχειρούμενη κρυπτανάλυση χαρακτηρίζεται και ως επίθεση (attack). Οι κρυπταναλυτές μπορεί να έχουν στη διάθεσή τους κρυπτογραφημένα μηνύματα, τα αντίστοιχα αρχικά μηνύματα, τους αλγόριθμους κρυπτογράφησης που χρησιμοποιήθηκαν, στατιστικά εργαλεία και τεχνικές, κτλ. Επίσης, θεωρείται ότι ο κρυπταναλυτής γνωρίζει τις λεπτομέρειες του κρυπτογραφικού αλγόριθμου, αν και αυτό δε συμβαίνει πάντα στην πράξη. Η υπόθεση αυτή είναι εύλογη γιατί όπως αναφέρεται συχνά στη βιβλιογραφία, αν η ασφάλεια των κρυπτογραφικών συστημάτων στηρίζεται στη μυστικότητά τους, τότε αυτή δεν μπορεί να είναι επαρκής. Αν στηρίζεται εκτός των άλλων και στη μυστικότητα των αλγορίθμων, κάτι το οποίο δεν συνιστάται, τότε πρόκειται κατά κανόνα για συστήματα με περιορισμένο πεδίο εφαρμογής.

Οι τύποι κρυπταναλυτικών επιθέσεων διαφοροποιούνται σύμφωνα με τους πόρους που έχει στη διάθεσή του ο επιτιθέμενος. Όλοι οι τύποι επιθέσεων προϋποθέτουν ότι ο κρυπταναλυτής γνωρίζει πλήρως τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης. Συνοπτικά, οι τέσσερις βασικοί τύποι επιθέσεων κρυπτανάλυσης, οι οποίοι αποτελούν τη βάση αξιολόγησης των κρυπτογραφικών συστημάτων είναι οι εξής:

Επίθεση κρυπτογραφημένου κειμένου (Ciphertext – only attack). Ο κρυπταναλυτής έχει στη διάθεσή του αρκετά κρυπτογραφημένα, με τον ίδιο αλγόριθμο και το ίδιο κλειδί, μηνύματα και επιδιώκει να αποκρυπτογραφήσει όσο πιο πολλά μηνύματα μπορεί ή και να προσδιορίσει το κρυπτογραφικό κλειδί που χρησιμοποιήθηκε ή ακόμα και να επινοήσει έναν αλγόριθμο που θα του επιτρέπει να υπολογίζει το αρχικό από το κρυπτογραφημένο μήνυμα.

Επίθεση γνωστού αρχικού κειμένου (Known – plaintext attack). Ο κρυπταναλυτής έχει στη διάθεσή του όχι μόνο κρυπτογραφημένα μηνύματα αλλά και τα αντίστοιχα αρχικά μηνύματα και επιδιώκει να προσδιορίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση των μηνυμάτων ή κάποιον αλγόριθμο που θα του επιτρέπει να υπολογίζει από το κρυπτογραφημένο μήνυμα το αντίστοιχο αρχικό που πλέον δεν γνωρίζει.

Επίθεση επιλεγμένων αρχικών κειμένων (Chosen – plaintext attack). Οι κρυπταναλυτές έχουν στη διάθεσή τους τα κρυπτογράμματα επιλεγμένων από τους ίδιους αρχικών μηνυμάτων. Ο στόχος είναι να βρεθεί το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων, ή να επινοηθεί ένας αλγόριθμος για την αποκρυπτογράφηση των νέων μηνυμάτων, τα οποία κρυπτογραφούνται με το ίδιο κλειδί.

Επίθεση επιλεγμένων κρυπτογραφημένων κειμένων (Chosen – ciphertext attack). Οι κρυπταναλυτές μπορούν να επιλέξουν διάφορα κρυπτογραφημένα μηνύματα και διαθέτουν ακόμα τα αντίστοιχα αρχικά μηνύματα, επιδιώκουν δε τον προσδιορισμό του κλειδιού που μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση.

Ένας ισχυρός αλγόριθμος κρυπτογράφησης θα είναι αδύνατον να «σπάσει» όχι μόνο από επιθέσεις γνωστού κειμένου (υποθέτοντας ότι ο εχθρός γνωρίζει όλο το μη κρυπτογραφημένο κείμενο για ένα δοθέν κρυπτογραφημένο κείμενο), αλλά και σε επιθέσεις προσαρμοζόμενου επιλεγμένου μη κρυπτογραφημένου κειμένου. Στον τύπο αυτό της επίθεσης ο επιτιθέμενος επιλέγει κάποιο συγκεκριμένο κείμενο και το

αναλύει τόσο στη μη κρυπτογραφημένη αλλά και στην κρυπτογραφημένη μορφή. Τα ευρήματα κάθε φάσης αξιοποιούνται για την επιλογή επόμενου κειμένου για ανάλυση, με τελικό στόχο την αποκρυπτογράφηση του επιθυμητού κειμένου (που πιθανότατα έχει υποκλαπεί).

9.7 Ψηφιακές Υπογραφές

Τα σύγχρονα πληροφοριακά συστήματα αποθηκεύουν και επεξεργάζονται σε ηλεκτρονική μορφή αυξανόμενο πλήθος από έγγραφα που δημιουργήθηκαν αρχικά στο χαρτί. Η κατοχή εγγράφων σε ηλεκτρονική μορφή επιτρέπει την ταχύτατη επεξεργασία και μετάδοση τους και βελτιώνει την συνολική αποτελεσματικότητα. Ωστόσο, η έγκριση ενός εγγράφου παραδοσιακά υποδεικνυόταν από μια γραπτή υπογραφή. Αυτό που απαιτείται λοιπόν, είναι το ηλεκτρονικό ανάλογο της γραπτής υπογραφής το οποίο να μπορεί να αναγνωριστεί ότι έχει την ίδια νομική αξία με την γραπτή υπογραφή. Η κρυπτογράφηση μπορεί να παρέχει ένα μέσο σύνδεσης ενός εγγράφου με ένα συγκεκριμένο άτομο, όπως γίνεται με την γραπτή υπογραφή. Οι ηλεκτρονικές ή ψηφιακές υπογραφές (digital signatures) μπορούν να χρησιμοποούν και τα δύο βασικά είδη κρυπτογράφησης, ιδιωτικού και δημόσιου κλειδιού, ωστόσο οι μέθοδοι δημόσιου κλειδιού είναι γενικότερα ευκολότεροι στην χρήση τους.

Ο χρήστης διαθέτει δύο κλειδιά (το δημόσιο και το ιδιωτικό) τα οποία έχουν κάποιο μαθηματικό συσχετισμό. Η σχέση των κλειδιών είναι τέτοια όπου αν κάποιος γνωρίζει το ένα κλειδί να είναι πρακτικά αδύνατον να υπολογίσει το άλλο. Το ένα κλειδί χρησιμοποιείται για τη δημιουργία της υπογραφής και το άλλο για την επαλήθευσή της. Η διαφοροποίηση από την κρυπτογράφηση, έγκειται στο ότι για τη δημιουργία της ηλεκτρονικής υπογραφής ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί και για την επαλήθευσή της ο παραλήπτης χρησιμοποιεί το δημόσιο κλειδί του αποστολέα.

Στη διαδικασία της δημιουργίας και επαλήθευσης της υπογραφής εμπλέκεται και η έννοια της συνάρτησης κατακερματισμού (ή κατατεμαχισμού -one way hash). Με την εφαρμογή της συνάρτησης κατακερματισμού, από ένα μήνυμα ανεξαρτήτου του μεγέθους του, παράγεται η «σύνοψή του», η οποία είναι μία σειρά από bits συγκεκριμένου μεγέθους (π.χ. 128 ή 160 bits). Η σύνοψη του μηνύματος (fingerprint ή message digest) είναι μία ψηφιακή αναπαράσταση του μηνύματος, είναι μοναδική για το μήνυμα και το αντιπροσωπεύει.

Η συνάρτηση κατακερματισμού είναι μονόδρομη διότι από την σύνοψη που δημιουργεί, είναι υπολογιστικά αδύνατον κάποιος να εξάγει το αρχικό μήνυμα. Η πιθανότητα δύο μηνύματα να έχουν την ίδια σύνοψη είναι εξαιρετικά μικρή. Αυτό σημαίνει ότι αν το μήνυμα του αποστολέα έχει κάποια συγκεκριμένη σύνοψη και το μήνυμα που λάβει ο παραλήπτης (χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού) παράγει διαφορετική σύνοψη, τότε το μήνυμα κατά την μετάδοσή του έχει αλλοιωθεί (μη ακεραιότητα). Οποιαδήποτε αλλαγή σε ένα μήνυμα συνεπάγεται και τη δημιουργία διαφορετικής σύνοψης.

Η ηλεκτρονική υπογραφή, στην ουσία είναι η κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα σύνοψη. Δηλαδή, η ψηφιακή υπογραφή, σε αντίθεση με την ιδιόχειρη υπογραφή, είναι διαφορετική για κάθε μήνυμα.

Θεωρώντας ότι ο αποστολέας έχει ένα συγκεκριμένο ζευγάρι κλειδιών και το ιδιωτικό του κλειδί είναι στην πλήρη κατοχή του, τότε το γεγονός ότι ο αποστολέας χρησιμοποιεί το ιδιωτικό του κλειδί για να κρυπτογραφήσει το μήνυμα, πιστοποιεί στον παραλήπτη που το αποκρυπτογραφεί με το αντίστοιχο δημόσιο κλειδί (του αποστολέα) την ταυτότητα του αποστολέα (αυθεντικότητα). Η ψηφιακή υπογραφή είναι ένας τρόπος αυθεντικοποίησης του αποστολέα του μηνύματος.

Μία ψηφιακή υπογραφή μπορεί να πλαστογραφηθεί εάν ο δικαιούχος του ιδιωτικού κλειδιού δεν το έχει υπό τον πλήρη έλεγχό του (π.χ. χάσει το μέσο στο οποίο έχει αποθηκευτεί το ιδιωτικό κλειδί).

Οι ψηφιακές υπογραφές μπορούν να επιτελέσουν τρείς διαφορετικές αλλά πολύ σημαντικές, για την ασφάλεια, λειτουργίες:

Ακεραιότητα (Integrity): Η ψηφιακή υπογραφή υποδεικνύει αν κάποιο αρχείο ή μήνυμα έχει μεταβληθεί. Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους.

Πιστοποίηση (Authentication): Η ψηφιακή υπογραφή κάνει μαθηματικά δυνατή την επιβεβαίωση του ονόματος του ατόμου που υπέγραψε κάποιο μήνυμα.

Απαγόρευση απάρνησης (Non-repudiation): Απαγόρευση απάρνησης (ή αδυναμία αποκήρυξης όπως αναφέρεται αλλιώς) σημαίνει ότι αφότου κάποιος χρήστης υπογράψει και στείλει κάποιο μήνυμα, δεν μπορεί αργότερα να ισχυριστεί ότι δεν υπέγραψε το συγκεκριμένο αυτό μήνυμα. Δεν μπορεί να απαρνηθεί την υπογραφή του γιατί το μήνυμα υπογράφθηκε χρησιμοποιώντας το ιδιωτικό του κλειδί (που υποθετικά τουλάχιστον, δεν το έχει κανείς άλλος). Η απαγόρευση απάρνησης μπορεί επίσης να διασφαλίσει ότι το προϊόν μιας επικοινωνίας έφτασε στον

προορισμό του άθικτο, χωρίς καμία αλλοίωση που θα μπορούσε να είχε συμβεί αν κάποιος υπέκλεπτε το μήνυμα, αλλάζοντας το και κατόπιν στέλνοντας το ξανά στον πραγματικό του προορισμό. Αυτή η λειτουργία είναι σημαντική κυρίως για την ηλεκτρονική αλληλογραφία.

Ωστόσο οι ηλεκτρονικές δοσοληψίες με χρήση ψηφιακών υπογραφών είναι πιθανόν ευπαθείς σε απάτη, όταν οι υπολογιστές παραβιάζονται ή προσβάλλονται από κάποιο ιομορφικό λογισμικό. Οι συμμετέχοντες μπορούν πιθανότατα να χρησιμοποιήσουν τέτοιου είδους απάτη για να επιχειρήσουν να απαρνηθούν μια δοσοληψία.

9.7.1 Δημιουργία και επαλήθευση ψηφιακής υπογραφής

Η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο διαδικασίες: τη δημιουργία της υπογραφής και την επαλήθευσή της. Παρακάτω, θα αναφέρουμε βήμα προς βήμα τις ενέργειες του αποστολέα και του παραλήπτη ώστε να γίνει κατανοητός ο μηχανισμός της δημιουργίας και επαλήθευσης της ψηφιακής υπογραφής.

Αποστολέας

Ο αποστολέας χρησιμοποιώντας κάποιον αλγόριθμο κατακερματισμού (one way hash) δημιουργεί τη σύνοψη του μηνύματος (message digest) που θέλει να στείλει. Ανεξάρτητα από το μέγεθος του μηνύματος, αυτό που θα παραχθεί θα είναι μία συγκεκριμένου μήκους σειρά ψηφίων. Με το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη. Αυτό που παράγεται είναι η ψηφιακή υπογραφή. Η υπογραφή είναι ουσιαστικά μία σειρά ψηφίων συγκεκριμένου πλήθους.

Η κρυπτογραφημένη σύνοψη (ψηφιακή υπογραφή) προσαρτάται στο κείμενο και το μήνυμα με τη ψηφιακή υπογραφή μεταδίδονται μέσω του δικτύου. Ο αποστολέας αν επιθυμεί μπορεί να κρυπτογραφήσει το μήνυμά του με το δημόσιο κλειδί του παραλήπτη.

Παραλήπτης

Ο παραλήπτης αποσπά από το μήνυμα την ψηφιακή υπογραφή η οποία είναι κρυπτογραφημένη, με το ιδιωτικό κλειδί του αποστολέα. Εφαρμόζοντας στο μήνυμα που έλαβε τον ίδιο αλγόριθμο κατακερματισμού, δημιουργεί τη σύνοψη του

μηνύματος. Στη συνέχεια, αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα, την κρυπτογραφημένη σύνοψη του μηνύματος (ψηφιακή υπογραφή).

Συγκρίνονται οι δύο συνόψεις και αν βρεθούν ίδιες, αυτό σημαίνει ότι το μήνυμα που έλαβε ο παραλήπτης είναι ακέραιο. Αν το μήνυμα έχει μεταβληθεί, η σύνοψη που θα παράγει ο παραλήπτης θα είναι διαφορετική από την σύνοψη που έχει κρυπτογραφηθεί.

Οι παρακάτω διεργασίες που περιγράφουν την διαδικασία παραγωγής μιας ψηφιακής υπογραφής και πιστοποίησης, γίνονται από το ανάλογο λογισμικό στον υπολογιστή του χρήστη.

Οι ψηφιακές υπογραφές βασίζονται στην μυστικότητα των κλειδιών και την σύνδεση ή δέσμευση του ιδιοκτήτη του κλειδιού και το ίδιο το κλειδί. Αν το κλειδί εκτεθεί (μέσω κλοπής, εξαναγκασμού ή απάτης), τότε η ηλεκτρονική πηγή ενός μηνύματος μπορεί να μην είναι η ίδια με τον ιδιοκτήτη του κλειδιού. Αν και η σύνδεση των κρυπτογραφικών κλειδιών με πραγματικούς ανθρώπους είναι ένα σημαντικό πρόβλημα, αυτό δεν κάνει απαραίτητα τις ψηφιακές υπογραφές λιγότερο ασφαλής από τις γραπτές υπογραφές. Η απάτη και ο εξαναγκασμός είναι προβλήματα και για τις γραπτές υπογραφές επίσης. Εκτός αυτού, οι γραπτές υπογραφές μπορούν εύκολα να πλαστογραφηθούν.

Πώς μπορεί λοιπόν ο παραλήπτης ενός μηνύματος να είναι βέβαιος ότι ο αποστολέας είναι αυτός που ισχυρίζεται ότι είναι; Το δημόσιο κλειδί του αποστολέα μπορεί να ανακληθεί από μια ιστοσελίδα ή από ένα σχετικό ευρετήριο, αλλά πόσο αξιόπιστο μπορεί να είναι αυτό; Καθένας θα μπορούσε να ζητήσει την έκδοση ενός ζεύγους κλειδιού υπό άλλο όνομα και στη συνέχεια να ανακοινώσει ότι το τάδε δημόσιο κλειδί είναι δικό του. Ο παραλήπτης θα πρέπει να διαθέτει περισσότερες και πραγματικά αξιόπιστες πληροφορίες για τον ιδιοκτήτη του κλειδιού. Η σημαντικότερη μέθοδος στην κατεύθυνση αυτή βασίζεται στην ύπαρξη Έμπιστων Τρίτων Φορέων/Οντοτήτων – ΕΤΦ (Trusted Third Parties, TTP), οι οποίοι και παρέχουν ηλεκτρονικά (ή ψηφιακά) πιστοποιητικά (certificates) όπως και θα δούμε παρακάτω.

9.8 Ψηφιακά Πιστοποιητικά

Τα μεγάλα δίκτυα όπως είναι και το Internet σ' ένα μεγάλο βαθμό στηρίζονται στην εμπιστοσύνη. Πρόκειται για έναν εικονικό κόσμο στον οποίο ο χρήστης δεν βλέπει τους ανθρώπους ή τους φορείς με τους οποίους επικοινωνεί παίρνοντας και

δίνοντας πληροφορίες. Δεν βλέπει για παράδειγμα τον χρήστη στον οποίο στέλνει e-mail αλλά εμπιστεύεται ότι είναι αυτός που ισχυρίζεται ότι είναι.

Στην περίπτωση όμως των οικονομικών συναλλαγών ή σημαντικών επικοινωνιών στα πλαίσια μεταφοράς δεδομένων σε ένα τοπικό δίκτυο μιας επιχείρησης για παράδειγμα, η εμπιστοσύνη δεν είναι αρκετή. Στο δίκτυο υπάρχουν hackers, crackers καθώς και άλλοι που θα ήθελαν να μάθουν τα προσωπικά, επαγγελματικά ή οικονομικά μυστικά, για παράδειγμα ενός διευθυντικού στελέχους της επιχείρησης. Κατά τον ίδιο τρόπο οι επιχειρήσεις πρέπει να γνωρίζουν ότι το πρόσωπο που στέλνει έναν αριθμό πιστωτικής κάρτας είναι πράγματι αυτός που δηλώνει ότι είναι και όχι ένας απατεώνας που κατόρθωσε να κλέψει τον αριθμό της πιστωτικής κάρτας κάποιου άλλου.

Ο σημαντικότερος τρόπος αποφυγής του προαναφερθέντος προβλήματος είναι η χρήση των ψηφιακών πιστοποιητικών (digital certificates). Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για να πιστοποιήσουν ότι το άτομο που στέλνει πληροφορίες ή έναν αριθμό πιστωτικής κάρτας ή ένα μήνυμα ή οτιδήποτε άλλο στο Internet είναι πραγματικά αυτό που δηλώνει ότι είναι. Τα πιστοποιητικά τοποθετούν τις πληροφορίες στον σκληρό δίσκο του χρήστη και χρησιμοποιούν τεχνολογία απόκρυψης για να δημιουργήσουν ένα μοναδικό ψηφιακό πιστοποιητικό για κάθε χρήστη. Όταν κάποιος που διαθέτει ένα ψηφιακό πιστοποιητικό επισκεφθεί κάποιο site ή στείλει e-mail το πιστοποιητικό αυτό παρουσιάζεται στο site ή επισυνάπτεται στο e-mail και πιστοποιεί ότι ο χρήστης είναι αυτός που ισχυρίζεται ότι είναι.

Τα ψηφιακά πιστοποιητικά είναι αρκετά ασφαλή επειδή χρησιμοποιούν πανίσχυρη τεχνολογία απόκρυψης. Στην πραγματικότητα είναι πιο ασφαλή ακόμη και από τις υπογραφές. Στην πραγματική ζωή μία υπογραφή μπορεί να πλαστογραφηθεί. Αντιθέτως, στο Internet δεν μπορεί να πλαστογραφηθεί το ψηφιακό πιστοποιητικό.

Τα ψηφιακά πιστοποιητικά εκδίδονται έναντι χρεώσεως από ιδιωτικές εταιρίες που ονομάζονται Digital Authorities. Μία τέτοια εταιρία είναι η πολύ γνωστή VeriSign. Τα ψηφιακά πιστοποιητικά περιλαμβάνουν διάφορες πληροφορίες όπως το όνομα του χρήστη, το όνομα της εταιρίας που το εκδίδει, έναν σειριακό αριθμό και άλλες παρόμοιες πληροφορίες. Οι πληροφορίες έχουν κωδικοποιηθεί μ' έναν τρόπο που τις κάνει μοναδικές για τον κάθε χρήστη. Όπως στα περισσότερα πράγματα στο Internet έτσι και στην περίπτωση των ψηφιακών πιστοποιητικών υπάρχει ένα πρότυπο που επικρατεί και είναι γνωστό με την ονομασία X.509.

Με την λήψη ενός μηνύματος με ηλεκτρονική υπογραφή, ο παραλήπτης επαληθεύοντας την ηλεκτρονική υπογραφή βεβαιώνεται ότι το μήνυμα είναι ακέραιο. Ο παραλήπτης για την επαλήθευση της ηλεκτρονικής υπογραφής, χρησιμοποιεί το δημόσιο κλειδί του αποστολέα. Αυτό όμως που δεν μπορεί να γνωρίζει ο παραλήπτης με βεβαιότητα, είναι αν ο αποστολέας του μηνύματος είναι όντως αυτός που ισχυρίζεται ότι είναι. Θεωρώντας ότι ο κάτοχος του ιδιωτικού κλειδιού είναι πράγματι αυτός που ισχυρίζεται ότι είναι (και η μυστικότητα του ιδιωτικού κλειδιού δεν έχει παραβιαστεί) ο αποστολέας του μηνύματος που υπέγραψε, δεν μπορεί να αρνηθεί το περιεχόμενο του μηνύματος που έστειλε (μη αποποίηση).

Κατά συνέπεια, απαιτείται να διασφαλιστεί ότι ο δικαιούχος του ιδιωτικού κλειδιού, και μόνον αυτός, δημιούργησε την ηλεκτρονική υπογραφή και ότι το δημόσιο κλειδί του αποστολέα που χρησιμοποιεί ο παραλήπτης για την επαλήθευση της υπογραφής είναι όντως του αποστολέα. Απαιτείται δηλαδή, η ύπαρξη ενός μηχανισμού τέτοιου, ώστε ο παραλήπτης να μπορεί να είναι σίγουρος για την ταυτότητα του προσώπου με το δημόσιο κλειδί. Ο μηχανισμός αυτός θα πρέπει να υλοποιείται από μία οντότητα που εμπνέει εμπιστοσύνη και που εγγυάται ότι σε ένα συγκεκριμένο πρόσωπο αντιστοιχεί το συγκεκριμένο δημόσιο κλειδί.

Ο Πάροχος Υπηρεσιών Πιστοποίησης είναι η οντότητα που παρέχει την υπηρεσία εκείνη με την οποία πιστοποιείται η σχέση ενός προσώπου με το δημόσιο κλειδί του. Ο τρόπος με τον οποίο γίνεται αυτό, είναι με την έκδοση ενός πιστοποιητικού (ένα ηλεκτρονικό αρχείο) στο οποίο ο Πάροχος Υπηρεσιών Πιστοποίησης πιστοποιεί την ταυτότητα του προσώπου και το δημόσιο κλειδί του.

Από τους σημαντικότερους τύπους ψηφιακών πιστοποιητικών είναι το πιστοποιητικό δημοσίου κλειδιού (public key certificate). Ο στόχος του πιστοποιητικού δημοσίου κλειδιού είναι η δημιουργία μιας σχέσης ταυτοποίησης μεταξύ του δημοσίου κλειδιού και του δικαιούχου του. Το πιστοποιητικό αναφέρει το δημόσιο κλειδί (το οποίο και είναι το αντικείμενο του πιστοποιητικού) και επιβεβαιώνει ότι το συγκεκριμένο πρόσωπο που αναφέρεται στο πιστοποιητικό είναι ο δικαιούχος του αντίστοιχου ιδιωτικού κλειδιού. Έτσι ο παραλήπτης που λαμβάνει ένα μήνυμα με ψηφιακή υπογραφή, μπορεί να είναι σίγουρος ότι το μήνυμα έχει σταλεί από το πρόσωπο που το υπογράφει.

Το ψηφιακό πιστοποιητικό, είναι στον ηλεκτρονικό κόσμο ότι είναι το διαβατήριο στο φυσικό κόσμο. Η συσχέτιση ενός δημοσίου κλειδιού με τον δικαιούχο του γίνεται με χρήση της ψηφιακής υπογραφής του Παρόχου Υπηρεσιών

Πιστοποίησης, όπου ο Πάροχος με την ψηφιακή του υπογραφή, υπογράφει το πιστοποιητικό του δικαιούχου. Αν ένας χρήστης εμπιστεύεται έναν Πάροχο Υπηρεσιών Πιστοποίησης, εμπιστεύεται και το πιστοποιητικό που ο Πάροχος εκδίδει.

Ένας Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει πιστοποιήσει ή να έχει πιστοποιηθεί από έναν άλλον, στα πλαίσια μίας σχέσης εμπιστοσύνης. Αν ο χρήστης δεν γνωρίζει έναν Πάροχο και δεν ξέρει αν πρέπει να εμπιστευθεί ένα πιστοποιητικό που αυτός έχει εκδώσει, και ο Πάροχος αυτός έχει δημιουργήσει μία σχέση εμπιστοσύνης με έναν άλλο Πάροχο που ο χρήστης εμπιστεύεται, τότε ο χρήστης μπορεί να εμπιστευθεί τον πρώτο Πάροχο. Ο χρήστης, μπορεί να επαληθεύσει τη ψηφιακή υπογραφή του Παρόχου Υπηρεσιών Πιστοποίησης που έχει εκδώσει ένα ψηφιακό πιστοποιητικό, χρησιμοποιώντας το δημόσιο κλειδί του Παρόχου, για το οποίο (δημόσιο κλειδί) ένας άλλος Πάροχος Υπηρεσιών Πιστοποίησης μπορεί να έχει εκδώσει πιστοποιητικό κ.λπ.

Ένα πιστοποιητικό εφόσον διαπιστωθεί ή υπάρχει υπόνοια ότι για κάποιους λόγους δεν είναι έγκυρο (π.χ. αν το ιδιωτικό κλειδί του δικαιούχου έχει γίνει γνωστό σε τρίτους ή το πρόσωπο εξαπάτησε τον Πάροχο Υπηρεσιών Πιστοποίησης ως προς τα στοιχεία της ταυτότητάς του κλπ), τότε ο Πάροχος Υπηρεσιών Πιστοποίησης προβαίνει στην ανάκλησή του, όπως ρυθμίζεται από τη νομοθεσία.

9.8.1 Τύποι Ψηφιακών Πιστοποιητικών

Η χρήση των σύγχρονων κρυπτογραφικών τεχνικών και των ψηφιακών πιστοποιητικών υπόσχονται έναν ασφαλή τρόπο χρήσης των υπηρεσιών του διαδικτύου που αφορούν την αυθεντικοποίηση των πελατών και των εξυπηρετητών, την ακεραιότητα των διακινούμενων δεδομένων, την αποφυγή προστριβών μεταξύ των συμμετεχόντων μερών, καθώς και την εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα.

Υπάρχουν διάφοροι τύποι ψηφιακών πιστοποιητικών, όπως:

- Client SSL certificates. Χρησιμοποιούνται για την αναγνώριση χρηστών από εξυπηρετητές μέσω SSL (clíent authentícatíon).
- Server SSL certificates. Χρησιμοποιούνται για την αναγνώριση των εξυπηρετητών μέσω SSL (server authentícatíon).

- S/MIME certificates. Χρησιμοποιούνται για την υπογραφή και κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου (email). Ένα πιστοποιητικό πελάτη μπορεί να χρησιμοποιηθεί και ως S/MIME και ως Client SSL certíficate.
- Object-signing certíficates. Χρησιμοποιούνται για την αναγνώριση υπογεγραμμένου κώδικα σε Java, JavaScrípt, καθώς και άλλων τύπων αρχείων.

Τα πιστοποιητικά χαρακτηρίζονται ακόμη και από το είδος της πληροφορίας που περιέχουν. Έτσι, υπάρχουν:

- Πιστοποιητικά ταυτότητας (Identity certíficates) που ταυτοποιούν μια οντότητα και
- Πιστοποιητικά χαρακτηριστικών (Attribute certíficates) που περιγράφουν τις ιδιότητες μιας οντότητας, όπως κάποιο δικαίωμα προσπέλασης ή τη συμμετοχή της σε μια ομάδα χρηστών.

10. ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΩΤΟΚΟΛΛΑ

10.1 Εισαγωγή στα πρωτόκολλα

Πρωτόκολλο (protocol) ονομάζουμε μια σειρά βημάτων, που αφορούν δύο ή περισσότερες οντότητες, σχεδιασμένα να φέρουν εις πέρας ένα έργο. Ας αναλύσουμε τον ορισμό αυτό. «Μια σειρά βημάτων» σημαίνει ότι το πρωτόκολλο είναι μια ακολουθία με αρχή και τέλος. Κάθε βήμα πρέπει να εκτελεστεί κατά σειρά και αφού έχει τελειώσει η εκτέλεση του αμέσως προηγούμενου βήματος. Το ότι «αφορά δύο ή περισσότερες οντότητες» σημαίνει ότι απαιτούνται τουλάχιστο δύο πρόσωπα για να εκτελέσουν το πρωτόκολλο· το πρωτόκολλο δεν έχει νόημα για ένα άτομο. Τέλος, «σχεδιασμένο να φέρει εις πέρας ένα έργο» σημαίνει ότι το πρωτόκολλο πρέπει να επιτυγχάνει κάτι.

Χαρακτηριστικά Πρωτοκόλλων

- Όλοι οι μετέχοντες στην διαδικασία του πρωτοκόλλου πρέπει να γνωρίζουν το πρωτόκολλο και όλα τα βήματα από πριν.
- Όλοι οι μετέχοντες στη διαδικασία του πρωτοκόλλου πρέπει να συμφωνήσουν στην χρήση του.
- Το πρωτόκολλο πρέπει να είναι σαφές και όχι αμφιλεγόμενο· κάθε βήμα πρέπει να είναι καλά ορισμένο, χωρίς να υπάρχει περίπτωση παρεξήγησης.
- Το πρωτόκολλο πρέπει να είναι πλήρες· θα πρέπει να υπάρχουν καθορισμένες ενέργειες για κάθε δυνατή περίπτωση.

Γενικά, τα βήματα εκτελούνται γραμμικά, το ένα μετά το άλλο, εκτός κι αν υπάρχουν οδηγίες για διακλάδωση σε κάποιο συγκεκριμένο βήμα. Κάθε βήμα περιλαμβάνει τουλάχιστο μία από τις δύο παρακάτω ενέργειες: εκτέλεση υπολογισμών από ένα ή περισσότερα εκ των προσώπων, ή αποστολή μηνυμάτων ανάμεσα στα πρόσωπα.

Κρυπτογραφικό πρωτόκολλο (cryptographic protocol) είναι εκείνο που χρησιμοποιεί κρυπτογραφία. Τα πρόσωπα μπορεί να είναι φίλοι και να εμπιστεύονται τυφλά ο ένας τον άλλο ή μπορεί να είναι ορκισμένοι εχθροί. Το κρυπτογραφικό πρωτόκολλο υλοποιεί κάποιο κρυπτογραφικό αλγόριθμο, άλλα συνήθως ο στόχος του πρωτοκόλλου είναι κάτι περισσότερο από απλή μυστικότητα. Οι οντότητες

μπορεί να θέλουν να υπολογίζουν από κοινού μία τυχαία ακολουθία ή να πείθουν η μια την άλλη για την ταυτότητά τους ή να υπογράφουν ταυτόχρονα ένα συμβόλαιο. Ο ρόλος της κρυπτογραφίας είναι να εμποδίζει ή να εντοπίζει τις υποκλοπές (eavesdropping) και την απάτη (cheating).

Γενικά πρέπει να ισχύει ό,τι:

Θα πρέπει να είναι αδύνατο να επιτευχθούν περισσότερα απ' όσα ορίζει το πρωτόκολλο.

Ο περιορισμός αυτός είναι πολύ δυσκολότερος απ' ότι ακούγεται. Σε μερικά πρωτόκολλα είναι δυνατόν κάποιος από τους μετέχοντες να διαπράξει απάτη. Σε άλλα είναι δυνατόν κάποιος υποκλοπέας να παρακάμψει το πρωτόκολλο και να αποκτήσει μυστικές πληροφορίες. Όπως με τους αλγόριθμους έτσι κι εδώ είναι ευκολότερο να αποδείξουμε την έλλειψη ασφάλειας παρά το αντίθετο.

10.1.1 Ο ρόλος των πρωτοκόλλων

Τα πρωτόκολλα χρησιμοποιούνται συχνά στην καθημερινή μας ζωή, στα παιχνίδια, στις εκλογές, στα ψώνια κτλ.

Στις μέρες μας όλο και περισσότερες ανθρώπινες συναλλαγές γίνονται μέσω υπολογιστών. Οι υπολογιστές χρειάζονται αυστηρώς καθορισμένα πρωτόκολλα για να πετύχουν αυτό που ο άνθρωπος θα έκανε χωρίς πολλή σκέψη.

Πολλά καθημερινά πρωτόκολλα βασίζονται στην ζωντανή παρουσία των εμπλεκόμενων προσώπων για να διασφαλιστεί η ασφάλεια και η ορθότητά τους. Με τους υπολογιστές δεν συμβαίνει το ίδιο.

Είναι αφελές να πιστεύουμε ότι οι άνθρωποι που χρησιμοποιούν ένα δίκτυο υπολογιστών είναι νομιμόφρονες. Είναι αφελές να πιστεύουμε πως οι διαχειριστές τέτοιων δικτύων είναι νομιμόφρονες. Είναι αφελές ακόμη και να πιστεύουμε ότι οι σχεδιαστές των δικτύων είναι νομιμόφρονες. Οι περισσότεροι βέβαια είναι, άλλα οι λίγοι που δεν είναι μπορούν να προξενήσουν σημαντική ζημιά. Ο αυστηρός καθορισμός των πρωτοκόλλων μας βοηθάει να εξετάζουμε τους τρόπους με τους οποίους μπορούν να παρακαμφθούν. Έτσι μπορούμε να αναπτύξουμε πρωτόκολλα που αποτρέπουν τέτοιες παρανομίες.

Εκτός από το να τυποποιούν την συμπεριφορά, τα πρωτόκολλα επιπλέον διαχωρίζουν την διαδικασία διεκπεραίωσης ενός έργου από τον μηχανισμό με τον οποίο επιτυγχάνεται αυτό.

10.1.2 Διαιτητευόμενα πρωτόκολλα (arbitrated protocols)

Ο διαιτητής (arbitrator) είναι μία αδιάφορη τρίτη οντότητα, που εμπιστευόμαστε για να διεκπεραιωθεί το πρωτόκολλο. «Αδιάφορη» σημαίνει ότι ο διαιτητής δεν έχει κανένα νόμιμο συμφέρον σε ότι αφορά το πρωτόκολλο και καμία προτίμηση σε ότι αφορά τα εμπλεκόμενα μέρη. Τα μέρη θεωρούν ό,τι λέει αληθές, ό,τι κάνει σωστό, και ότι θα αναλάβει να φέρει εις πέρας τον ρόλο του. Οι διαιτητές βοηθούν στο να ολοκληρωθεί ένα πρωτόκολλο ανάμεσα σε δύο αμοιβαία φιλύποπτα μέρη.

Στην καθημερινή μας ζωή τον ρόλο διαιτητή παίζουν συχνά δικηγόροι και συμβολαιογράφοι. Η έννοια του διαιτητή είναι τόσο παλιά όσο και η κοινωνία και παίζει σημαντικό ρόλο σ’ αυτήν.

Η έννοια αυτή μπορεί να μεταφερθεί και στον κόσμο των υπολογιστών, αλλά υπάρχουν ορισμένα προβλήματα:

- Είναι ευκολότερο να εμπιστευτείς ένα ουδέτερο τρίτο πρόσωπο αν γνωρίζεις την ταυτότητά του και το έχεις συναντήσει. Δύο πρόσωπα που δεν εμπιστεύονται ο ένας τον άλλο πιθανότατα δεν θα εμπιστευτούν ούτε κάποιον απρόσωπο διαιτητή κάπου μέσα στο δίκτυο.
- Το δίκτυο θα πρέπει να συντηρεί την δαπάνη της μίσθωσης του διαιτητή.
- Το πρωτόκολλο γίνεται πιο αργό με τη χρησιμοποίηση διαιτητή.
- Ο διαιτητής πρέπει να επεμβαίνει σε οποιαδήποτε συναλλαγή γίνεται στο δίκτυο. Αποτελεί, λοιπόν, κώλυμα για μια ευρεία εφαρμογή ενός πρωτοκόλλου. Αύξηση των διαιτητών μετριάζει το πρόβλημα, αλλά αυξάνει το κόστος.
- Από τη στιγμή που όλοι στο δίκτυο εμπιστεύονται τον διαιτητή, αποτελεί σημείο ευπάθειας για την ασφάλεια του δικτύου.

Παρόλα αυτά, η διαιτησία έχει εφαρμογή σε αρκετά πρωτόκολλα.

10.1.3 Επιδικαζόμενα πρωτόκολλα (adjudicated protocols)

Εξαιτίας του μεγάλου κόστους πληρωμής διαιτητών, τα διαιτητευόμενα πρωτόκολλα μπορούν να διαιρεθούν σε δύο υπό-πρωτόκολλα. Το πρώτο είναι ένα μη διαιτητευόμενο υπό-πρωτόκολλο, που ακολουθείται κάθε φορά που κάποιοι θέλουν να εφαρμόσουν το πρωτόκολλο. Το δεύτερο είναι ένα διαιτητευόμενο υπό-πρωτόκολλο, που εκτελείται μόνο στην περίπτωση διαφωνίας. Το ειδικό αυτό είδος διαιτητή ονομάζεται κριτής (adjudicator).

Ο κριτής είναι επίσης αδιάφορος και έμπιστος. Τα επιδικαζόμενα πρωτόκολλα βασίζονται στην τιμιότητα των εμπλεκόμενων οντοτήτων. Αν, όμως, κάποιος υποψιάζεται απάτη, υπάρχει ένας όγκος καταγεγραμμένων δεδομένων με τα οποία μπορεί μια έμπιστη τρίτη οντότητα να ανακαλύψει την απάτη. Σε ένα καλοσχεδιασμένο τέτοιο πρωτόκολλο ο κριτής μπορεί να ανακαλύψει και την ταυτότητα του απατεώνα. Ο αναπόφευκτος εντοπισμός του δράστη λειτουργεί ως αποτρεπτικό στοιχείο.

Διαφορά κριτή-δικαστή

- Ο διαιτητή, δεν παίρνει απευθείας μέρος σε όλα τα πρωτόκολλα.
- Ο κριτής καλείται μόνο για να αποφανθεί αν το πρωτόκολλο εκτελέστηκε σωστά, και μόνο όταν αυτό είναι αναγκαίο·

10.1.4 Αυτοδύναμα πρωτόκολλα (self-enforcing protocols)

Τα αυτοδύναμα πρωτόκολλα είναι τα καλύτερα. Η διαδικασία του πρωτοκόλλου εγγυάται από μόνη της την νομιμότητα. Δεν χρειάζεται διαιτητής για να εφαρμοστεί το πρωτόκολλο. Ούτε κριτής για να λυθούν διαφωνίες. Το πρωτόκολλο είναι έτσι σχεδιασμένο ώστε να μην υπάρχουν διαφωνίες. Αν κάποιος προσπαθήσει να διαπράξει απάτη, οι υπόλοιποι εντοπίζουν την απάτη του και το πρωτόκολλο διακόπτεται.

Στην καλύτερη περίπτωση, όλα τα πρωτόκολλα θα ήταν αυτοδύναμα. Δυστυχώς, δεν μπορεί να σχεδιαστεί αυτοδύναμο πρωτόκολλο για κάθε περίπτωση.

10.2 Επιθέσεις εναντίων πρωτοκόλλων

Κρυπτογραφικές επιθέσεις μπορούν να γίνουν κατά των αλγορίθμων που χρησιμοποιούνται στα πρωτόκολλα, κατά των τεχνικών που χρησιμοποιήθηκαν για την εφαρμογή αυτών των αλγορίθμων και πρωτοκόλλων, ή κατά των ίδιων των πρωτοκόλλων. Κατά την μελέτη των πρωτοκόλλων θα θεωρήσουμε ότι οι αλγόριθμοι και οι τεχνικές που χρησιμοποιούνται είναι ασφαλείς.

Υπάρχουν διάφοροι τρόποι για να προσβληθεί ένα πρωτόκολλο.

Παθητική Προσβολή

Στην παθητική προσβολή κάποιος που δεν παίρνει μέρος στο πρωτόκολλο μπορεί να υποκλέψει μέρος ή και όλο το πρωτόκολλο. Ο επιτιθέμενος δεν επηρεάζει το πρωτόκολλο, απλά προσπαθεί να αποκτήσει πληροφορίες παρατηρώντας το πρωτόκολλο. Αυτό το είδος επίθεσης αντιστοιχεί στην προσβολή βάση κρυπτογραφήματος. Επειδή η παθητική προσβολή είναι δύσκολο να εντοπιστεί, τα πρωτόκολλα προσπαθούν να την εμποδίσουν παρά να την εντοπίσουν.

Ενεργή Προσβολή

Στην ενεργή προσβολή χρειάζεται ενεργή παρέμβαση. Ο επιτιθέμενος να προσπαθεί να μεταβάλει το πρωτόκολλο προς όφελός του. Θα μπορούσε να υποδύεται κάποιο άλλο πρόσωπο, να προσθέτει επιπλέον μηνύματα στο πρωτόκολλο, να διαγράφει νόμιμα μηνύματα, να αντικαθιστά μηνύματα, να μεταδίδει ξανά παλιότερα μηνύματα, να διακόπτει μια γραμμή επικοινωνίας, ή να μεταβάλει αποθηκευμένες πληροφορίες.

Οι παθητικοί επιτιθέμενοι επιχειρούν να αποκτήσουν πληροφορίες για τα εμπλεκόμενα μέρη. Μαζεύουν τα μηνύματα που ανταλλάσσονται και προσπαθούν να τα αναλύσουν. Από την άλλη οι ενεργές προσβολές έχουν πιο ευρύ φάσμα στόχων. Ο επιτιθέμενος θα μπορούσε να επιθυμεί την συλλογή πληροφοριών, την μείωση της απόδοσης του συστήματος, την αλλοίωση αποθηκευμένων πληροφοριών, ή την μη εξουσιοδοτημένη πρόσβαση.

Οι ενεργές επιθέσεις είναι πιο επιβλαβείς, ιδιαίτερα σε πρωτόκολλα όπου τα διάφορα πρόσωπα δεν εμπιστεύονται το ένα το άλλο. Ο επιτιθέμενος δεν χρειάζεται να είναι ξένος προς το σύστημα. Θα μπορούσε να είναι κάποιος χρήστης του

συστήματος ή ο διαχειριστής του συστήματος. Θα μπορούσαν ακόμα να υπάρχουν πολλοί συνεργαζόμενοι επιτιθέμενοι.

Είναι, επίσης, δυνατόν ο επιτιθέμενος να είναι κάποιος από τους μετέχοντες στο πρωτόκολλο. Μπορεί να ψεύδεται κατά την εφαρμογή του πρωτοκόλλου ή να μην εφαρμόζει καν το πρωτόκολλο. Αυτό το είδος επιτιθέμενου ονομάζεται παραβάτης (cheater). Οι παθητικοί παραβάτες (passive cheaters) ακολουθούν το πρωτόκολλο, αλλά επιχειρούν να αποκτήσουν περισσότερες πληροφορίες απ' ότι θα επέτρεπε το πρωτόκολλο. Οι ενεργοί παραβάτες (active cheaters) διακόπτουν την εξέλιξη του πρωτοκόλλου προσπαθώντας έτσι να εξαπατήσουν τα άλλα μέλη.

Είναι δύσκολο να διατηρηθεί ένα πρωτόκολλο ασφαλές αν οι πλειοψηφία των χρηστών είναι ενεργοί παραβάτες, άλλα μερικές φορές είναι δυνατόν τα υπόλοιπα μέλη να αντιληφθούν την απάτη. Οπωσδήποτε, πάντως, ένα πρωτόκολλο θα πρέπει να είναι ασφαλές έναντι παθητικών παραβατών.

10.3 Ιδιότητες των κρυπτογραφικών πρωτοκόλλων

Μετά την εκτέλεση ενός τέτοιου πρωτοκόλλου, οι εμπλεκόμενες οντότητες θα πρέπει να έχουν την δυνατότητα να πιστεύουν ότι επικοινωνούν μεταξύ τους και όχι με κάποιον εισβολέα, και ταυτόχρονα ότι μοιράζονται αποκλειστικά μεταξύ τους ένα μυστικό, που μπορεί να χρησιμοποιηθεί ως κλειδί συνόδου στις μελλοντικές επικοινωνίες τους. Παρακάτω αναφέρονται οι ιδιότητες ενός ορθού πρωτοκόλλου.

- Προφύλαξη του κλειδιού συνόδου (session key safeness). Θεωρούμε ότι ένα πρωτόκολλο έχει την ιδιότητα της προφύλαξης του κλειδιού συνόδου, όταν, δεδομένου ότι το πρωτόκολλο τερμάτισε φυσιολογικά, η Μαρία έχει επικοινωνήσει με ασφάλεια με τον Κώστα (χρησιμοποιώντας το κλειδί συνόδου), και κανείς τρίτος δεν γνωρίζει το κλειδί συνόδου.
- Ακριβής πιστοποίηση (authentication correctness). Θεωρούμε ότι ένα πρωτόκολλο έχει την ιδιότητα της ακριβούς πιστοποίησης, όταν οι εμπλεκόμενες οντότητες είναι μόνο οι πιστοποιημένες. Αν εντοπιστεί κάποιος εισβολέας πριν τον φυσιολογικό τερματισμό του πρωτοκόλλου, τότε το πρωτόκολλο σταματά, εμφανίζοντας προειδοποίηση. Για να τερματίσει το πρωτόκολλο φυσιολογικά, θα πρέπει να έχουν επιβεβαιωθεί οι ταυτότητες όλων των εμπλεκόμενων οντοτήτων.

- Ιδιότητα μη επανάληψης (non-replayable property). Θεωρούμε ότι ένα πρωτόκολλο έχει την ιδιότητα της μη επανάληψης, αν τα δεδομένα που μεταδίδονται σε κάθε εφαρμογή του πρωτοκόλλου δεν βοηθούν τον αντίπαλο. Δηλαδή, ο αντίπαλος δεν μπορεί ούτε να κατανοήσει αλλά ούτε και να αναμεταδώσει τα δεδομένα που υποκλέπτει, χωρίς να γίνει αντιληπτός.
- Μικρός πλεονασμός (low redundancy property). Θεωρούμε ότι ένα πρωτόκολλο έχει μικρό ή μηδενικό πλεονασμό, αν δεν περιλαμβάνει κάτι το μη απαραίτητο για να πετύχει τους στόχους του (δηλαδή την προφύλαξη του κλειδιού συνόδου, την ακριβής πιστοποίηση και την ιδιότητα μη επανάληψης). Η ιδιότητα αυτή είναι περισσότερο σχετική με την αποδοτικότητα και όχι με την ασφάλεια του πρωτοκόλλου.

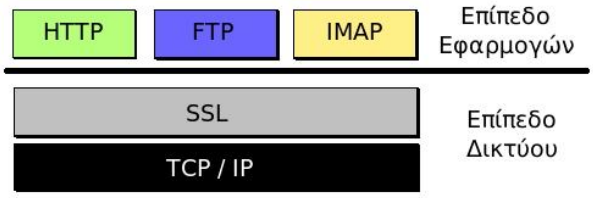
10.4 Το πρωτόκολλο SSL

Το πρωτόκολλο SSL (Secure Sockets Layer) είναι ένα γενικού σκοπού πρωτόκολλο για την αποστολή κρυπτογραφημένης πληροφορίας μέσω του internet. Αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP (διακίνησης υπερκειμένου), το FTP (μεταφορά αρχείων), το telnet (επίπεδο 7 εφαρμογής) κοκ.

Το πρωτόκολλο SSL παρεμβάλλεται μεταξύ των πρωτοκόλλων εφαρμογής και του TCP/IP (καλύπτει τα επίπεδα 3 και 4 δρομολόγησης και μεταφοράς), χρησιμοποιώντας το πρωτόκολλο TCP/IP για λογαριασμό των πρωτοκόλλων υψηλότερου επιπέδου και παρέχοντας την εξής επιπρόσθετη λειτουργικότητα:

- Πιστοποίηση του εξυπηρέτη προς τον εξυπηρετούμενο.
- Πιστοποίηση του εξυπηρετούμενου προς τον εξυπηρέτη.
- Κρυπτογράφηση της επικοινωνίας.



Η λειτουργικότητα αυτή είναι θεμελιώδης για ασφαλή επικοινωνία στο διαδίκτυο για τους παρακάτω λόγους:

- Πιστοποίηση του εξυπηρέτη προς τον εξυπηρετούμενο. Ο εξυπηρετούμενος μπορεί να διακριβώσει την ταυτότητα του εξυπηρέτη. Το λογισμικό του εξυπηρετούμενου μπορεί να χρησιμοποιήσει ένα σύνολο από τεχνικές κρυπτογραφίας δημόσιου κλειδιού για να ελέγξει ότι το πιστοποιητικό και η δημόσια ταυτότητα του εξυπηρέτη είναι έγκυρα και έχουν εκδοθεί από μία αρχή πιστοποίησης την οποία ο εξυπηρετούμενος εμπιστεύεται. Η σημασία του ελέγχου μπορεί να είναι μεγάλη, αν π.χ. αποστέλλονται αριθμοί πιστωτικών καρτών ή απόρρητα δεδομένα και πρέπει να εξασφαλισθεί ότι μόνο ο προτιθέμενος εξυπηρετητής τα λαμβάνει.
- Πιστοποίηση του εξυπηρετούμενου προς τον εξυπηρέτη. Ο εξυπηρετητής διακριβώνει την ταυτότητα του χρήστη, με τις ίδιες τεχνικές που χρησιμοποιούνται για την πιστοποίηση του εξυπηρέτη προς τον εξυπηρετούμενο. Έτσι ελέγχεται ότι το πιστοποιητικό και η δημόσια ταυτότητα του εξυπηρετούμενου είναι έγκυρα και έχουν εκδοθεί από μία αρχή πιστοποίησης την οποία ο εξυπηρετητής εμπιστεύεται. Η σημασία του ελέγχου μπορεί να είναι μεγάλη, αν π.χ. αποστέλλονται εμπιστευτικά δεδομένα και ο εξυπηρετητής θέλει να εξασφαλίσει ότι μόνο ο προτιθέμενος παραλήπτης τα λαμβάνει.
- Κρυπτογράφηση της επικοινωνίας. Το πρωτόκολλο SSL κρυπτογραφεί όλη την επικοινωνία μεταξύ εξυπηρέτη και εξυπηρετούμενου. Τα δεδομένα κρυπτογραφούνται από τον αποστολέα και αποκρυπτογραφούνται από τον παραλήπτη, επιτυγχάνοντας έτσι υψηλό βαθμό εμπιστευτικότητας. Η εμπιστευτικότητα είναι σημαντική και για τους δύο ενεχόμενους σε

οποιαδήποτε ιδιωτική συναλλαγή. Επιπρόσθετα, όλα τα δεδομένα που αποστέλλονται μέσω μιας κρυπτογραφημένης σύνδεσης SSL προστατεύονται με ένα μηχανισμό για ανίχνευση παρεμβάσεων, εντοπισμό δηλαδή προσπαθειών για αλλοίωσή τους κατά τη μεταφορά.

Το πρωτόκολλο SSL περιλαμβάνει δύο επί μέρους πρωτόκολλα: το πρωτόκολλο εγγραφών SSL και το πρωτόκολλο χειραψίας SSL. Το πρωτόκολλο εγγραφών SSL καθορίζει τη μορφή που χρησιμοποιείται για τη μετάδοση των δεδομένων. Το πρωτόκολλο χειραψίας SSL ορίζει μία ακολουθία μηνυμάτων που πρέπει να ανταλλαχθούν μεταξύ εξυπηρέτη και εξυπηρετούμενου προκειμένου να εγκαθιδρυθεί μία σύνδεση μεταξύ τους. Τα μηνύματα αυτά ανταλλάσσονται με στόχο:

- Να πιστοποιηθεί ο εξυπηρετητής στον εξυπηρετούμενο
- Να επιτραπεί στον εξυπηρέτη και στον εξυπηρετούμενο να συμφωνήσουν πάνω στους αλγόριθμους κρυπτογραφίας που θα χρησιμοποιηθούν για την επικοινωνία.
- Προαιρετικά, να πιστοποιηθεί ο εξυπηρετούμενος στον εξυπηρέτη.
- Να δημιουργηθούν «διαμοιραζόμενα μυστικά» μέσω τεχνικών κρυπτογραφίας δημόσιου κλειδιού. Τα «διαμοιραζόμενα μυστικά» θα χρησιμοποιηθούν για την κρυπτογράφηση της επικοινωνίας.
- Εγκαθίδρυση του κρυπτογραφημένου διαύλου επικοινωνίας.

10.4.1 Η χειραψία του πρωτοκόλλου SSL

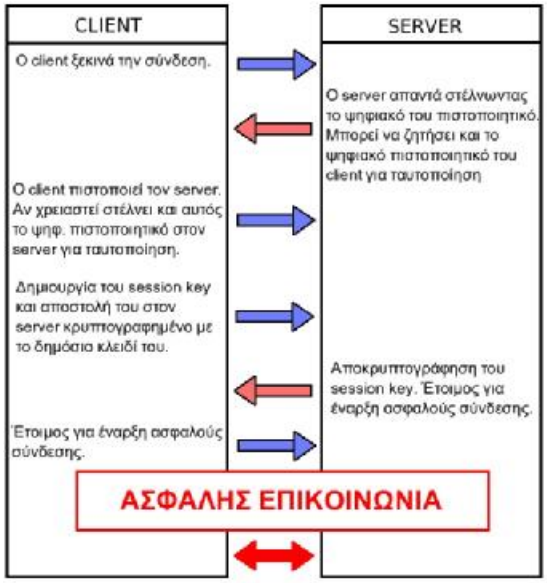
Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρ' όλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται

μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

Τα βήματα που περιλαμβάνονται κατά τη διάρκεια της χειραψίας είναι γενικώς τα ακόλουθα:

1. Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.
2. Ο server απαντά στέλνοντας παρόμοιες πληροφορίες με προηγουμένως συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού του, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.
3. Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.
4. Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο, χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Δηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.
5. Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
6. Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
7. Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

Η διαδικασία της χειραψίας φαίνεται πιο παραστατικά στο σχήμα που ακολουθεί.



10.4.2 Επιβάρυνση από το SSL

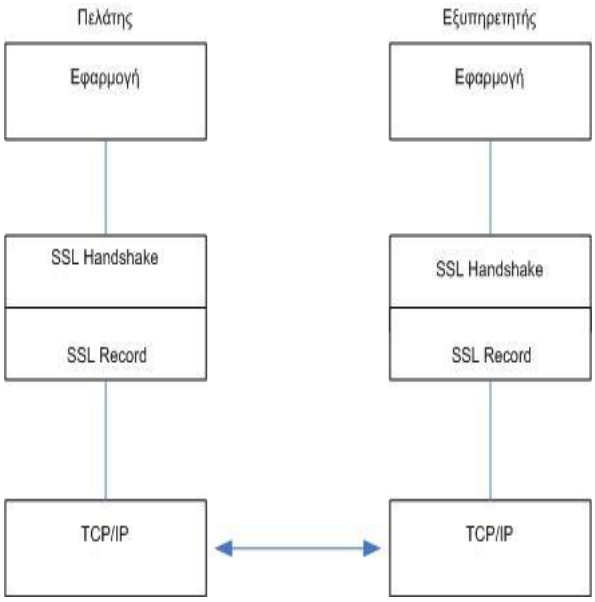
Η χρήση του πρωτοκόλλου SSL αυξάνει τα διακινούμενα πακέτα μεταξύ των δύο μηχανών και καθυστερεί την μετάδοση των πληροφοριών επειδή χρησιμοποιεί μεθόδους κρυπτογράφησης και αποκρυπτογράφησης. Ειδικότερα οι διάφορες καθυστερήσεις εντοπίζονται στα εξής σημεία:

- Στην αρχική διαδικασία χειραψίας όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται τα κλειδιά της συνόδου.
- Στην διαδικασία κρυπτογράφησης και αποκρυπτογράφησης που γίνεται στους δύο υπολογιστές με αποτέλεσμα να δαπανώνται υπολογιστικοί πόροι και χρόνος.
- Στην καθυστέρηση μετάδοσης των κρυπτογραφημένων δεδομένων αφού αυτά αποτελούνται από περισσότερα bytes σε σχέση με την αρχική μη κρυπτογραφημένη πληροφορία.

Λόγω αυτών των επιβαρύνσεων που εισάγει το πρωτόκολλο SSL, χρησιμοποιείται πλέον μονάχα σε περιπτώσεις όπου πραγματικά χρειάζεται ασφαλής σύνδεση (πχ μετάδοση κωδικών χρήστη ή αριθμών πιστωτικών καρτών μέσω του διαδικτύου) και όχι σε περιπτώσεις απλής επίσκεψης σε μία ιστοσελίδα.

10.4.3 Αρχιτεκτονική του SSL

- Το SSL μπορεί να λειτουργήσει πάνω από οποιοδήποτε πρωτόκολλο μεταφοράς. Δεν εξαρτάται από την ύπαρξη του TCP/IP και υποστηρίζει πρωτόκολλα εφαρμογών όπως τα HTTP, FTP και TELNET. Το TCP/IP (Transmission Control Protocol/Internet Protocol) είναι το πρωτόκολλο επικοινωνίας (communication protocol) για την επικοινωνία ανάμεσα σε υπολογιστές που είναι συνδεδεμένοι στο διαδίκτυο. Τα αρχικά TCP/IP αναφέρονται σε δύο από τα σημαντικότερα πρωτόκολλα που χρησιμοποιούνται στο διαδίκτυο, δηλ. στο TCP και στο IP. Το FTP (File Transfer Protocol) είναι ένα πρωτόκολλο μεταφοράς αρχείων, το οποίο φροντίζει για τη διακίνηση αρχείων μέσα στο διαδίκτυο, και το TELNET είναι ουσιαστικά μια υπηρεσία του διαδικτύου με την οποία οι χρήστες αποκτούν απευθείας πρόσβαση σε άλλους υπολογιστές στο διαδίκτυο.
- Είναι σημαντικό κάθε καινούργιο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το μοντέλο διασύνδεσης ανοικτών συστημάτων (Open System Interconnection, OSI), έτσι ώστε να μπορεί να αντικαταστήσει εύκολα κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων. Το SSL λειτουργεί προσθετικά σε σχέση με την υπάρχουσα δομή του OSI και όχι ως πρωτόκολλο αντικατάστασης. Επιπλέον η χρήση του SSL δεν αποκλείει τη χρήση άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, όπως για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο εφαρμογής πάνω από το SSL. Το S/HTTP (Secure HTTP) πρωτόκολλο φροντίζει για την ασφαλή μεταφορά δεδομένων στο διαδίκτυο.



Αρχιτεκτονική Τοποθέτηση του SSL

- Το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης, η οποία έχει τρεις βασικές ιδιότητες:
- Οι επικοινωνούντες μπορούν να αυθεντικοποιούνται αμοιβαία χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού.
- Επιτυγχάνεται εμπιστευτικότητα των μεταδιδόμενων δεδομένων αφού η σύνδεση κρυπτογραφείται διαφανώς μετά από μια αρχική χειραψία και τον καθορισμό ενός κλειδιού συνόδου.
- Προστατεύεται η ακεραιότητα των μεταδιδόμενων δεδομένων, καθώς τα μηνύματα αυθεντικοποιούνται διαφανώς και ελέγχονται ως προς την ακεραιότητα τους κατά τη μετάδοση με χρήση MACs.

SSL record protocol και SSL handshake protocol

- Το πρωτόκολλο SSL αποτελείται από δύο επιμέρους πρωτόκολλα, το SSL record protocol και το SSL handshake protocol. Το SSL record protocol παρέχει υπηρεσίες αυθεντικοποίησης, εμπιστευτικότητας και ακεραιότητας δεδομένων, καθώς επίσης και προστασία από επιθέσεις με επανεκπομπή μηνυμάτων. Συγκεκριμένα το πρωτόκολλο αυτό τοποθετεί τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει. Επίσης εκτελεί την αντίστροφη διαδικασία για τα παραλαμβανόμενα πακέτα. Το SSL handshake protocol είναι ένα πρωτόκολλο αυθεντικοποίησης και ανταλλαγής κλειδιών το

οποίο επίσης διαπραγματεύεται, αρχικοποιεί και συγχρονίζει τις παραμέτρους ασφάλειας. Συγκεκριμένα το πρωτόκολλο αυτό διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του εξυπηρετητή και του πελάτη αν αυτό ζητηθεί. Μετά την ολοκλήρωση του SSL handshake protocol, τα δεδομένα των εφαρμογών μπορούν να αποστέλλονται μέσω του SSL record protocol ακολουθώντας τις συμφωνημένες παραμέτρους ασφάλειας.

10.4.4 Αντοχή του SSL σε Γνωστές Επιθέσεις

Επίθεση Λεξικού (Dictionary Attack)

Κατά την επίθεση αυτή, ένα τμήμα του μη κρυπτογραφημένου κειμένου βρίσκεται στην κατοχή κακόβουλων προσώπων. Το τμήμα αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί ένα κομμάτι που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του κειμένου έχει βρεθεί.

- Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα (128 bits). Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν 128 bits κλειδιά και παρ' όλο που τα 88 bits αυτών μεταδίδονται χωρίς κρυπτογράφηση, ο υπολογισμός 240 διαφορετικών ακολουθιών καθιστά την επίθεση εξαιρετικά δύσκολη.
- Βίαιη Επίθεση (Brute Force Attack)
- Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι ατελέσφορη.
- Επίθεση Επανάληψης (Replay Attack)
- Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ πελάτη - εξυπηρετητή και προσπαθεί να χρησιμοποιήσει ξανά τα μηνύματα του πελάτη για να αποκτήσει πρόσβαση στον εξυπηρετητή, έχουμε επίθεση τύπου replay attack. Όμως το SSL κάνει χρήση του αναγνωριστικού συνόδου (connection-

ID), το οποίο παράγεται από τον εξυπηρετητή με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια αναγνωριστικά σύνδεσης.

- Επίθεση Παρεμβολής (Man-In-The-Middle-Attack)
- Η επίθεση Man-In-The-Middle-Attack συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του εξυπηρετητή και του πελάτη. Αφού επεξεργαστεί τα μηνύματα του πελάτη και τα τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον εξυπηρετητή. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον εξυπηρετητή. Δηλαδή, προσποιείται στον πελάτη ότι είναι ο εξυπηρετητής και αντίστροφα.
- Το SSL υποχρεώνει τον εξυπηρετητή να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατη.

11. Συστήματα ανίχνευσης εισβολών

11.1 Βασικές Έννοιες

Ένα μεγάλο ερώτημα που ταλανίζει πάντα τους υπευθύνους ασφαλείας δικτύου υπολογιστών μιας επιχείρησης ή ενός οργανισμού είναι το πώς θα αντιληφθεί η επιχείρηση αν κάποιος εισέβαλε στο δίκτυό της. Ο εισβολέας δεν θα έχει αφήσει αποτυπώματα. Αν έχει εγκατασταθεί ένα ισχυρό firewall με ισχυρές δυνατότητες καταγραφής μπορεί να βρει αποδείξεις μιας επίθεσης στα αρχεία καταγραφής, αλλά ένας έξυπνος εισβολέας μπορεί να σβήσει ακόμη και αυτά τα ίχνη.

Για να δει επομένως τι ακριβώς συμβαίνει, χρειάζεται ένα σύστημα ανίχνευσης εισβολών. Για να δώσουμε τον ορισμό του συστήματος ανίχνευσης εισβολών θα πρέπει αρχικά να ορίσουμε την εισβολή.

Εισβολή ορίζεται οποιαδήποτε ακολουθία πράξεων που έχει σαν σκοπό να διαβάλλει την ακεραιότητα, την αξιοπιστία ή την διαθεσιμότητα ενός υπολογιστικού πόρου.

Ανίχνευση εισβολής καλείται το πρόβλημα του εντοπισμού πράξεων που έχουν σαν σκοπό να διαβάλλουν την ακεραιότητα, την αξιοπιστία ή την διαθεσιμότητα ενός υπολογιστικού πόρου.

Σύστημα Ανίχνευσης Εισβολών ορίζουμε την παρακολούθηση και ανάλυση των συμβάντων που λαμβάνουν χώρα σε υπολογιστές ή δίκτυα, με σκοπό να εντοπισθούν ενδείξεις προσπαθειών εισβολής. Οι προσπάθειες «εισβολής» περιλαμβάνουν ίχνη από απόπειρες για παραβίαση της ακεραιότητας, εμπιστευτικότητας ή διαθεσιμότητας των πληροφοριακών πόρων, καθώς επίσης και προσπάθειες για παράκαμψη των μηχανισμών ασφάλειας. Μια τέτοια εισβολή μπορεί να προέρχεται:

- Από ‘εξωτερικούς’ προς το εταιρικό δίκτυο χρήστες, οι οποίοι κανονικά δεν έχουν δικαίωμα πρόσβασης στο πληροφοριακό σύστημα, αλλά προσπαθούν να το προσπελάσουν.
- Από ‘εσωτερικούς’ χρήστες που έχουν περιορισμένα δικαιώματα πρόσβασης αλλά επιχειρούν ενέργειες που η πολιτική ασφάλειας τους απαγορεύει.
- Από ‘εσωτερικούς’ χρήστες, οι οποίοι έχουν κατάλληλα δικαιώματα πρόσβασης για τις πράξεις στις οποίες προβαίνουν, αλλά ασκούν τα

δικαιώματα αυτά με καταχρηστικό τρόπο. Για παράδειγμα, ένας υπάλληλος της μισθοδοσίας έχει δικαίωμα να τροποποιεί τους μισθούς των υπαλλήλων, αλλά η παροχή στον εαυτό του αύξησης 80% χωρίς τη σχετική εντολή από τη διοίκηση είναι μια περίπτωση καταχρηστικής άσκησης του δικαιώματός του.

Τα συστήματα ανίχνευσης εισβολής (Intrusion Detection Systems-IDS) είναι συστήματα που συντίθενται από υλικό και λογισμικό και έχουν ως στόχο την αυτοματοποίηση της ανίχνευσης εισβολών. Εξ' ορισμού ένα IDS απλά ανιχνεύει επιθέσεις και τις παρουσιάζει στο διαχειριστή ασφαλείας του δικτύου έτσι ώστε να αντιδρά γρήγορα σε μια επίθεση που δέχεται το δίκτυό του. Τα IDS συστήματα ανιχνεύουν και αναλύουν περίεργη δικτυακή κίνηση και αποφασίζουν αν πρόκειται για κάποιου είδους επίθεση ή όχι.

11.2 Τύποι συστημάτων ανίχνευσης εισβολής

Οι βασικοί τύποι των συστημάτων ανίχνευσης εισβολής είναι δύο το Network – Based (NIDSs) και το Host – Based (HIDSs).

Network – Based IDS

Τα Network – Based IDS είναι τα πιο διαδεδομένα και εξετάζουν τη διερχόμενη δικτυακή κίνηση (traffic) για ίχνη εισβολής. Συνήθως αποτελείται από δύο μέρη: τους αισθητήρες και τον σταθμό διαχείρισης / ανάλυσης. Ο αισθητήρας βρίσκεται σε ένα τομέα του δικτύου και παρακολουθεί για ύποπτη κίνηση. Ο σταθμός διαχείρισης λαμβάνει τις ενδείξεις κινδύνου από τους αισθητήρες και τις μεταβιβάζει στον διαχειριστή του συστήματος, δηλαδή στον διαχειριστή ασφαλείας του δικτύου.

Οι αισθητήρες είναι συνήθως συστήματα που υπάρχουν μόνο για να παρακολουθούν το δίκτυο. Έχουν ένα δικτυακό interface που αναλύει τα πάντα, δηλαδή λαμβάνουν όλη την δικτυακή κίνηση, όχι μόνο ότι προορίζεται για τη δικιά τους IP διεύθυνση, αλλά και το διερχόμενο από αυτούς traffic με σκοπό την περαιτέρω ανάλυση. Αν ανιχνεύσουν κάτι ύποπτο το μεταβιβάζουν στον σταθμό διαχείρισης / ανάλυσης. Ο σταθμός διαχείρισης / ανάλυσης μπορεί να δείξει τα σήματα κινδύνου, που έλαβε από τους αισθητήρες ή να πραγματοποιήσει επιπλέον ανάλυση.

Πλεονεκτήματα

1. Τα Δικτυακά συστήματα ανίχνευσης εισβολών λειτουργούν και ανιχνεύουν επιθέσεις σε πραγματικό χρόνο, οπότε προσφέρουν ταχύτατη ενημέρωση για την εξέλιξη μιας επίθεσης, ενώ μπορούν να προστατέψουν αυτόματα το δίκτυο πριν ακόμα γίνει ζημιά. Για παράδειγμα μπορεί να γίνει δυναμική ρύθμιση του firewall ώστε να σταματήσει τη σύνδεση με τη συγκεκριμένη IP από την οποία γίνεται η επίθεση.
2. Τα Network – Based IDSs έχουν την τάση να είναι καλύτερα αυτό-διατηρούμενα από ότι τα host – based. Τρέχουν σε ένα συγκεκριμένο σύστημα και η εγκατάστασή τους είναι απλή και πραγματοποιείται σε μια τοποθεσία στο δίκτυο που δίνει τη δυνατότητα παρακολούθησης ευαίσθητης κίνηση δεδομένων, χωρίς εξουσιοδότηση ή κάποιων ειδών πρόσβασης με κατάχρηση προνομίων εξουσιοδότησης.
3. Ένα Network – Based IDS δεν απαιτεί μετατροπές στους servers μιας επιχείρησης ή στους hosts για να εγκατασταθεί. Αυτό είναι μεγάλο όφελος, γιατί συνήθως οι servers έχουν κλειστές ανοχές όσο αφορά τη CPU, το I/O και την χωρητικότητα του δίσκου. Η εγκατάσταση επιπλέον λογισμικού ίσως να δημιουργήσει προβλήματα λειτουργικότητας.
4. Το Network – Based IDS δεν αποτελεί κρίσιμο παράγοντα για την λειτουργικότητα του δικτύου, και αυτό γιατί δεν λειτουργεί ως δρομολογητής ή ως κάποια άλλη κρίσιμη συσκευή. Άρα, τυχόν αποτυχία στο σύστημα του IDS δε θα έχει σημαντική επίδραση στην επιχείρηση. Ένα επιπλέον όφελος είναι ότι πιθανότατα θα συναντήσουμε λιγότερη αντίδραση από ανθρώπους εντός του εργασιακού περιβάλλοντος καθώς δεν θα απαιτηθεί να εγκαταστήσουν αυτοί κάτι στα συστήματά τους.
5. Τα Δικτυακά σύστημα ανίχνευσης εισβολών ανιχνεύουν επιθέσεις που τα host-based συστήματα δεν μπορούν να ανιχνεύσουν, όπως π.χ. επιθέσεις που βασίζονται στα περιεχόμενα των IP πακέτων.
6. Τα δικτυακά συστήματα ανίχνευσης εμποδίζουν τη διαγραφή των στοιχείων μιας επίθεσης από έναν επιτιθέμενο, αφού λόγω του ότι λειτουργούν σε πραγματικό χρόνο μπορούν να αποθηκεύουν τα στοιχεία αυτά σε ειδικούς χώρους. Έτσι ο επιτιθέμενος δεν μπορεί να διαγράψει τις αποδείξεις της επίθεσης του.

7. Με τη σωστή τοποθέτηση τους (έξω από το προστατευόμενο δίκτυο) τα συστήματα ανίχνευσης εισβολών μπορούν να δουν επιθέσεις που προορίζονταν για το δίκτυο αλλά αποτράπηκαν από το firewall, και γενικότερα μπορούν να βοηθήσουν στη συλλογή πληροφοριών για το τι είδους προσπάθειες επίθεσης γίνονται στο δίκτυο, έτσι ώστε να υπάρξει η δυνατότητα καλύτερης διαμόρφωσης της πολιτικής ασφάλειας του δικτύου.

Μειονεκτήματα

1. Ένα Network – Based IDS απλά εξετάζει τη δικτυακή σύνδεση στον τομέα που είναι συνδεδεμένο και μόνο. Δεν μπορεί να ανιχνεύσει μία επίθεση που γίνεται σε διαφορετικό τμήμα του δικτύου. Για να καλύψει τις ανάγκες του σε δικτυακή κάλυψη, ένας μεγάλος οργανισμός θα πρέπει να αγοράσει πολλούς αισθητήρες κάτι που σημαίνει επιπλέον κόστος.
2. Τα Network – Based IDS συνήθως χρησιμοποιούν ανάλυση signatures για να καλύψουν τις προδιαγραφές απόδοσης. Έτσι ανιχνεύονται κοινές προγραμματισμένες επιθέσεις από εξωτερικές πηγές, αλλά αυτή η μέθοδος δεν είναι επαρκής για πιο πολύπλοκα είδη επιθέσεων. Αυτές απαιτούν καλύτερη ικανότητα για ανάλυση του περιβάλλοντος.
3. Ένα σύστημα ανίχνευσης επιθέσεων μπορεί να χρειαστεί να μεταδώσει μεγάλες ποσότητες δεδομένων στο κεντρικό σύστημα ανάλυσης. Κάποιες φορές αυτό σημαίνει ότι οποιοδήποτε εξεταζόμενο πακέτο παράγει μία μεγαλύτερη ποσότητα κίνησης δεδομένων. Πολλά τέτοια συστήματα χρησιμοποιούν επιθετικές μεθόδους ελάττωσης δεδομένων για να μειώσουν το παραγόμενο traffic επικοινωνίας. Επίσης, προωθούν αρκετές από τις διαδικασίες επιλογής ενέργειας στον αισθητήρα μόνο και χρησιμοποιούν το σύστημα ανάλυσης ως οθόνη της κατάστασης του δικτύου ή ως κέντρο επικοινωνίας, παρά για πραγματική ανάλυση. Το μειονέκτημα εδώ είναι ότι παρέχεται ελάχιστος συντονισμός μεταξύ των αισθητήρων, δηλαδή οποιοσδήποτε αισθητήρας δεν γνωρίζει αν κάποιος άλλος έχει ανιχνεύσει μια επίθεση. Ένα τέτοιο σύστημα δεν μπορεί συνήθως να ανιχνεύσει συνεργατικές ή πολύπλοκες επιθέσεις.
4. Ένα Network – Based IDS δεν μπορεί να αναλύσει κρυπτογραφημένες πληροφορίες μέσα σε ένα δίκτυο, οπότε και δεν μπορούν να ανιχνεύσουν τυχόν επιθέσεις και πληροφορίες σε κρυπτογραφημένη μορφή.

Host – Based IDSs

Τα Host – Based IDSs παρακολουθούν τη δραστηριότητα χρηστών και εφαρμογών στο τοπικό μηχάνημα για ίχνη εισβολής. Αυτού του είδους τα IDSs παρέχουν πιο ακριβή πληροφορία για την ύπαρξη ή μη κάποιας επίθεσης και αυτό γιατί μπορούν να καταλάβουν τι συμβαίνει κάθε φορά στο σύστημα. Έτσι αν συμβεί μια άγνωστης μορφής επίθεση κατά την οποία γίνεται προσπάθεια να επιτευχθεί η δυσλειτουργία του υπολογιστή, το Host – Based IDS θα το αναγνωρίσει ως επίθεση, ενώ αντίθετα το Network – Based IDS δεν θα αντιληφθεί την επίθεση. Γενικά θεωρείται πως η χρήση Host – Based IDS έχει καλύτερα αποτελέσματα από την χρήση Network – Based IDS

Τα Host – Based IDSs ψάχνουν για ίχνη εισβολής στο τοπικό σύστημα του host. Χρησιμοποιούν συχνά το μηχανισμό ελέγχου και καταγραφής του host σαν πηγή πληροφοριών για ανάλυση. Πιο συγκεκριμένα ψάχνουν για ασυνήθη δραστηριότητα που περιορίζεται στον τοπικό host, όπως logins, παράξενη πρόσβαση σε αρχεία, μη εγκεκριμένη αύξηση δικαιωμάτων ή μετατροπές σε δικαιώματα του συστήματος.

Πλεονεκτήματα

1. Ένα Host – Based IDS μπορεί να αποτελέσει πολύ δυνατό εργαλείο ανάλυσης πιθανών επιθέσεων. Για παράδειγμα, είναι σε θέση μερικές φορές να πει τι ακριβώς έκανε ο εισβολέας, ποιες εντολές εκτέλεσε, ποια αρχεία έτρεξε και ποιες ρουτίνες του συστήματος κάλεσε αντί για μια αόριστη υπόθεση ότι προσπάθησε να εκτελέσει μια επικίνδυνη εντολή. Άρα τα Host – Based IDSs συνήθως παρέχουν πολύ πιο λεπτομερείς και σχετικές πληροφορίες από ότι τα Network – Based IDSs.
2. Τα Host – Based IDSs έχουν μικρότερους false positive ρυθμούς από ότι τα network based. Αυτό συμβαίνει γιατί το εύρος των εντολών που εκτελούνται σε ένα συγκεκριμένο host είναι πολύ πιο εστιασμένο, παρά τα είδη της κίνησης πακέτων που ρέουν σε ένα δίκτυο. Αυτή η ιδιότητα μπορεί να μειώσει την πολυπλοκότητα των Host – Based μηχανισμών.
3. Μπορούν να χρησιμοποιηθούν σε περιβάλλοντα όπου δεν χρειάζεται πλήρης ανίχνευση εισβολών ή όταν δεν υπάρχει διαθέσιμο bandwidth για επικοινωνία αισθητήρα – σταθμού ανάλυσης. Τα Host – Based IDSs είναι πλήρως αυτοσυντηρούμενα, κάτι που τους επιτρέπει, σε κάποιες περιπτώσεις, να

εκτελούνται από read-only μέσα. Έτσι, οι εισβολείς δύσκολα μπορούν να εξουδετερώσουν το IDS.

4. Σε ένα Host – Based σύστημα είναι ευκολότερο να σχηματιστεί μία ενεργή αντίδραση σε περίπτωση επίθεσης, όπως ο τερματισμός μιας υπηρεσίας ή το logging off ενός επιτιθέμενου χρήστη
5. Τα Host Based συστήματα ανίχνευσης εισβολών μπορούν να χρησιμοποιηθούν και σε κρυπτογραφημένα περιβάλλοντα δικτύου, καθώς τα δεδομένα αποκρυπτογραφούνται μόλις εισάγονται στο σύστημα.

Μειονεκτήματα

1. Τα Host – Based IDSs απαιτούν εγκατάσταση στο σύστημα που θέλουμε να προστατεύσουμε. Αν, για παράδειγμα, έχουμε έναν server που πρέπει να τον προστατέψουμε θα πρέπει να εγκατασταθεί το IDS στον server αυτόν. Όπως αναφέρθηκε και παραπάνω, αυτό μπορεί να προκαλέσει προβλήματα χωρητικότητας. Σε μερικές περιπτώσεις, αυτό μπορεί να προκαλέσει και προβλήματα ασφαλείας μιας και το προσωπικό που είναι υπεύθυνο για την ασφάλεια του συστήματος ίσως να μην έχει πρόσβαση στον server όταν χρειαστεί.
2. Ένα άλλο πρόβλημα είναι ότι έχουν την τάση να εξαρτώνται από το υπάρχον σύστημα καταγραφής (logging system) και ελέγχου του server. Εάν ο server δεν λειτουργεί έτσι ώστε η καταγραφή και ο έλεγχος να είναι σε ικανοποιητικό επίπεδο, θα πρέπει να γίνει αλλαγή στις ρυθμίσεις του. Αυτό αποτελεί τεράστιο πρόβλημα αλλαγής στη διαχείριση του server. Πώς είναι δυνατή η επαρκής πρόβλεψη των αποτελεσμάτων, αν χρειαστεί η προσθήκη δυνατότητας καταγραφής (logging);
3. Αυτά τα συστήματα είναι σχετικά ακριβά. Πολλοί οργανισμοί δεν έχουν την οικονομική δυνατότητα να προστατέψουν ολόκληρα δικτυακά τμήματα με τη χρήση Host – Based IDSs. Αντίθετα, θα πρέπει να επιλέξουν ποια συστήματα θα προστατέψουν και ποια όχι. Αυτό το γεγονός αφήνει μεγάλα κενά στην κάλυψη της ανίχνευσης εισβολών στο δίκτυο, αφού ένας εισβολέας σε ένα γειτονικό, αλλά απροστάτευτο σύστημα μπορεί να υποκλέψει πληροφορίες ή άλλο πολύτιμο υλικό από το δίκτυο.
4. Τα Host – Based IDSs είναι πιο ευάλωτα, σε μεγαλύτερο ακόμα βαθμό από τοπικούς περιορισμούς. Αγνοούν εντελώς το περιβάλλον του δικτύου, άρα ο

χρόνος ανάλυσης που απαιτείται για την εκτίμηση ζημιών από πιθανή εισβολή αυξάνει γραμμικά με τον αριθμό των host που προστατεύονται. Για παράδειγμα αν ένας άνθρωπος χρειάζεται t χρόνο για να ερευνήσει ένα περιστατικό σε 1 ένα σύστημα, θα χρειαστεί 2t για δύο συστήματα, 3t για τρία κοκ

5. Τέλος, Τα host based συστήματα απαιτούν εγκατάσταση στη συγκεκριμένη συσκευή που θέλουμε να προστατέψουμε. Δηλαδή πρέπει να διαμορφώνονται και να ρυθμίζονται ξεχωριστά για κάθε σύστημα στο οποίο εγκαθίστανται πρώτη φορά, κάτι που δημιουργεί προβλήματα στο προσωπικό που τα διαχειρίζεται.

11.3 Τεχνικές ανάλυσης επιθέσεων

Μια άλλη κατηγοριοποίηση των IDS γίνεται με βάση την τεχνική που χρησιμοποιούν για να ανιχνεύσουν τις εισβολές.

Υπάρχουν έξι κατηγορίες εισβολών:

1. Προσπάθεια εισόδου στο σύστημα, που ανιχνεύεται από τυπικά προφίλ συμπεριφοράς ή παραβιάσεις περιορισμών ασφαλείας.
2. Κρυφή επίθεση, που ανιχνεύεται επίσης από τα τυπικά προφίλ συμπεριφοράς.
3. Διείσδυση στο σύστημα ελέγχου ασφαλείας, η οποία ανιχνεύεται με συνεχή παρακολούθηση συγκεκριμένων προτύπων δραστηριότητας.
4. Διαρροή, που γίνεται αντιληπτή με μια τυπική χρήση των πόρων του συστήματος.
5. Denial of Service (άρνηση εκτέλεσης εφαρμογής), που επίσης γίνεται αντιληπτή από χρήση πόρων του συστήματος.
6. Κακόβουλη χρήση, που ανιχνεύεται μέσω τυπικής συμπεριφοράς προφίλ, παραβιάσεων κανόνων ασφαλείας, ή με χρήση ειδικών προνομίων.

Οι τεχνικές που χρησιμοποιούνται στην ανίχνευση εισβολών χωρίζονται σε δύο είδη:

Ανίχνευση Διαταραχών (Anomaly Detection)

Οι τεχνικές ανίχνευσης διαταραχών καταλήγουν στο συμπέρασμα ότι όλες οι επιθετικές δραστηριότητες είναι αναγκαστικά ανωμαλίες. Αυτό σημαίνει ότι αν

μπορούσαμε να καθιερώσουμε ένα “σύνηθες προφίλ δραστηριότητας” για ένα σύστημα, θα ήμασταν σε θέση, θεωρητικά, να σημαδέψουμε όλες τις καταστάσεις του συστήματος που αποκλίνουν από το καθιερωμένο προφίλ. Αυτό θα γίνει με βάση ένα, στατιστικά, σημαντικό νούμερο προσπαθειών εισβολής. Παρόλα αυτά αν συλλογιστούμε ότι το σύνολο των επιθετικών δραστηριοτήτων αλλάζει την κατάσταση του συνόλου των δραστηριοτήτων διαταραχής παρά να το αφήνει στην αρχική μορφή, βγάζουμε κάποιες ενδιαφέρουσες εκδοχές:

- Ασυνήθεις δραστηριότητες που δεν έχουν χαρακτήρα εισβολής χαρακτηρίζονται ως επιθετικές.
- Επιθετικές δραστηριότητες που δεν είναι ασυνήθεις, καταλήγουν σε false negatives (γεγονότα δεν χαρακτηρίζονται επιθέσεις, ενώ στην πραγματικότητα είναι).

Αυτό είναι ένα ιδιαίτερα επικίνδυνο πρόβλημα και μάλιστα σοβαρότερο από το πρόβλημα των false positive (γεγονότα που χαρακτηρίζονται ως επιθέσεις, ενώ δεν στην πραγματικότητα δεν είναι).

Τα κυριότερα ζητήματα λοιπόν, στην ανίχνευση διαταραχών σε συστήματα ανίχνευσης επιθέσεων, είναι να γίνονται οι επιλογές στα επίπεδα των ορίων, ώστε κανένα από τα δύο παραπάνω προβλήματα να μην μεγιστοποιείται. Σημαντική είναι, επίσης και η επιλογή των χαρακτηριστικών στην παρακολούθηση δεδομένων. Τα συστήματα ανίχνευσης διαταραχών είναι υπολογιστικά ακριβά, λόγω του κόστους του ελέγχου και του της συνεχούς ανανέωσης (updating) των μετρικών του προφίλ ενός συστήματος.

Ανίχνευση Κακής Συμπεριφοράς (Misuse Detection)

Η ιδέα πίσω από την misuse detection είναι ότι υπάρχουν τρόποι αναπαράστασης επιθέσεων με τη μορφή ενός προτύπου ή signature, ώστε ακόμα και παραλλαγές της επίθεσης να μπορούν να ανιχνευτούν. Άρα τα συστήματα μπορούν να ανιχνεύσουν πολλά ή όλα τα γνωστά πρότυπα εισβολής, αλλά δεν είναι αποτελεσματικά σε άγνωστες τεχνικές επίθεσης. Σημαντικό είναι να τονίσουμε πως τα anomaly detection συστήματα προσπαθούν να μαντέψουν το συμπλήρωμα της «κακής» συμπεριφοράς, ενώ τα misuse detection συστήματα προσπαθούν να αναγνωρίσουν γνωστές «κακές» συμπεριφορές. Το σημαντικότερο ζήτημα στα misuse detection συστήματα είναι το πώς θα δημιουργήσουμε signatures που να

περιγράφουν όλες τις πιθανές παραλλαγές μιας σχετικής επίθεσης και πώς θα δημιουργήσουμε signatures που αγνοούν την μη-επιθετική δραστηριότητα.

11.4 Χρησιμότητα των IDS

Τα συμβάντα ασφαλείας που ανιχνεύονται από ένα IDS είναι τριών ειδών:

- «Κακά» συμβάντα, όπως αυτά που συμβαίνουν κατά τη διάρκεια μιας επίθεσης.
- Συμβάντα κακής ρύθμισης του συστήματος, όπως αυτά που έχουν ως αποτέλεσμα την δυσλειτουργία των συστημάτων και οφείλονται σε λανθασμένη ρύθμιση των παραμέτρων λειτουργίας τους.
- Συμβάντα αναποτελεσματικότητας, όπως αναποτελεσματικής δικτυακής κίνησης.

Τα παραπάνω συμβάντα ασφαλείας συνήθως κατηγοριοποιούνται και με βάση την σοβαρότητάς τους, δηλαδή με βάση την ικανότητα που έχουν να βλάψουν το δίκτυο, αλλά και βάση της συχνότητάς τους, δηλαδή τον ρυθμό εμφάνισής τους στο δίκτυο. Τα συμβάντα που είναι πιο συχνά και σοβαρά, όπως για παράδειγμα το σκουλήκι Nimda, είναι πιο σημαντικό να εντοπιστούν άμεσα από αυτά που είναι πιο σπάνια ή έχουν μικρότερη επίδραση, όπως για παράδειγμα μια σάρωση θυρών από έναν «περίεργο» εργαζόμενο της εταιρείας. Ακόμη είναι σημαντικό να γίνεται και διαχωρισμός μεταξύ της σάρωσης ενός ασήμαντος συστήματος και ενός συστήματος που έχει σημαντικό ρόλο στην λειτουργία του δικτύου της εταιρείας.

Οι πληροφορίες που λαμβάνονται για καθένα από τους παραπάνω τύπους συμβάντων έχουν διαφορετική σημασία για τον διαχειριστή ασφαλείας του δικτύου. Για συμβάντα του πρώτου τύπου λαμβάνονται πληροφορίες που έχουν να κάνουν με τον τρόπο αντιμετώπισης των απειλών σε συστήματα που έχουν ή μπορούν να κυριευτούν από κάποιον κακόβουλο χρήστη. Για συμβάντα του δεύτερου τύπου, ο διαχειριστής λαμβάνει πληροφορίες σχετικές με λανθασμένες ρυθμίσεις συστημάτων και μπορεί έτσι να βοηθηθεί στην σωστή ρύθμιση των παραμέτρων λειτουργίας τους. Για τον τρίτο τύπο συμβάντων ο διαχειριστής λαμβάνει πληροφορίες που τον βοηθούν να βελτιστοποιήσει τον τρόπο λειτουργίας του δικτύου για το οποίο είναι υπεύθυνος.

Επομένως η χρήση ενός IDS στο δίκτυο έχει περισσότερα οφέλη από όσα πιθανά να φανταζόταν κάποιος. Καταρχήν παρέχει ένα δεύτερο επίπεδο προστασίας, κάτι που μειώνει ακόμη περισσότερο την πιθανότητα να παραβιαστεί η ασφάλεια ενός συστήματος του δικτύου. Το IDS με τον μηχανισμό καταγραφής συμβάντων και ειδοποίησης του υπευθύνου ασφαλείας δίνει την δυνατότητα για άμεση ή έμμεση αντίδραση σε κάθε ειδοποίηση. Αν υπάρχει αυτόματος μηχανισμός αντίδρασης έναντι της όποιας απειλής, για παράδειγμα με την χρήση κάποιου Intrusion Prevention System, τότε η επίθεση αντιμετωπίζεται άμεσα, πριν καν εξαπλωθεί τόσο ώστε να προκαλέσει επιπλέον και μεγαλύτερης έκτασης ζημιές. Σε περίπτωση που δεν υπάρχει τέτοιος μηχανισμός διαθέσιμος, η αντιμετώπιση της απειλής γίνεται από τον υπεύθυνο ασφαλείας ο οποίος αναλαμβάνει να εκτελέσει τις κατάλληλες ενέργειες για απομάκρυνση του κινδύνου που εμφανίστηκε στο δίκτυο.

Με την χρήση ενός IDS μπορούμε άμεσα να αναγνωρίσουμε λάθη στις ρυθμίσεις ενός δικτύου ή ενός εξυπηρετητή. Σε τόσο πολύπλοκα συστήματα λανθασμένες ρυθμίσεις παραμέτρων είναι πολύ συχνό φαινόμενο και μπορεί να συμβεί σε πολλά και διαφορετικά σημεία. Ευτυχώς για όλους μας τα σημερινά συστήματα είναι αρκετά ανεκτικά σε τέτοια λάθη και πολλές φορές κάνουν αυτό που πρέπει, με μειωμένη όμως απόδοση. Συχνά, η μειωμένη αυτή απόδοση δεν γίνεται αντιληπτή από τον χρήστη και επομένως οι όποιες λανθασμένες ρυθμίσεις παραμένουν. Επιπλέον, επειδή σε πολύ κρίσιμα συστήματα υπάρχουν και άλλα που αναλαμβάνουν δράση σε περίπτωση σφάλματος του πρωτεύοντος, γίνεται πολύ προσπάθεια για την ορθή λειτουργία αυτού του μηχανισμού αδιάλειπτης λειτουργίας και επομένως δεν βελτιώνονται οι ρυθμίσεις του πρωτεύοντος συστήματος. Ωστόσο ρυθμίζοντας κατάλληλα το βασικό σύστημα, ελαττώνουμε την συχνότητα έναρξης λειτουργίας του δευτερεύοντος μηχανισμού. Με την χρήση ενός IDS μπορούμε να ανιχνεύσουμε περιπτώσεις λανθασμένης δικτυακής κίνησης που οφείλεται σε λανθασμένη παραμετροποίηση των συστημάτων και επομένως να διορθώσουμε τις ρυθμίσεις των συστημάτων. Με τον τρόπο αυτό βελτιστοποιείται η συνολική λειτουργία του δικτύου και προσφέρονται αποδοτικότερες υπηρεσίες. Για παράδειγμα, μπορεί μια συσκευή να έχει αποθηκευμένο ένα λάθος κωδικό πρόσβασης σε αρχεία. Το IDS θα ανιχνεύσει τις αποτυχημένες προσπάθειες σύνδεσης και θα ειδοποιήσει τον διαχειριστή για το συμβάν. Αυτός με τη σειρά του θα δει που οφείλεται αυτό και θα ρυθμίσει πλέον κατάλληλα την συσκευή. Πολλά

αντίστοιχα λάθη μπορούν να διορθωθούν επειδή το IDS θα ανιχνεύσει την μη φυσιολογική δικτυακή κίνηση και τα συμβάντα που αυτή προκαλεί.

Ένα τρίτο όφελος από την χρήση ενός IDS στο δίκτυο είναι ότι μπορεί να βοηθήσει στην βελτιστοποίηση της δικτυακής κίνησης ή τουλάχιστον να προσφέρει στον διαχειριστή του δικτύου μια καλύτερη παρουσίαση του τρόπου λειτουργίας του δικτύου του. Με χρήση της τεχνικής «Ανίχνευσης Διαταραχών» που περιγράφηκε παραπάνω, το IDS δημιουργεί προφίλ «κανονικής» κίνησης και αντιδρά σε ότι αποκλίνει από το προφίλ αυτό. Αυτό, εκτός από το ότι του δίνει την δυνατότητα ανίχνευσης διαταραχών, επιτρέπει στο διαχειριστή να έχει μια άποψη της χρήσης των πόρων και της γενικότερης συμπεριφοράς του δικτύου σε περιόδους κανονικής λειτουργίας του δικτύου. Αυτό επιτρέπει στον διαχειριστή να προβεί σε κατάλληλες ενέργειες βελτίωσης της συνολικής λειτουργίας του δικτύου

Τέλος ένα βασικό χαρακτηριστικό της χρήσης IDS σε ένα δίκτυο, είναι ότι λειτουργεί ως αποτρεπτικό στοιχείο για τους κακόβουλους χρήστες. Από την στιγμή που γίνει γνωστό πως οι όποιες κακόβουλες ενέργειες ανιχνεύονται και τιμωρούνται, οι χρήστες το σκέφτονται διπλά πριν προβούν σε τέτοιες ενέργειες. Με τον τρόπο αυτό αυξάνεται η ασφάλεια του δικτύου, καθώς θα μειωθεί ο αριθμός των χρηστών που θα «δοκιμάσουν» τις δυνατότητες του συστήματος IDS, απλά και μόνο από φόβο μη γίνουν αντιληπτοί.

Από τα παραπάνω γίνεται εμφανές πως παρά το κόστος εγκατάστασης και χρήσης ενός συστήματος IDS στο δίκτυο, τα πλεονεκτήματα είναι τόσα ώστε αντισταθμίζεται το κόστος αυτό και αξίζει να γίνει συχνότερη η εμφάνιση τέτοιων συστημάτων προστασίας στα δίκτυα. Η χρήση συστημάτων IDS κρίνεται απαραίτητη για κάθε δίκτυο το οποίο θέλει να θεωρείται ασφαλές

11.5 Επίθεση σε Συστήματα Ανίχνευσης Εισβολής (Alert Flooding)

Οι προειδοποιήσεις (alerts) είναι ένας γρήγορος τρόπος ενημέρωσης των διαχειριστών ότι τα firewalls έχουν παραβιαστεί, τα δίκτυα βρίσκονται κάτω από εισβολή, οι σκληροί δίσκοι έχουν γεμίσει και όλων των ειδών άλλα προβλήματα. Οι προειδοποιήσεις μπορούν να πάρουν διάφορες μορφές σε διαφορετικές πλατφόρμες και προϊόντα συμπεριλαμβανομένων των ακολούθων:

- Παράθυρα pop – up στην κονσόλα του διαχειριστή.

- Ηλεκτρονικά μηνύματα που στέλνονται στο γραμματοκιβώτιο (mailbox) του διαχειριστή.
- Ηχογραφημένα ή γραπτά μηνύματα στο κινητό.
- Ηχητικά σήματα, οπτικές ενδείξεις ή άλλοι μέθοδοι για την πρόκληση της προσοχής.

Όταν ένα σύστημα IDS εντοπίζει μια πιθανή επίθεση στο δίκτυο, τυπικά παράγει μια προειδοποίηση για να ενημερώσει τους διαχειριστές για την κατάσταση. Αυτό τους επιτρέπει να ερευνήσουν το πρόβλημα, και να αποφασίσουν αν μια πραγματική επίθεση βρίσκεται σε εξέλιξη ή αν η προειδοποίηση ήταν λανθασμένη (false positive alert).

Ο καταιγισμός προειδοποιήσεων (alert flooding) είναι μια επίθεση που προσπαθεί να συντρίψει ένα σύστημα καταγραφής εισβολής με να το αναγκάσει να παράγει πάρα πολλές προειδοποιήσεις. Ο εισβολέας μπορεί να πετύχει κάτι τέτοιο με το να στείλει ένα μεγάλο πλήθος πακέτων που είναι ειδικά σχεδιασμένα για να προκαλέσουν το IDS να παράγει προειδοποιήσεις. Το αποτέλεσμα είναι ένας καταιγισμός προειδοποιήσεων που μπορεί να καταβάλλει τους διαχειριστές και να κρύψει λιγότερο φανερές προσπάθειες εισβολής στο σύστημα. Αν παραχθούν πάρα πολλές προειδοποιήσεις τότε η επίθεση αυτή μιμείται την επίδραση μιας επίθεσης άρνησης εξυπηρέτησης (Denial Of Service attack).

Αυτού του είδους η επίθεση είναι πιο αποτελεσματική ενάντια σε συστήματα ανίχνευσης εισβολής που στηρίζονται σε υπογραφές και λιγότερο αποτελεσματική ενάντια σε συστήματα που βασίζονται στην ανίχνευση ανωμαλιών.

11.6 Αντιδράσεις των Συστημάτων Ανίχνευσης Εισβολών

Οι αντιδράσεις των συστημάτων ανίχνευσης εισβολών διακρίνονται γενικά σε δύο κατηγορίες, τις ενεργές αντιδράσεις και τις παθητικές αντιδράσεις.

Ενεργές Αντιδράσεις

Στις ενεργές αντιδράσεις το σύστημα προσπαθεί να λάβει κάποια μέτρα για να τεκμηριώσει καλύτερα ή να αναχαιτίσει την επίθεση. Προς την κατεύθυνση αυτή το σύστημα ανίχνευσης εισβολών μπορεί να προβεί σε μία ή περισσότερες από τις ακόλουθες ενέργειες:

1. **Συλλογή περισσοτέρων πληροφοριών**, με κύριο στόχο την καλύτερη αξιολόγηση της επίθεσης ή/και τη συλλογή στοιχείων για νομικές ενέργειες. Προς την κατεύθυνση αυτή μπορεί να αυξηθεί η ευαισθησία των «αισθητήρων» π.χ. αρχείων καταγραφής, πακέτων δικτύου που αναλύονται κ.λ.π. ή να υπάρξουν «ερωτήσεις» προς το σύστημα από το οποίο εκπορεύεται η επίθεση για να διαπιστωθεί ποιοι χρήστες είναι συνδεδεμένοι κ.α.
2. **Τροποποίηση περιβάλλοντος**. Η κατεύθυνση αυτή αποσκοπεί στο να οδηγήσει την επίθεση σε αποτυχία. Αυτό μπορεί να επιτευχθεί με αποστολή προς τον επιτιθέμενο πακέτων τερματισμού σύνδεσης που να φαίνεται ότι προέρχονται από το υπό επίθεση σύστημα, με επαναρύθμιση firewalls και δρομολογητών και υπηρεσιών εισάγοντας απαγορεύσεις για διευθύνσεις IP, θυρών, δικτυακών πρωτοκόλλων, υπηρεσιών ή φυσικών συνδέσεων.
3. **Αντεπίθεση,** η οποία συνίσταται σε χρήση τεχνικών για αδρανοποίηση του επιτιθέμενου ή συλλογή πληροφοριών για αυτόν. Θα μπορούσε έτσι να υπάρξει καταιγισμός δικτυακών πακέτων προς το σύστημα απ' όπου φαίνεται να ξεκινά η επίθεση, ή εξαπόλυση επιθέσεων προς υπηρεσίες που αυτός προσφέρει. Η αντεπίθεση δεν είναι πρακτική που πρέπει να εφαρμόζεται στη γενική περίπτωση, καθώς μπορεί να έχει νομικές επιπτώσεις (η αυτοδικία δεν θεωρείται νόμιμη ενέργεια) και μπορεί επίσης να «θυμώσει» τους εισβολείς, με συνέπεια να εξαπολύσουν πιο «σκληρές» επιθέσεις. Είναι τέλος πιθανόν μία αντεπίθεση να έχει ως αποτέλεσμα να «χτυπηθούν» αθώοι, καθώς σε δημόσια δίκτυα (π.χ. δίκτυα IP) δεν υπάρχει ισχυρή διακρίβωση της ταυτότητας προέλευσης των δικτυακών πακέτων, και έτσι αυτή μπορεί να έχει πλαστογραφηθεί. Σε μία περίπτωση πλαστογραφίας της ταυτότητας προέλευσης, στη διάρκεια της αντεπίθεσης θα «χτυπηθεί» το σύστημα που φαίνεται στην ταυτότητα προέλευσης των δικτυακών πακέτων, το οποίο όμως δεν θα είναι το σύστημα από το οποίο προέρχεται η επίθεση. Αν πρόκειται σε οποιαδήποτε περίπτωση να χρησιμοποιηθεί τεχνική αντεπίθεσης, αυτή πρέπει να γίνει υπό την εποπτεία ειδικών.

Παθητικές Αντιδράσεις

Οι παθητικές αντιδράσεις συνίστανται κυρίως σε ειδοποιήσεις και συναγερμούς για το προσωπικό ασφάλειας. Οι ειδοποιήσεις αυτές μπορούν να έχουν

κυμαινόμενο βαθμό λεπτομέρειας και μπορούν να εμφανίζονται σε ειδικό χώρο του συστήματος ανίχνευσης εισβολών, σε παράθυρο μηνύματος, σε συσκευές τηλεειδοποίησης, με μηνύματα σε κινητά κ.ά. Μολονότι και το ηλεκτρονικό ταχυδρομείο θα μπορούσε να χρησιμοποιηθεί για ειδοποιήσεις αυτής της μορφής, είναι επισφαλές να βασισθεί κανείς σ' αυτό καθώς ο εισβολέας ενδέχεται να «μπλοκάρει» την αποστολή μηνυμάτων.

Για την αναφορά των προβλημάτων μπορεί να χρησιμοποιηθεί και το πρωτόκολλο SNMP, το οποίο είναι ένα ευρέως διαδεδομένο στάνταρ. Η προσέγγιση αυτή έχει το πλεονέκτημα ότι παρέχει τη δυνατότητα ολοκλήρωσης με συστήματα διαχείρισης δικτύου, αξιοποιώντας περαιτέρω μια δαπανηρή υποδομή (λογισμικού και επικοινωνίας), και ολοκληρώνοντας τις λειτουργίες διαχείρισης.

Συνολικά, η παθητικές αντιδράσεις είναι λιγότερο απαιτητικές σε πόρους από τις ενεργές αντιδράσεις.

11.7 Η 'Αυτοάμυνα' των Συστημάτων Ανίχνευσης Εισβολής

Σε πολλές περιστάσεις το ίδιο το σύστημα ανίχνευσης εισβολών μπορεί να αποτελέσει στόχο επιθέσεων με στόχο την ανίχνευση, την παράκαμψη ή την αχρήστευσή του. Θα πρέπει έτσι να λαμβάνονται μέτρα ώστε το ίδιο το IDS να μην γίνεται στόχος ή και να μπορεί να αποκρούει τέτοιου είδους επιθέσεις. Στα μέτρα αυτά μπορούν να εντάσσονται:

1. Η αποφυγή της κοινοποίησης της παρουσίας του IDS με δικτυακά μηνύματα, ακόμη και σε περιπτώσεις συναγερμού. Αν είναι απολύτως απαραίτητο να εκπεμφθεί μήνυμα, είναι σκόπιμο να εκπέμπεται με πλαστή δικτυακή διεύθυνση.
2. Συνολικά είναι καλό τα στοιχεία που συλλέγονται από το σύστημα ανίχνευσης εισβολών να διακινούνται από ξεχωριστά κανάλια επικοινωνίας, προκειμένου να μην εντοπίζεται η κυκλοφορία αυτή από τους πιθανούς εισβολής. Αν αυτό είναι αδύνατον, επιβάλλεται η χρήση κρυπτογράφησης και ισχυρών μηχανισμών διακρίβωσης ταυτότητας. Η κρυπτογράφηση προστατεύει τα διακινούμενα στοιχεία από το να αποκαλυφθούν στους εισβολείς, ενώ η ισχυρή διακρίβωση ταυτότητας αποτρέπει τους εισβολείς από το να αποστείλουν πλαστογραφημένα στοιχεία στο σύστημα ανίχνευσης εισβολών με στόχο την παραπλάνησή του.

3. Το ίδιο το σύστημα ανίχνευσης εισβολών δεν πρέπει να παρέχει δικτυακώς προσπελάσιμες υπηρεσίες, όπως απομακρυσμένης σύνδεσης, ηλεκτρονικού ταχυδρομείου κ.λπ., καθώς αυτές αφ' ενός θα αποκαλύψουν την ύπαρξή του, αφ' ετέρου μπορούν να αξιοποιηθούν από τους εισβολείς σε επιθέσεις εναντίον του συστήματος ανίχνευσης εισβολών.

11.8 Αρχεία καταγραφής παρακολούθησης

Ένα θεμελιώδες εργαλείο για την ανίχνευση εισβολής είναι το αρχείο καταγραφής παρακολούθησης (*audit record* ή *log file*), το οποίο περιέχει ως ένα βαθμό, τις δραστηριότητες των χρηστών του συστήματος. Βασικά χρησιμοποιούνται δύο τύποι αρχείων παρακολούθησης:

Τοπικά αρχεία παρακολούθησης

Σχεδόν όλα τα πληροφοριακά συστήματα πολλαπλών χρηστών περιλαμβάνουν κάποιο είδος λογισμικού καταγραφής στατιστικών στοιχείων (accounting) που συλλέγει πληροφορίες για τις δραστηριότητες των χρηστών. Το πλεονέκτημα χρήσης αυτών των αρχείων είναι ότι δεν χρειάζεται επιπλέον λογισμικό συλλογής πληροφοριών. Το μειονέκτημα είναι ότι τα τοπικά αρχεία παρακολούθησης μπορεί να μην περιέχουν τις απαιτούμενες πληροφορίες για κάθε περίπτωση ή να μην τις περιέχουν σε μια βολική μορφή.

Αρχεία παρακολούθησης για την ανίχνευση

Είναι ένα σύστημα συλλογής πληροφοριών το οποίο παράγει καταγραφές παρακολούθησης οι οποίες περιέχουν μόνο εκείνες τις πληροφορίες που απαιτούνται από το σύστημα ανίχνευσης εισβολής. Ένα πλεονέκτημα αυτής της προσέγγισης είναι ότι μπορεί να χρησιμοποιηθεί σε ένα μεγάλο εύρος συστημάτων αφού είναι ανεξάρτητη από τον κατασκευαστή. Το βασικό μειονέκτημα είναι ο επιπλέον φόρτος που προκύπτει από την ύπαρξη δύο πακέτων λογισμικού καταγραφής να εκτελούνται στο ίδιο σύστημα, καθώς και το κόστος απόκτησης.

Τα αρχεία καταγραφής είναι ανεκτίμητα όταν το σύστημα επανακάμπτει από κάποιο συμβάν παραβίασης της ασφάλειας. Συχνά τα αρχεία αυτά θα πληροφορήσουν τον διαχειριστή με ποιο τρόπο επιτέθηκε ο εισβολέας, και ακόμη θα του δώσουν στοιχεία για την ταυτότητα του. Μερικές φορές, τα αρχεία καταγραφής

μπορούν να χρησιμοποιηθούν σαν αποδεικτικά στοιχεία σε δικαστικές διαδικασίες. Για όλους τους παραπάνω λόγους σχεδόν πάντα είναι προτιμότερο να τηρούνται υπερβολικά πολλά αρχεία καταγραφής παρά υπερβολικά λίγα.

Ωστόσο, το πρώτο μέλημα ενός εισβολέα μόλις αποκτήσει πρόσβαση στο σύστημα είναι να κρύψει τα ίχνη του από τα αρχεία καταγραφής παρακολούθησης, είτε σβήνοντας τα, είτε διαγράφοντας επιλεκτικά εγγραφές από αυτά. Υπάρχουν εργαλεία λογισμικού όπως το Clean και το Zap2 που μπορούν αυτόματα να κάνουν αυτήν την δουλειά που ονομάζεται *log cleaning*. Ο μόνος τρόπος παρεμπόδισης αυτού είναι η δημιουργία ενός υπολογιστή- εξυπηρετητή ο οποίος θα συλλέγει στοιχεία για τα αρχεία παρακολούθησης από τους υπόλοιπους υπολογιστές στο δίκτυο. Ο συγκεκριμένος υπολογιστής δεν πρέπει να προσφέρει δικτυακές υπηρεσίες και δεν πρέπει να υποστηρίζει λογαριασμούς χρηστών παρά μόνο των διαχειριστών. Η βασική ιδέα πίσω από αυτό το σχέδιο είναι η προστασία του υπολογιστή που θα αποθηκεύει τα αρχεία καταγραφής από τον εισβολέα ακόμη και αν ο τελευταίος αποκτήσει πρόσβαση σε άλλα μηχανήματα στο δίκτυο.

Η ανάλυση των αρχείων παρακολούθησης είναι ένα βασικό στοιχείο της υπολογιστικής ασφάλειας, και η ανάλυση τους μπορεί να αποκαλύψει διάφορα στοιχεία για μια εισβολή.

Όμως αυτά τα αρχεία μπορούν να αναλυθούν και για άλλους λόγους, όπως η παρακολούθηση της απόδοσης του υπολογιστικού συστήματος ή κάποιας συγκεκριμένης εφαρμογής για να προσδιοριστούν οι ανάγκες αναβάθμισης του συστήματος. Εκατοντάδες διαφορετικά είδη λογισμικού ανάλυσης αρχείων παρακολούθησης (*log analysis software*) είναι διαθέσιμα στο εμπόριο, αλλά τα καλύτερα απο αυτά θα πρέπει να περιέχουν το λιγότερο τις εξής λειτουργίες:

- Υποστήριξη μεγάλου πλήθους διαφορετικών τύπων αρχείων παρακολούθησης.
- Προχωρημένες επιλογές φιλτραρίσματος (filtering) και αναζήτησης (query).
- Ισχυρές δυνατότητες αναφοράς, συμπεριλαμβανομένων των γενικών και αναλυτικών αναφορών.
- Αυτοματοποίηση της ανάλυσης σε πραγματικό χρόνο και την παραγωγή αναφορών.
- Απλό και εύκολο στην χρήση.

Όπως μας πληροφορούν οι Θόδωρος Κομνηνός και Ευάγγελος Σπυράκης, στο βιβλίο τους “Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων: Αναχαιτίστε τους εισβολείς”, τα δεδομένα που συλλέγονται πρέπει να περιλαμβάνουν κάθε προσπάθεια παραβίασης των επιπέδων ασφάλειας από ένα άτομο, διεργασία ή άλλη οντότητα του δικτύου. Αυτό περιλαμβάνει είσοδο στο σύστημα (*login*), έξοδο από το σύστημα (logout), πρόσβαση με δικαιώματα διαχειριστή, και κάθε άλλη δραστηριότητα κατά τη διαδικασία πρόσβασης ή αλλαγή της κατάστασης. Είναι ιδιαίτερα σημαντικό να καταγράφεται πότε γίνεται πρόσβαση με χρήση λογαριασμών “guest” ή ανώνυμη πρόσβαση σε δημόσιους εξυπηρετητές.

Τα στοιχεία που πρέπει να συγκεντρωθούν δεν είναι απαραίτητα τα ίδια για όλες τις εγκαταστάσεις και για διαφορετικούς τύπους προσβάσεων μέσα στο ίδιο πληροφοριακό σύστημα. Γενικά, η πληροφορία που πρέπει να συλλεχθεί περιλαμβάνει: το όνομα χρήστη (username) και το όνομα του κόμβου (hostname) για login και logout, δικαιώματα προηγούμενης και νέας πρόσβασης για αλλαγή των δικαιωμάτων πρόσβασης και ημερομηνία και ώρα (timestamp). Φυσικά, υπάρχει πολύ περισσότερη πληροφορία που μπορεί να συγκεντρωθεί, και η οποία εξαρτάται από το τι κάνει το σύστημα και πόσος είναι ο προσφερόμενος χώρος για την αποθήκευση της συλλεγόμενης πληροφορίας.

11.9 Λοιπά Εργαλεία Ασφάλειας (Security Tools)

Εκτός από το λογισμικό ανίχνευσης εισβολής που αποτελεί το αντίστοιχο του συναγερμού στον κόσμο της πληροφορικής υπάρχουν και κάποια άλλα προγράμματα που εντάσσονται και αυτά στην γενικότερη κατηγορία των εργαλείων ασφαλείας (*security tools*). Τα περισσότερα προγράμματα αυτού του είδους που είναι διαθέσιμα σήμερα γράφθηκαν σε πανεπιστήμια ή από ανεξάρτητους ειδικούς και διανέμονται ελεύθερα στο διαδίκτυο, ωστόσο υπάρχουν και αρκετά πολύ καλά εμπορικά προγράμματα του είδους.

Έτσι λοιπόν εκτός από τα προγράμματα ανίχνευσης εισβολής υπάρχουν τέσσερα επιπρόσθετα είδη εργαλείων που θα μπορούσε κάποιος να χρησιμοποιήσει:

Εργαλεία στιγμιότυπου (Snapshot tools).

Είναι εργαλεία που λαμβάνουν μια γενική εικόνα (snapshot) του συστήματος και ψάχνουν για πιθανές αδυναμίες.

Τα snapshot ή static audit tools εξετάζουν το σύστημα για αδυναμίες και παράγουν αναφορές με τα ευρήματα τους. Μπορούν να διεξάγουν εκατοντάδες ελέγχους μέσα σε σύντομο χρονικό διάστημα. Ένα snapshot πρόγραμμα θα πρέπει να εκτελείται σε τακτική βάση όχι λιγότερο από μια φορά τον μήνα, και πιθανότατα τουλάχιστον μια φορά την εβδομάδα. Οι αναφορές που παράγονται θα πρέπει να εξετάζονται προσεκτικά και να λαμβάνονται υπ'όψιν. Επίσης, προσοχή θα πρέπει να δοθεί έτσι ώστε καμία από αυτές τις αναφορές να μην είναι προσβάσιμη σε άλλους: εξ' ορισμού, οι "τρύπες" ασφαλείας που περιγράφονται στις αναφορές μπορούν εύκολα να χρησιμοποιηθούν από εισβολείς.

Εργαλεία ανίχνευσης αλλαγής (Change-detecting tools ή file integrity checkers).

Είναι εργαλεία που εξετάζουν το σύστημα περιοδικά, ψάχνοντας για μη εξουσιοδοτημένες αλλαγές.

Είναι σημαντικό να εξετάζεται το υπολογιστικό σύστημα σε τακτική βάση για μη εξουσιοδοτημένες αλλαγές. Αυτό γιατί ένα από τα πρώτα πράγματα που κάνει ένας εισβολέας μόλις εισβάλει σε ένα σύστημα είναι να το τροποποιήσει έτσι ώστε να μπορέσει με ευκολία να αποκτήσει ξανά πρόσβαση στο μέλλον, ή να αποκρύψει τις αποδείξεις της εισβολής. Ψάχνοντας για αλλαγές δεν θα εμποδίσει μια εισβολή αλλά μπορεί να αφυπνίσει τον διαχειριστή ότι το σύστημα του έχει δεχθεί επίθεση. Καθώς οι περισσότερες εισβολές δεν παρατηρούνται για κάποιο χρονικό διάστημα, τα εργαλεία ανίχνευσης αλλαγής ίσως να αποτελούν τον μόνο τρόπο ειδοποίησης του διαχειριστή για την παρουσία ενός εισβολέα έτσι ώστε να λάβει τα κατάλληλα μέτρα.

Πιο συγκεκριμένα, η συχνότερη μέθοδος παρακολούθησης αλλαγών στα αρχεία είναι ο υπολογισμός ενός ελεγκτικού αθροίσματος (*checksum*) των αρχείων συστήματος αμέσως μετά την εγκατάσταση του λειτουργικού συστήματος. Το ελεγκτικό άθροισμα είναι μια υπολογιζόμενη τιμή που βασίζεται στα περιεχόμενα του αρχείου.

Οποιαδήποτε αλλαγή στα περιεχόμενα του αρχείου μεταβάλλει το ελεγκτικό άθροισμα. Το άθροισμα αυτό δημιουργείται χρησιμοποιώντας έναν έλεγχο κυκλικού πλεονασμού ή για μεγαλύτερη ασφάλεια χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους όπως ο MD5 ή ο SHA-1 (Secure Hash Algorithm). Αν η αρχική τιμή του αθροίσματος με μια μεταγενέστερη διαφέρουν, τότε έχει συμβεί αλλαγή στα περιεχόμενα του αρχείου.

Όταν δύο ή περισσότερα άτομα διαχειρίζονται ένα πληροφοριακό σύστημα, οι αναφορές που παράγονται από τα προγράμματα ανίχνευσης αλλαγής αποτελούν

έναν εύκολο τρόπο ενημέρωσης του κάθε διαχειριστή για τις ενέργειες των συναδέλφων του.

Υπάρχουν αρκετά δωρεάν αλλά και εμπορικά προγράμματα ανίχνευσης αλλαγών. Μερικά από τα ποιο γνωστά είναι τα AIDE, FileChecker, fsum, L5, Integrit, SP1, Tripwire και yafic. Το LANguard File Integrity Checker της εταιρείας Gfi είναι ένα γνωστό δωρεάν πρόγραμμα που μπορεί να προειδοποιήσει τους διαχειριστές συστημάτων με Windows NT, 2000 ή XP όταν τα αρχεία συστήματος τροποποιούνται, σβήνονται ή προσθέτονται. Πολλά συστήματα ανίχνευσης εισβολής περιλαμβάνουν file integrity checkers, όπως επίσης και κάποια firewalls και αντι-ιικά προγράμματα.

Εργαλεία σάρωσης δικτύου (Network scanning tools).

Είναι εργαλεία που εξετάζουν το δίκτυο αυτόματα , ψάχνοντας για δικτυακές αδυναμίες. Αυτά τα εργαλεία ψάχνουν για γνωστά σφάλματα ασφάλειας. Επίδοξοι εισβολείς χρησιμοποιούν σε καθημερινή βάση αυτά τα εργαλεία για να ελέγξουν κάθε είδους υπολογιστικό δίκτυο, έτσι ο κάθε διαχειριστής μπορεί κάλλιστα να τα χρησιμοποιήσει για να ελέγξει το δικό του δίκτυο.

Σύστημα προστασίας εφαρμογής (Application Protection System).

Ένα σύστημα προστασίας εφαρμογής (*application protection system – APS*) είναι σχεδιασμένο για να συμπληρώνει το σύστημα ανίχνευσης εισβολής με το να εξετάζει την κίνηση από τον Παγκόσμιο Ιστό (*HTTP traffic*) ψάχνοντας για ύποπτα μοτίβα.

Ενώ το σύστημα ανίχνευσης εισβολής προειδοποιεί τους διαχειριστές για την παρουσία ύποπτης κίνησης, το σύστημα προστασίας εφαρμογής γενικά μπλοκάρει τέτοια κίνηση και δεν την αφήνει να φθάσει τους διακομιστές Παγκόσμιου Ιστού (*Web servers*). Η διαχείριση ενός τέτοιου συστήματος συνήθως στηρίζεται σε πολιτικές που καθορίζουν ποιοι τύποι κίνησης Παγκόσμιου Ιστού θεωρούνται κακόβουλοι ή βλαβεροί για τους διακομιστές Παγκόσμιου Ιστού. Το μεγάλο πλεονέκτημα αυτών των συστημάτων είναι ότι συχνά μπορούν να εντοπίσουν νέους τύπους επίθεσης ακόμη και πριν αυτοί να έχουν αναγνωριστεί από τους οργανισμούς προστασίας του διαδικτύου.

Μια πλειάδα κατασκευαστών προσφέρουν λογισμικό APS, όπως οι εταιρείες Kavado, Protegrity, Sanctum και Stratum8.

Τα αυτοματοποιημένα εργαλεία ασφαλείας είναι ένας χαμηλού κόστους και ιδιαίτερα αποτελεσματικός τρόπος εξέτασης και βελτίωσης της ασφάλειας ενός

πληροφοριακού συστήματος. Ωστόσο αρκετά από αυτά τα εργαλεία χρησιμοποιούνται συστηματικά και από επίδοξους εισβολείς που ψάχνουν για αδυναμίες σε συστήματα συνδεδεμένα με το Διαδίκτυο. Έτσι το να μην χρησιμοποιούνται και από τους διαχειριστές συστημάτων αυτόματα τους θέτει σε μειονεκτική θέση απέναντι στους εισβολείς. Σε μια γενικότερη προσπάθεια ενοποίησης πολλών ειδών παρόμοιων προγραμμάτων σε μια εφαρμογή, αρκετά από τα προγράμματα ανίχνευσης εισβολής περιλαμβάνουν πολλά στοιχεία από τα υπόλοιπα εργαλεία ασφάλειας.

12. Πολιτικές ασφάλειας των πληροφοριακών συστημάτων

12.1 Βασικές έννοιες

Γενικά στο πλαίσιο της λειτουργίας ενός οργανισμού μια πολιτική αποτελεί το σύνολο των οδηγιών της διοίκησης για τον τρόπο με τον οποίο πρέπει να λειτουργεί ο οργανισμός. Περιλαμβάνει δηλαδή γενικές προτάσεις-δηλώσεις (high-level statements) που έχουν στόχο να καθοδηγήσουν τη λήψη αποφάσεων σχετικά με τα τρέχοντα και μελλοντικά ζητήματα που αντιμετωπίζουν τα μέλη του οργανισμού. Πολλές φορές στον όρο 'πολιτική' αποδίδεται η έννοια των γενικευμένων απαιτήσεων, στις οποίες θα πρέπει να ανταποκρίνεται η δράση και οι επιλογές των ανθρώπων τους οποίους αφορά η πολιτική.

Πολιτική ασφάλειας πληροφοριακών συστημάτων

Η πολιτική ασφάλειας των πληροφοριακών συστημάτων, αν και μπορεί να διαφέρει σημαντικά από οργανισμό σε οργανισμό, περιλαμβάνει γενικά το σκοπό και τους στόχους της ασφάλειας, οδηγίες, διαδικασίες, κανόνες, ρόλους και υπευθυνότητες που αφορούν την προστασία των πληροφοριακών συστημάτων του οργανισμού. Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην πολιτική ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων προστασίας για την ασφάλεια των πληροφοριακών συστημάτων. Η πολιτική ασφάλειας διατυπώνεται σε ένα έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να ακολουθούν όλα τα μέλη του οργανισμού, στις δραστηριότητές τους που έχουν σχέση με τα πληροφοριακά συστήματα που καλύπτει η πολιτική.

Στην πολιτική ασφάλειας, δηλαδή, καθορίζονται οι στόχοι της ασφάλειας, καθώς και ο τρόπος με τον οποίο οι στόχοι αυτοί θα υλοποιηθούν. Βασικό συστατικό στοιχείο, επομένως, κάθε πολιτικής ασφάλειας πληροφοριακών συστημάτων είναι η περιγραφή των κανόνων και των διαδικασιών που πρέπει να ακολουθούνται για την προστασία των πληροφοριακών συστημάτων, καθώς και ο καθορισμός των συγκεκριμένων ρόλων και αρμοδιοτήτων που απαιτούνται για την υλοποίηση της πολιτικής ασφάλειας.

Η εφαρμογή μιας πολιτικής ασφάλειας σε έναν οργανισμό έχει δεσμευτικό χαρακτήρα για όλα τα μέλη του οργανισμού. Αυτό σημαίνει ότι η τήρηση των

διαδικασιών και οδηγιών που προβλέπει η πολιτική ασφάλειας, και η εφαρμογή των μέτρων ασφάλειας που προδιαγράφονται σε αυτήν, είναι υποχρεωτική για όλους τους χρήστες των πληροφοριακών συστημάτων.

Οδηγίες, Διαδικασίες και Μέτρα προστασίας

Οι πολιτικές ασφάλειας δηλώνουν τους στόχους για την ασφάλεια των πληροφοριακών συστημάτων και τα γενικά μέσα για την επίτευξή τους, ενώ οι οδηγίες (guidelines), που περιλαμβάνονται στην πολιτική ασφάλειας, αποσκοπούν στη δημιουργία του κατάλληλου πλαισίου για την επίτευξη των στόχων της πολιτικής ασφάλειας. Οι διαδικασίες (procedures) δίνουν συγκεκριμένες κατευθύνσεις για την υλοποίηση και εφαρμογή των οδηγιών της πολιτικής.

Τέλος, μια Πολιτική Ασφάλειας συνοδεύεται από ένα σύνολο μέτρων προστασίας (security measures, security controls), ή αντιμέτρων (countermeasures) ή μέτρων ασφάλειας (security measures, security controls) όπως αλλιώς λέγονται, η εφαρμογή των οποίων παρέχει στα πληροφοριακά συστήματα το επίπεδο ασφάλειας που προσδιορίζεται στην πολιτική ασφάλειας. Η Πολιτική Ασφάλειας μαζί με το σύνολο των μέτρων προστασίας αποτελούν το Σχέδιο Ασφάλειας (Security Plan) για τα πληροφοριακά συστήματα ενός οργανισμού.

12.2 Σκοπιμότητα πολιτικής ασφάλειας πληροφοριακών συστημάτων

Στο πλαίσιο των δραστηριοτήτων για τη διαχείριση της ασφάλειας των πληροφοριακών συστημάτων σε ένα οργανισμό, μια από τις σημαντικότερες δραστηριότητες είναι η ανάπτυξη και εφαρμογή της πολιτικής ασφάλειας. Η ανάπτυξη της πολιτικής ασφάλειας αποτελεί μια διαδικασία που λαμβάνει χώρα ταυτόχρονα με τις υπόλοιπες επιχειρηματικές διαδικασίες του οργανισμού και σχετίζεται όχι μόνο με το πληροφοριακό σύστημα, το οποίο άμεσα αφορά, αλλά και με τον οργανισμό μέσα στον οποίο το πληροφοριακό σύστημα λειτουργεί. Η διαδικασία της ανάπτυξης και της εφαρμογής της πολιτικής ασφάλειας των πληροφοριακών συστημάτων έχει κρίσιμη σημασία για τον οργανισμό, καθώς πολλές από τις λειτουργίες του βασίζονται στα συστήματα αυτά. Στις επόμενες παραγράφους περιγράφονται η σκοπιμότητα και η αναγκαιότητα για τη δημιουργία και εφαρμογή μιας πολιτικής ασφάλειας.

Καθοδήγηση της επιλογής και υλοποίησης των μέτρων ασφαλείας

Η άμεση αντιμετώπιση προβλημάτων ασφάλειας του πληροφοριακού συστήματος σε μια επιχείρηση ή έναν οργανισμό συνδέεται, τις περισσότερες φορές, με την αγορά αντίστοιχων προϊόντων ασφάλειας (υλικού ή λογισμικού) για την υιοθέτηση κάποιων μέτρων προστασίας των πληροφοριακών συστημάτων. Τα προϊόντα αυτά συνήθως χρησιμοποιούνται χωρίς να υπάρχει η απαραίτητη οργανωτική υποδομή, γεγονός που τα καθιστά αναποτελεσματικά.

Επίσης, η προστασία των πληροφοριακών συστημάτων απαιτεί την υλοποίηση μιας πληθώρας διαφορετικών μέτρων ασφάλειας, άλλα από τα οποία μπορεί να είναι τεχνικής φύσης (όπως για παράδειγμα οι έξυπνες κάρτες για τον έλεγχο πρόσβασης), άλλα διοικητικής φύσης (όπως ο καθορισμός διαδικασιών ελέγχου και συστήματος κυρώσεων για τους παραβάτες της πολιτικής ασφάλειας). Θα πρέπει επομένως να εξασφαλιστεί η συνεπής υλοποίηση όλων των μέτρων ασφάλειας, τόσο για να αποφευχθεί η περίπτωση επικαλύψεων, εφαρμογή δηλαδή μέτρων προστασίας που αντιμετωπίζουν τις ίδιες απειλές, όσο και για να μην υπάρχουν συγκρούσεις και ασυμβατότητες, υλοποίηση δηλαδή μέτρων προστασίας με αντικρουόμενους στόχους.

Δημιουργία 'καναλιού επικοινωνίας' μεταξύ των εμπλεκόμενων

Η διαχείριση της ασφάλειας των πληροφοριακών συστημάτων είναι μια διαδικασία στην οποία εμπλέκονται πολλοί φορείς, οι οποίοι μπορεί να βρίσκονται τόσο εντός όσο και εκτός του οργανισμού. Οι ρόλοι εντός του οργανισμού που έχουν σημαντική εμπλοκή στην ασφάλεια των πληροφοριακών συστημάτων περιλαμβάνουν, μεταξύ άλλων, τους χρήστες και τους διαχειριστές των συστημάτων αυτών, τους υπεύθυνους για την ασφάλεια, και τα διοικητικά στελέχη του οργανισμού. Η καλή επικοινωνία και συνεργασία όλων των εμπλεκομένων (stakeholders) είναι βασική προϋπόθεση για την αποτελεσματική διαχείριση της ασφάλειας των πληροφοριακών συστημάτων. Η πολιτική ασφάλειας, που αποτελεί το έγγραφο στο οποίο δηλώνονται τόσο οι στόχοι όσο και τα γενικά μέτρα για την ασφάλεια των πληροφοριακών συστημάτων, μπορεί να αποτελέσει ένα σημαντικό σημείο αναφοράς για την επικοινωνία και διαπραγμάτευση μεταξύ των εμπλεκομένων φορέων, ώστε να δημιουργηθεί μια κοινή αντίληψη για την αναγκαιότητα της ασφάλειας.

Εξασφάλιση και διαχείριση των απαραίτητων πόρων

Η προστασία των πληροφοριακών συστημάτων ενός οργανισμού είναι μια δαπανηρή σε πόρους διαδικασία. Οι σύγχρονοι οργανισμοί δαπανούν σημαντικά ποσά για την προμήθεια και εφαρμογή μέτρων ασφάλειας καθώς και για την υλοποίηση των συναφών διαδικασιών, όπως είναι για παράδειγμα ο έλεγχος και η πιστοποίηση της ασφάλειας των πληροφοριακών συστημάτων, ενώ παράλληλα απαιτείται και η εμπλοκή έμπειρου και εξειδικευμένου προσωπικού. Για τους λόγους αυτούς, η ασφάλεια των πληροφοριακών συστημάτων θα πρέπει να αντιμετωπίζεται σαν ένα αυτοτελές έργο (project) μέσα στον οργανισμό. Θα πρέπει από την αρχή της προσπάθειας αυτής να αναγνωρίζονται οι διαφορετικοί εμπλεκόμενοι και τα συμφέροντά τους, να χρονοπρογραμματίζονται όλες οι ενέργειες που απαιτούνται και να δεσμεύονται οι απαραίτητοι πόροι. Η εμπλοκή και ενεργός συμμετοχή της διοίκησης είναι πολύ σημαντική στη φάση αυτή, τόσο γιατί δίνεται έμφαση στους στόχους της ασφάλειας, όσο και γιατί διασφαλίζονται οι αναγκαίοι πόροι. Η ανάπτυξη μιας πολιτικής ασφάλειας, επομένως, βοηθά σημαντικά στην αποδοτική διαχείριση της ασφάλειας των πληροφοριακών συστημάτων σε έναν οργανισμό.

Εδραίωση της σημασίας της ασφάλειας των Πληροφοριακών Συστημάτων στον οργανισμό.

Η δέσμευση της διοίκησης ενός οργανισμού για την ασφάλεια των πληροφοριακών του συστημάτων όπως διατυπώνεται στην πολιτική ασφάλειας, καθιστά την ασφάλεια σημαντικό ζήτημα στην διοικητική ‘ατζέντα’ του οργανισμού. Έτσι η σπουδαιότητα της ασφάλειας θεμελιώνεται μεταξύ των μελών του οργανισμού και διασφαλίζεται η εφαρμογή των μέτρων προστασίας από τους χρήστες των πληροφοριακών συστημάτων.

Καλλιέργεια ‘κουλτούρας ασφάλειας’.

Η εφαρμογή πολιτικής ασφάλειας των πληροφοριακών συστημάτων, αποτελεί ένα βασικό βήμα για την δημιουργία μιας ‘κουλτούρας ασφάλειας’. Με τον όρο αυτό, εννοούμε ότι οι χρήστες των πληροφοριακών συστημάτων αποκτούν κοινή αντίληψη και γνώση για την ανάγκη προστασίας και τους στόχους ασφάλειας. Δημιουργούνται έτσι κοινές πρακτικές και πεποιθήσεις που αφορούν στην ανάγκη και τους τρόπους προστασίας των πληροφοριακών συστημάτων και αναπτύσσεται κουλτούρα ασφάλειας.

Η σημασία που έχει η κουλτούρα ασφάλειας σε έναν οργανισμό φαίνεται στα ακόλουθα: Μια πολιτική ασφάλειας, όσο πλήρης και λεπτομερειακή και αν είναι, δε μπορεί ποτέ να καλύψει το σύνολο των απαιτήσεων για την ασφάλεια των πληροφοριακών συστημάτων, αφενός διότι η τεχνολογία αναπτύσσεται με γοργούς ρυθμούς, αφετέρου διότι οι λειτουργίες των περισσότερων οργανισμών δεν είναι στατικές, αλλά αλλάζουν σε συνάρτηση με το περιβάλλον, που είναι δυναμικό και επίσης μεταβάλλεται με γρήγορους ρυθμούς. Συνεπώς, είναι αναμενόμενο οι χρήστες των πληροφοριακών συστημάτων να αντιμετωπίζουν καταστάσεις ή νέες απειλές κατά των πληροφοριακών συστημάτων που δεν έχουν προβλεφθεί, και για τις οποίες δεν υπάρχει σαφής καθοδήγηση από το έγγραφο στο οποίο περιγράφεται η πολιτική ασφάλειας. Στις περιπτώσεις αυτές, οι χρήστες των πληροφοριακών συστημάτων θα πρέπει να έχουν μια γενικότερη γνώση και να συμμερίζονται τους στόχους της πολιτικής ασφάλειας, ώστε να είναι σε θέση να δράσουν με τρόπο που θα συντελεί στην προστασία των πληροφοριακών συστημάτων. Επομένως, η κουλτούρα ασφάλειας συμβάλλει στην αποτελεσματικότερη αντιμετώπιση των απειλών κατά των πληροφοριακών συστημάτων.

Ικανοποίηση νομικών υποχρεώσεων του οργανισμού

Οι στόχοι ασφάλειας των πληροφοριακών συστημάτων και τα μέτρα προστασίας που απαιτείται να λάβει ένας οργανισμός, εξαρτώνται επίσης από το νομικό και κανονιστικό πλαίσιο που διέπει τη λειτουργία του. Η εφαρμογή πολιτικής ασφάλειας για τα πληροφοριακά συστήματα αποτελεί σε πολλές περιπτώσεις νομική υποχρέωση για έναν οργανισμό. Για παράδειγμα, ένα νοσοκομείο θα πρέπει να ικανοποιεί τις απαιτήσεις για την προστασία των ευαίσθητων προσωπικών δεδομένων που αφορούν την υγεία των ασθενών του και τυγχάνουν επεξεργασίας ή είναι αποθηκευμένα στο πληροφοριακό του σύστημα.

Υποστήριξη επιχειρηματικών αναγκών.

Πολλές λειτουργίες των σύγχρονων οργανισμών εξαρτώνται από τα πληροφοριακά συστήματα, κατά συνέπεια η ασφάλεια των πληροφοριακών συστημάτων είναι πολύ σημαντική για την ικανότητα του οργανισμού να λειτουργεί απρόσκοπτα. Εκτός αυτού, όμως, η εφαρμογή πολιτικής ασφάλειας των πληροφοριακών συστημάτων, συμβάλει στην υποστήριξη των επιχειρηματικών

δραστηριοτήτων καθώς αποτελεί βασικό στοιχείο για την ανάπτυξη σχέσεων εμπιστοσύνης με τους πελάτες και των επιχειρηματικούς εταίρους του οργανισμού.

12.3 Αρχές διαμόρφωσης πολιτικής ασφάλειας

Πολιτική ασφάλειας των πληροφοριακών συστημάτων για έναν οργανισμό μπορεί να αναπτύξουν είτε στελέχη του οργανισμού που διαθέτουν τις απαιτούμενες γνώσεις και εμπειρία, για παράδειγμα ο ειδικός της ασφάλειας για τα πληροφοριακά συστήματα, εφόσον υπάρχει τέτοια θέση στον οργανισμό, είτε κάποιος εξωτερικός σύμβουλος με τα αντίστοιχα προσόντα. Σε κάθε περίπτωση όμως, είτε δηλαδή η ανάπτυξη της πολιτικής ασφάλειας γίνεται εσωτερικά από μέλη του οργανισμού είτε εξωτερικά, θα πρέπει να λαμβάνονται υπόψη τα σημεία που περιγράφονται στις ακόλουθες παραγράφους.

Θα πρέπει επίσης να αναφερθεί ότι υπάρχουν ειδικές περιπτώσεις πληροφοριακών συστημάτων για τα οποία η σχετική Πολιτική Ασφάλειας θα πρέπει να ακολουθεί συγκεκριμένες, κατά περίπτωση, αρχές και πρότυπα. Χαρακτηριστικές περιπτώσεις τέτοιων πληροφοριακών συστημάτων αποτελούν για παράδειγμα τα Ιατρικά Πληροφορικά Συστήματα.

12.3.1 Εμπλεκόμενοι στην ανάπτυξη των Πολιτικών Ασφάλειας

Η ανάπτυξη της πολιτικής ασφάλειας των πληροφοριακών συστημάτων ενός οργανισμού βασίζεται στην καταγραφή των απαιτήσεων ασφάλειας, με βάση τις οποίες διαμορφώνονται οι στόχοι της ασφάλειας, και στον προσδιορισμό των τρόπων για την επίτευξη των στόχων αυτών. Οι απαιτήσεις ασφάλειας μπορεί να προέρχονται από διαφορετικές πηγές, όπως:

- Οι χρήστες των πληροφοριακών συστημάτων.
- Η διοίκηση του οργανισμού που επιθυμεί την απρόσκοπτη χρήση των πληροφοριακών συστημάτων στις λειτουργίες του οργανισμού.
- Οι πελάτες του οργανισμού, εφόσον δεδομένα που τους αφορούν αποτελούν συνιστώσα του πληροφοριακού συστήματος.
- Το νομικό και ρυθμιστικό πλαίσιο στο οποίο λειτουργεί ο οργανισμός.

Η πολιτική ασφάλειας θα πρέπει να ικανοποιεί όλες τις απαιτήσεις ασφάλειας που προκύπτουν για τα πληροφοριακά συστήματα, και μάλιστα με αναλογικό τρόπο, δηλαδή τα μέτρα και οι οδηγίες που περιλαμβάνει να εξασφαλίζουν το επιθυμητό επίπεδο ασφάλειας.

12.3.2 Ανάλυση επικινδυνότητας και πολιτικής ασφάλειας

Η διαμόρφωση της πολιτικής ασφάλειας για τα πληροφοριακά συστήματα ενός οργανισμού έπεται της αξιολόγησης του επιπέδου ασφάλειας των συστημάτων αυτών. Η αξιολόγηση της ασφάλειας μπορεί να γίνει με διάφορους τρόπους, οι συνηθέστεροι εκ των οποίων είναι η εκπόνηση μιας μελέτης ανάλυσης επικινδυνότητας (Risk Analysis) και η χρήση κάποιων από τα πρότυπα (standards) διαχείρισης της ασφάλειας.

Για την αξιολόγηση, ή αλλιώς αποτίμηση, του επιπέδου ασφάλειας των πληροφοριακών συστημάτων μπορεί να εφαρμοστεί κάποια από τις μεθόδους ανάλυσης επικινδυνότητας, οι πιο διαδεδομένες από τις οποίες είναι η SBA (Security By Analysis), η MARION και η CRAMM (CCTA Risk Analysis and Management Method). Σε αυτήν την περίπτωση, η διαμόρφωση της πολιτικής ασφάλειας γίνεται με βάση τα αποτελέσματα της ανάλυσης επικινδυνότητας. Σημαντικά πλεονεκτήματα της πρακτικής αυτής είναι ότι η πολιτική ασφάλειας ανταποκρίνεται στις ιδιαίτερες ανάγκες του οργανισμού για τον οποίο έχει μελετηθεί η επικινδυνότητα, και ότι το επίπεδο της παρεχόμενης ασφάλειας με την κατάλληλη επιλογή των μέτρων προστασίας είναι αντίστοιχο των κινδύνων που τα πληροφοριακά συστήματα του οργανισμού αντιμετωπίζουν. Μειονέκτημα της προσέγγισης αυτής είναι το στοιχείο του υποκειμενισμού που εμπεριέχεται στις μεθόδους ανάλυσης επικινδυνότητας, τα αποτελέσματα των οποίων εξαρτώνται σε μεγάλο βαθμό από την εμπειρία και τις γνώσεις του αναλυτή.

12.3.3 Ανάπτυξη πολιτικών ασφάλειας βασισμένη σε πρότυπα

Η αξιοποίηση των διαθέσιμων προτύπων διαχείρισης της ασφάλειας αποτελεί επίσης συνήθη πρακτική για την ανάπτυξη πολιτικών ασφάλειας για τα πληροφοριακά συστήματα των οργανισμών. Τέτοια πρότυπα είναι τα ISO 17799 και GMITS. Τα πρότυπα αυτά περιλαμβάνουν και κάποια οργανωσιακά και διοικητικά

μέτρα για την προστασία των πληροφοριακών συστημάτων, κατά συνέπεια μπορούμε με βάση αυτά να διαμορφώσουμε οργανωσιακές πολιτικές ασφάλειας. Οι πολιτικές ασφάλειας που αναπτύσσονται με βάση τα πρότυπα ασφάλειας περιέχουν συγκεκριμένες ενότητες, που αποσκοπούν στην ικανοποίηση του συνόλου των απαιτήσεων ασφάλειας για τα πληροφοριακά συστήματα.

Η προσέγγιση αυτή μπορεί να διευκολύνει σημαντικά την ανάπτυξη μιας πολιτικής ασφάλειας, μειώνοντας την πολυπλοκότητα της όλης διαδικασίας καθώς και το χρόνο που αυτή απαιτεί, παρουσιάζει όμως και σημαντικά μειονεκτήματα. Το σημαντικότερο μειονέκτημα έχει να κάνει με το γεγονός ότι οι οργανισμοί έχουν διαφορετικές ανάγκες ασφάλειας, οι οποίες δύσκολα μπορούν να καλυφθούν από το γενικευμένο περιεχόμενο των προτύπων. Ένα άλλο μειονέκτημα προκύπτει από το κατά βάση τεχνικό περιεχόμενο των προτύπων, όπου δεν αποδίδεται μεγάλη σημασία στους κοινωνικούς παράγοντες ασφάλειας των πληροφοριακών συστημάτων. Ακόμα, ο γενικός χαρακτήρας των προτύπων μπορεί να δημιουργήσει σύγκρουση μεταξύ των γενικών απαιτήσεων ασφάλειας που απορρέουν από το πρότυπα και των ειδικών απαιτήσεων που προκύπτουν από τη λειτουργία του οργανισμού. Τέλος, τα πρότυπα ασφάλειας δεν παρέχουν ουσιαστική βοήθεια στην διαδικασία λήψης αποφάσεων στο πλαίσιο της διαχείρισης της ασφάλειας.

12.3.4 Περιεχόμενο των πολιτικών ασφάλειας

Η δημιουργία πολιτικής ασφάλειας των πληροφοριακών συστημάτων για έναν οργανισμό ολοκληρώνεται με τη δημιουργία ενός, ή περισσοτέρων, εγγράφων στα οποία μπορούν, και πρέπει, να ανατρέχουν οι χρήστες για να αναζητούν οδηγίες και διαδικασίες για δράση σε ζητήματα που αφορούν την ασφάλεια των πληροφοριακών συστημάτων. Τα έγγραφα αυτά θα πρέπει να μπορούν να συμβουλεύονται όλοι οι εμπλεκόμενοι με τα πληροφορικά συστήματα σε έναν οργανισμό: από το ανώτερο επίπεδο διοίκησης, τον υπεύθυνο ασφάλειας και τους ειδικούς των πληροφοριακών συστημάτων έως τους απλούς χρήστες. Για το σκοπό αυτό, μια πολιτική ασφάλειας θα πρέπει να δίνει σαφείς και κατανοητές απαντήσεις στα ακόλουθα, τουλάχιστον, ερωτήματα :

- Ποιοι είναι οι λόγοι που οδήγησαν στη δημιουργία της πολιτικής ασφάλειας; Θα πρέπει δηλαδή να δηλώνονται ο σκοπός και οι στόχοι που η δημιουργία της πολιτικής ασφάλειας εξυπηρετεί.

- Ποια είναι τα αγαθά του πληροφοριακού συστήματος που χρειάζονται προστασία; (για παράδειγμα πληροφορίες, εφαρμογές, υλικό κλπ).
- Ποιοι είναι οι υπεύθυνοι για την προστασία των αγαθών αυτών; (για παράδειγμα μπορεί να ορίζεται ως υπεύθυνος ο υπεύθυνος ασφάλειας του πληροφοριακού συστήματος, ή οι χρήστες των εφαρμογών). Στην πολιτική ασφάλειας θα πρέπει να καθορίζονται οι ρόλοι και οι υπευθυνότητες των μελών του οργανισμού σε σχέση με την ασφάλεια των πληροφοριακών συστημάτων.
- Ποιο είναι το εύρος της πολιτικής ασφάλειας στο πλαίσιο του οργανισμού; Ένας οργανισμός μπορεί να διαθέτει πολλά υπολογιστικά συστήματα που είναι διασπαρμένα σε διάφορα τμήματά του, ακόμα και σε γεωγραφικά απομακρυσμένους χώρους. Επομένως, στην πολιτική ασφάλειας θα πρέπει να καθορίζονται σαφώς τα όρια εφαρμογής της, σε σχέση με τον οργανισμό.
- Με ποιους τρόπους θα διαπιστωθεί ο βαθμός συμμόρφωσης των χρηστών σε αυτά που προβλέπει η πολιτική ασφάλειας; Θα πρέπει επίσης να προβλέπονται διαδικασίες και ποινές για τις περιπτώσεις παραβίασης της πολιτικής ασφάλειας από τους χρήστες.
- Πότε ισχύει η πολιτική ασφάλειας; Θα πρέπει δηλαδή να καθορίζονται τα χρονικά πλαίσια μέσα στα οποία θα πρέπει να εφαρμόζεται η πολιτική ασφάλειας.

12.3.5 Άξονες της Πολιτικής Ασφάλειας

Οι οδηγίες και τα μέτρα προστασίας που καθορίζει μια πολιτική ασφάλειας πρέπει να καλύπτουν μια ευρεία κατηγορία απαιτήσεων ασφάλειας, ανάλογα βέβαια με τις ιδιαιτερότητες που παρουσιάζει κάθε οργανισμός. Στη συνέχεια θα περιγράψουμε τους κυριότερους άξονες με βάση τους οποίους μπορούμε να διαμορφώσουμε μια πολιτική ασφάλειας. Κάθε άξονας αντιπροσωπεύει ένα σύνολο οδηγιών που αφορούν συγκεκριμένους τομείς ασφάλειας των πληροφοριακών συστημάτων.

Ζητήματα προσωπικού (Personnel Security)

Ο στόχος των οδηγιών και των μέτρων ασφάλειας που ανήκουν σε αυτή την κατηγορία είναι η μείωση της επικινδυνότητας που οφείλεται σε ανθρώπινα λάθη, απάτη, κλοπή ή κατάχρηση των πόρων του πληροφοριακού συστήματος. Ακόμα, με τα μέτρα ασφάλειας αυτής της κατηγορίας επιχειρείται η κατάρτιση και ενημέρωση των χρηστών των πληροφοριακών συστημάτων σε ζητήματα και απειλές ασφάλειας, ώστε να είναι σε θέση να εφαρμόσουν την πολιτική ασφάλειας στο πλαίσιο των καθημερινών δραστηριοτήτων τους. Οι οδηγίες αυτές μπορεί να αφορούν:

- Τον καθορισμό ρόλων και υπευθυνοτήτων για την προστασία των αγαθών του πληροφοριακού συστήματος καθώς και την εφαρμογή των μέτρων ασφάλειας που περιλαμβάνονται στην πολιτική.
- Τις διαδικασίες επιλογής νέου προσωπικού, ειδικά στις περιπτώσεις εκείνες που πρέπει να πληρωθεί μια θέση που χειρίζεται ευαίσθητα ή κρίσιμα για τον οργανισμό δεδομένα και εφαρμογές, όπως οικονομικά στοιχεία και εμπιστευτικές πληροφορίες.
- Τη συμμόρφωση με το νομικό πλαίσιο για την προστασία των προσωπικών και ευαίσθητων προσωπικών δεδομένων και την προστασία της πνευματικής ιδιοκτησίας (για παράδειγμα να μην επιτρέπεται η χρήση λογισμικού που δεν έχει αποκτηθεί με νόμιμο τρόπο).
- Την κατάρτιση και ενημέρωση των χρηστών στην εφαρμογή των μέτρων ασφάλειας που προδιαγράφονται στην πολιτική ασφάλειας, όπως για παράδειγμα η σωστή διαχείριση των συνθηματικών για την ελεγχόμενη πρόσβαση στις πληροφορίες.
- Την αντιμετώπιση και αναφορά περιστατικών ασφάλειας. Στην πολιτική ασφάλειας θα πρέπει να καθορίζεται η διαδικασία με την οποία οι χρήστες πρέπει να αντιμετωπίσουν την πραγματοποίηση μιας απειλής κατά του πληροφοριακού συστήματος. Επίσης, θα πρέπει να προσδιορίζεται το κανάλι επικοινωνίας μέσω του οποίου η πληροφορία για την πραγματοποίηση ενός περιστατικού ασφάλειας που αντιλήφθηκε ένας χρήστης θα φθάσει στον υπεύθυνο στο συντομότερο δυνατό χρονικό διάστημα. Η δυνατότητα ενός οργανισμού να αντιμετωπίσει τις απειλές που σχετίζονται με το πληροφοριακό του σύστημα εξαρτάται από την άμεση επισήμανση των παραβιάσεων της

ασφάλειας και την εκτέλεση των προβλεπόμενων στην πολιτική ασφάλειας δράσεων.

Φυσική ασφάλεια

Τα μέτρα προστασίας που υποστηρίζουν τη φυσική ασφάλεια έχουν ως κύριο στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στο χώρο του οργανισμού, και της καταστροφής των αγαθών του πληροφοριακού συστήματος. Αυτό επιτυγχάνεται με τη δημιουργία επάλληλων περιμέτρων φυσικής ασφάλειας, στη λογική των ομόκεντρων κύκλων, όπου στο κέντρο (εσώτερο κύκλο) τοποθετούνται τα αγαθά που πρέπει να προστατευθούν. Οι οδηγίες για τα μέτρα ασφάλειας αυτά αφορούν συνήθως στις εξής περιπτώσεις:

- Έλεγχο φυσικής πρόσβασης σε κρίσιμους για το πληροφοριακό σύστημα χώρους, όπως για παράδειγμα ο χώρος που βρίσκονται οι εξυπηρετητές των εφαρμογών (server room), ο χώρος που αποθηκεύονται ευαίσθητα δεδομένα, σε ηλεκτρονική ή φυσική μορφή. Τα μέτρα φυσικής ασφάλειας μπορεί να περιλαμβάνουν, για παράδειγμα, τον περιορισμό της κίνησης των επισκεπτών ενός οργανισμού σε συγκεκριμένους χώρους, με τη συνοδεία μελών του οργανισμού, τη χρήση μαγνητικών ή ‘έξυπνων’ καρτών για την είσοδο σε κάποιους χώρους κλπ.
- Προστασία της υγείας (safety) των εργαζομένων με βάση αυτά που καθορίζονται στη σχετική νομοθεσία.

Έλεγχος πρόσβασης στα πληροφορικά συστήματα

Η πρόσβαση των χρηστών των πληροφοριακών συστημάτων στις πληροφορίες και τις εφαρμογές θα πρέπει να καθορίζεται με βάση τις επιχειρηματικές ανάγκες και τις απαιτήσεις ασφάλειας. Μια πρακτική που συνήθως χρησιμοποιείται για τον καθορισμό των δικαιωμάτων πρόσβασης είναι η εφαρμογή της “need to know” αρχής, με βάση την οποία δικαίωμα πρόσβασης στις πληροφορίες, τις εφαρμογές και τα υπολογιστικά συστήματα αποδίδεται στους χρήστες που χρειάζονται την πρόσβαση για την εκτέλεση της εργασίας τους. Οι οδηγίες που αφορούν τον έλεγχο πρόσβασης στα πληροφοριακά συστήματα συνήθως συνοδεύονται από τον καθορισμό των ρόλων και των υπευθυνοτήτων των χρηστών.

Διαχείριση υλικού και λογισμικού

Οι οδηγίες που ανήκουν σε αυτόν τον άξονα διαμόρφωσης των πολιτικών ασφάλειας καλύπτουν τις εξής περιπτώσεις:

- Προμήθεια και Συντήρηση Υλικού. Για την αγορά και χρήση προϊόντων υλικού (hardware products) θα πρέπει να ακολουθούνται οι οδηγίες που περιλαμβάνονται στην πολιτική ασφάλειας με στόχο την διατήρηση του επιθυμητού επιπέδου ασφάλειας. Για το σκοπό αυτό θα πρέπει να καθορίζονται οι απαιτήσεις ασφάλειας που διέπουν την αγορά καθώς και τη συντήρηση του υλικού, όπως για παράδειγμα η ύπαρξη πιστοποίησης του επιπέδου ασφάλειας με κάποια από τα γνωστά πρότυπα (για παράδειγμα ITSEC, TCSEC, CC) των προϊόντων που θα αγοραστούν.
- Ανάπτυξη και Συντήρηση Λογισμικού. Στην πολιτική ασφάλειας θα πρέπει επίσης να προσδιορίζονται οι διαδικασίες για την ανάπτυξη και συντήρηση των εφαρμογών των πληροφοριακών συστημάτων. Θα πρέπει να καλύπτονται οι ακόλουθες περιπτώσεις:
  - Αγορά έτοιμων προϊόντων (πακέτων λογισμικού) από εξωτερικούς προμηθευτές.
  - Ανάπτυξη και συντήρηση λογισμικού από αναδόχους.
  - Εσωτερική ανάπτυξη και συντήρηση των εφαρμογών.

Συμμόρφωση με νομικές υποχρεώσεις

Η αναγκαιότητα της πολιτικής ασφάλειας μπορεί να πηγάζει και από την τυπική υποχρέωση του οργανισμού να ακολουθεί το σχετικό νομικό και κανονιστικό πλαίσιο για τη λειτουργία του. Στις περιπτώσεις, για παράδειγμα, πληροφοριακών συστημάτων που περιλαμβάνουν προσωπικά ή ευαίσθητα προσωπικά δεδομένα, η πολιτική ασφάλειας θα πρέπει να λαμβάνει υπόψη και να ικανοποιεί τις απαιτήσεις του Νόμου 2472 για το χειρισμό των δεδομένων αυτών. Επομένως, η πολιτική ασφάλειας των πληροφοριακών συστημάτων ενός οργανισμού θα πρέπει να συμπεριλαμβάνει στους στόχους της και τη συμμόρφωση με το νομικό πλαίσιο, καθώς και οδηγίες και μέτρα για την υλοποίηση του στόχου αυτού.

Διαδικασίες διαχείρισης της πολιτικής ασφάλειας

Ένα σημαντικό κομμάτι της πολιτικής ασφάλειας περιγράφει και προσδιορίζει τις λοιπές δραστηριότητες που πρέπει να συνοδεύουν την εφαρμογή της, ώστε να

είναι αποτελεσματική η διαχείριση της ασφάλειας των πληροφοριακών συστημάτων. Αυτές οι διαδικασίες περιλαμβάνουν:

- Την αξιολόγηση και αναθεώρηση της πολιτικής. Η πολιτική ασφάλειας θα πρέπει να αξιολογείται και να αναθεωρείται, τόσο ως προς το περιεχόμενο όσο και ως προς τις διαδικασίες εφαρμογής της.
- Τον έλεγχο και τη συμμόρφωση με την πολιτική ασφάλειας. Στην πολιτική ασφάλειας θα πρέπει να καθορίζονται οι διαδικασίες με τις οποίες ελέγχεται (auditing) η εφαρμογή της πολιτικής από τους χρήστες των πληροφοριακών συστημάτων, καθώς και οι διαδικασίες για το χειρισμό των περιστατικών μη συμμόρφωσης με αυτή.

Οργανωτική δομή

Η εφαρμογή της πολιτικής ασφάλειας προϋποθέτει την ύπαρξη κατάλληλης οργανωτικής δομής, όπως η δημιουργία των κατάλληλων ρόλων, η θέσπιση διαδικασιών για τον εντοπισμό και την αναφορά περιστατικών ασφάλειας κλπ. Με τη δημιουργία των κατάλληλων ρόλων, όπως ο ρόλος του υπευθύνου ασφάλειας, δημιουργείται η απαραίτητη οργανωτική δομή για την υλοποίηση των διαδικασιών διαχείρισης της πολιτικής ασφάλειας.

Σχέδιο συνέχισης λειτουργίας

Ορισμένες φορές κρίνεται σκόπιμο στην πολιτική ασφάλειας των πληροφοριακών συστημάτων που αναπτύσσουμε για έναν οργανισμό, να συμπεριλάβουμε και κάποιες οδηγίες και διαδικασίες για το τι πρέπει να γίνει μετά την πραγματοποίηση ενός σημαντικού περιστατικού ασφάλειας, ώστε οι λειτουργίες του οργανισμού που στηρίζονταν στο κομμάτι αυτό του πληροφοριακού συστήματος που υπέστη ζημία από το περιστατικό να εξακολουθήσουν να πραγματοποιούνται με κάποιους εναλλακτικούς τρόπους και για το διάστημα που απαιτείται για την επαναφορά της πλήρους λειτουργικότητας του πληροφοριακού συστήματος.

12.4 Γενικά χαρακτηριστικά πολιτικών ασφάλειας

Όταν δημιουργείται μια πολιτική ασφάλειας πληροφοριακών συστημάτων για έναν οργανισμό, ή όταν γίνεται αναθεώρηση ή αξιολόγηση μιας ήδη υπάρχουσας πολιτικής, θα πρέπει να λαμβάνονται υπόψη οι ακόλουθοι παράγοντες:

- Πληρότητα: Οι οδηγίες και τα μέτρα ασφάλειας που περιλαμβάνονται στην πολιτική ασφάλειας θα πρέπει να καλύπτουν την προστασία του συνόλου των πληροφοριακών συστημάτων καθώς και τις διαδικασίες και λειτουργίες της διαχείρισής τους.
- Επικαιρότητα: Ο προσδιορισμός των τεχνικών μέτρων προστασίας θα πρέπει να γίνεται με βάση τις τρέχουσες τεχνολογικές εξελίξεις.
- Γενικευσιμότητα: Η σύνθεση των πληροφοριακών συστημάτων ενός οργανισμού μπορεί να μεταβάλλεται συχνά, ανάλογα με τις ανάγκες του οργανισμού (για παράδειγμα προμήθεια νέων συστημάτων υλικού και λογισμικού, διασύνδεση με άλλα πληροφοριακά συστήματα κλπ.). Η πολιτική ασφάλειας θα πρέπει να μπορεί, με τις αντίστοιχες παρεμβάσεις, να καλύπτει αλλαγές ή επεκτάσεις. Σε περιπτώσεις σημαντικών μεταβολών βέβαια, η πολιτική ασφάλειας θα πρέπει να αναθεωρείται και να διαμορφώνεται εκ νέου, ως αποτέλεσμα μιας νεότερης ανάλυσης επικινδυνότητας, η οποία θα αναγνωρίσει και θα αξιολογήσει πιθανές απειλές, οι οποίες δεν υπήρχαν έως τότε, και την επίπτωση από την πραγματοποίηση αυτών των απειλών στα αγαθά του πληροφοριακού συστήματος.
- Σαφής και κατανοητή. Η πολιτική ασφάλειας απευθύνεται στο σύνολο των μελών του οργανισμού, και θα πρέπει να είναι εύκολα κατανοητή από όλους. Για το λόγο αυτό δε θα πρέπει να περιέχει πολλούς τεχνικούς και εξειδικευμένους όρους που θα δυσκολέψουν την κατανόηση, άρα και την εφαρμογή της. Επίσης, στην πολιτική ασφάλειας δε θα πρέπει να υπάρχουν αντικρουόμενα ή αμφίσημα σημεία.
- Τεχνολογική Ανεξαρτησία. Πολλά από τα μέτρα προστασίας και τις οδηγίες που περιλαμβάνονται στην πολιτική ασφάλειας μπορεί να υλοποιούνται με τεχνολογικά μέσα, ή η υλοποίησή τους να απαιτεί τη χρήση κάποιων τεχνολογικών εργαλείων. Είναι όμως σημαντικό, η περιγραφή των μέτρων αυτών να μη δεσμεύει τον οργανισμό και τους ανθρώπους που θα κάνουν την επιλογή σε συγκεκριμένα προϊόντα, αλλά να θέτει τις προδιαγραφές με βάση τις οποίες ο υπεύθυνος ασφάλειας θα μπορέσει να επιλέξει τα περισσότερο κατάλληλα συστήματα λογισμικού και υλικού, ανάλογα με το κόστος, τις ανάγκες και τις ιδιαίτερες συνθήκες που επικρατούν στον οργανισμό.

- Καταλληλότητα. Οι ανάγκες ασφάλειας διαφέρουν σε μεγάλο βαθμό από οργανισμό σε οργανισμό, όπως διαφορετικά είναι και τα χαρακτηριστικά κάθε οργανισμού. Επομένως, θα πρέπει η πολιτική ασφάλειας να αναπτύσσεται με γνώμονα τις ιδιαιτερότητες και τις ανάγκες του συγκεκριμένου οργανισμού και του περιβάλλοντος στο οποίο αυτός λειτουργεί.
- Εφαρμοσιμότητα. Συχνά τα μέτρα προστασίας που εισάγονται με την πολιτική ασφάλειας και οι οδηγίες και διαδικασίες που περιλαμβάνονται σε αυτή δυσχεραίνουν κατά τρόπο δυσανάλογο, σε σχέση με την προστασία που παρέχουν, τις δραστηριότητες των χρηστών των πληροφοριακών συστημάτων. Το αποτέλεσμα σε τέτοιες περιπτώσεις, κυρίως όταν η εφαρμογή της πολιτικής ασφάλειας δεν είναι πολύ αυστηρή, είναι να μένουν ορισμένα μέτρα προστασίας ανενεργά, με συνέπεια την αύξηση των επικινδυνότητας για τα πληροφοριακά συστήματα. Θα πρέπει επομένως να διερευνάται η εφαρμοσιμότητα της πολιτικής ασφάλειας, σε σχέση με τον οργανισμό που θα ενταχθεί.

Βιβλιογραφία

- Κάτσικα Σ., Γκρίτζαλη Δ., Γκρίτζαλη Σ., Ασφάλεια πληροφοριακών συστημάτων, εκδόσεις Νέων Τεχνολογιών, Αθήνα 2004.
- Κιουντούζης Ε., ‘’Μοντέλα ασφάλειας πληροφοριακών συστημάτων’’, Ασφάλεια πληροφοριών, Τεχνικά, Νομικά και κοινωνικά θέματα, εκδόσεις ΕΠΥ, Αθήνα 1995.
- Κομνηνού Θ., Σπυράκη Π., ‘’Ασφάλεια δικτύων και υπολογιστικών συστημάτων.

Ηλεκτρονικές αναφορές

- Δρ. Μπόζιός Ελευθέριος http://www.it.teithe.gr/ ~vaf (Σημειώσεις εφαρμοσμένης ασφάλειας πληροφοριακών συστημάτων ΑΤΕΙ Θεσ/κης, τμήμα πληροφορικής)
- Ηλεκτρονική ελεύθερη εγκυκλοπαίδεια Wikipedia, Http://www.wikipedia.org
- Ελληνική δικτυακή πύλη ενημέρωσης, http://www.flash.gr
- Ελληνική δικτυακή πύλη ενημέρωσης, http://www.in.gr
- e-Business Forum, http://www.ebusinessforum.gr
- Μηχανή αναζήτησης Google, http://www.google.gr
- http://www.w3.org
- http://www.w3.org/security

Λέξεις κλειδιά

Ασφάλεια, διαδίκτυο, authentication tools, encryption protocols and tools, smart cards, digital signatures, firewalls, proxies (προγράμματα εφαρμογών).