Τ.Ε.Ι ΜΕΣΟΛΟΓΓΙΟΥ
ΤΜΗΜΑ Ε.Π.Δ.Ο

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΣΠΟΥΔΑΣΤΡΙΑ

ΕΛΕΝΗ ΖΕΡΒΟΥ

ΘΕΜΑ

ΑΣΦΑΛΕΙΑ ΔΙΑ-ΔΙΚΤΥΑΚΗΣ ΔΙΑΚΙΝΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

(ΚΡΥΠΤΟΓΡΑΦΙΑ, ΤΑΥΤΟΤΗΤΕΣ, ΠΙΣΤΟΠΟΙΗΤΙΚΑ)
ΕΦΑΡΜΟΓΕΣ ΜΕ SSL ΚΑΙ PGP

ΕΙΣΗΓΗΤΗΣ ΚΑΘΗΓΗΤΗΣ: **ΝΙΚΟΛΑΟΣ ΚΟΣΜΑΣ**

ΜΕΣΟΛΟΓΓΙ ΔΕΚΕΜΒΡΙΟΣ 2006

ΠΡΟΛΟΓΟΣ

Η αλματώδης εξέλιξη του Internet μέσα στην τελευταία δεκαετία έχει ανοίξει νέους ορίζοντες στις έννοιες πολιτισμός και κοινωνία και μας έχει φέρει αντιμέτωπους με νέες προκλήσεις αλλά και με την ανάγκη της προσαρμογής συμβάσεων και κανόνων συμπεριφοράς που κατά γενική αποδοχή ισχύουν στον πραγματικό κόσμο (ή κόσμο των ατόμων) στο νέο status της ψηφιακής κοινωνίας (ή κόσμου των bits). Μια από τις κοινώς αποδεκτές ως θεμελιώδεις αξίες της ανθρώπινης κοινωνίας είναι η προστασία του απαραβίαστου της προσωπικής ζωής, των προσωπικών δεδομένων και του απόρρητου της αλληλογραφίας, που είναι αξίες κατοχυρωμένες συνταγματικά στα περισσότερα κράτη του κόσμου και προστατεύονται από διεθνείς οργανισμούς.

Το Internet, που αυτή τη στιγμή «στεγάζει» δεκάδες εκατομμυρίων χρήστες, και μάλιστα με εκθετικούς ρυθμούς αύξησης, και είναι χώρος επικοινωνίας, κοινωνικοποίησης, εκπαίδευσης και οικονομικής δραστηριότητας με διαρκώς αυξανόμενη δύναμη , είναι η νέα ψηφιακή κοινωνία. Και η συζήτηση πάνω στην εξασφάλιση της προστασίας της ιδιωτικής ζωής στο Internet έχει εξελιχθεί σε μείζον θέμα συμπεριλαμβάνοντας από απλούς χρήστες και οργανισμούς, μέχρι μεγάλες εταιρίες και κυβερνήσεις.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ ΠΡΩΤΟ

Βασικές Γνώσεις Κρυπτογραφίας

Η κρυπτογραφία είναι ένας κλάδος των μαθηματικών που ασχολείται με το μετασχηματισμό των δεδομένων. Η κρυπτογραφία είναι παραδοσιακά συνδεδεμένη με τη μυστικότητα των δεδομένων. Επιπλέον, η σύγχρονη κρυπτογραφία μπορεί να παρέχει πολλές υπηρεσίες στο τομέα της ασφάλειας, όπως για παράδειγμα ηλεκτρονικές υπογραφές, και πιστοποίηση ότι τα δεδομένα δεν έχουν μεταβληθεί. Επίσης, οι σύγχρονες κρυπτογραφικές τεχνικές μπορούν να εξασφαλίσουν την εμπιστευτικότητα (confidentiality) και την ακεραιότητα (integrity) των δεδομένων, ενώ χρησιμοποιούνται σε πολλές προηγμένες τεχνικές πιστοποίησης ταυτότητας.

1.1 Ιστορική Αναδρομή της Κρυπτογραφίας

Η γνώση για την κρυπτογραφία μπορεί να εξακριβωθεί από τους αρχαίους χρόνους. Δεν είναι δύσκολο να καταλάβουμε γιατί: μόλις τρεις άνθρωποι χρησιμοποίησαν την ικανότητα της ανάγνωσης και της γραφής, υπήρχε η πιθανότητα οι δύο από αυτούς να θέλουν να ανταλλάξουν γράμματα χωρίς ένας τρίτος να μπορεί να τα διαβάσει.

Στην αρχαία Ελλάδα, οι Σπαρτιάτες στρατιώτες χρησιμοποιούσαν μια μορφή κρυπτογραφίας έτσι ώστε οι στρατιώτες να μπορούν να ανταλλάξουν μεταξύ τους μυστικά μηνύματα. Τα μηνύματα ήταν γραμμένα σε στενές ταινίες περγαμηνής, η οποία ήταν τυλιγμένη σε κυλινδρικές σκυτάλες. Αφού ξετύλιγαν την περγαμηνή, η γραφή μπορούσε να διαβαστεί μόνο από κάποιον που είχε μια άλλη σκυτάλη με το ίδιο ακριβώς μέγεθος. Αυτό το πρωτόγονο σύστημα ήταν μια λογική διεργασία προστασίας μηνυμάτων από κλοπή και από τον άνθρωπο που τα μετέφερε.

Σήμερα σκοπός της κρυπτογραφίας είναι να προστατεύσει τις ηλεκτρονικές επικοινωνίες. Πολλοί ερευνητές έχουν εντοπίσει τρόπους να κωδικοποιήσουν τα μηνύματα με μυστικούς κώδικες, έτσι ώστε μόνο οι παραλήπτες να μπορούν να τα αποκωδικοποιήσουν. Η κρυπτογραφία είναι πολύ σημαντική, διότι χωρίς αυτήν τα μηνύματα μπορούν να υποκλέπτονται.

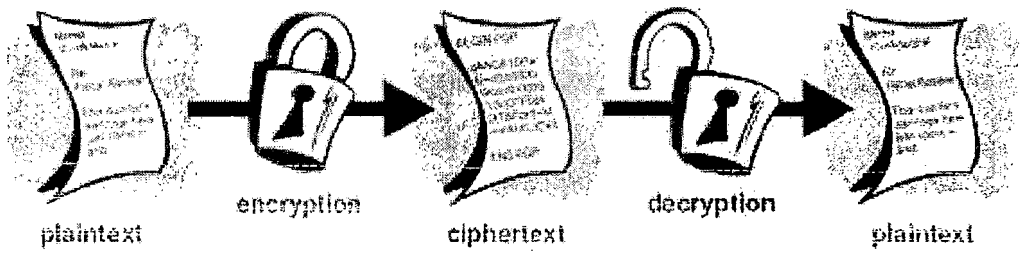
1.2 Κρυπτογραφία (encryption)

Κρυπτογραφία είναι η διεργασία μετασχηματισμού ενός μηνύματος σε μια ακατανόητη μορφή με τη χρήση ενός κρυπτογραφικού αλγόριθμου, έτσι ώστε αυτό να μην είναι αναγνώσιμο από τρίτα μέρη (εκτός του νόμιμου παραλήπτη).

1.3 Αποκρυπτογράφηση (decryption)

Αποκρυπτογράφηση είναι η διεργασία ανάκτησης του αρχικού μηνύματος (plaintext) σε αναγνώσιμη μορφή από μια ακατανόητη έκδοσή του που έχει παραχθεί από μια κρυπτογράφηση. Η αποκρυπτογράφηση εκτελείται από κάποιο εξουσιοδοτημένο μέρος, σε αντίθεση με την κρυπτανάλυση που αναλύεται παρακάτω.

Στην εικόνα 1.1 φαίνεται η διαδικασία κρυπρογράφησης και αποκρυπτογράφησης:



Εικόνα 1.1

1.4 Στοιχεία της κρυπτογράφησης

1.4.1. **Αρχικό κείμενο (plaintext):** Το αρχικό κείμενο είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μια διεργασία κρυπτογράφησης, δηλαδή κρυπτογραφείται.

1.4.2. **Κρυπτογραφημένο κείμενο (ciphertext):** Είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγορίθμου πάνω στο αρχικό κείμενο.

1.4.3. **Αλγόριθμος Κρυπτογράφησης:** Κάθε κρυπτογραφική τεχνική βασίζεται σε δύο συστατικά: έναν αλγόριθμο (ή μέθοδο κρυπτογράφησης), και το κρυπτογραφικό κλειδί. Στα μοντέρνα κρυπτογραφικά συστήματα, οι αλγόριθμοι είναι σύνθετοι μαθηματικοί τύποι, ενώ τα κλειδιά είναι μεγάλες ακολουθίες από δυαδικά ψηφία. Για να καταστεί δυνατή η κρυπτογραφημένη επικοινωνία δύο μερών, πρέπει αυτά να χρησιμοποιούν τον ίδιο αλγόριθμο, και σε μερικές περιπτώσεις το ίδιο ή συμβατά κρυπτογραφικά κλειδιά. Στο σχήμα παρακάτω φαίνεται η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης.

1.4.4. **Κλειδιά Κρυπτογράφησης:** Η ανθεκτικότητα μιας κρυπτογράφησης εξαρτάται από το μέγεθος των κλειδιών που χρησιμοποιούνται παρά από τους αλγορίθμους. Το μέγεθος των κλειδιών μετριέται σε bits. Γενικά, μεγάλου μεγέθους κλειδιά παρέχουν ανθεκτικότερη κρυπτογράφηση. Για παράδειγμα η κρυπτογράφηση 128-bit με τον αλγόριθμο RC4 είναι 3078 φορές ανθεκτικότερη από την 40-bit RC4 κρυπτογράφηση.

1.4.5. **Μήκος κλειδιών:** Διαφορετικοί αλγόριθμοι απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης. Για παράδειγμα ένας αλγόριθμος συμμετρικής κρυπτογράφησης με κλειδί μεγέθους 128 bit παρέχει ανθεκτικότερη κρυπτογράφηση από τον αλγόριθμο κρυπτογράφησης δημόσιου κλειδιού RSA με το ίδιο μέγεθος κλειδιού. Για αυτό πρέπει να χρησιμοποιηθεί από τον RSA κλειδί μεγέθους 512 bit προκειμένου η κρυπτογράφηση να θεωρηθεί ανθεκτική, ενώ οι συμμετρικοί αλγόριθμοι επιτυγχάνουν περίπου το ίδιο επίπεδο ανθεκτικότητας με κλειδί μεγέθους 64 bit.

1.5 Κρυπτανάλυση

Η προσπάθεια να σπάσει μια συγκεκριμένη κρυπτογραφική τεχνική ονομάζεται κρυπτανάλυση. Είναι η διεργασία αποκρυπτογράφησης ενός μηνύματος από ένα μη εξουσιοδοτημένο άτομο.

1.6 Τι μπορούμε να επιτύχουμε με την κρυπτογράφηση

- Η κρυπτογράφηση μπορεί να παίξει σημαντικό ρόλο στις καθημερινές μας υπολογιστικές και επικοινωνιακές μας ανάγκες.
- Η κρυπτογράφηση μπορεί να προστατεύσει πληροφορίες που βρίσκονται στον υπολογιστή μας και να μην επιτρέπει την πρόσβαση κάποιου τρίτου προσώπου, με ή χωρίς την άδεια μας.
- Η κρυπτογράφηση μπορεί να προστατεύσει δεδομένα κατά την διάρκεια μεταφορά τους από ένα υπολογιστικό σύστημα σε άλλο.
- Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να εντοπίσει σκόπιμες ή τυχαίες αλλαγές στα δεδομένα μας.
- Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για να επικυρώσει την ταυτότητα του δημιουργού.

Πέρα από αυτά τα πλεονεκτήματα, υπάρχουν και κάποια όρια τα οποία πρέπει να γνωρίζουμε για να αποφεύγουμε τα ανεπιθύμητα αποτελέσματα:

- Η κρυπτογράφηση δεν μπορεί να προστατεύσει τα δεδομένα μας από κάποιον εισβολέα που επιθυμεί να τα σβήσει.
- Ο εισβολέας έχει την δυνατότητα να τροποποιήσει και να ορίσει ένα πρόγραμμα κρυπτογράφησης, έτσι ώστε να μπορεί να αποκρυπτογραφήσει όλα τα μηνύματα με το δικό του κλειδί. Μπορεί να αποθηκεύσει όλα τα κλειδιά σε ένα δικό του αρχείο για να τα χρησιμοποιήσει μετέπειτα.
- Ο εισβολέας μπορεί να έχει πρόσβαση στα αρχεία μας πριν τα αποκρυπτογραφήσουμε ή αφού τα αποκρυπτογραφήσουμε.
- Ο εισβολέας μπορεί να βρει ένα σχετικά εύκολο τρόπο να αποκρυπτογραφεί τα δεδομένα που εμείς κρυπτογραφούμε με την βοήθεια κάποιου αλγορίθμου.

Για όλους τους παραπάνω λόγους, συμπεραίνουμε ότι η κρυπτογράφηση είναι ένα κομμάτι της ολικής στρατηγικής ασφαλείας που διαθέτουμε. Η κρυπτογράφηση δεν είναι υποκατάστατο άλλων μέτρων ασφαλείας, όπως είναι ο απαραίτητος έλεγχος πρόσβασης στον υπολογιστή μας.

1.7 Αντοχή κρυπτογράφησης

Η ικανότητα ενός κρυπτογραφικού συστήματος να προστατεύσει την πληροφορία από μια επίθεση ονομάζεται η αντοχή του. Η αντοχή εξαρτάται από τους εξής παράγοντες:

- Η μυστικότητα του κλειδιού.
- Η δυσκολία να μαντέψουμε το κλειδί, ή να βρούμε τα πιθανά κλειδιά.
- Η δυσκολία να αναστρέψουμε έναν αλγόριθμο κρυπτογράφησης χωρίς να γνωρίζουμε το κλειδί.
- Η ύπαρξη άλλων δρόμων (όπως η πίσω πόρτα), με τους οποίους μπορούμε να αποκρυπτογραφήσουμε ποιο εύκολα ένα αρχείο χωρίς να γνωρίζουμε το κλειδί κρυπτογράφησης.

- Η ικανότητα να αποκρυπτογραφήσουμε ένα ολόκληρο κρυπτογραφημένο μήνυμα αν γνωρίζουμε τον τρόπο με τον οποίον αποκρυπτογραφήθηκε ένα μέρος αυτού.
- Η ιδιοκτησία και η γνώση των χαρακτηριστικών του αρχικού κειμένου από τον επιτιθέμενο.

Ο στόχος στον σχεδιασμό κρυπτογραφικών συστημάτων είναι η δημιουργία ενός αλγορίθμου που θα είναι δύσκολο να αναστραφεί χωρίς το κλειδί. Η δυσκολία της αναστροφής αυτής πρέπει να είναι ισοδύναμη με την προσπάθεια που απαιτείται για να μαντέψουμε το κλειδί προσπαθώντας με πιθανές λύσεις κάθε φορά. Για να μπορέσουμε να κρατήσουμε την διαδικασία αναστροφής του αλγορίθμου πολύ δύσκολη χρειάζεται να χρησιμοποιηθούν μαθηματικά υψηλού επιπέδου.

Η κρυπτογραφική δύναμη δεν μπορεί ποτέ να αποδειχθεί θετική, μπορεί όμως να γίνει το αντίθετο. Όταν σχεδιάζεται ένας νέος αλγόριθμος, ο δημιουργός του θεωρεί ότι είναι τέλειος. Θεωρεί ότι είναι τόσο δυνατός, που δεν υπάρχει περίπτωση να αποκρυπτογραφηθεί ένα κείμενο χωρίς την χρήση του σωστού κλειδιού. Επιπλέον, ένας σχεδιαστής προσπαθεί να σπάσει τον αλγόριθμο με ήδη γνωστούς τρόπους επιθέσεων. Με την πάροδο όμως του χρόνου ανακαλύπτονται νέες τεχνικές επίθεσης που δημοσιεύονται και μπορούν να χρησιμοποιηθούν.

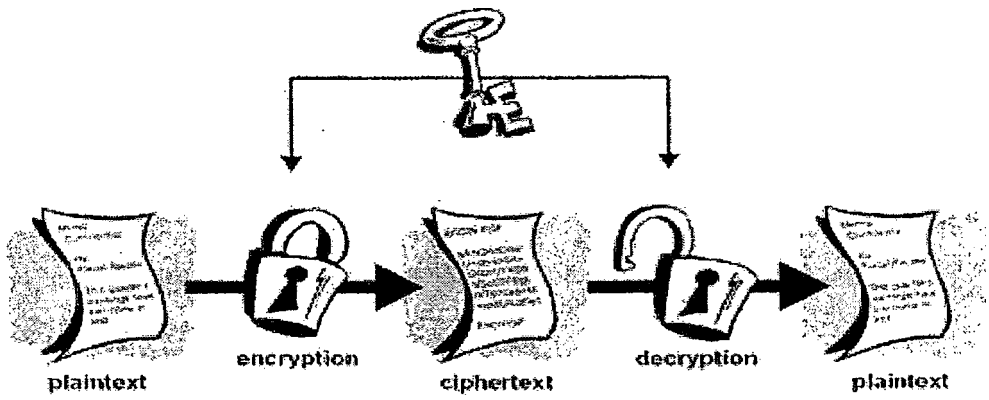
Έτσι, επιβάλλεται να είμαστε πολύ προσεκτικοί με τους νέους κρυπτογραφικούς αλγορίθμους. Οι περισσότεροι από αυτούς έχουν στοιχειώδη ελαττώματα που τους καθιστούν ακατάλληλους.

1.8 Αλγόριθμοι κρυπτογράφησης και συναρτήσεις

Σήμερα υπάρχουν δυο σημαντικά είδη κρυπτογραφικών αλγορίθμων:

- **Κρυπτογραφία προσωπικού κλειδιού (private key cryptography),** η οποία χρησιμοποιεί το ίδιο κλειδί για να κρυπτογραφήσει και να αποκρυπτογραφήσει το μήνυμα. Επίσης, είναι γνωστά και σαν κρυπτογραφία συμμετρικού κλειδιού (symmetric key cryptography).

Στην εικόνα 1.2 φαίνεται η κρυπτογραφία ενός συμμετρικού κλειδιού:

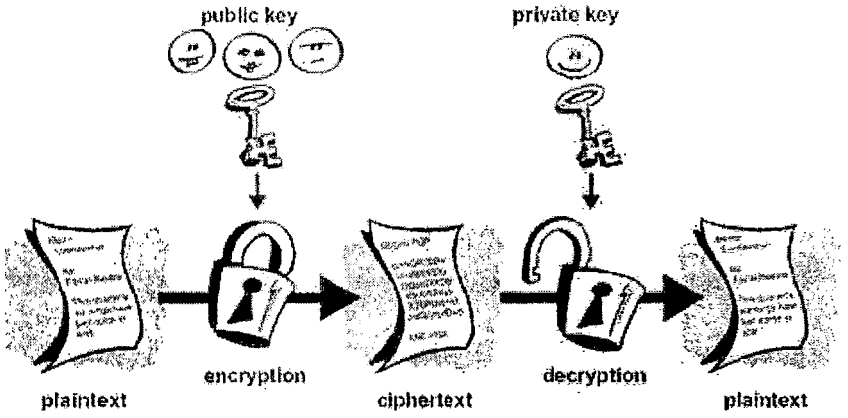


Εικόνα 1.2

- **Κρυπτογραφία δημόσιου κλειδιού (public key cryptography),** η οποία χρησιμοποιεί ένα δημόσιο κλειδί (public key) για να κρυπτογραφήσει το μήνυμα, και ένα προσωπικό κλειδί (private key) για να το αποκρυπτογραφήσει. Λέγεται δημόσιο κλειδί γιατί μπορούμε να κάνουμε αυτό το κλειδί δημοσίως γνωστό χωρίς να διακινδυνεύσουμε την

μυστικότητα του μηνύματος ή του κλειδιού αποκρυπτογράφησης. Επίσης, είναι γνωστά και σαν κρυπτογραφία ασύμμετρου κλειδιού (asymmetric key cryptography).

Στην εικόνα 1.3 φαίνεται η κρυπτογραφία ενός ασύμμετρου κλειδιού:



Εικόνα 1.3

1.8.1. **Η κρυπτογραφία προσωπικού κλειδιού**, χρησιμοποιείται συχνότερα για να προστατεύσει πληροφορίες στον σκληρό δίσκο ενός υπολογιστή, ή για να κρυπτογραφήσει πληροφορίες που μεταφέρονται μέσω επικοινωνιακού συνδέσμου ανάμεσα σε δύο διαφορετικές μηχανές. Γενικά, είναι πολύ πιο γρήγορη από την κρυπτογραφία δημόσιου κλειδιού και πιο εύκολη στην εφαρμογή. Δυστυχώς όμως έχει ένα πρόβλημα που έχει περιορίσει την χρήση της: για να ανταλλάξουν δύο άτομα με ασφάλεια τα μηνύματά τους, πρέπει πρώτα να ανταλλάξουν με ασφάλεια το κλειδί κρυπτογράφησης.

1.8.2. **Αντίθετα, οι αλγόριθμοι δημόσιου κλειδιού**, ξεπερνούν αυτό το πρόβλημα. Τα άτομα που θέλουν να επικοινωνήσουν δημιουργούν ένα δημόσιο και ένα προσωπικό κλειδί. Το δημόσιο κλειδί δημοσιεύεται, έτσι ώστε να μπορεί ο καθένας να το αποκτήσει. Αν κάποιος κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί του παραλήπτη, τότε μόνο ο παραλήπτης θα μπορέσει να αποκρυπτογραφήσει και να διαβάσει το μήνυμα χρησιμοποιώντας το προσωπικό του κλειδί.

Η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται περισσότερο για δημιουργία ψηφιακών υπογραφών στα δεδομένα, όπως στο ηλεκτρονικό ταχυδρομείο για να πιστοποιήσει την προέλευση και την ακεραιότητα των δεδομένων. Στην περίπτωση των ψηφιακών υπογραφών, το προσωπικό κλειδί χρησιμοποιείται για την δημιουργία της ψηφιακής υπογραφής και το δημόσιο κλειδί για την επικύρωση αυτής. Όταν ο παραλήπτης λαμβάνει ένα γράμμα, ψηφιακά υπογεγραμμένο με το προσωπικό κλειδί του αποστολέα, μπορεί να το επικυρώσει χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα.

Οι αλγόριθμοι δημόσιου κλειδιού είναι απίστευτα αργοί. Είναι 10 με 100 φορές αργότεροι από τους αλγορίθμους συμμετρικού κλειδιού. Για το λόγο αυτό υπάρχει και ένα τρίτο σύστημα κρυπτογράφησης:

1.8.3. **Κρυπτογραφία διασταύρωσης δημόσιου / προσωπικού κλειδιού**. Σε αυτό το σύστημα, χρησιμοποιείται αργότερη κρυπτογραφία δημόσιου κλειδιού για ανταλλαγή ενός τυχαίου κλειδιού συνόδου, το οποίο

χρησιμοποιείται σαν βάση του αλγόριθμου κρυπτογράφησης προσωπικού κλειδιού. Ένα κλειδί συνόδου χρησιμοποιείται μόνο για εφαρμογές κρυπτογράφησης και μετά καταστρέφεται. Σχεδόν όλες οι πρακτικές εφαρμογές της κρυπτογραφίας δημόσιου κλειδιού είναι συστήματα διασταύρωσης.

Τα τελευταία χρόνια υπάρχει ένα νέο είδος συνάρτησης που χρησιμοποιείται σε συνδυασμό με την κρυπτογραφία δημόσιου κλειδιού:

1.8.4. **Συναρτήσεις αποσύνθεσης μηνύματος (message digest functions).** Μια συνάρτηση αποσύνθεσης μηνύματος δημιουργεί ένα μοναδικό πρότυπο από bits για μια δοσμένη είσοδο. Η τιμή αποσύνθεσης υπολογίζεται με τέτοιο τρόπο ώστε να είναι αδύνατο να υπολογιστεί μια είσοδος από ένα τεμαχισμένο μήνυμα χρησιμοποιώντας την ίδια τιμή της αποσύνθεσης. Οι αποσυνθέσεις μηνυμάτων θεωρούνται συχνά σαν δακτυλικά αποτυπώματα για αρχεία.

1.9 Αλγόριθμοι συμμετρικού κλειδιού (Private Key)

Οι αλγόριθμοι αυτοί χρησιμοποιούνται για μεγάλο όγκο δεδομένων ή για δεδομένα με συνεχή ροή. Είναι σχεδιασμένοι να εκτελούνται με ταχύτητα και έχουν μεγάλο αριθμό πιθανόν κλειδιών. Οι καλύτεροι αλγόριθμοι συμμετρικού κλειδιού φτάνουν το τέλειο: αν ένα δεδομένο κρυπτογραφηθεί με ένα δοσμένο κλειδί, δεν υπάρχει τρόπος να το αποκρυπτογραφήσεις χωρίς να έχει το ίδιο κλειδί.

Οι αλγόριθμοι συμμετρικού κλειδιού μπορούν να χωριστούν σε δύο κατηγορίες: Σε αυτούς που κρυπτογραφούν ένα κομμάτι δεδομένων μόνο μιας ή αλγορίθμους μπλοκ, και σε αυτούς που κάνουν την κρυπτογράφηση byte παρά byte σε δεδομένα συνεχής ροής ή αλγορίθμους συρμού.

Σήμερα υπάρχουν πολλοί αλγόριθμοι συμμετρικού κλειδιού. Περιγράφονται μερικοί από αυτούς για την ασφάλεια στο Web:

1.9.1. **DES. (Data Encryption Standard).** Ανήκει στην κατηγορία των Secret Keys, δηλαδή των συμμετρικών αλγορίθμων. Αναπτύχθηκε στις αρχές τις δεκαετίας του 70, εφαρμόστηκε επίσημα από την κυβέρνηση των Ηνωμένων Πολιτειών το 1977 και σαν ANSI πρότυπο το 1981. Είναι ένας μπλοκ αλγόριθμος που χρησιμοποιεί κλειδί 56-bit και έχει πολλές λειτουργίες ανάλογα με τον σκοπό που χρησιμοποιείται. Είναι πολύ δυνατός αλγόριθμος και αν κάποιος προσπαθήσει να σπάσει την κωδικοποίηση πρέπει να δοκιμάσει 2^{55} διαφορετικά κλειδιά. Νεότερες τεχνικές που βασίζονται στην διαφορική κρυπτανάλυση δίνουν από υπολογιστικής πλευράς ελαφρώς καλύτερα αποτελέσματα. Την εποχή που καθιερώθηκε ο αλγόριθμος και με βάση τα τότε δεδομένα σε σχέση με τις υπολογιστικές δυνατότητες των υπαρχόντων συστημάτων, ήταν πρακτικά ανέφικτο και πολυδάπανο να "σπάσει" αυτού του είδους η κρυπτογράφηση σε κάποιο λογικό πλαίσιο χρόνου. Με τη ραγδαία εξέλιξη των υπολογιστικών συστημάτων κάτι τέτοιο έχει γίνει σχετικά εφικτό, ωστόσο εξακολουθεί να είναι πολυέξοδο από την πλευρά της απαιτούμενης υπολογιστικής ισχύος. Μία από τις τελευταίες προσπάθειες "επίθεσης" εναντίον του DES στηρίχτηκε στη "γραμμική κρυπτανάλυση".

1.9.2. **DESX.** Είναι μια απλή μετατροπή του DES αλγόριθμου για να βελτιώσει την ασφάλεια και να κάνει την αναζήτηση κλειδιού πιο δύσκολη.

1.9.3. **Triple – DES.** Αυτός ο αλγόριθμος είναι μια παραλλαγή του DES, είναι πιο αργός, έχει μέγεθος κλειδιού 168-bit και είναι πρακτικά αδύνατο να σπαστεί. Μετατρέπει τον αλγόριθμο DES τουλάχιστον δυο φορές πιο ασφαλές και χρησιμοποιεί τον DES αλγόριθμο τρεις φορές με τρία διαφορετικά κλειδιά.

1.9.4. **IDEA. (International Data Encryption Algorithm).** Είναι ένας συμμετρικός αλγόριθμος. Αναπτύχθηκε από τους James L. Massey και Xuejia Lai στην Ζυρίχη της Ελβετίας και η δημοσίευσή του έγινε το 1990. Είναι πολύ ασφαλής και χρησιμοποιεί κλειδί 128-bit. Από τα θετικά χαρακτηριστικά του είναι ότι αντιστέκεται πολύ καλύτερα συγκριτικά με τον DES σε τεχνικές, όπως η διαφορική και η γραμμική κρυπτανάλυση. Χρησιμοποιείται και από το πρόγραμμα PGP.

1.9.5. **RC2.** Είναι ένας αλγόριθμος γρηγορότερος από τον DES, ο οποίος έχει σχεδιαστεί ως αντικαταστάτης του. Έχει την δυνατότητα να χρησιμοποιεί κλειδιά μεταβλητού μεγέθους. Αναπτύχθηκε από τον Ronald Rivest και κρατείται σαν επαγγελματικό μυστικό από την RSA Data Security. Η ονομασία του προέρχεται ή από το "Ron's Code" ή από το "Rivest's Cipher". Είναι μπλοκ αλγόριθμος και ανακαλύφθηκε το 1996 από ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet. Πωλείται με μια λειτουργία, όπου μπορείς να χρησιμοποιήσεις κλειδιά από 1-bit έως 2048-bit. Συνήθως το μήκος του φτάνει στα 40-bit και είναι πολύ ευάλωτος στην επίθεση έρευνας κλειδιού.

1.9.6. **RC4.** Αναπτύχθηκε από τον Ronald Rivest και κρατείται σαν επαγγελματικό μυστικό από την RSA Data Security. Είναι αλγόριθμος συρμού και ανακαλύφθηκε το 1994 από ένα ανώνυμο μήνυμα που βρέθηκε στο Usenet. Χρησιμοποιεί κλειδιά μήκους 1-bit έως 2048-bit και περιορίζεται σε 40-bit κλειδιά για προγράμματα που εξάγονται.

1.9.7. **RSA.** Προτάθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Είναι από τους πιο δημοφιλείς αλγορίθμους δημοσίου κλειδιού, προσφέροντας τη δυνατότητα κρυπτογράφησης αλλά και πιστοποίησης. Τα δημόσια και τα ιδιωτικά κλειδιά κατασκευάζονται με τη χρήση δύο πολύ μεγάλων πρώτων αριθμών και ο αλγόριθμος στηρίζει τη δύναμή του στη δυσκολία που υπάρχει όσον αφορά στο να παραγοντοποιηθούν πολύ μεγάλοι αριθμοί.

1.9.8. **RC5.** Είναι ένας αλγόριθμος μπλοκ, αναπτύχθηκε από τον Ronald Rivest και δημοσιεύτηκε το 1994. Επιτρέπει από τον χρήστη να ορίζει το μήκος του κλειδιού, το μέγεθος του μπλοκ δεδομένων και το πόσες φορές να γίνει η κρυπτογράφηση.

1.9.9. **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. Ο αλγόριθμος στηρίζεται στο πρόβλημα των διακριτών λογαρίθμων. Στην αρχική ανάπτυξή του ο αλγόριθμος ήταν ευάλωτος σε αυτό που ονομάστηκε "Επίθεση Ενδιάμεσου Προσώπου" (Middleperson Attack), όπου αν κάποιος είχε τη δυνατότητα να ελέγχει πλήρως τα μηνύματα που ανταλλάσσονται ανάμεσα σε δύο άτομα, μπορούσε να υποκλέψει τα πάντα, εδραιώνοντας δύο διαφορετικές κωδικοποιημένες κατά τα άλλα επικοινωνίες με τα δύο άκρα. Το 1992

δόθηκε λύση στο πρόβλημα, εισάγοντας ένα αρχικό στάδιο πιστοποίησης πριν από την καθαυτού διαδικασία, οδηγώντας σε αυτό που ονομάζεται "Authenticated Diffie - Hellman Key Agreement" και χρησιμοποιείται ευρέως σήμερα.

1.10 Επιθέσεις στους αλγορίθμους συμμετρικού κλειδιού

Υπάρχουν διάφοροι τρόποι με τους οποίους ένας αλγόριθμος συμμετρικού κλειδιού μπορεί να δεχθεί επίθεση. Ο πιο απλός είναι η δοκιμή όλων των δυνατών κλειδιών μέχρι να προκύψει κάποιο κείμενο που φαίνεται να έχει λογικό περιεχόμενο. Αυτό μπορεί να φαίνεται μια όχι και τόσο εύκολη δυνατότητα αλλά αν το μέγεθος του κλειδιού είναι σχετικά μικρό, τότε είναι εφικτό. Ωστόσο όταν χρησιμοποιούνται μεγάλα κλειδιά, για παράδειγμα με 128 bits, αυτή η μέθοδος γίνεται ανέφικτη.

Για να μπορέσουμε να προστατεύσουμε πληροφορίες πρέπει να χρησιμοποιήσουμε την κρυπτογραφία. Οι άνθρωποι από τους οποίους προσπαθούμε να κρύψουμε την πληροφορία θα αντιγράψουν το κρυπτογράφημα και θα προσπαθήσουν να το αποκρυπτογραφήσουν με δυναμικές επιθέσεις. Το κρυπτογραφικό σύστημα πρέπει να αντιστέκεται σε τέτοιες επιθέσεις.

Παρακάτω αναλύονται οι επιθέσεις κατά των κρυπτογραφημένων πληροφοριών:

- Επιθέσεις αναζήτησης κλειδιού
- Επιθέσεις κρυπτανάλυσης
- Επιθέσεις βασισμένες στο σύστημα κρυπτογράφησης

1.10.1. **Επιθέσεις αναζήτησης κλειδιού (key search attack):** Ο ευκολότερος τρόπος να σπάσεις τον κώδικα, είναι να δοκιμάζεις όλα τα πιθανά κλειδιά το ένα μετά το άλλο. Οι πιο πολλές προσπάθειες θα αποτύχουν, αλλά κάποια θα επιτύχει και είτε θα επιτρέψει στον cracker να μπει στο σύστημα ή θα του επιτρέψει να αποκρυπτογραφήσει το κρυπτογράφημα. Αυτές οι επιθέσεις λέγονται επιθέσεις αναζήτησης κλειδιού ή key search attack.

Δεν υπάρχει τρόπος να αμυνθούμε εναντίον αυτού του τρόπου επίθεσης, γιατί δεν μπορούμε να εμποδίσουμε τον επιτιθέμενο να προσπαθήσει να αποκρυπτογραφήσει το κρυπτογραφημένο μήνυμα μας, με κάθε πιθανό κλειδί.

Συχνά υπάρχουν πολλά κλειδιά να δοκιμαστούν και δεν υπάρχει χρόνος να δοκιμαστούν όλα, έτσι δεν υπάρχει πιθανότητα να αναζητηθούν αποτελεσματικά. Από την άλλη, πολλές επιθέσεις είναι ευκολότερες διότι οι χρήστες διαλέγουν κλειδιά βασισμένα σε μικρά password με χαρακτήρες που μπορούν να εκτυπωθούν.

Ο αλγόριθμος κρυπτογράφησης RC4, ο οποίος χρησιμοποιείται συχνά σε εφαρμογές www, χρησιμοποιεί μήκος κλειδιών από 1 μέχρι 2048 bits, αλλά συχνά χρησιμοποιεί μυστικό κλειδί μήκους 40 bits ή 128 bits.

Σπάσιμο κωδικών με κλειδί 40 bit και το "κόστος δυνατότητας σπασίματος".

Το 1994 ήταν δυνατό να φτιαχτεί ένας υπολογιστής αξίας 20.000 δολαρίων που θα μπορούσε να εξετάζει 150.000 κλειδιά σε ένα δευτερόλεπτο και το 1997 ένας κώδικας των 40 bit αποκωδικοποιήθηκε μόνο σε 3.5 ώρες. Η ισχύς των υπολογιστών αυξήθηκε σημαντικά από

τότε ώστε πλέον μπορούν να σπάσουν και κώδικες με μεγαλύτερα κλειδιά. Αυτό οδήγησε του ερευνητές που εργάζονται στον τομέα της κρυπτογραφίας να δημιουργήσουν τον όρο "κόστος δυνατότητας σπασίματος". Αυτό είναι ο αριθμός των bits που πρέπει να προστεθούν σε ένα κλειδί ενός κρυπτογραφικού αλγορίθμου ώστε να τον κρατήσουν ασφαλή σε σχέση με την τρέχουσα ποσότητα υπολογιστικής ισχύος.

Από την άλλη πλευρά, ένα κλειδί 128 bit έχει μεγαλύτερη ανθεκτικότητα σε μια επίθεση. Αυτό γιατί ένα 128 bit κλειδί επιτρέπει $2^{128} *(3.4*10^{38})$ πιθανά κλειδιά. Εάν υπήρχε ένας υπολογιστής που θα μπορούσε να δοκιμάσει ένα δισεκατομμύριο κλειδιά το δευτερόλεπτο, και είχαμε ένα δισεκατομμύριο από αυτούς τους υπολογιστές, αυτοί θα έπαιρναν 10^{13} χρόνια να δοκιμάζουν κάθε πιθανό 128 bit RC4 κλειδί. Αυτός ο χρόνος μετριέται κατά προσέγγιση χιλιάδες φορές μεγαλύτερος από την ηλικία του σύμπαντος, που εκτιμήθηκε πρόσφατα σαν $1.8 * 10^{10}$ χρόνια.

Από αυτή την ανάλυση, φαίνεται πως ο RC4 με κλειδί 128 bit μήκος, είναι επαρκής για πολλές κρυπτογραφικές ανάγκες σήμερα αλλά και για πάντα. Δυστυχώς όμως υπάρχουν κάποιοι παράγοντες που καθιστούν αυτή τη λύση, τεχνικά, νομικά και πολιτικά ακατάλληλη για πολλές εφαρμογές.

1.10.2. **Επιθέσεις κρυπτανάλυσης (cryptanalysis):** Εάν το μήκος του κλειδιού ήταν ο μόνος παράγοντας που καθόριζε την ασφάλεια ενός κρυπτογραφήματος τότε ο καθένας που θα ήθελε να ανταλλάζει μυστικά μηνύματα θα χρησιμοποιούσε κώδικες με 128 bit κλειδιά, και όλοι αυτοί που σπάνε κώδικες θα έπρεπε να βρουν άλλη δουλειά.

Ο λόγος που η κρυπτογραφία έχει μεγάλο ενδιαφέρον είναι το γεγονός ότι οι κρυπτογραφικοί αλγόριθμοι δεν ανταποκρίνονται στις προσδοκίες μας. Οι επιθέσεις αναζήτησης κλειδιού σπάνια χρειάζονται να γνωρίζουν τα περιεχόμενα ενός κρυπτογραφημένου μηνύματος. Αντίθετα, οι κρυπτογραφικοί αλγόριθμοι μπορούν να νικηθούν χρησιμοποιώντας συνδυασμούς από βελτιωμένα μαθηματικά. Το αποτέλεσμα είναι ότι πολλά κρυπτογραφημένα μηνύματα αποκρυπτογραφούνται χωρίς να ξέρουμε το κλειδί. Ένας επιδέξιος αναλυτής μπορεί κάποιες φορές να αποκρυπτογραφήσει ένα κείμενο χωρίς να ξέρει τον κρυπτογραφικό αλγόριθμο.

Οι στόχοι μιας επίθεσης κρυπτανάλυσης είναι δύο: Ο κρυπταναλυτής, αν έχει το κρυπτογράφημα να μπορεί να ανακαλύψει το καθαρό κείμενο και όταν το έχει να βρει το κλειδί με το οποίο κρυπτογραφήθηκε. Οι επιθέσεις που ακολουθούν χρησιμοποιούνται όταν ο κρυπτογραφικός αλγόριθμος είναι γνωστός:

- **Επίθεση γνωστού κειμένου:** Αυτή η τεχνική βασίζεται στο γεγονός ότι ο υποκλοπέας έχει ένα παράδειγμα απλού κειμένου μαζί με το αντίστοιχο του κωδικοποιημένο μήνυμα. Από αυτά ο υποκλοπέας μπορεί να υπολογίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση και στη συνέχεια μπορεί να το χρησιμοποιήσει για να αποκωδικοποιήσει εύκολα και άλλα μηνύματα. Η απόκτηση ενός δείγματος κρυπτογραφημένου κειμένου και του αντίστοιχου αρχικού κειμένου είναι αρκετές φορές αρκετά εύκολη αφού πολλές φορές μέρος των μηνυμάτων που ανταλλάσσονται είναι αρκετά απλό να

βρεθεί, για παράδειγμα να έχουν κάποια σταθερή μορφή επικεφαλίδας κ.λ.π.

- **Επίθεση επιλεγμένου κειμένου:** Σε αυτό το είδος επίθεσης ζητά από τον υπολογιστή που εκτελεί την αποκρυπτογράφηση να κωδικοποιήσει ένα ειδικό κομμάτι κειμένου, το οποίο έχει επιλεγεί ώστε η γνώση του αντίστοιχου κρυπτογραφημένου κειμένου να παρέχει αρκετά στοιχεία για το κλειδί.

- **Διαφορική επίθεση κρυπτανάλυσης:** Εδώ ο υποκλοπέας δημιουργεί μια σειρά μηνυμάτων που διαφέρουν ελάχιστα μεταξύ τους και εξετάζει πάλι την αντίστοιχη κρυπτογραφημένη έκδοση τους. Με τον τρόπο αυτό ο υποκλοπέας μπορεί να αποκτήσει σημαντικές πληροφορίες για το κλειδί.

- **Διαφορική επίθεση λαθών:** Αυτή είναι μια επίθεση με hardware όπου η συσκευή κωδικοποίησης δέχεται πίεση συγκεκριμένης μορφής ώστε να κάνει λάθη. Η συσκευή είναι εκτεθειμένη σε περιβαλλοντικούς παράγοντες (ζέστη, ακτινοβολία) οι οποίοι επιλέγονται για να την παρασύρουν να κάνει λάθη κατά την διάρκεια της κρυπτογράφησης ή της αποκρυπτογράφησης. Αυτά τα λάθη μπορούν να αναλυθούν και από αυτά να εξετάσουμε την εσωτερική κατάσταση της συσκευής, συμπεριλαμβάνοντας και το κλειδί κρυπτογράφησης ή και τον αλγόριθμο.

  Ο πραγματικός τρόπος να καθορίσουμε εάν ένας αλγόριθμος είναι δυνατός είναι να τον δημοσιεύσουμε και να περιμένουμε από κάποιον να βρει μια αδυναμία του. Αυτή η διαδικασία εξέτασης λαθών δεν είναι τέλεια. Δεν πρέπει να εμπιστευόμαστε άτομα που υποστηρίζουν ότι έχουν αναπτύξει έναν αλγόριθμο κρυπτογράφησης και δεν μας λένε τον τρόπο που δουλεύει.[6] Αν ένας αλγόριθμος χρησιμοποιείται για να αποθηκεύει πολύτιμες πληροφορίες, τότε ένας επιτιθέμενος θα κλέψει ένα αντίγραφο του προγράμματος που εφαρμόζει τον αλγόριθμο και θα αποσυνθέσει το πρόγραμμα για να μάθει τον τρόπο που δουλεύει. Η κρυπτογραφική ασφάλεια εξαρτάται από την ερευνητική εξέταση και ειλικρίνεια.

1.10.3. **Επιθέσεις βασισμένες στο σύστημα κρυπτογράφησης (system based attacks):** Ένας άλλος τρόπος να σπάσουμε ένα κρυπτογραφικό σύστημα είναι να επιτεθούμε στο κρυπτογραφικό σύστημα που χρησιμοποιεί έναν αλγόριθμο, χωρίς να επιτεθούμε στον κρυπτογραφικό αλγόριθμο.

Ένα παράδειγμα είναι ο VC-I Video, ένας κρυπτογραφικός αλγόριθμος που στο παρελθόν χρησιμοποιούταν για δορυφορική μετάδοση προγράμματος τηλεόρασης. Υπήρχαν πειρατές που πουλούσαν αποκωδικοποιητές με δυνατότητες υποκλοπής κλειδιών μεταφοράς, και στη συνέχεια αυτά τα κλειδιά τα χρησιμοποιούσαν για να αποκρυπτογραφήσουν την μετάδοση. Ήταν ένας ασφαλής κρυπτογραφικός αλγόριθμος αλλά το σύστημα σαν σύνολο ήταν αδύνατο.

1.11 Αλγόριθμοι δημόσιου κλειδιού

Η ύπαρξη κρυπτογραφίας δημόσιου κλειδιού προτάθηκε αρχικά το 1976 από δυο Αμερικανούς ερευνητές, τον Whitfield Diffie και τον Martin Hellman, ως ένας τρόπος

για να μην υπάρχει η ανάγκη μετάδοσης του κλειδιού ανάμεσα σε δυο πλευρές όπως συμβαίνει στην κρυπτογραφία συμμετρικού κλειδιού. Οι λεπτομέρειες της μεθόδου είναι πολύπλοκες και απαιτούν αρκετές γνώσεις μαθηματικών, συνεπώς το μόνο που μπορούμε να πούμε εδώ είναι ότι βασίστηκε αρχικά στο γεγονός ότι το να βρεθούν οι πρώτοι παράγοντες αριθμών μεγαλύτερων από π.χ. 10100 είναι υπολογιστικά δύσκολο που είναι σχεδόν απίθανο να γίνει.

Ο παραλήπτης ενός μηνύματος που χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιεί δυο κλειδιά με τον ακόλουθο τρόπο:

- Δημοσιοποιεί το δημόσιο κλειδί του π.χ. σε ένα site.
- Οποιοσδήποτε θέλει να στείλει μήνυμα στον κάτοχο του κλειδιού αυτού χρησιμοποιεί το δημόσιο κλειδί για να κάνει την κρυπτογράφηση.

Το κρυπτογραφημένο κείμενο αποκρυπτογραφείται από τον παραλήπτη που εφαρμόζει τον κατάλληλο αλγόριθμο αποκρυπτογράφησης χρησιμοποιώντας το ιδιωτικό κλειδί.

Με αυτό τον τρόπο δεν χρειάζεται ο παραλήπτης να δημοσιοποιήσει το κλειδί που χρησιμοποιείται για αποκρυπτογράφηση.

Υπάρχουν διάφορες τεχνολογίες της κρυπτογραφίας δημοσίου κλειδιού. Ορισμένα άλλα δύσκολά υπολογιστικά προβλήματα προτάθηκαν για κρυπτογραφία δημοσίου κλειδιού. Όμως η ανάλυση ενός μεγάλου αριθμού άντεξε στο χρόνο και είναι η ιδέα πίσω από την κρυπτογραφία δημοσίου κλειδιού. Οι τεχνολογίες που αναπτύχθηκαν θα εξεταστούν παρακάτω:

1.11.1. **Diffie - Hellman Ανταλλαγή κλειδιού (key exchange):** Αυτή είναι μια τεχνική για την ανταλλαγή ενός συμμετρικού κλειδιού χρησιμοποιώντας δημόσιο κλειδί. Οι δυο πλευρές που συμμετέχουν σε αυτή τη διαδικασία ανταλλάζουν αρχικά πληροφορίες σχετικά με κάποιο συμμετρικό κλειδί χρησιμοποιώντας μεθόδους δημοσίου κλειδιού και στη συνέχεια χρησιμοποιούν το συμφωνηθέν κλειδί για να επικοινωνήσουν.

1.11.2. **RSA.:** Ο RSA είναι σίγουρα το πιο γνωστό σύστημα κρυπτογράφησης δημοσίου κλειδιού. Αναπτύχθηκε από τρεις καθηγητές του MIT: τον Ronald Rivest, τον Adi Shamir και τον Leonard Adelman. Ο RSA μπορεί να χρησιμοποιηθεί για την αποστολή δεδομένων μέσω μιας μη ασφαλούς γραμμής και μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία ψηφιακών υπογραφών: σειρών χαρακτήρων δηλαδή που πιστοποιούν ότι ο αποστολέας του μηνύματος είναι αυτός που ισχυρίζεται πως είναι. Το κλειδί μπορεί να είναι οποιουδήποτε μήκους, ανάλογα με την εφαρμογή που χρησιμοποιείται.

1.11.3. **ElGamal system:** Δημιουργήθηκε από τον Taher ElGamal. Είναι ένα κρυπτογραφικό σύστημα δημοσίου κλειδιού που βασίζεται στο πρωτόκολλο ανταλλαγής κλειδιών Diffie - Hellman. Μπορεί επίσης να χρησιμοποιηθεί για ψηφιακές υπογραφές όπως και ο RSA.

1.11.4. **DSS. (Digital Signature Standard):** Αναπτύχθηκε από την αμερικανική εθνική υπηρεσία ασφάλειας (National Security Agency) και υιοθετήθηκε ως ομοσπονδιακό πρότυπο επεξεργασίας πληροφοριών από την αμερικανική εθνική υπηρεσία τυποποιήσεων (National Institute for Standards and Technology). Στην αρχική του μορφή μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές, ωστόσο μπορεί να

τροποποιηθεί για κανονική μεταφορά δεδομένων. Η τεχνική αυτή βασίζεται στον αλγόριθμο Digital Signature Algorithm. Αν και ο αλγόριθμος DSA επιτρέπει κλειδιά οποιουδήποτε μήκους, μόνο κλειδιά ανάμεσα σε 512 bits και 1024 bits επιτρέπονται στον DSS.

1.12 Επιθέσεις στους αλγορίθμους δημόσιου κλειδιού

Οι αλγόριθμοι δημόσιου κλειδιού είναι πιο ευάλωτοι στις επιθέσεις, σε σύγκριση με τους αλγόριθμους συμμετρικού κλειδιού. Αυτό γιατί ο επιτιθέμενος έχει ένα αντίγραφο του δημόσιου κλειδιού που χρησιμοποιήθηκε για την κρυπτογράφηση του μηνύματος. Η δουλειά του επιτιθέμενου είναι ευκολότερη γιατί το ίδιο μήνυμα πιθανώς να υποδηλώνει με ποιόν αλγόριθμο έχει κρυπτογραφηθεί.

Υπάρχουν δυο είδη επιθέσεων σε συστήματα δημοσίου κλειδιού:

1.12.1. **Επιθέσεις με δεδομένα (factoring attacks):** Πρωτύτερα αναφέρθηκε ότι οι γνωστές μέθοδοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται στην τεράστια δυσκολία επίλυσης αντεστραμμένων προβλημάτων. Όποιος μπορεί να αναλύσει μεγάλους αριθμούς μπορεί να σπάσει και ένα σύστημα δημοσίου κλειδιού βασιζόμενος σε ανάλυση. Αυτό δεν είναι απίθανο: μαθηματικοί που δουλεύουν στην περιοχή την θεωρίας αριθμών έχουν μελετήσει προβλήματα ανάλυσης για καιρό και είναι πετυχημένοι με αριθμούς που έχουν συγκεκριμένα χαρακτηριστικά. Μια τέτοια επίθεση είναι η RSA-129. Η πιο διάσημη επίθεση ανάλυσης έγινε στον αριθμό RSA-129 (129 ψηφία). Αυτός ο μεγάλος αριθμός παρουσιάστηκε σε ένα τεύχος του περιοδικού Popular Science το 1977. Τελικά αναλύθηκε από μια ομάδα ερευνητών υπό τον Arjen Lenstra.

1.12.2. **Επίθεση αλγοριθμική:** Η άλλη τεχνική που εφαρμόζεται για το σπάσιμο μιας κρυπτογραφίας δημοσίου κλειδιού είναι να βρεθεί κάποιο μειονέκτημα στον αλγόριθμο που χρησιμοποιείται. Για παράδειγμα, ένα από τα πρώτα προβλήματα που παρουσιάστηκαν είναι το superincreasing knapsack problem. Βρέθηκε ότι είναι εύκολο να εξακριβωθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί σε ένα σύστημα με αυτό το πρόβλημα.

1.13 Συναρτήσεις αποσύνθεσης μηνυμάτων (message digest functions)

Η προηγούμενη ενότητα ασχολήθηκε με τις τεχνικές που χρησιμοποιούνται στη κρυπτογραφία. Αυτή η ενότητα θα ασχοληθεί με το πως η κρυπτογράφηση παίζει σημαντικό ρόλο στην προφύλαξη ενός συνδεδεμένου στο δίκτυο συστήματος.

Μια αποσύνθεση μηνύματος δεν είναι τίποτα περισσότερο από έναν αριθμό, έναν ειδικό αριθμό που βγαίνει από έναν ανακατεμένο κώδικα (hush code). Αυτός ο κώδικας προέρχεται από μια συνάρτηση (message digest function) που είναι δύσκολο να αντιστραφεί. Ο μοναδικός αριθμός αυτός έχει συνήθως 128 με 256 bits μήκος.

Μια καλή συνάρτηση αποσύνθεσης μηνύματος θα πρέπει να έχει τα εξής χαρακτηριστικά:

- Κάθε κομμάτι της εισόδου στη συνάρτηση θα πρέπει να επηρεάζει το αποτέλεσμα.
- Αν κάποιο bit στην είσοδο της συνάρτησης ανασκόπησης μηνύματος μεταβληθεί, τότε κάθε bit στο αποτέλεσμα της συνάρτησης θα έχει πιθανότητα 50% να αλλάξει.

- Θα πρέπει να είναι υπολογιστικά ανέφικτο να βρεθεί κάποιο αρχείο το οποίο δίνει το ίδιο αποτέλεσμα όταν εισαχθεί στη συνάρτηση με ένα άλλο αρχείο.

Οι συναρτήσεις αποσύνθεσης μηνυμάτων ονομάζονται και συναρτήσεις μιας κατεύθυνσης γιατί παράγουν τιμές που είναι δύσκολο να αντιστραφούν, ανθεκτικές στην επίθεση και μοναδικές.

Υπάρχει μια σειρά συναρτήσεων αποσύνθεσης μηνύματος και σχετικών τεχνολογιών που έχουν αναπτυχθεί:

1.13.1. **HMAC (Hashed Message Authentication Code):** Αυτή είναι μια τεχνική που χρησιμοποιείται για να ελέγχεται αν κάποιο αρχείο έχει τροποποιηθεί. Χρησιμοποιεί και μια συνάρτηση αποσύνθεσης μηνύματος και ένα ιδιωτικό κλειδί. Μια συνάρτηση αποσύνθεσης μηνύματος χρησιμοποιείται στο κείμενο, κρυπτογραφείται και στέλνεται με το κείμενο. Ο παραλήπτης αποκρυπτογραφεί την αποσύνθεση του μηνύματος, χρησιμοποιεί τη συνάρτηση αποσύνθεσης πάνω στο κείμενο και συγκρίνει τα δυο αποτελέσματα. Αν συμφωνούν τότε το μήνυμα έφτασε ασφαλές.

1.13.2. **MD2. Message Digest #2:** Είναι μια συνάρτηση αποσύνθεσης μηνύματος που αναπτύχθηκε από τον Ronald Rivest. Είναι η πιο ασφαλής από όλες τις συναρτήσεις του, αλλά είναι υπολογιστικά αργότερη. Παράγει ως αποτέλεσμα έναν αριθμό αποσύνθεσης 128 bit.

1.13.3. **MD4. Message Digest #4:** Επίσης αναπτύχθηκε από τον Ronald Rivest. Είναι γρηγορότερη από την MD2 αλλά όχι ασφαλής. Παράγει αριθμό αποσύνθεσης 128 bit.

1.13.4. **MD5. Message Digest #5:** Αναπτυγμένη από τον Ronald Rivest. Περισσότερο ασφαλής και ευρέως χρησιμοποιημένη, το καλοκαίρι του 1996 ανακαλύφθηκαν ατέλειες που επέτρεπαν να υπολογιστούν κάποιες συγκρούσεις. Παράγει αριθμό αποσύνθεσης 128 bit.

1.13.5. **SHA. Secure Hash Algorithm:** Αναπτυγμένη από την NSA και σχεδιασμένη για χρήση με την National Institute for Standards and Technology's Digital Signature Standard (NIST's DSS). Μετά την δημοσίευσή της θεωρήθηκε ανασφαλής από την NIST. Παράγει αριθμό αποσύνθεσης 160 bit.

1.13.6. **SHA-1. Secure Hash Algorithm -1:** Αναθεωρημένη έκδοση της SHA. Δεν είναι γνωστό ότι είναι ασφαλέστερη από την προηγούμενη έκδοση. Παράγει αριθμό αποσύνθεσης 128 bit.

Πέρα από αυτές τις συναρτήσεις, μπορούμε να χρησιμοποιήσουμε παραδοσιακά συστήματα συμμετρικής μπλοκ κρυπτογράφησης, όπως ο DES, σαν συναρτήσεις αποσύνθεσης. Για να χρησιμοποιήσουμε μια κρυπτογραφική συνάρτηση σαν συνάρτηση αποσύνθεσης απλά τρέχουμε την συνάρτηση με την μέθοδο ανατροφοδότησης. Για κλειδί χρησιμοποιούμε ένα κλειδί που επιλέγεται τυχαία και ταιριάζει στην εφαρμογή. Κρυπτογραφούμε ολόκληρο το αρχείο εισόδου. Το τελευταίο κομμάτι του κρυπτογραφήματος είναι ο αριθμός αποσύνθεσης.

1.14 Οι συναρτήσεις αποσύνθεσης μηνυμάτων στην πράξη

Δεν χρησιμοποιούνται μόνες τους για κρυπτογραφικές και αποκρυπτογραφικές λειτουργίες. Αντίθετα, χρησιμοποιούνται για την δημιουργία ψηφιακών υπογραφών

και για κώδικες επικύρωσης μηνυμάτων, και για την δημιουργία των κλειδιών κρυπτογράφησης από τα passphrases.

Ένα απλό και αφελές παράδειγμα είναι να θυμάστε το password itbilhpway από τη φράση 'In the beginning I liked hash potatoes, what about you'. Η συνάρτηση παίρνει απλά το πρώτο γράμμα κάθε λέξης. Έτσι ο χρήστης μπορεί να θυμάται ένα σχετικά δύσκολο password. Οι συναρτήσεις αποσύνθεσης μηνύματος χρησιμοποιούνται επίσης σε ψηφιακές υπογραφές.

1.15 Χρήσεις των συναρτήσεων αποσύνθεσης μηνυμάτων

Οι συναρτήσεις αποσύνθεσης μηνυμάτων χρησιμοποιούνται σήμερα για πολλούς λόγους:

- Είναι πολύ γρηγορότερες από τις παραδοσιακές συναρτήσεις συμμετρικού κλειδιού αλλά μοιράζονται πολλές κρυπτογραφικές τεχνικές και δυνατότητες.
- Δεν υπάρχει κανένας περιορισμός ευρεσιτεχνίας σε καμία συνάρτηση αποσύνθεσης μηνυμάτων.
- Δεν υπάρχουν περιορισμοί εξαγωγής στις συναρτήσεις αποσύνθεσης μηνυμάτων.
- Χρησιμοποιώντας έναν αριθμό αποσυνθεμένου μηνύματος, μπορούμε να δημιουργήσουμε κλειδιά κρυπτογράφησης για κρυπτογραφήματα συμμετρικού κλειδιού. Έτσι επιτρέπουμε στους χρήστες να χρησιμοποιούν passphrase. Το κλειδί κρυπτογράφησης δημιουργείται από υπολογισμούς πάνω στον αριθμό αποσυνθεμένου μηνύματος της φράσης που είχε χρησιμοποιηθεί.
- Ο αριθμός του αποσυνθεμένου μηνύματος μπορεί να χρησιμοποιηθεί σε κώδικες επικύρωσης μηνυμάτων, οι οποίοι χρησιμοποιούν ένα κοινό μυστικό ανάμεσα στα δύο μέρη για να αποδείξουν ότι ένα μήνυμα είναι γνήσιο. Οι κώδικες επικύρωσης μηνυμάτων για να αναγνωριστούν επισυνάπτονται στο τέλος του μηνύματος.
- Οι αποσυνθέσεις μηνυμάτων είναι η βάση πολλών προτύπων ψηφιακών υπογραφών. Αντί να υπογράφουμε όλο το κείμενο, τα πιο πολλά πρότυπα ψηφιακών υπογραφών απλά υπογράφουν ένα αποσυνθεμένο μήνυμα του κειμένου.
- Οι κώδικες επικύρωσης μηνυμάτων βασίζονται στις αποσυνθέσεις μηνυμάτων που παρέχουν ασφάλεια στα περισσότερα πρωτόκολλα του internet.
- Προγράμματα όπως το PGP χρησιμοποιούν τον αριθμό αποσύνθεσης για να μετατρέψουν ένα passphrase που δίνεται από έναν χρήστη σε ένα κλειδί κρυπτογράφησης, το οποίο χρησιμοποιείται για συμμετρική κρυπτογράφηση.

1.16 Επιθέσεις στις συναρτήσεις αποσύνθεσης μηνυμάτων

Υπάρχουν δύο είδη επιθέσεων:

- Η πρώτη επίθεση είναι: να βρούμε δύο μηνύματα που έχουν τον ίδιο αριθμό αποσύνθεσης.

- Η δεύτερη επίθεση είναι: έχοντας ένα συγκεκριμένο μήνυμα, πρέπει να βρεθεί ένα δεύτερο μήνυμα που να έχει τον ίδιο κώδικα αποσύνθεσης.

Τέλος, αποτελούν ένα σημαντικό στοιχείο της κρυπτογράφησης δημόσιου κλειδιού και των κρυπτογραφικών συστημάτων, και μια επίθεση μπορεί να σημαίνει εξασθένιση του κρυπτογραφικού συστήματος. Γι' αυτό όταν εντοπιστεί μια αδυναμία σε μια συνάρτηση αποσύνθεσης, ο αλγόριθμος που χρησιμοποιεί αποσύρεται και τοποθετείται κάποιος άλλος στη θέση του.

1.17 Υποδομή δημόσιου κλειδιού (Public Key Infrastructure)

Είναι ένας συνδυασμός από προγράμματα, τεχνολογίες κρυπτογράφησης και υπηρεσίες, μπορεί να πιστοποιηθεί (επαληθευθεί) η ταυτότητα ενός φυσικού προσώπου που συναλλάσσεται στο Internet καθώς και να προστατευθεί η ασφάλεια των διαδικτυακών συναλλαγών.

Στην κρυπτογράφηση δημόσιου κλειδιού κάθε χρήστης απαιτείται να φτιάξει δύο κλειδιά:

- **Ένα δημόσιο κλειδί,** για να στέλνομε κρυπτογραφημένα μηνύματα στον παραλήπτη και να επικυρώνουμε την ψηφιακή υπογραφή του αποστολέα.
- **Ένα προσωπικό κλειδί,** το οποίο χρησιμοποιείται από τον παραλήπτη για να αποκωδικοποιήσει τα κρυπτογραφημένα μηνύματα που λαμβάνει και για να υπογράψει με την ψηφιακή υπογραφή του ο αποστολέας.

  Τα δημόσια κλειδιά είναι σχεδιασμένα να δημοσιεύονται και να διανέμονται ευρέως, ενώ τα προσωπικά κλειδιά είναι σχεδιασμένα να κρατιούνται μυστικά.

  Ένας απλός τύπος δημόσιου και προσωπικού κλειδιού περιέχει ελάχιστη πληροφορία εκτός από τις πραγματικές τιμές που χρειάζονται για να γίνει η κρυπτογράφηση και η αποκρυπτογράφηση. Χρειαζόμαστε πιο πολλές πληροφορίες να αποθηκεύονται σε κάθε δημόσιο κλειδί. Μαζί με την πληροφορία κρυπτογράφησης μπορεί να θέλουμε να αποθηκεύσουμε το όνομα του χρήστη ή και κάποια άλλη πληροφορία ταυτότητας.

  Η περιοχή του ονόματος μπορεί να συμπληρωθεί με οποιοδήποτε στοιχείο θέλουμε.

ΚΕΦΑΛΑΙΟ ΔΕΥΤΕΡΟ

ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΟ WEB

2.1. Οι λειτουργίες της κρυπτογράφησης

Η κρυπτογραφία εκτελεί τις εξής λειτουργίες στα σύγχρονα πληροφοριακά συστήματα:

- **Εμπιστευτικότητα (Confidentiality):** Είναι η κρυπτογράφηση (κωδικοποίηση) των δεδομένων ή και των μηνυμάτων και συνεπώς η προστασία τους από τρίτα, μη εξουσιοδοτημένα άτομα. Αυτό σημαίνει ότι τα δεδομένα ή τα μηνύματα δεν μπορεί ούτε καν να τα δει κάποιος τρίτος, πόσο μάλλον να τα τροποποιήσει.
- **Ακεραιότητα (Integrity):** Είναι η προστασία των δεδομένων ή και των μηνυμάτων από ενδεχόμενη τροποποίησή τους από τρίτα, μη εξουσιοδοτημένα άτομα. Αυτό σημαίνει ότι τα δεδομένα ή τα μηνύματα μπορεί να τα δει κάποιος τρίτος αλλά όχι και να τα τροποποιήσει.
- **Μη Άρνηση Αποδοχής (Non - Repudiation):** Σημαίνει με απλά λόγια ότι αυτός που έστειλε το μήνυμα δεν έχει τη δυνατότητα να ισχυρισθεί ότι δεν ήταν αυτός που το δημιούργησε και το έστειλε.
- **Πιστοποίηση (Authentication):** Είναι η επιβεβαίωση της ταυτότητας του αποστολέα, η εξακρίβωση δηλαδή ότι όντως είναι αυτός που ισχυρίζεται ότι είναι και βασίζεται στον συνδυασμό του δημόσιου και του ιδιωτικού κλειδιού.

2.2. Κρυπτογραφικά συστήματα που χρησιμοποιούνται σήμερα

Τα τελευταία χρόνια έχουν αναπτυχθεί αρκετά κρυπτογραφικά συστήματα για το Internet. Υπάρχουν οι παρακάτω κατηγορίες:

- **PGP (Pretty Good Privacy):** Για την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και αρχείων, δημοφιλέστερο πρόγραμμα είναι το PGP (Pretty Good Privacy). Οι αλγόριθμοι του PGP είναι γνωστοί και ασφαλείς. Ο πηγαίος κώδικάς του είναι διαθέσιμος στο κοινό, γεγονός που επέτρεψε σε ειδικούς επιστήμονες των κλάδων της πληροφορικής και της κρυπτογραφίας να το εξετάσουν και να αναζητήσουν σφάλματα ή "κερκόπορτες" (back doors).
- **S/MIME:** Ένα άλλο πρόγραμμα που κάνει format για κρυπτογράφηση ηλεκτρονικού ταχυδρομείου είναι το S/MIME.

Μια άλλη κατηγορία είναι τα πρωτόκολλα δικτύου που χρησιμοποιούνται για να παρέχουν εμπιστευτικότητα, ακεραιότητα, αναγνώριση ταυτότητας σε περιβάλλον δικτύου. Αυτά τα συστήματα χρειάζονται αλληλεπίδραση πραγματικού χρόνου ανάμεσα στον client και ενός server για να δουλέψουν σωστά. Τα πιο δημοφιλή είναι:

- **PCT:** Αυτό είναι ένα προϊόν της Microsoft το οποίο είναι παρόμοιο με το SSL, το οποίο θα περιγράψουμε λεπτομερέστερα στη συνέχεια. Καθώς το SSL γίνεται όλο και πιο δημοφιλές, αναμένεται ότι αυτή η τεχνολογία τελικά σχεδόν δεν θα χρησιμοποιείται.
- **S-HTTP:** Αυτή είναι μια έκδοση του πρωτοκόλλου HTTP το οποίο επιτρέπει ασφαλείς συναλλαγές μέσω δικτύου. Ωστόσο, καθώς οι κατασκευαστές browser δεν έδειξαν μεγάλο ενδιαφέρον για αυτό, σχεδόν δεν χρησιμοποιείται καθόλου.
- **SET:** Αυτό είναι ένα πρωτόκολλο το οποίο χρησιμοποιείται για αποστολή στοιχείων πιστωτικών καρτών μέσω του Internet. Έχει τρία στοιχεία: ένα ηλεκτρονικό πορτοφόλι που υπάρχει στον υπολογιστή του πελάτη, έναν διακομιστή SET, για τον οποίο είναι υπεύθυνος κάποιος πωλητής ή έμπορος και ένα διακομιστή πληρωμών που υπάρχει σε μια τράπεζα ή εταιρεία πιστωτικών καρτών.
- **DNSSEC:** Αυτά είναι τα αρχικά για το Domain Name System Security Standard. Σχεδιάστηκε για να αποτρέψει επιθέσεις όπως το DNS spoofing. Και πάλι αυτό χρησιμοποιεί κρυπτογραφία δημοσίου κλειδιού. Κάθε DNS server σχετίζεται με ένα ζευγάρι δημοσίου / ιδιωτικού κλειδιού. Κάθε όνομα πεδίου στο Internet έχει ένα δημόσιο κλειδί το οποίο χρησιμοποιείται από τους υπολογιστές για να το πιστοποιήσουν.
- **Kerberos:** Αυτό είναι ένα δικτυακό σύστημα ασφαλείας το οποίο αναπτύχθηκε στο MIT. Χρησιμοποιεί κρυπτογραφία συμμετρικού κλειδιού για τη μετάδοση μηνυμάτων.
- **Ανταλλαγή κλειδιών Diffie - Hellman:** Μια χρήση της κρυπτογραφίας δημοσίου κλειδιού είναι στην μετάδοση μιας μυστικής πληροφορίας, όπως ένα κλειδί που χρησιμοποιείται σε ένα συμμετρικό σύστημα. Ένα παράδειγμα είναι το σύστημα ανταλλαγής κλειδιών των Diffie - Hellman. Αυτή είναι μια τεχνική που χρησιμοποιείται για να προστατέψει ένα κλειδί που χρησιμοποιείται σε συμμετρικά συστήματα. Με αυτό, οι δυο πλευρές που πρόκειται να επικοινωνήσουν πρώτα ανταλλάσσουν πληροφορίες για το συμμετρικό κλειδί χρησιμοποιώντας κρυπτογραφία δημοσίου κλειδιού.
- **CyberCash:** Είναι ένα πρωτόκολλο για αποστολή ασφαλών εντολών πληρωμής μέσω του Internet.
- **SSL:** Αυτή η τεχνολογία αναπτύχθηκε αρχικά από τη Netscape Corporation για τον browser Netscape Navigator. Λειτουργεί σαν ένα επίπεδο που υπάρχει ανάμεσα σε πρωτόκολλα όπως το HTTP και το FTP και υποκείμενα πρωτόκολλα που υπάρχουν στο TCP/IP. Το SSL υποστηρίζει δυο υποπρωτόκολλα. Το πρώτο είναι το SSL record protocol. Αυτό χρησιμοποιείται για την μετάδοση μεγάλων όγκων δεδομένων. Το δεύτερο πρωτόκολλο είναι το χειραψίας SSL, το οποίο χρησιμοποιείται για να εγκαταστήσει τους κωδικούς και τους αλγορίθμους που θα χρησιμοποιηθούν για τη μεταφορά δεδομένων. Είναι μια μορφή πρωτοκόλλου "χειραψίας" το οποίο αρχικοποιεί τις ρυθμίσεις δυο υπολογιστών που συμμετέχουν με μια μεταφορά δεδομένων μέσω του SSL.
- **SSH:** Είναι ένα πρωτόκολλο που χρησιμοποιείται για την κρυπτογράφηση ενός απομακρυσμένου τερματικού.

2.1.1. **PGP (Pretty Good Privacy):** Γράφτηκε από τον Phil Zimmerman και κυκλοφόρησε τον Ιούνιο του 1991. Είναι ένα ολοκληρωμένο σύστημα που προσφέρει κρυπτογραφική προστασία των e-mails και των αρχείων. Είναι ένα σύνολο από standards που περιγράφουν τα formats των κρυπτογραφημένων μηνυμάτων, των κλειδιών και των ψηφιακών υπογραφών. Χρησιμοποιείται εδώ και αρκετά χρόνια, και οι ειδικοί της κρυπτογραφίας το θεωρούν σε μεγάλο βαθμό αξιόπιστο.

Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει τη χρήση της.

Πρόκειται βέβαια για εμπορικό πρόγραμμα, μπορεί ωστόσο να χρησιμοποιηθεί χωρίς χρέωση για μη επαγγελματική χρήση. Επίσης, υπάρχουν και εκδόσεις open source / free software (λογισμικό ανοιχτού /ελεύθερου κώδικα και δωρεάν διανομής), όπως το gnupgp. Το PGP ήταν αρχικά διαθέσιμο από την PGP Inc. Η εταιρία εξαγοράστηκε από τη Network Associates, η οποία ανέλαβε την εξέλιξη και τις αναβαθμίσεις του προγράμματος. Στις αρχές του 2002 η Network Associates ανακοίνωσε ότι θα σταματήσει την πώληση και υποστήριξη του PGP. Αργότερα, όμως, αποφασίσθηκε η επανασύσταση της PGP Corporation, η οποία αναπτύσσει τη νέα έκδοση (8.0) του προγράμματος και θα αναλάβει την υποστήριξή του.

Ο χρήστης προγραμμάτων τύπου PGP πρέπει αρχικά να δημιουργήσει ένα ζευγάρι κλειδιών (key pair), δημόσιο και ιδιωτικό. Παρέχει το δημόσιο κλειδί σε όλους τους παραλήπτες είτε με e-mail είτε δημοσιεύοντας το στο Internet. Το ιδιωτικό κλειδί παραμένει κρυφό, στο σταθμό εργασίας του χρήστη, και δεν θα πρέπει να διαρρεύσει, καθώς εξασφαλίζει την αποτελεσματικότητα της κρυπτογράφησης.

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί. Αυτή είναι μια μονόδρομη διαδικασία: αφού κρυπτογραφηθεί το μήνυμα, δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με το ιδιωτικό κλειδί. Για το λόγο αυτό, είναι σημαντικό να μη διαρρεύσει. Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να εισάγει την "passphrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

Κάθε χρήστης του PGP διατηρεί λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί (keyring). Για την προστασία της λίστας, την υπογράφει ο ίδιος με το ιδιωτικό του κλειδί.

Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παράσχει ισχυρή ταυτοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας. Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές

διεξάγονται αποκλειστικά με άμεση επικοινωνία των χρηστών. Επιπλέον, δεν παρέχει την επιλογή της ανωνυμίας, καθώς η χρήση μιας διεύθυνσης e-mail που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών.

2.1.2. **S/MIME (Multipurpose Internet Mail Extensions):** Είναι ένα standard για αποστολή αρχείων με binary attachments μέσω του Internet. Το Secure / MIME είναι μια επέκταση του MIME standard για την αναγνώριση των κρυπτογραφημένων e-mail. Αντίθετα από το PGP, το S/MIME εφαρμόστηκε σαν ένα εργαλείο που σχεδιάστηκε για να προστίθεται σε διάφορα πακέτα ηλεκτρονικού ταχυδρομείου. Επειδή προέρχεται από την RSA Data Security και περιλαμβάνει άδειες για όλους τους απαιτούμενους αλγορίθμους, και επειδή οι μεγαλύτερες εταιρίες που πουλούν συστήματα e-mail ήδη έχουν επιχειρηματική σχέση με την RSA Data Security, είναι πιθανό να υιοθετηθεί περισσότερο από το PGP, παρά από πωλητές e-mail προγραμμάτων.

Προσφέρει εμπιστευτικότητα, επειδή ο κρυπτογραφικός του αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώριση γνησιότητας με την χρήση του X.509 δημόσιου κλειδιού πιστοποιητικών και προσφέρει απαγόρευση απάρνησης λόγο των κρυπτογραφικά υπογεγραμμένων μηνυμάτων. Το σύστημα χρησιμοποιείται με δυνατή ή αδύνατη κρυπτογράφηση.

Για να μπορούμε να στείλουμε κρυπτογραφικά μηνύματα σε κάποιον με το S/MIME, πρέπει να έχουμε ένα αντίγραφο του δημόσιου κλειδιού του. Τα ποιο πολλά προγράμματα που χρησιμοποιούν το σύστημα αυτό κάνουν χρήση των X.509.

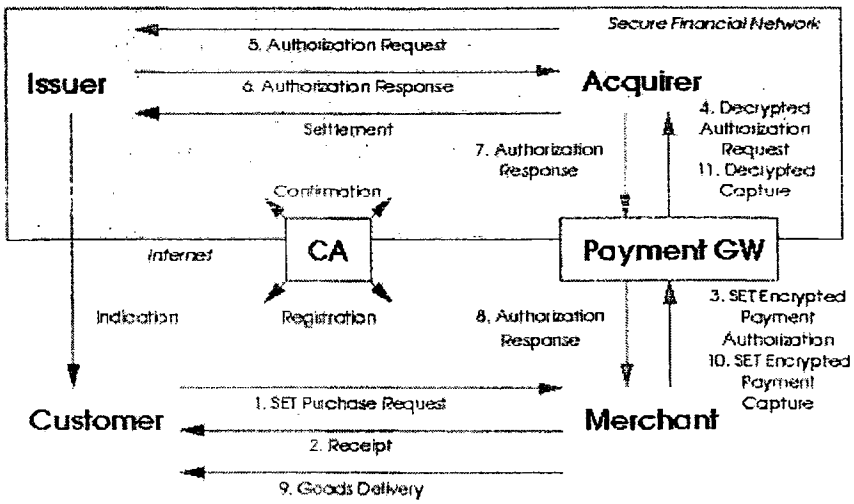
2.1.3. **PCT (Private Communications Technology):** Είναι ένα ασφαλές πρωτόκολλο επιπέδου μεταφοράς, παρόμοιο με το SSL, το οποίο αναπτύχθηκε από την Microsoft, σαν απάντηση στα προβλήματα που παρουσίασε το SSL 2.0 και το SSL 3.0.

Αν και η Microsoft υποστηρίζει το SSL 3.0, σκοπεύει να συνεχίσει να υποστηρίζει το PCT γιατί χρησιμοποιείται από μεγάλους πελάτες της, στα εταιρικά τους δίκτυα.

2.1.4. **S-HTTP:** Το σύστημα αυτό χρησιμοποιείται για υπογραφή και κρυπτογράφηση πληροφοριών που στέλνονται μέσω του HTTP πρωτοκόλλου. Σχεδιάστηκε πριν κυκλοφορήσει το SSL. Περιλαμβάνει μερικά κομψά χαρακτηριστικά, όπως η ικανότητα να προϋπογράφει κείμενα που βρίσκονται μέσα σε ένα web server. Δυστυχώς, είναι ένα νεκρό πρωτόκολλο επειδή η Netscape και η Microsoft δεν μπόρεσαν να το εφαρμόσουν στους browsers.

2.1.5. **SET:** Είναι σχεδιασμένο για την αποστολή κρυπτογραφημένων αριθμών πιστωτικών καρτών μέσω Internet. Έχει τρία μέρη που το αποτελούν: ένα ηλεκτρονικό πορτοφόλι που υπάρχει στον υπολογιστή του χρήστη, ένα server που τρέχει στα εμπορικά web sites και ένα SET server πληρωμής που τρέχει στις διάφορες τράπεζες εμπόρων.

Στην εικόνα 2.1 φαίνεται μια πληρωμή SET:



Εικόνα 2.1

Το πρώτο πράγμα που πρέπει να κάνει ο χρήστης όταν χρησιμοποιεί το SET είναι να δώσει τα στοιχεία της πιστωτικής του κάρτας στο ηλεκτρονικό του πορτοφόλι. Αυτά θα αποθηκευτούν σε ένα κρυπτογραφημένο αρχείο στον υπολογιστή του χρήστη. Παράλληλα, το πρόγραμμα που διαχειρίζεται το SET στον υπολογιστή του χρήστη θα παράγει ένα δημόσιο και ένα ιδιωτικό κλειδί.

Όταν πραγματοποιείται μια αγορά από ένα χρήστη του SET, οι λεπτομέρειες της πιστωτικής κάρτας κρυπτογραφούνται με το δημόσιο κλειδί. Στέλνονται στον έμπορο που παρέχει το αγαθό το οποίο θα πληρωθεί με την πιστωτική κάρτα. Ο διακομιστής του εμπόρου προσθέτει μια ψηφιακή υπογραφή στις λεπτομέρειες της πιστωτικής κάρτας για να καθορίσει την ταυτότητα του εμπόρου. Έπειτα όλα μαζί στέλνονται στην τράπεζα ή στον υπολογιστή της εταιρίας με την πιστωτική κάρτα. Έτσι ο υπολογιστής επιβεβαιώνει την κάρτα και στέλνει μια απόδειξη στον έμπορο και στον πελάτη. Ένα πλεονέκτημα αυτής της τεχνολογίας είναι ότι ο έμπορος δεν μπορεί να δει τις λεπτομέρειες της πιστωτικής κάρτας που χρησιμοποιούνται στην τράπεζα και η τράπεζα δε γνωρίζει τι αγόρασε ο πελάτης.

Το SET προσφέρει εμπιστευτικότητα για τους αριθμούς των πιστωτικών καρτών, καθώς κρυπτογραφούνται χρησιμοποιώντας τον αλγόριθμο RSA. Δεν προσφέρει εμπιστευτικότητα για τα υπόλοιπα στοιχεία της συναλλαγής του χρήστη. Αυτή ήταν μια αναγκαία λύση για να κερδισθεί η έγκριση για εξαγωγή του προγράμματος SET χωρίς περιορισμούς. Παρέχει ακεραιότητα, αναγνώριση ταυτότητας και απαγόρευση απάρνησης χρησιμοποιώντας συναρτήσεις αποσύνθεσης μηνύματος και ψηφιακές υπογραφές.

2.1.6. **DNSSEC (Domain Name System Security Standard):** Σχεδιάστηκε για να φέρει την ασφάλεια στο Domain Name System Security (DNS). Δημιουργεί ένα παράλληλο δημόσιο κλειδί υποδομής κτισμένο πάνω στο DNS σύστημα. Κάθε DNS Domain καθορίζεται από ένα δημόσιο κλειδί. Ένα τέτοιο κλειδί μπορούμε να το αποκτήσουμε με έναν έμπιστο τρόπο από το εν λόγω domain ή αυτό μπορεί να φορτωθεί από πριν μέσα σε ένα

DNS server χρησιμοποιώντας το αρχείο boot του server. Αναγνωρίζεται για τις ασφαλείς ανανεώσεις πληροφοριών στους DNS servers, κάνοντας το καλύτερο για απομακρυσμένη διαχείριση.

2.1.7. **Kerberos:** Αυτό είναι ένα σύστημα ασφαλείας δικτύου το οποίο αναπτύχθηκε στο MIT και χρησιμοποιήθηκε από την αρχή στις Ηνωμένες Πολιτείες. Αντίθετα με άλλα συστήματα, δεν χρησιμοποιεί τεχνολογία δημόσιου κλειδιού. Χρησιμοποιεί κρυπτογραφία συμμετρικού κλειδιού για τη μετάδοση μηνυμάτων προς και από υπολογιστές και χρησιμοποιείται για πιστοποίηση χρηστών. Κάθε χρήστης του Kerberos έχει ένα δικό του password, ο Kerberos το χρησιμοποιεί για να αποκρυπτογραφήσει μηνύματα που στέλνονται σε αυτόν τον χρήστη, ώστε να μην μπορούν να διαβαστούν από κανέναν άλλο. Υπάρχουν εκδόσεις του Kerberos για διάφορα δημοφιλή πρωτόκολλα του Internet όπως του POP3, του Telnet και του FTP.

Ο Kerberos είναι ένα δύσκολο σύστημα στο να διαμορφωθεί και να διαχειριστεί. Για να λειτουργήσει θα πρέπει η κάθε μεριά να έχει ένα Kerberos server που θα είναι ασφαλές. Αυτός ο Kerberos server κρατά ένα αντίγραφο των password κάθε χρήστη. Αν ο Kerberos server εκτίθεται, κάθε password χρήστη πρέπει να αλλάζει.

2.1.8. **CyberCash:** Είναι ένα πρωτόκολλο ηλεκτρονικής πληρωμής παρόμοιο με το σκοπό του SET. Τα μέρη του είναι μοντέλα ανάπτυξης στο CyberCash. Θα λέγαμε ότι είναι μια παραλλαγή προϊόντος.

2.1.9. **SSL (Secure Socket Layer):** Είναι ένα κρυπτογραφικό πρωτόκολλο για ασφαλή κανάλια επικοινωνίας διπλής κατεύθυνσης. Οι SSL συνδέσεις συχνά ξεκινούν από την πλευρά web browser εξαιτίας ενός ειδικού προθέματος στην URL διεύθυνση. Προσφέρει εμπιστευτικότητα, εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα, εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώριση γνησιότητας με την χρήση του X.509 v3 δημόσιου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγω των κρυπτογραφικά υπογεγραμμένων μηνυμάτων.

2.1.10. **SSH (Secure Shell):** Είναι ένα ασφαλές κέλυφος. Παρέχει κρυπτογραφικά προστατευμένα εικονικά τερματικά (Telnet) και λειτουργίες μεταφοράς αρχείων. Μη εμπορικές εκδόσεις του είναι διαθέσιμες από πολλές εκδόσεις UNIX συστημάτων. Το SSH είναι διαθέσιμο για Windows, Unix και Macintosh συστήματα από την Data Fellows.

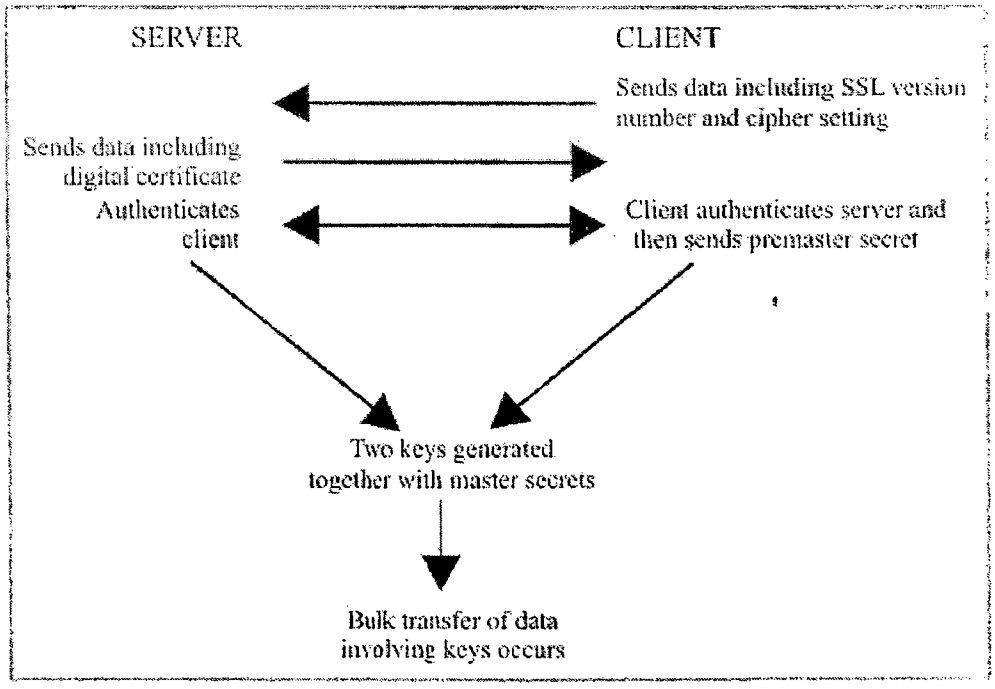
ΚΕΦΑΛΑΙΟ ΤΡΙΤΟ

SSL (Secure Socket Layer)

Το SSL, είναι ένα γενικού σκοπού πρωτόκολλο για την αποστολή κρυπτογραφημένης πληροφορίας μέσω του Internet. Αναπτύχθηκε από την Netscape και έγινε προσιτό από το πλατύ κοινό από τον Web Browser και server της Netscape. Η ιδέα ήταν να μιμηθούν τις πωλήσεις μιας εταιρίας με κρυπτογραφικά ενεργοποιημένους web servers διανέμοντας έναν free client ο οποίος εφάρμοζε τα ίδια κρυπτογραφικά πρωτόκολλα.

Από τότε ενσωματώθηκε μέσα σε πολλούς web servers και η υποστήριξη του θεωρείται αναγκαία. Χρησιμοποιείται και για no – web εφαρμογές όπως είναι το secure Telnet. Θεωρείται ένα από τα ποιο δημοφιλή πρωτόκολλα κρυπτογράφησης.

Στην εικόνα 3.1 φαίνεται η ανάλυση του πρωτόκολλου SSL:



Εικόνα 3.1

3.1. Τι είναι το SSL

Είναι ένα επίπεδο που υπάρχει ανάμεσα στη σειρά του TCP/IP πρωτοκόλλου και στο επίπεδο εφαρμογής. Ενώ το TCP/IP πρωτόκολλο απλά στέλνει ένα ανώνυμο free – error ρεύμα πληροφοριών ανάμεσα στους δυο υπολογιστές, το SSL προσθέτει πολυάριθμες λειτουργίες σε αυτό το ρεύμα. Μερικές από αυτές είναι:

- **Αυθεντικοποίηση διακομιστή SSL**. Αυτό επιτρέπει σε ένα πελάτη να πιστοποιήσει την ταυτότητα ενός διακομιστή. Το SSL χρησιμοποιεί κρυπτογραφία δημοσίου κλειδιού για να πιστοποιήσει την ψηφιακή

υπογραφή ενός διακομιστή και να πιστοποιήσει ότι αυτό εκδόθηκε από μια έγκυρη αρχή πιστοποίησης.

- **Αυθεντικοποίηση πελάτη SSL.** Με παρόμοιο τρόπο με τον οποίο πιστοποιούνται οι διακομιστές, πιστοποιούνται και οι πελάτες. Ένας διακομιστής που υποστηρίζει SSL μπορεί να ελέγξει τις ψηφιακές υπογραφές των πελατών για να διασφαλίσει ότι αυτοί είναι αυτοί που λένε πριν τους στείλει τυχόν ευαίσθητα δεδομένα.
- **Κρυπτογραφία SSL.** Το SSL χρησιμοποιεί μια ποικιλία τεχνικών συμμετρικής κρυπτογραφίας για να την αποστολή και λήψη δεδομένων.

Η κρυπτογραφία είναι ένας αναπτυσσόμενος τομέας, και τα κρυπτογραφικά πρωτόκολλα δεν λειτουργούν αν τα δυο μέρη επικοινωνίας δεν χρησιμοποιούν τους ίδιους αλγορίθμους. Για το λόγο αυτό το SSL είναι επεκτάσιμο και μπορεί να προσαρμοστεί εύκολα. Όταν ένα πρόγραμμα που χρησιμοποιεί SSL προσπαθεί να επικοινωνήσει με ένα άλλο, τότε τα δυο προγράμματα συγκρίνουν ηλεκτρονικά στοιχεία και καθορίζουν ποιος είναι ο δυνατότερος κρυπτογραφικός αλγόριθμος που διαθέτουν. Η συναλλαγή αυτή ονομάζεται SSL Hello.

Σχεδιάστηκε για χρήση σε παγκόσμιο επίπεδο, αλλά αναπτύχθηκε στις Ηνωμένες Πολιτείες και συμπεριλαμβάνεται μέσα στα προγράμματα που πωλούνται από εταιρίες των ΗΠΑ για χρήση στο εξωτερικό. Περιέχει πολλές λειτουργίες έτσι ώστε να μπορεί να συμμορφώνεται με τις κυβερνητικές περιοριστικές πολιτικές σε θέματα εξαγωγής κρυπτογραφικών συστημάτων.

3.2. Εκδώσεις του SSL

Η έκδοση 1.0 του πρωτοκόλλου χρησιμοποιήθηκε μέσα στο Netscape. Η έκδοση 2.0 συμπεριλήφθηκε με το Netscape Navigator 1 και 2. Αφού το SSL 2.0 δημοσιεύτηκε, η Microsoft δημιούργησε ένα παρόμοιο secure link πρωτόκολλο, το λεγόμενο PCT, που ξεπέρασε κάποιες ελλείψεις του SSL 2.0. Τα πλεόνεκτήματα του PCT ενσωματώθηκαν στο SSL 3.0. Αυτό το πρωτόκολλο χρησιμοποιήθηκε σαν τη βάση για το Transport Layer Security (TLS) πρωτόκολλο που αναπτύχθηκε από την Internet Engineering Task Force (IETF).

3.3. Τα χαρακτηριστικά του SSL 3.0

Αυτό το πρωτόκολλο προσφέρει πολλά χαρακτηριστικά θεωρητικού αλλά και πρακτικού ενδιαφέροντος:

3.3.1. **Διαχωρισμός των καθηκόντων:** Χρησιμοποιεί ξεχωριστούς αλγόριθμους για την κρυπτογράφηση, την απόδειξη γνησιότητας και την ακεραιότητα των δεδομένων με διαφορετικά μυστικά κλειδιά (secrets keys) για κάθε λειτουργία. Το κυριότερο πλεονέκτημα αυτού του διαχωρισμού είναι ότι τα μεγαλύτερα κλειδιά μπορούν να χρησιμοποιηθούν για την απόδειξη της γνησιότητας και για την ακεραιότητα των δεδομένων, ενώ τα μικρότερα κλειδιά για την μυστικότητα. Αυτό είναι χρήσιμο για τα προϊόντα που σχεδιάζονται με σκοπό την εξαγωγή τους στις Ηνωμένες Πολιτείες, γιατί ομοσπονδιακές ρυθμίσεις τοποθετούν περιορισμούς στο θέμα του μήκους των κλειδιών που χρησιμοποιούνται για την εμπιστευτικότητα, ενώ δεν χρησιμοποιούνται περιορισμοί για την περίπτωση της ακεραιότητας και της απόδειξης γνησιότητας.

Το SSL v3 παρέχεται για τις συνδέσεις που δεν κρυπτογραφούνται αλλά αποδεικνύεται η γνησιότητα τους και προστατεύονται εναντίον προμελετημένων αλλοιώσεων από κάποιον επιτηδευμένο attacker. Αυτό είναι χρήσιμο σε περίπτωση που η κρυπτογράφηση είναι απαγορευμένη από το νόμο, όπως στην Γαλλία.

Η επιλογή των αλγορίθμων και του μήκους των κλειδιών καθορίζεται από τον SSL server, αλλά περιορίζεται και από τις δυο πλευρές, τον server και τον client.

3.3.2. **Αποτελεσματικότητα:** Οι SSL εφαρμογές μπορούν να αποθηκεύουν κρυφά ένα μυστικό (master secret) που διατηρείται αναλλοίωτο μεταξύ των SSL συνδέσεων. Αυτό επιτρέπει στις καινούριες συνδέσεις να ξεκινήσουν αμέσως την ασφαλή επικοινωνία, χωρίς να χρειάζεται να εκτελέσουν περισσότερες λειτουργίες δημόσιου κλειδιού.

3.3.3. **Πιστοποιητικό βασισμένο στην απόδειξη γνησιότητας:** Παρέχει γνησιότητα και στον client και στον server, μέσω της χρήσης ψηφιακών πιστοποιητικών και ψηφιακών υπογεγραμμένων προκλήσεων αναγνώρισης. Χρησιμοποιεί τα X.503 v3 πιστοποιητικά, ενώ η IETF τυποποίηση του SSL (TLS) χρησιμοποιεί διαφορετικά είδη πιστοποιητικών καθώς είναι τυποποιημένα. Η απόδειξη γνησιότητας είναι ένα προαιρετικό μέρος του πρωτοκόλλου, μολονότι τα πιστοποιητικά του server είναι αποτελεσματικά εξουσιοδοτημένα από τις σημερινές SSL εφαρμογές.

3.3.4. **Αγνωστικό πρωτόκολλο (Protocol Agnostic):** Αν και το SSL σχεδιάστηκε για να τρέχει στην κορυφή του TCP/IP, αυτό στην πραγματικότητα μπορεί να τρέξει στην κορυφή κάθε αξιόπιστου connection - oriented πρωτοκόλλου, όπως είναι το X.25 ή το OSI. Το SSL δεν μπορεί να τρέξει στην κορυφή ενός μη αξιόπιστου πρωτοκόλλου, όπως το IP User Datagram Protocol (UDP).

3.3.5. **Προστασία ενάντια στις man-in-the-middle και replay επιθέσεις:** Το SSL μπορεί να είναι ευάλωτο σε μια μορφή επίθεσης που αποκαλείται επίθεση man-in-the-middle. Στην επίθεση αυτή παρεμβάλλεται ένας υπολογιστής ή πρόγραμμα μεταξύ του πελάτη και του διακομιστή. Ο ενδιάμεσος υπολογιστής ή πρόγραμμα αρχίζει τη διαδικασία της χειραψίας με τον πελάτη και δημιουργεί ένα δικό του master secret και συνεπώς δυο κλειδιά. Αυτά τα κλειδιά στη συνέχεια χρησιμοποιούνται για να κρυπτογραφήσουν και να αποκρυπτογραφήσουν πληροφορίες που θα έπρεπε να μεταφέρονται μεταξύ του πελάτη και του πραγματικού διακομιστή.

Το επόμενο βήμα είναι να πιστοποιηθεί η ψηφιακή υπογραφή του εκδότη του πιστοποιητικού. Το κλειδί το οποίο χρησιμοποιείται για αυτό βρίσκεται στα στοιχεία της αρχής πιστοποίησης που βρίσκεται στον πελάτη.

Αν αυτή η διαδικασία πετύχει τότε ο πελάτης μπορεί να νοιώθει ασφαλής ότι το πιστοποιητικό του διακομιστή είναι έγκυρο.

Το επόμενο βήμα είναι να ελέγξει αν το όνομα domain στο πιστοποιητικό του διακομιστή ταιριάζει στο όνομα domain του διακομιστή. Αυτό γίνεται για να διαπιστωθεί αν μπορεί να συμβαίνει μια επίθεση man-in-the-

middle. Αφού γίνει και αυτό το βήμα, μπορεί πλέον να γίνει και η πιστοποίηση του πελάτη.

Το SSL δίνει προστασία ενάντια σε αυτή την επίθεση κάνοντας χρήση ψηφιακών πιστοποιητικών για να επιτρέψει στον web χρήστη να μάθει το επικυρωμένο (validated) όνομα του web site. Δυστυχώς, ο Netscape Navigator κρύβει αυτή την πληροφορία, κάνοντας την προσιτή μόνο στους χρήστες που επιλέγουν την εντολή View Document Info.

Σε μια replay επίθεση, ο επιτιθέμενος αντιγράφει (capture) τις επικοινωνίες ανάμεσα στα δύο μέρη και επαναλαμβάνει τα μηνύματα. Για παράδειγμα, ένας επιτιθέμενος ίσως αντιγράψει ένα μήνυμα ανάμεσα σε ένα χρήστη και ένα οικονομικό ίδρυμα (π.χ. μια τράπεζα) έχοντας πληροφορηθεί ότι η ηλεκτρονική πληρωμή ίσως να γίνει. Επαναλαμβάνοντας αυτό το μήνυμα, μπορεί να προκαλέσει πολλές άλλες ηλεκτρονικές πληρωμές.

3.3.6. **Υποστήριξη για συμπίεση:** Το SSL εξασφαλίζει για το μέλλον την δυνατότητα να συμπιέζει τα δεδομένα του χρήστη πριν αυτά κρυπτογραφηθούν. Υποστηρίζει πολλούς αλγορίθμους συμπίεσης. Παρόλα αυτά δεν υπάρχει σήμερα κάποια SSL εφαρμογή που να ενσωματώνει την συμπίεση.

3.3.7. **Συμβατότητα με το πρωτόκολλο SSL 2.0:** Οι SSL v3 servers μπορούν να δέχονται συνδέσεις από SSL v2 clients και να χειρίζονται το μήνυμα αυτόματα χωρίς να υπάρχει ανάγκη να συνδεθεί ξανά ο client.

3.4. Ψηφιακά Πιστοποιητικά

Η ανάγκη προστασίας δεδομένων καθώς και η ασφαλής ηλεκτρονική επικοινωνία που επιτάσσουν οι αυξανόμενες ηλεκτρονικές συναλλαγές στο διαδίκτυο, οδήγησαν στην δημιουργία υποδομής και χρήση των ψηφιακών πιστοποιητικών. Πρόκειται για μια ραγδαία εξελισσόμενη τεχνολογική περιοχή που επηρεάζει άμεσα τους χρήστες του διαδικτύου.

Το SSL κάνει εκτεταμένη χρήση των πιστοποιητικών δημόσιου κλειδιού για την απόδειξη γνησιότητας τόσο του client όσο και του server στις SSL συναλλαγές. Το SSL κάνει χρήση των X.509 v3 πιστοποιητικών για τον έλεγχο των RSA ζεύγος κλειδιών, και ένα τροποποιημένο X.509 πιστοποιητικό για τον έλεγχο δημοσίων κλειδιών από το U.S. Department of Defense Forteza /DMS πρωτόκολλο ανταλλαγής κλειδιών.

Το SSL υποστηρίζει τα εξής είδη πιστοποιητικών:

- RSA πιστοποιητικά δημόσιου κλειδιού με δημόσια κλειδιά αυθαίρετου μήκους.
- RSA πιστοποιητικά δημόσιου κλειδιού που περιορίζονται στα 512 bits, για χρήση στα κρυπτογραφικά λογισμικά που πρόκειται να εξαχθούν.
- RSA πιστοποιητικά μόνο για υπογραφή, τα οποία περιέχουν RSA δημόσια κλειδιά που χρησιμοποιούνται μόνο για υπογραφή δεδομένων και όχι για κρυπτογράφηση.
- DSS πιστοποιητικά.
- Diffie - Hellman πιστοποιητικά.

Η χρήση των πιστοποιητικών είναι προαιρετική. Το SSL απαιτεί πιστοποιητικά server εκτός αν οι SSL εφαρμογές και του client και του server χρησιμοποιούν το Diffie Hellman πρωτόκολλο ανταλλαγής κλειδιών. Σήμερα., τα προϊόντα της Netscape δεν εφαρμόζουν τους αλγορίθμους Diffie - Hellman.

3.5. SSL Εφαρμογές

Το SSL σχεδιάστηκε τον Ιούλιο του 1994 και ήταν ένα από τα επιχειρηματικά πλάνα της Netscape. Η Netscape σχεδιάστηκε για να δημιουργήσει έναν browser που θα επέτρεπε στον χρήστη να εκτελεί κρυπτογραφημένες επικοινωνίες με τους servers της Netscape χρησιμοποιώντας ένα πρωτόκολλο δικής της ιδιοκτησίας.

3.5.1. **SSL Netscape:** Η πρώτη εφαρμογή του SSL ήταν στους browsers και servers της Netscape, που ποτέ δεν πουλήθηκαν ξεχωριστά.

3.5.2. **SSLRef:** Μετά τον σχηματισμό του Netscape Navigator, η Netscape δημιούργησε μια αναφορά SSL εφαρμογή η οποία διανεμόταν μέσα στις Ηνωμένες Πολιτείες. Αυτό το πρόγραμμα ονομάζεται SSLRef και είναι γραμμένο σε C. Η 2.0 αναφορά του δημοσιεύτηκε τον Απρίλιο του 1995.

Η SSLRef δεν χρησιμοποιεί κανένα από τους RC2 και RCA αλγόριθμους. Δυστυχώς, πολλά προγράμματα που χρησιμοποιούν το SSL, περιέχουν μόνο τους RC2 και RCA αλγόριθμους. Συνεπώς, για να συνδυάσεις ένα πρόγραμμα βασισμένο στην SSLRef με ένα πρόγραμμα όπως η Netscape Navigator, είναι απαραίτητο να υπάρχουν άδειες ξεχωριστά για τον RC2 και RCA αλγόριθμους από την RSA Data Security.

Η SSLRef εφαρμογή εφαρμόζει επίσης την χρήση του RSA κρυπτογραφικού αλγορίθμου, ο οποίος πρέπει να έχει άμεσα ή έμμεσα άδεια χρήσης από την RSA Data Security μέσα στις Ηνωμένες Πολιτείες.

3.5.3. **SSLeay:** Είναι μια ανεξάρτητη εφαρμογή του SSL 3.0, αναπτύχθηκε από τον Eric Young, ένα προγραμματιστή από την Αυστραλία. Είναι ελεύθερα διαθέσιμη σε όλο τον κόσμο μέσα από έναν μεγάλο αριθμό anonymous FTP sites. Χρησιμοποιεί εφαρμογές των RC2 και RCA κρυπτογραφικών αλγορίθμων βασισμένες σε αλγορίθμους που δημοσιεύτηκαν ανώνυμα στο Usenet sci.crypt news-group το Σεπτέμβριο του 1994 (RC4) και τον Φεβρουάριο του 1996 (RC2).

Εκτός από τους RC2 και RCA κρυπτογραφικούς αλγορίθμους, το SSLeay περιλαμβάνει τους IDEA, DES, και Triple Des. Ο Eric Young θεωρεί ότι ο Triple Des είναι ευρέως αποδεκτός για την ασφάλειά του καθώς έχει μελετηθεί για περισσότερα από 20 χρόνια. Ισχυρίζεται ότι μπορεί να κρυπτογραφεί με ρυθμούς 410k/sec σε ένα Pentium 100, και 940k/sec σε ένα P6/200, που είναι μια λογική μετάδοση. Ο απλός DES μετριέται στα 1160k/sec και 2467k/sec αντίστοιχα και είναι αρκετά γρήγορος (56-bit κλειδί).

3.5.4. **SSL Java:** Υπάρχουν και εφαρμογές του SSL στην Java. Μερικές από αυτές είναι:

- Η J/SSL από την Baltimore Technologies είναι μια εφαρμογή κρυπτογραφίας στην Java.
- Η Phaos έχει αναπτύξει δύο εφαρμογές, την SSLava Toolkit και την JSAFE.

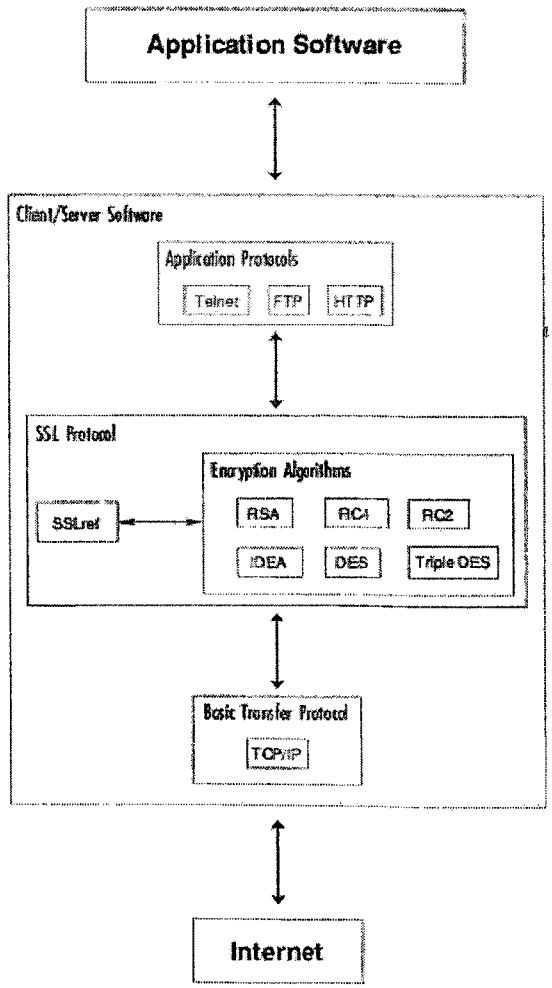
3.6. Επίδοση εκτέλεσης

Το SSL μειώνει την ταχύτητα μετάδοσης της πληροφορίας μέσω του Internet. Η επίδοση της επιβράδυνσης είναι αποτέλεσμα της κρυπτογράφησης και αποκρυπτογράφησης δημόσιου κλειδιού που απαιτείται για να αρχικοποιηθεί η πρώτη SSL σύνδεση. Σε σύγκριση με αυτό, οι επιπλέον κρυπτογραφήσεις και αποκρυπτογραφήσεις δεδομένων με τους RC2, RC4 ή DES είναι πρακτικά ασήμαντες.

Μερικοί χρήστες αναφέρουν ότι η επιβράδυνση φτάνει το 50%, συγκρινόμενη με την αποστολή πληροφορίας χωρίς την χρήση SSL. Χρήστες της SPARC Station 10s έχουν αναφέρει ότι η κρυπτογράφηση και αποκρυπτογράφηση δημόσιου κλειδιού απαιτεί περίπου τρία CPU δευτερόλεπτα ανά χρήστη με ένα κλειδί 124-bit.

Αυτό σημαίνει πως θα υπάρχει μια παύση τριών δευτερολέπτων ανάμεσα στο άνοιγμα μιας σύνδεσης σε έναν SSL server και στην απόκτηση μια HTML σελίδας από τον server. Επειδή το SSL μπορεί να αποθηκεύει κρυφά ένα μυστικό "master secret", αυτή η καθυστέρηση επιδρά μόνο στην πρώτη SSL συναλλαγή μεταξύ του client και του server.

Στην εικόνα 3.2 φαίνεται το λογισμικό του SSL Πρωτόκολλου:



Εικόνα 3.2

Αν έχουμε ένα γρήγορο υπολογιστή και μια αργή σύνδεση στο δίκτυο το επιπλέον του SSL μπορεί να είναι ασήμαντο, ειδικά αν στέλνουμε μεγάλες ποσότητες

πληροφοριών πάνω από μια απλή SSL σύνοδο ή πάνω από πολλαπλές SSL συνόδους που χρησιμοποιούν ένα κοινό "master secret".

Από την άλλη πλευρά, αν απαιτούμε να σερβίρουμε μεγάλο μέγεθος SSL HTTP αιτήσεων μέσα σε ένα λεπτό, πρέπει να προβούμε στην αγορά ενός γρήγορου υπολογιστή ή να λάβουμε βοήθεια από το Hardware, για τις λειτουργίες του δημόσιου κλειδιού. Πολλοί οργανισμοί για να μειώσουν την επίδραση του SSL, μεταδίδουν καθαρά τον όγκο των πληροφοριών και χρησιμοποιούν το SSL για κρυπτογράφηση ευαίσθητων δεδομένων. Αυτό δεν είναι καθόλου ασφαλές για τον χρήστη, διότι απειλείται από μια επίθεση λόγω του ότι τα μη κρυπτογραφημένα αρχεία μπορούν να τροποποιηθούν κατά την μετάδοσή τους, καθώς αυτά στέλνονται από τον client στον server, με ένα εξεζητημένο πρόγραμμα φιλτράρισμα πακέτων και εισαγωγή νέων στοιχείων.

Για παράδειγμα, θα μπορούσε να αλλαχθεί το action tag σε μια HTML form, έτσι ώστε αντί να τοποθετείται ο αριθμός μιας πιστωτικής κάρτας στο κατάλληλο σύστημα επεξεργασίας, να τοποθετείται σε έναν πειρατικό υπολογιστή στην Αμερική. Αν υποθέσουμε πως ο χειριστής του πειρατικού συστήματος μπορεί να πάρει ένα ψηφιακά υπογεγραμμένο ID (singed digital ID) από τον δικό του SSL server, τότε είναι πολύ δύσκολο για ένα χρήστη που εξαπατήθηκε με αυτή την τεχνική να ανακαλύψει ότι ήταν θύμα μιας επίθεσης.

3.7. TLS

Το 1995, το IETF έκανε την πρώτη σκέψη για την υιοθεσία του SSL σαν μέρος ενός νέου προτύπου το TLS. Ένα μέρος του πρωτοκόλλου δημοσιεύτηκε στις 6 Μαρτίου του 1997.

Το TLS είναι πολύ παρόμοιο με το SSL 3.0, με λίγες αλλαγές. Αντί της χρήσης του MD5, το TLS χρησιμοποιεί την HMAC ασφαλή συνάρτηση αποσύνθεσης κλειδιών. Επίσης, έχει λίγο διαφορετικό τρόπο κρυπτογράφησης σε σχέση με το SSL 3.0.

3.8. SSL: Από την πλευρά του χρήστη

Ο Netscape Navigator αλλά και ο Microsoft Internet Explorer περιέχουν εκτεταμένη υποστήριξη για το SSL.

Ο Netscape Navigator χρησιμοποιεί το όρο "secure document" σαν μια συντομογραφία για την φράση "documents that are transmitted using SSL".

Φυσικά, τα έγγραφα που μεταφέρονται χρησιμοποιώντας SSL δεν είναι περισσότερο ασφαλή ή ανασφαλή από ότι τα έγγραφα που στέλνονται μη κρυπτογραφημένα. Απλώς είναι κρυπτογραφικά προστατευμένα ενάντια στο κρυφάκουσμα και στην τροποποίηση του περιεχομένου τους κατά την διάρκεια μεταφοράς τους.

3.9. Επιλέγοντας λειτουργίες στους Browsers (Browser Preferences)

Ο Netscape Navigator και ο Internet Explorer ελέγχουν την SSL συμπεριφορά μέσω της χρήσης διαφόρων πινάκων ελέγχου (panels).

3.9.1. **Netscape Navigator Browser:** Ο νέος Netscape έχει λειτουργίες anti-spyware. Πρόσφατα η Netscape ανακοίνωσε την κυκλοφορία της έκδοσης 8.1 του browser της, στην οποία έχουν ενσωματωθεί νέες λειτουργίες για την ακόμη καλύτερη προστασία των χρηστών από spyware και phishing. Τα εργαλεία αυτά, θα εξετάζουν τα αρχεία που κατεβάζει ο χρήστης καθώς και εκείνα που στέλνονται σε αυτόν χωρίς να τα ζητήσει. Ακόμη, θα

επιτρέπει στους χρήστες να πραγματοποιούν και ολοκληρωμένους ελέγχους της μνήμης και του δίσκου του υπολογιστή.

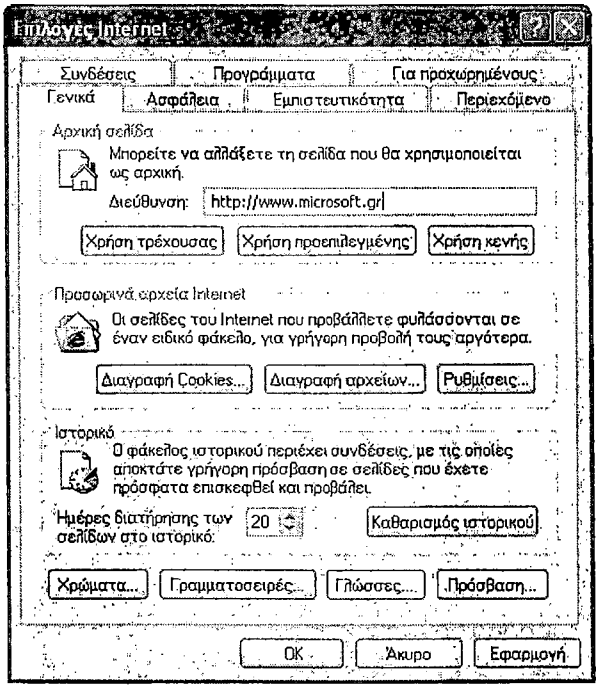
Άλλες λειτουργίες ασφαλείας περιλαμβάνουν μια ενημερωμένη μαύρη λίστα με sites που πιθανώς εξασκούν την πρακτική του phishing και ένα security center, στο οποίο θα μπορούν οι χρήστες να ανατρέχουν, όποτε πιστεύουν ότι πρέπει να λάβουν μέτρα για την ασφάλειά τους. Η κίνηση της Netscape να ενισχύσει αυτές ακριβώς τις δυνατότητες του browser της, είναι αποτέλεσμα της τάσης που θέλει τα κακόβουλα προγράμματα να εκμεταλλεύονται τις αδυναμίες των browsers, μη εξαιρουμένου και του Netscape.

Ο χρήστης με την επιλογή του Navigator μπορεί να επιλέξει πότε θέλει να έχει προειδοποιήσεις ασφαλείας, έτσι το πρόγραμμα ειδοποιεί τον χρήστη με τους τρόπους που αναφέρονται παρακάτω:

- Όταν ένα μη κρυπτογραφημένο έγγραφο εμφανιστεί στην οθόνη και ένα κρυπτογραφημένο έγγραφο ζητηθεί.
- Όταν ένα κρυπτογραφημένο έγγραφο εμφανιστεί στην οθόνη και ένα μη κρυπτογραφημένο έγγραφο ζητηθεί.
- Όταν ένα έγγραφο εμφανιστεί στην οθόνη και συνδυάζει κρυπτογραφημένα ή μη κρυπτογραφημένα δεδομένα.
- Όταν μια CGI φόρμα εκτελεστεί χωρίς κρυπτογράφηση, χρησιμοποιώντας τα (GET και POST).

3.9.2. Internet Explorer Browser:

Στην εικόνα 3.3 φαίνεται ο πίνακας ελέγχου του Internet Explorer 6.0:



Εικόνα 3.3

Οι επιλογές του Explorer μοιάζουν με του Navigator. Παρακάτω αναλύονται οι επιλογές που αναφέρονται στο SSL:

- Ο χρήστης πρέπει να προειδοποιείται πριν μια CGI φόρμα εκτελεστεί χωρίς κρυπτογράφηση. Μπορούμε να ρυθμίσουμε τον Explorer έτσι ώστε να μας προειδοποιεί μόνο όταν στέλνουμε περισσότερες από μια γραμμή κειμένου χωρίς κρυπτογράφηση.
- Ο χρήστης πρέπει να προειδοποιείται όταν γίνεται εναλλαγή ανάμεσα στη λήψη κρυπτογραφημένων και μη κρυπτογραφημένων εγγράφων.
- Ο χρήστης πρέπει να προειδοποιείται για τους servers που απονέμουν άκυρα πιστοποιητικά (invalid site certificates).

ΚΕΦΑΛΑΙΟ ΤΕΤΑΡΤΟ

ΤΑΥΤΟΠΟΙΗΣΗ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΗ ΤΟΥ ΧΡΗΣΤΗ

Για τα περισσότερα υπολογιστικά και δικτυακά συστήματα, οι διαδικασίες ταυτοποίησης και πιστοποίησης των χρηστών είναι η πρώτη γραμμή άμυνας για την ασφάλεια του συστήματος. Οι διαδικασίες ταυτοποίησης και πιστοποίησης των χρηστών έχουν σκοπό να εμποδίσουν την πρόσβαση μη εξουσιοδοτημένων χρηστών στο υπολογιστικό ή δικτυακό σύστημα.

Οι διαδικασίες ταυτοποίησης και πιστοποίησης είναι ένα κρίσιμο στοιχείο της ασφάλειας ενός δικτύου δεδομένων. Σε αυτές βασίζονται οι τεχνικές για έλεγχο πρόσβασης και σύνδεση της δραστηριότητας του συστήματος με συγκεκριμένους χρήστες που την προκάλεσαν. Ο όρος ταυτοποίηση περιγράφει τη διαδικασία κατά την οποία ο χρήστης δηλώνει την ταυτότητά του στο σύστημα. Ο όρος πιστοποίηση περιγράφει τη διαδικασία με την οποία ο χρήστης επιβεβαιώνει τον ισχυρισμό για την ταυτότητα του.

4.1. Συστήματα ταυτοποίησης και πιστοποίησης χρήστη

Υπάρχουν τρεις κατηγορίες συστημάτων για να πιστοποιηθεί η ταυτότητα ενός χρήστη, τα οποία μπορούν να χρησιμοποιηθούν είτε αυτόματα είτε σε συνδυασμό:

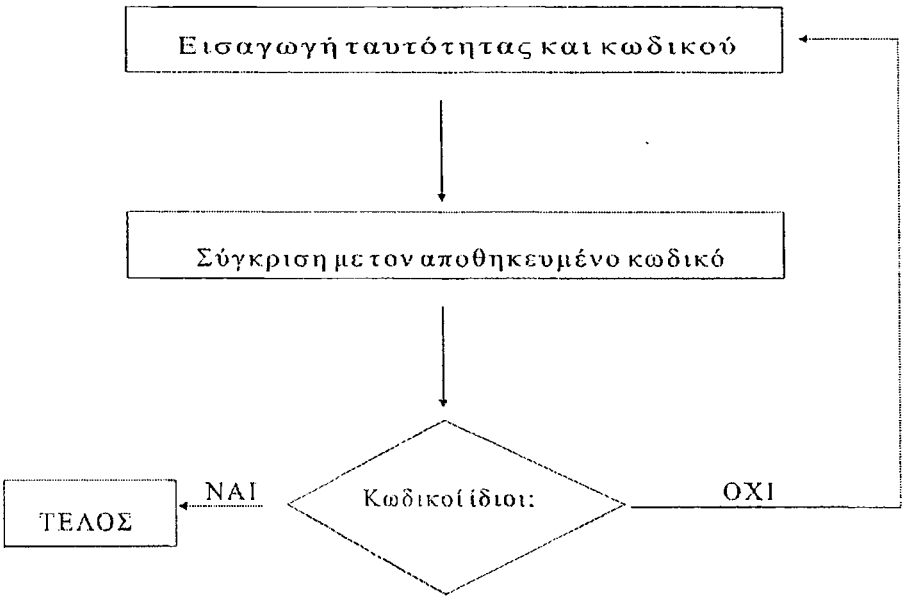
- **Συστήματα που βασίζονται σε πληροφορία / γνώση που παρέχει ο χρήστης,** όπως είναι ένας κωδικός πρόσβασης (password), ένας προσωπικός κωδικός πιστοποίησης (PIN), και ένα κρυπτογραφικό κλειδί.
- **Συστήματα που βασίζονται σε κάποιο αντικείμενο που κατέχει ο χρήστης,** όπως είναι η ATM κάρτα, και η έξυπνη κάρτα (smart card).
- **Συστήματα που βασίζονται σε κάποιο προσωπικό χαρακτηριστικό του χρήστη.** Σε αυτή την κατηγορία ανήκουν οι μέθοδοι που βασίζονται στην βιομετρία, όπως ο έλεγχος φωνής, του γραφικού χαρακτήρα, και των δακτυλικών αποτυπωμάτων.

4.1.1. **Συστήματα που βασίζονται στην πληροφορία:** Είναι ο συνδυασμός ενός κωδικού ονόματος χρήστη (login name) με μια πληροφορία που κατέχει ο χρήστης. Σε αυτή την κατεύθυνση, η σημαντικότερη κατηγορία είναι οι μηχανισμοί που βασίζονται στους συμβατικούς κωδικούς πρόσβασης (passwords).

Κωδικοί πρόσβασης (passwords): Τα συστήματα ταυτοποίησης και πιστοποίησης απαιτούν από το χρήστη την εισαγωγή ενός κωδικού ονόματος και ενός κωδικού πρόσβασης. Το σύστημα συγκρίνει τον κωδικό πρόσβασης με έναν αποθηκευμένο κωδικό πρόσβασης που έχει συνδυαστεί με το συγκεκριμένο κωδικό όνομα. Αν οι δύο κωδικοί πρόσβασης ταυτίζονται, η ταυτότητα του χρήστη πιστοποιείται επιτυχώς, και ο χρήστης αποκτά πρόσβαση στον λογαριασμό του.

Μηχανισμοί πιστοποίησης ταυτότητας βασισμένοι σε κωδικούς πρόσβασης χρησιμοποιούνται για την ασφάλεια υπολογιστικών συστημάτων. Τέτοιοι μηχανισμοί έχουν ενσωματωθεί σε πολλά λειτουργικά συστήματα, και τόσο οι χρήστες όσο και οι διαχειριστές συστημάτων είναι εξοικειωμένοι με αυτά. Οι μηχανισμοί που βασίζονται σε κωδικούς πρόσβασης μπορούν να παρέχουν ικανοποιητικό επίπεδο ασφαλείας, υπό την προϋπόθεση ότι διαχειρίζονται σωστά και φυλάσσονται επαρκώς.

Στην εικόνα 4.1 Φαίνεται η διαδικασία ταυτοποίησης και πιστοποίησης με βάση τον κωδικό πρόσβασης:



Εικόνα 4.1

Η ασφάλεια ενός συστήματος που βασίζεται σε κωδικούς πρόσβασης εξαρτάται από το βαθμό που οι κωδικοί αυτοί παραμένουν μυστικοί. Παρόλα αυτά, υπάρχουν αρκετοί τρόποι να αποκαλυφθούν, όπως:

- **Κωδικοί πρόσβασης που είναι εύκολο να μαντευθούν:** Συνήθως οι χρήστες διαλέγουν κωδικούς που μπορούν να τους θυμούνται εύκολα, όπως ονόματα ατόμων, ομάδων. Ένας εισβολέας μπορεί εύκολα να μαντέψει έναν τέτοιου είδους κωδικό. Από την άλλη, αν οι χρήστες δυσκολεύονται να απομνημονεύσουν τους κωδικούς πρόσβασης, τότε τους κρατούν γραμμένους σε κάποιο σημείο. Πολλά υπολογιστικά συστήματα έχουν προκαθορισμένους κωδικούς για τους λογαριασμούς που χρησιμοποιούνται για την διαχείριση του συστήματος. Επειδή αυτοί οι κωδικοί πρόσβασης είναι τυποποιημένοι, μπορούν να μαντευθούν εύκολα. Αν και αυτό το πρόβλημα έχει επισημανθεί εδώ και πολλά χρόνια, πολλοί διαχειριστές δεν έχουν αλλάξει αυτούς τους κωδικούς πρόσβασης. Ένας άλλος τρόπος να αποκαλυφθεί ένας κωδικός πρόσβασης είναι η παρακολούθηση του χρήστη την στιγμή που τον εισάγει.
- **Αποκάλυψη των κωδικών πρόσβασης:** Πολλοί χρήστες συνηθίζουν να μοιράζονται τους κωδικούς πρόσβασης μεταξύ τους. Για παράδειγμα,

πολλοί συνάδελφοι γνωρίζουν ο ένας τον κωδικό πρόσβασης του άλλου για να μπορούν να μοιράζονται αρχεία.

- **Ηλεκτρονική Παρακολούθηση:** Όταν οι κωδικοί πρόσβασης μεταδίδονται στο υπολογιστικό σύστημα, μπορούν να υποκλαπούν μέσω ηλεκτρονικής παρακολούθησης του διαύλου μετάδοσης. Η παρακολούθηση μπορεί να γίνει είτε στο ίδιο πληροφοριακό σύστημα (εγκατάσταση Trojan horse), είτε στο δικτυακό υποσύστημα που χρησιμοποιείται για τη μετάδοση. Αξίζει να σημειωθεί ότι αυτό το πρόβλημα δεν μπορεί να λυθεί με απλή κρυπτογράφηση, γιατί κάθε φορά η κρυπτογράφηση του ίδιου κωδικού πρόσβασης δίνει το ίδιο αποτέλεσμα, οπότε ο κρυπτογραφημένος κωδικός πρόσβασης μπορεί να χρησιμοποιηθεί από κάποιον εισβολέα.
- **Πρόσβαση στο αρχείο με τους κωδικούς πρόσβασης:** Στην περίπτωση που το αρχείο με τους κωδικούς πρόσβασης των εξουσιοδοτημένων χρηστών δεν προστατεύεται, αυτό μπορεί να κλαπεί και να μεταφερθεί μέσω δικτύου σε άλλο, απομακρυσμένο υπολογιστικό σύστημα. Τα αρχεία με τους κωδικούς πρόσβασης σχεδόν πάντοτε προστατεύονται με τεχνικές μονόδρομης κρυπτογράφησης, ώστε οι κωδικοί πρόσβασης να μην είναι διαθέσιμοι στον διαχειριστή του συστήματος ή στους εισβολείς, ακόμα και αν αποκτήσουν πρόσβαση στο συγκεκριμένο αρχείο. Παρόλα αυτά, αφού το αρχείο με τους κωδικούς πρόσβασης μεταφερθεί σε κάποιο άλλο υπολογιστικό σύστημα, οι κρυπτογραφήσεις πολλών συμβολοσειρών μπορούν να συγκριθούν με τα περιεχόμενα του αρχείου, ώστε να ανακαλυφθούν οι κωδικοί πρόσβασης.

4.1.2. **Συστήματα που βασίζονται στην κατοχή:** Τα περισσότερα συστήματα αυτής της κατηγορίας συνδυάζουν ένα αντικείμενο που ο χρήστης έχει στην κατοχή του (ATM κάρτα, «έξυπνη κάρτα») με πληροφορία που ο χρήστης γνωρίζει, ώστε να επιτύχουν μεγαλύτερη ασφάλεια από τα συστήματα της προηγούμενης κατηγορίας. Συνήθως, το αντικείμενο που ο χρήστης έχει στην κατοχή του καλείται κουπόνι ή κάρτα, και τα συστήματα διακρίνονται σε αυτά που χρησιμοποιούν κάρτες μνήμης (memory tokens) και έξυπνες κάρτες (smart tokens).

Κάρτες μνήμης (memory tokens): Οι κάρτες μνήμης αποθηκεύουν, αλλά και επεξεργάζονται πληροφορία. Η πιο συνηθισμένη μορφή καρτών μνήμης είναι οι μαγνητικές κάρτες, στις οποίες μια στενή λωρίδα μαγνητικού υλικού προσαρμόζεται στην επιφάνεια της κάρτας. Στο μαγνητικό υλικό καταγράφονται κάποιες πληροφορίες, οι οποίες αποτελούν τμήμα των δεδομένων πιστοποίησης. Η πιο συνηθισμένη χρήση αυτής της τεχνικής είναι στις Αυτόματες Ταμειακές Μηχανές, στις οποίες η μαγνητική κάρτα συνδυάζεται με τον προσωπικό κωδικό ταυτοποίησης.

Είναι φανερό ότι οι διαδικασίες πιστοποίησης που βασίζονται στον συνδυασμό μιας κάρτας μνήμης με ένα PIN παρέχουν υψηλότερα επίπεδα ασφαλείας από τις διαδικασίες πιστοποίησης που βασίζονται μόνο σε κωδικούς πρόσβασης. Ένας εισβολέας για να προσποιηθεί ότι είναι κάποιος εξουσιοδοτημένος χρήστης πρέπει να έχει στην κατοχή του τόσο μια έγκυρη κάρτα όσο και το έγκυρο PIN για αυτή την κάρτα. Προφανώς,

αυτό είναι αρκετά πιο δύσκολο από την υποκλοπή ενός κωδικού πρόσβασης, αφού τα ονόματα των χρηστών είναι διαθέσιμα σε όλους.

Παρόλα αυτά πιο σύνθετες τεχνικά επιθέσεις είναι πιθανές εναντίον ενός συστήματος που βασίζεται σε κάρτες μνήμης και PINs. Για παράδειγμα, μια ομάδα έκλεψε ένα ATM και το εγκατέστησε σε ένα εμπορικό κατάστημα. Με αυτό τον τρόπο απέκτησαν πρόσβαση σε έγκυρους αριθμούς λογαριασμών και στα αντίστοιχα PINs, κατασκεύασαν ψεύτικες κάρτες, και τις χρησιμοποίησαν για την ανάληψη χρημάτων από κανονικά ATM.

Επίσης, άλλα προβλήματα στη χρήση τέτοιων τεχνικών αφορούν στο κόστος, τη διαχείριση, την απώλεια των καρτών, τη δυσαρέσκεια των χρηστών και την παραχώρηση των PINs. Συγκεκριμένα, το κόστος αυξάνεται σημαντικά από τις ειδικές συσκευές οι οποίες διαβάζουν τις μαγνητικές κάρτες, επιτρέπουν την εισαγωγή των PINs, και αποφασίζουν αν τα δεδομένα είναι έγκυρα, ώστε ο χρήστης να αποκτήσει πρόσβαση. Η απώλεια της μαγνητικής κάρτας εμποδίζει την πρόσβαση του χρήστη, μέχρι αυτή να αντικατασταθεί. Αυτό δημιουργεί επιπλέον διαχειριστικό κόστος, αλλά αυξάνει τις πιθανότητες η ασφάλεια του συστήματος να παραβιαστεί από αυτόν που θα βρει το κουπόνι. Επίσης, οι χρήστες πολλές φορές δεν καταλαβαίνουν την ανάγκη χρήσης καρτών για την πιστοποίηση ταυτότητας σε ένα υπολογιστικό σύστημα. Το φαινόμενο αυτό μπορεί να αντιμετωπιστεί με ενημέρωση των χρηστών για την αναγκαιότητα αυξημένων μέτρων για την ασφάλεια του συστήματος.

Έξυπνες κάρτες (smart tokens): Μια έξυπνη κάρτα επεκτείνει την λειτουργικότητα μιας κάρτας μνήμης ενσωματώνοντας ένα ή περισσότερα ολοκληρωμένα κυκλώματα στην ίδια την κάρτα. Όταν χρησιμοποιείται για πιστοποίηση ταυτότητας, μια έξυπνη κάρτα συνήθως συνδυάζεται με ένα PIN. Υπάρχουν πολλοί τύποι έξυπνων καρτών, οι οποίοι διακρίνονται κυρίως με βάση τα φυσικά χαρακτηριστικά, το περιβάλλον αλληλεπίδρασης και τα πρωτόκολλα που χρησιμοποιούνται.

Όσον αφορά στα φυσικά χαρακτηριστικά, οι έξυπνες κάρτες έχουν ενσωματωμένο ένα μικροεπεξεργαστή, ενώ τα χαρακτηριστικά μιας κατηγορίας ορίζονται σε διεθνή τυποποίηση που έχει επεξεργαστεί από τον ISO.

Οι έξυπνες κάρτες έχουν είτε χειροκίνητο, είτε ηλεκτρονικό περιβάλλον αλληλεπίδρασης. Στην πρώτη περίπτωση, η κάρτα έχει μικρή οθόνη ή και πληκτρολόγιο που επιτρέπει στο χρήστη να αλληλεπιδρά με την κάρτα. Οι έξυπνες κάρτες με ηλεκτρονικό περιβάλλον αλληλεπίδρασης προσπελαύνονται (ανάγνωση, ενημέρωση, εγγραφή) μέσω ειδικών συσκευών.

Υπάρχουν πολλοί τύποι πρωτοκόλλων που μπορούν να χρησιμοποιηθούν για πιστοποίηση με χρήση έξυπνης κάρτας. Διακρίνονται τρεις μεγάλες, γενικές κατηγορίες πρωτοκόλλων, τα πρωτόκολλα στατικής ανταλλαγής κωδικών πρόσβασης, τα πρωτόκολλα δυναμικής δημιουργίας κωδικών πρόσβασης, και τα πρωτόκολλα ερώτησης - απόκρισης.

Τα σημαντικότερα πλεονεκτήματα των έξυπνων καρτών είναι ότι είναι ευέλικτες και μπορούν να δώσουν λύση σε πολλά προβλήματα που

σχετίζονται με την ασφάλεια των διαδικασιών πιστοποίησης. Παρέχουν μεγαλύτερη ασφάλεια από τις μαγνητικές κάρτες και δίνουν μια απάντηση στο πρόβλημα της ηλεκτρονικής παρακολούθησης, με τη μέθοδο των κωδικών πρόσβασης μιας χρήσης. Συγκεκριμένα, οι έξυπνες κάρτες που χρησιμοποιούν πρωτόκολλα δυναμικής δημιουργίας κωδικών πρόσβασης ή ερώτησης - απόκρισης δημιουργούν κωδικούς πρόσβασης μιας χρήσης, δηλαδή κωδικούς πρόσβασης που είναι έγκυροι μόνο για τη συγκεκριμένη χρονική στιγμή. Προφανώς, η αποκάλυψη μέσω ηλεκτρονικής παρακολούθησης ενός κωδικού πρόσβασης μιας χρήσης δεν έχει νόημα, γιατί αυτός δεν μπορεί να χρησιμοποιηθεί πάλι.

Επίσης, οι έξυπνες κάρτες μειώνουν τον κίνδυνο της κατασκευής πλαστών αντιγράφων, γιατί πρόκειται για σύνθετες κατασκευές, και η μνήμη μιας έξυπνης κάρτας δεν μπορεί να διαβαστεί, αν ο χρήστης δεν πιστοποιήσει την ταυτότητα του. Επιπλέον, επιτρέπουν στους χρήστες να έχουν πρόσβαση στο σύνολο των υπολογιστικών συστημάτων ενός οργανισμού, πιστοποιώντας την ταυτότητα τους μόνο μια φορά στην αρχή κάθε συνόδου. Εκτός από τις έξυπνες κάρτες, παρόμοια δυνατότητα παρέχεται και από εφαρμογές που λειτουργούν σαν εξυπηρετητές πιστοποίησης για το σύνολο των υπολογιστικών συστημάτων ενός οργανισμού, όπως το Kerberos και το SPX.

Για παράδειγμα, το σύστημα Kerberos είναι ένα σύστημα πιστοποίησης ταυτότητας χρηστών ειδικά σχεδιασμένο για περιβάλλοντα δικτύων υπολογιστών, τα οποία δεν είναι φυσικά ασφαλή, με την έννοια ότι οι επίδοξοι εισβολείς μπορούν να παρακολουθούν τα δεδομένα που διακρίνονται σε αυτά. Το μοντέλο που χρησιμοποιείται στο σύστημα Kerberos βασίζεται στο μοντέλο διανομής κλειδιών, που παρουσιάστηκε από τους Needham και Schroeder. Το μοντέλο αυτό επιτρέπει σε οντότητες να επικοινωνούν και να πιστοποιούν την ταυτότητα τους πάνω από δίκτυα δεδομένων, εξαλείφοντας τους κινδύνους από υποκλοπή των δεδομένων πιστοποίησης με χρήση κωδικών πρόσβασης μιας χρήσης ή συστημάτων ερώτησης - απόκρισης. Επίσης, ο Kerberos παρέχει δυνατότητες επιβεβαίωσης ακεραιότητας των δεδομένων, και μυστικότητα με χρήση κρυπτογραφικών τεχνικών, όπως το DES.

Τα βασικότερα μειονεκτήματα έχουν να κάνουν με το κόστος χρήσης και συντήρησης, και τη δυσαρέσκεια των χρηστών. Οι έξυπνες κάρτες είναι λιγότερο τρωτές στην υποκλοπή του PIN, επειδή απαιτείται από τον χρήστη να πιστοποιήσει την ταυτότητα του στην ίδια την κάρτα. Από την άλλη πλευρά, οι έξυπνες κάρτες κοστίζουν περισσότερο από τις κάρτες μνήμης, και είναι πιο σύνθετες στο σχεδιασμό τους και στη λειτουργία τους.

Ένα από τα βασικά προβλήματα στη χρήση των έξυπνων καρτών είναι ότι αυτές που έχουν ηλεκτρονικό περιβάλλον αλληλεπίδρασης απαιτούν τη χρήση ειδικών συσκευών για ανάγνωση / εγγραφή της κάρτας, ενώ αυτές που έχουν χειροκίνητο περιβάλλον αλληλεπίδρασης απαιτούν κάποιες επιπλέον ενέργειες από την πλευρά του χρήστη. Η πρώτη περίπτωση αυξάνει σημαντικά το κόστος εγκατάστασης και συντήρησης του συστήματος, ενώ η δεύτερη αυξάνει τη δυσαρέσκεια των χρηστών, που απαιτούν από τα υπολογιστικά συστήματα να είναι φιλικά προς το χρήστη.

Επίσης, η χρήση ενός συστήματος πιστοποίησης ταυτότητας που βασίζεται σε έξυπνες κάρτες έχει σημαντικές απαιτήσεις σε διαχείριση, ενώ στην περίπτωση ταυτόχρονης χρήσης κρυπτογραφικών κλειδιών απαιτείται επιπλέον σύστημα διαχείρισης για αυτά.

4.1.3. **Συστήματα που βασίζονται στην βιομετρία:** Οι διαδικασίες που βασίζονται στη βιομετρία χρησιμοποιούν κάποια ατομικά χαρακτηριστικά για να πιστοποιήσουν την ταυτότητα του χρήστη. Συνήθως χρησιμοποιούνται χαρακτηριστικά όπως τα δακτυλικά αποτυπώματα, τα χαρακτηριστικά του ματιού, η χροιά της φωνής και ο γραφικός χαρακτήρας.

Η αρχή λειτουργίας των συστημάτων βιομετρίας μπορεί να αναλυθεί σε δύο βήματα. Στη φάση αρχικοποίησης του συστήματος, δημιουργείται ένα προφίλ που περιγράφει τη μορφή του επιλεγμένου χαρακτηριστικού για κάθε χρήστη. Αυτό το προφίλ σχετίζεται με το συγκεκριμένο χρήστη και αποθηκεύεται για μελλοντική χρήση. Σε κάθε προσπάθεια πιστοποίησης, μια ειδική συσκευή ανιχνεύει τη μορφή του επιλεγμένου χαρακτηριστικού στο άτομο που προσπαθεί να αποκτήσει πρόσβαση, και εφόσον ταιριάζει με το προφίλ που έχει αποθηκευτεί, παρέχεται πρόσβαση.

Αν και τα τελευταία χρόνια τέτοιου είδους συστήματα είναι διαθέσιμα για χρήση, αυτά είναι τεχνικά πολύπλοκα και ιδιαίτερα ακριβά, ενώ σημαντικά προβλήματα μπορεί να εμφανιστούν όσον αφορά στη αποδοχή τους από τους τελικούς χρήστες. Από την άλλη πλευρά, η τεχνολογία που βασίζεται στην βιομετρία εξελίσσεται γρήγορα, και τα συστήματα γίνονται όλο και πιο αξιόπιστα, και πιο φιλικά προς το χρήστη.

Τα συστήματα βιομετρίας μπορούν να παρέχουν πολύ υψηλό βαθμό ασφαλείας, αλλά η τεχνολογία που χρησιμοποιούν δεν είναι τόσο ώριμη όσο στην περίπτωση των καρτών μνήμης και των έξυπνων καρτών. Επιπλέον, στην περίπτωση εφαρμογής τέτοιων συστημάτων ανακύπτουν δυσκολίες που οφείλονται στο γεγονός ότι είναι δύσκολο να αποθηκευτεί για μελλοντική σύγκριση ένα ατομικό χαρακτηριστικό με ακρίβεια και λεπτομέρεια. Επίσης, κάποια ατομικά χαρακτηριστικά ενδέχεται να μεταβάλλονται σημαντικά, όπως για παράδειγμα η φωνή ενός ανθρώπου που πάσχει από κρυολόγημα ή έχει βραχνιάσει.

Εξ 'αιτίας του σημαντικού κόστους και των τεχνικών δυσκολιών, αυτή τη στιγμή τα συστήματα βιομετρίας είναι κατάλληλα μόνο για περιβάλλοντα στα οποία απαιτείται πολύ υψηλός βαθμός ασφαλείας.

4.2. Διαχείριση Δεδομένων Πιστοποίησης

Η διαχείριση των δεδομένων πιστοποίησης είναι ένα από τα πιο κρίσιμα σημεία στο σχεδιασμό και τη λειτουργία ενός συστήματος πιστοποίησης. Ο φόρτος διαχείρισης σε ένα σύστημα ταυτοποίησης και πιστοποίησης ταυτότητας μπορεί να είναι ιδιαίτερα σημαντικός. Η διαχείριση συνήθως περιλαμβάνει τη δημιουργία, τη διανομή και την αποθήκευση των δεδομένων πιστοποίησης.

Για τα συστήματα που βασίζονται στους κωδικούς πρόσβασης, η διαδικασία διαχείρισης κυρίως περιλαμβάνει τον ορισμό της πολιτικής ορισμού και ανανέωσης των κωδικών πρόσβασης και τη συντήρηση του αρχείου στο οποίο αποθηκεύονται οι κωδικοί πρόσβασης. Για τα συστήματα που βασίζονται σε κουπόνια / κάρτες, η

διαχείριση περιλαμβάνει τη δημιουργία και τη διανομή των καρτών και των PINs, και την εγκατάσταση και τη συντήρηση του συστήματος που θα αναγνωρίζει τα έγκυρα ζευγάρια από κάρτες και PINs. Για τα συστήματα βιομετρίας, η διαδικασία διαχείρισης κυρίως αφορά στη δημιουργία και την αποθήκευση των προφίλ των χρηστών.

Ο διαχειριστής του συστήματος πρέπει να φροντίζει ώστε τα δεδομένα πιστοποίησης να είναι πάντα ενημερωμένα, προσθέτοντας, διαγράφοντας και ανανεώνοντας τα δεδομένα, ανάλογα με την κατάσταση του συστήματος. Με αυτό τον τρόπο εξασφαλίζεται ότι τα δεδομένα πιστοποίησης χρησιμοποιούνται από τους εξουσιοδοτημένους χρήστες, και όχι από άλλα άτομα τα οποία έχουν μάθει ή υποκλέψει τα δεδομένα πιστοποίησης. Επιπλέον, η διαχείριση των δεδομένων πιστοποίησης πρέπει να χειρίζεται περιπτώσεις χαμένων ή κλεμμένων κωδικών πρόσβασης ή καρτών, και περιπτώσεις κλεμμένων ή μοιραζόμενων λογαριασμών.

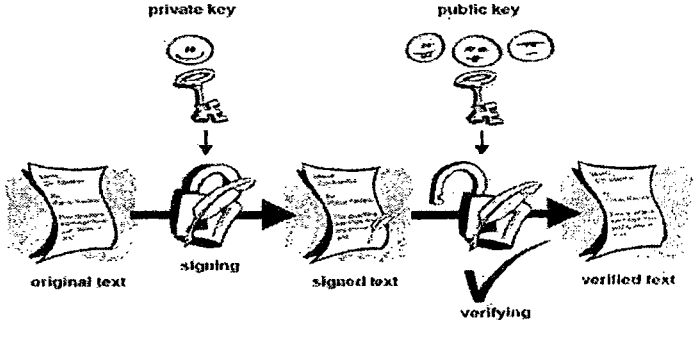
Μια χρήσιμη πρακτική στη κατεύθυνση της ανακάλυψης λογαριασμών που χρησιμοποιούνται από μη εξουσιοδοτημένους χρήστες είναι να πληροφορείται ο χρήστης, κατά τη διαδικασία login, πότε χρησιμοποιήθηκε ο λογαριασμός του τελευταία φορά. Στην περίπτωση που η τελευταία χρήση του λογαριασμού δεν έγινε από τον εξουσιοδοτημένο χρήστη, θα πρέπει να ενημερώνεται ο διαχειριστής του συστήματος.

Μια άλλη διάσταση της διαχείρισης των δεδομένων πιστοποίησης είναι η ασφαλής αποθήκευση τους. Η διάσταση αυτή είναι ιδιαίτερα σημαντική στην περίπτωση συστημάτων που βασίζονται σε κωδικούς πρόσβασης. Όπως το σύνολο της πληροφορίας, τα δεδομένα πιστοποίησης, κατά κύριο λόγο, πρέπει να πληρούν τις αρχές της εμπιστευτικότητας, της ακεραιότητας, και της διαθεσιμότητας. Αν τα δεδομένα πιστοποίησης δεν είναι εμπιστευτικά, τότε διαφορετικά άτομα θα μπορούν να χρησιμοποιούν την ταυτότητα ενός και μόνου χρήστη. Αν τα δεδομένα πιστοποίησης μπορούν να παραποιηθούν, τότε καταλύεται η ακεραιότητα του συστήματος. Επίσης, αν τα δεδομένα πιστοποίησης δεν είναι διαθέσιμα, κανένας χρήστης δεν μπορεί να προσπελάσει στο σύστημα.

4.3. Ψηφιακές Υπογραφές για Αναγνώριση Ταυτότητας

Η ψηφιακή υπογραφή μπορεί να χρησιμοποιηθεί για να επιβεβαιώσει τον αποστολέα του μηνύματος. Για παράδειγμα, ο παραλήπτης ενός μηνύματος ηλεκτρονικού ταχυδρομείου μπορεί να επιβεβαιώσει το πρόσωπο που έχει υπογράψει το μήνυμα, και ότι η πληροφορία του μηνύματος δεν έχει τροποποιηθεί από τη στιγμή που αυτό υπογράφτηκε. Επίσης, ο αποστολέας του μηνύματος δεν μπορεί να αρνηθεί ότι έστειλε το συγκεκριμένο μήνυμα με το συγκεκριμένο περιεχόμενο.

Στην εικόνα 4.2 φαίνεται μια ψηφιακή υπογραφή για αναγνώριση ταυτότητας:



Εικόνα 4.2

Τα συστήματα ηλεκτρονικών υπογραφών που είναι διαθέσιμα σήμερα βασίζονται σε κρυπτογραφικές τεχνικές, και παρέχουν τόση ασφάλεια όσο και η γραπτή υπογραφή. Τα συστήματα ηλεκτρονικών υπογραφών βασίζονται στη μυστικότητα των κρυπτογραφικών κλειδιών και στην ανάθεση του κρυπτογραφικού κλειδιού στον κάτοχό του. Αν το κρυπτογραφικό κλειδί υποκλαπεί, τότε ο υποκλοπέας μπορεί να προσποιηθεί ότι είναι ο πραγματικός κάτοχος του κλειδιού.

Τόσο τα κρυπτογραφικά συστήματα μυστικού κλειδιού όσο και αυτά δημόσιου κλειδιού μπορούν να χρησιμοποιηθούν για την υλοποίηση ψηφιακών υπογραφών. Παρόλα αυτά, τα συστήματα δημόσιου κλειδιού είναι πιο ευέλικτα και κατάλληλα για αυτό το σκοπό.

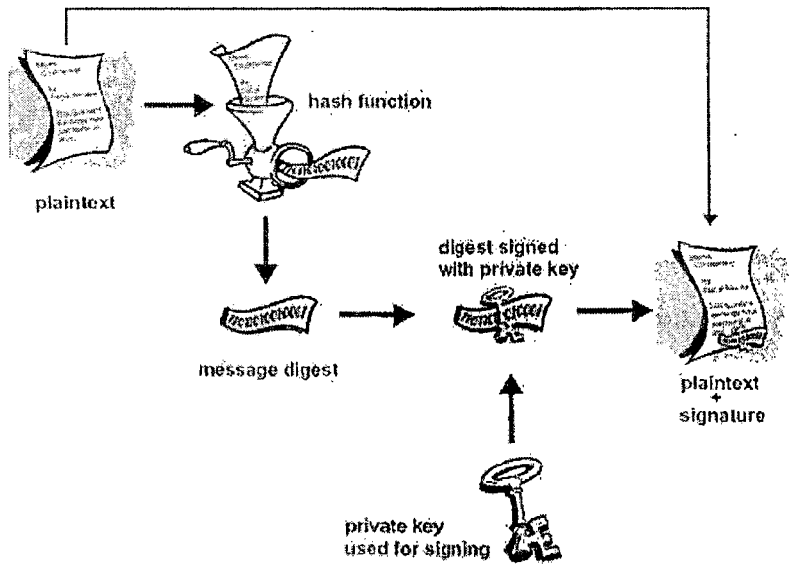
Στην περίπτωση των συστημάτων μυστικού κλειδιού, οι ηλεκτρονικές υπογραφές μπορούν να υλοποιηθούν με την χρήση του κωδικού πιστοποίησης δεδομένων. Για παράδειγμα, για ένα ζευγάρι οντοτήτων που επικοινωνεί με χρήση ενός κοινού μυστικού κλειδιού, όταν μια οντότητα λάβει ένα αρχείο που έχει υπογραφεί με έναν κωδικό πιστοποίησης μηνύματος, τότε μπορεί εύκολα να επιβεβαιώσει, με χρήση του κοινού κρυπτογραφικού κλειδιού, ότι το μήνυμα έχει σταλθεί από την άλλη οντότητα., και δεν έχει τροποποιηθεί στη διαδρομή. Αυτή η απλή διαδικασία έχει το μειονέκτημα ότι προϋποθέτει εμπιστοσύνη μεταξύ των δυο οντοτήτων που επικοινωνούν. Πιο προηγμένες τεχνικές μπορούν να χρησιμοποιηθούν για άρση της υπόθεσης για εμπιστοσύνη μεταξύ των δύο οντοτήτων. Αξίζει να σημειωθεί ότι η ομοσπονδιακή κυβέρνηση των Ηνωμένων Πολιτειών έχει ήδη εγκρίνει τη χρήση της τεχνολογίας κωδικού πιστοποίησης μηνύματος σαν εναλλακτικό της γραπτής υπογραφής.

Τα συστήματα δημόσιου κλειδιού είναι τα πλέον κατάλληλα για την υλοποίηση ηλεκτρονικών υπογραφών, που σε αυτή την περίπτωση ονομάζονται και ψηφιακές υπογραφές (digital signatures). Τα δεδομένα υπογράφονται (κρυπτογραφούνται) με χρήση του ιδιωτικού κλειδιού του αποστολέα. Για να επιταχυνθεί η διαδικασία, συνήθως κρυπτογραφείται μόνο η σύνοψη των δεδομένων που αντιστοιχείται στα δεδομένα από μια ασφαλή hash συνάρτηση.

Η κρυπτογραφημένη σύνοψη του μηνύματος ονομάζεται ψηφιακή υπογραφή και αποθηκεύεται ή μεταδίδεται μαζί με τα δεδομένα. Η ταυτότητα του αποστολέα, καθώς και η ακεραιότητα των δεδομένων μπορούν εύκολα να πιστοποιηθούν από οποιονδήποτε, με χρήση του δημόσιου κλειδιού του αποστολέα. Το χαρακτηριστικό αυτό είναι ιδιαίτερα επιθυμητό όταν για παράδειγμα μια εταιρεία προωθεί λογισμικό, το οποίο είναι πιστοποιημένο ότι δεν έχει ιούς ή άλλο επιβλαβή κώδικα.

Η εταιρεία μπορεί να υπογράψει ψηφιακά το μήνυμα, και κάθε παραλήπτης μπορεί να χρησιμοποιήσει το δημόσιο κλειδί της εταιρείας ώστε να επιβεβαιώσει ότι το λογισμικό που παρέλαβε συνεχίζει να είναι αυτό που απέστειλε η εταιρεία, και επομένως μπορεί να εγκατασταθεί άφοβα. Το NIST έχει δημοσιεύσει τις τυποποιήσεις FIPS 186, Digital Signature Standard, FIPS 180, Secure Hash Standard (SHS), σχετικά με την υλοποίηση ψηφιακών υπογραφών και ασφαλών υπογραφών hash συναρτήσεων.

Στην εικόνα 4.3 Φαίνεται η υλοποίηση μιας ασφαλής ψηφιακής υπογραφής με την χρήση μιας hash συνάρτησης:



Εικόνα 4.3

Σε περιβάλλοντα που δεν χρησιμοποιούνται κρυπτογραφικές τεχνικές για υλοποίηση ηλεκτρονικών υπογραφών, υπάρχουν μερικές πρακτικές μέθοδοι, που προσφέρουν ικανοποιητικό βαθμό ασφάλειας, για να διαπιστωθεί η πραγματική ταυτότητα του αποστολέα ενός ηλεκτρονικού μηνύματος.

Μια απλή μέθοδος συνίσταται στον έλεγχο της διαδρομής του μηνύματος στο δίκτυο. Στα μηνύματα ηλεκτρονικού ταχυδρομείου που διακινούνται στο internet σημειώνονται ο κόμβος του αποστολέα και η πλήρης διαδρομή του μηνύματος στο δίκτυο.

Όταν δύο μέρη επικοινωνούν μέσω ενός πάροχου δικτυακών υπηρεσιών (π.χ. Internet service provider) τότε ο πάροχος μπορεί να ελέγξει και να επιβεβαιώσει τον αποστολέα του μηνύματος και την ακεραιότητα των δεδομένων.

Εφόσον υπάρχει εμπιστοσύνη μεταξύ των οντοτήτων που επικοινωνούν ο παραλήπτης ενός μηνύματος μπορεί εύκολα να επιβεβαιώσει τον αποστολέα και το περιεχόμενο στέλνοντας ένα μήνυμα επιβεβαίωσης.

Τέλος, τα εξερχόμενα μηνύματα και το περιεχόμενο τους πρέπει να καταγράφονται στα αρχεία δραστηριότητας του συστήματος για ενδεχόμενη μελλοντική χρήση.

4.4. Ζητήματα υλοποίησης και διαχείρισης κρυπτογραφικών κλειδιών

Οι κρυπτογραφικές τεχνικές μπορούν να υλοποιήσουν αρκετές χρήσιμες λειτουργίες και να προσφέρουν πολύ υψηλά επίπεδα ασφαλείας. Στην πράξη όμως, τα επίπεδα ασφαλείας που προσφέρονται από τις κρυπτογραφικές τεχνικές εξαρτώνται σε μεγάλο βαθμό από την υλοποίηση και τη διαχείριση των κρυπτογραφικών κλειδιών.

4.4.1. **Επιλογή Τυποποιήσεων:** Πολλοί οργανισμοί τυποποίησης έχουν εκδώσει πρότυπα για το σχεδιασμό, την υλοποίηση και την χρήση κρυπτογραφικών τεχνικών σε μεγάλα υπολογιστικά συστήματα και δίκτυα δεδομένων. Οι λύσεις που έχουν τυποποιηθεί είναι ευρέως αποδεκτές, έχουν αξιολογηθεί και εγκριθεί από ομάδες ειδικών στις περιοχές που καλύπτουν, και εγγυώνται διαλειτουργικότητα μεταξύ εξοπλισμού διαφορετικών κατασκευαστών.

Η χρήση κρυπτογραφικών τεχνικών σε ένα μεγάλο οργανισμό πρέπει να βασίζεται σε διεθνείς τυποποιήσεις οι οποίες επιλέχθηκαν κατά το σχεδιασμό της πολιτικής ασφαλείας του οργανισμού με βάση το λόγο απόδοσης / κόστος, τη διεθνή αποδοχή τους, τη διαλειτουργικότητα, και τη δυνατότητα αποδοτικής εφαρμογής τους στο συγκεκριμένο οργανισμό. Αξίζει να σημειωθεί ότι η χρήση τυποποιήσεων όπως το DES και το DSS είναι εδώ και μερικά χρόνια υποχρεωτική για τα υπολογιστικά συστήματα των ομοσπονδιακών υπηρεσιών των Η.Π.Α.

4.4.2. **Υλοποίηση σε Υλικό και Λογισμικό:** Όλες οι κρυπτογραφικές τεχνικές μπορούν να υλοποιηθούν είτε σε υλικό (hardware) είτε σε λογισμικό (software). Κάθε επιλογή έχει τα δικά της πλεονεκτήματα και μειονεκτήματα σε σχέση με το επίπεδο ασφαλείας που προσφέρει, το κόστος, την αποδοτικότητα, το βαθμό αποδοχής από τους τελικούς χρήστες.

Γενικά, η υλοποίηση σε λογισμικό είναι φθηνότερη, αλλά είναι και πιο αργή, και θεωρείται ότι προσφέρει χαμηλότερο επίπεδο ασφαλείας, επειδή το λογισμικό είναι ευκολότερο να τροποποιηθεί ή να παρακαμφθεί από ότι ένα τμήμα υλικού.

Σε πολλές περιπτώσεις, οι κρυπτογραφικές τεχνικές υλοποιούνται σε υλικό (π.χ. σε ολοκληρωμένα κυκλώματα ή σε ROMs) αλλά η χρήση τους ελέγχεται από λογισμικό. Το λογισμικό απαιτεί προστασία για την ακεραιότητα του, ώστε να εξασφαλίζεται ότι το αντίστοιχο τμήμα του υλικού θα τροφοδοτείται με σωστή πληροφορία, και δεν θα παρακάμπτεται. Τέτοιου είδους υβριδικές λύσεις είναι αποδεκτές τόσο τεχνικά όσο και από άποψη κόστους, αλλά χρειάζεται προσεκτική διαχείριση και των δύο μερών.

4.4.3. **Διαχείριση κρυπτογραφικών κλειδιών:** Η ασφάλεια των κρυπτογραφικών κλειδιών είναι πολύ σημαντική, αφού από αυτήν εξαρτάται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων που προφυλάσσονται με χρήση κρυπτογραφικών τεχνικών.

Όλα τα κρυπτογραφικά κλειδιά πρέπει να προστατεύονται από τροποποίηση, και τα ιδιωτικά / μυστικά κλειδιά πρέπει να προστατεύονται από υποκλοπή και μη εξουσιοδοτημένη χρήση. Η διαχείριση πρέπει να περιλαμβάνει τα πρωτόκολλα και τις διαδικασίες που εφαρμόζονται σε όλο τον κύκλο ζωής των κλειδιών, ο οποίος περιλαμβάνει τη δημιουργία, τη διανομή στους εξουσιοδοτημένους χρήστες, την αποθήκευση, τη χρήση, την καταστροφή, και τη φύλαξη κλειδιών που δεν είναι πλέον σε χρήση.

Όταν χρησιμοποιούνται συστήματα μυστικού κλειδιού, τα κρυπτογραφικά κλειδιά πρέπει να διανέμονται στις οντότητες που επιθυμούν να επικοινωνήσουν, και να προφυλάσσονται από αντικατάσταση, τροποποίηση ή υποκλοπή. Η διαδικασία αυτή μπορεί να είναι απαιτητική, αν και ο αριθμός των χρηστών είναι μεγάλος ή αυτοί κατανέμονται σε μεγάλη γεωγραφική έκταση. Υπάρχουν αυτοματοποιημένες διαδικασίες και διεθνείς τροποποιήσεις για τη διαχείριση κρυπτογραφικών κλειδιών για συστήματα μυστικού κλειδιού σε διάφορα υπολογιστικά περιβάλλοντα (π.χ. FIPS 171, Key Management Using ANSI X9.17).

Για τα συστήματα δημόσιου κλειδιού, το σημαντικότερο πρόβλημα διαχείρισης είναι η σύνδεση ενός χρήστη με το δημόσιο κλειδί. Για μια μικρή ομάδα χρηστών, το πρόβλημα μπορεί να λυθεί με τη γνωστοποίηση του συνόλου των δημοσίων κλειδιών σε όλους τους χρήστες (π.χ. μέσω ενός CD-ROM, ή μιας WWW τοποθεσίας). Όταν το πλήθος των χρηστών είναι σημαντικό, ή κατανέμονται σε μεγάλη γεωγραφική έκταση, τότε απαιτείται υπολογιστική υποδομή για την καταγραφή και την αναζήτηση των δημόσιων κλειδιών των χρηστών. Σύγχρονα, κατανεμημένα συστήματα καταλόγου, (π.χ. τυποποίηση X.500 Directory Services) μπορούν να δώσουν λύση σε αυτό το πρόβλημα, αλλά χρειάζονται σημαντική επένδυση σε υπολογιστική και δικτυακή υποδομή, ενώ έχουν απαιτήσεις σε θέματα διαχείρισης. Στα συστήματα δημόσιου κλειδιού, οι χρήστες αναλαμβάνουν σημαντικές ευθύνες σε θέματα διαχείρισης, όπως τη δημιουργία του ζεύγους των κλειδιών, την κοινοποίηση του δημόσιου κλειδιού, την προστασία του ιδιωτικού κλειδιού, την ανανέωση του ζεύγους κλειδιών σε περίπτωση υποκλοπής, και τη φύλαξη παλαιών κλειδιών για την αναγνώριση εγγράφων που υπογράφτηκαν στο παρελθόν.

4.5. Ασφάλεια Υλοποίησης των Κρυπτογραφικών Τεχνικών

Κάθε κρυπτογραφική τεχνική υλοποιείται σε ένα τμήμα υλικού, λογισμικού, ή firmware. Η σωστή λειτουργία της κρυπτογραφικής τεχνικής προϋποθέτει ασφαλή και λεπτομερή σχεδιασμό, υλοποίηση, και χρήση του τμήματος που υλοποιεί την κρυπτογραφική τεχνική, ενώ το τμήμα πρέπει να προστατεύεται από τη λαθροχειρία.

Η τυποποίηση FIPS 140-1, Security Requirements for Cryptographic Modules, καθορίζει τις απαιτήσεις ασφαλείας σε φυσικό και λογικό επίπεδο για τα τμήματα που υλοποιούν κρυπτογραφικές τεχνικές. Η τυποποίηση ορίζει τέσσερα επίπεδα ασφαλείας για τα κρυπτογραφικά τμήματα, με κάθε επίπεδο να παρέχει υψηλότερο επίπεδο ασφαλείας από το προηγούμενο. Τα τέσσερα επίπεδα παρέχουν δυνατότητα για αποδοτικές και οικονομικά αποδεκτές λύσεις που είναι κατάλληλες για οργανισμούς και περιβάλλοντα με διαφορετικές απαιτήσεις ασφαλείας.

Μια καλή λύση για την επιβεβαίωση της ασφαλούς υλοποίησης των κρυπτογραφικών τεχνικών είναι η προμήθεια τμημάτων τα οποία έχουν πιστοποιηθεί από αρμόδιους διεθνής ή εθνικούς οργανισμούς.

4.6. Εφαρμογή Κρυπτογραφίας σε Δίκτυα Δεδομένων

Η χρήση κρυπτογραφικών τεχνικών σε περιβάλλον δικτύων δεδομένων απαιτεί την εξέταση και άλλων παραγόντων. Για παράδειγμα, θα πρέπει να επιβεβαιωθεί ότι τα πρωτόκολλα και ο εξοπλισμός επικοινωνίας είναι διαφανή, και επιτρέπουν την μετάδοση των διαφόρων μορφών κρυπτογραφημένης πληροφορίας χωρίς προβλήματα. Επίσης, θα πρέπει η κρυπτογραφημένη πληροφορία να μορφοποιηθεί πριν τη μετάδοσή της με τρόπο που να μην δημιουργεί προβλήματα (π.χ. να ερμηνεύεται σαν ακολουθία από χαρακτήρες ελέγχου) στις δικτυακές ή άλλες εφαρμογές που εμπλέκονται στη μετάδοση.

Η πληροφορία σε ένα δίκτυο δεδομένων μπορεί να κρυπτογραφηθεί είτε σε κάθε σύνδεσμο επικοινωνίας, είτε μεταξύ των δύο οντοτήτων που επικοινωνούν.

Η κρυπτογράφηση της πληροφορίας που μεταδίδεται σε ένα σύνδεσμο επικοινωνίας (π.χ. δορυφορική ζεύξη, τηλεφωνικό κύκλωμα) συνήθως γίνεται από τον παροχέα επικοινωνίας. Επειδή η κρυπτογράφηση της πληροφορίας που μεταδίδεται σε κάποιο

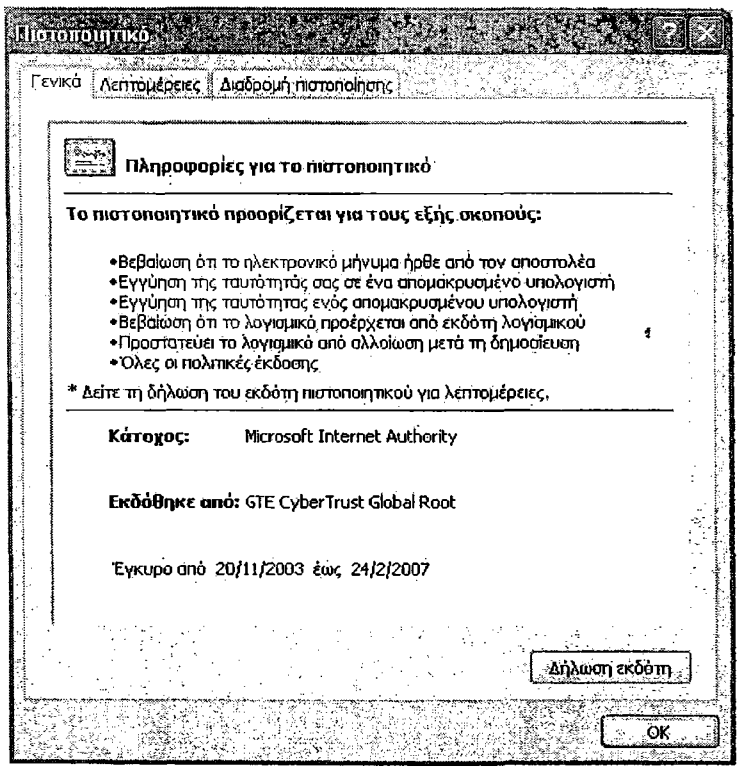
σύνδεσμο επικοινωνίας αφορά και στις πληροφορίες δρομολόγησης, η πληροφορία πρέπει να αποκρυπτογραφείται μεταξύ των κόμβων επικοινωνίας, ώστε να γίνεται σωστά η δρομολόγηση.

Η κρυπτογράφηση της πληροφορίας μεταξύ των οντοτήτων που επικοινωνούν συνήθως γίνεται με ευθύνη των οντοτήτων. Αν και η πληροφορία που ανταλλάσσεται είναι κρυπτογραφημένη, τα δεδομένα δρομολόγησης είναι σε κανονική μορφή, και η δρομολόγηση των πακέτων πληροφορίας γίνεται χωρίς προβλήματα. Αξίζει να σημειωθεί ότι και οι δύο μορφές κρυπτογραφημένης επικοινωνίας μπορεί να εφαρμοστούν ταυτόχρονα.

4.7. Αρχές Πιστοποίησης – Ψηφιακά Πιστοποιητικά

Πιστοποίηση είναι η διαδικασία της αντιστοίχησης ενός δημόσιου κλειδιού σε ένα άτομο, οργανισμό ή άλλη οντότητα. Για το σκοπό αυτό χρησιμοποιούνται ψηφιακά πιστοποιητικά τα οποία αποτελούν το μέσο με το οποίο μεταδίδονται με ασφαλή τρόπο οι τιμές των δημοσίων κλειδιών και οι πληροφορίες του κατόχου σου σχετίζονται με αυτά. Η πιστοποίηση αποτελεί μια βασική λειτουργία όλων των Υποδομών Δημόσιου Κλειδιού – ΥΔΚ (Public Key Infrastructures - PKI).

Στην εικόνα 4.4 φαίνεται ένα ψηφιακό πιστοποιητικό με τα στοιχεία του:



Εικόνα 4.4

4.7.1. **Ψηφιακά Πιστοποιητικά:** Είναι ηλεκτρονικά έγγραφα που χρησιμοποιούνται για την αναγνώριση ενός προσώπου / εξυπηρετητή / οργανισμού και την συσχέτισή του με ένα δημόσιο κλειδί. Η απόκτηση ενός ηλεκτρονικού πιστοποιητικού γίνεται μετά από αίτηση σε μια Αρχή Πιστοποίησης – ΑΠ (Certificate Authority – CA). Η Αρχή Πιστοποίησης επιβεβαιώνει την ταυτότητα του αιτούντος και εκδίδει το πιστοποιητικό που περιλαμβάνει τα εξής στοιχεία:

- Το όνομα και πληροφορίες αναγνώρισης του χρήστη στον οποίο αναφέρεται το πιστοποιητικό.
- Το δημόσιο κλειδί του χρήστη.
- Την ημερομηνία λήξης του πιστοποιητικού.
- Το όνομα και την ψηφιακή υπογραφή της Αρχής Πιστοποίησης που το εξέδωσε.
- Ένα σειριακό αριθμό πιστοποιητικού.
- Ένα σύνολο ψηφιακών υπογραφών για το χρήστη.

Το πρότυπο X.509 είναι το πλέον διαδεδομένο πρότυπο 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 (clients) και των εξυπηρετητών (servers), την ακεραιότητα των διακινούμενων δεδομένων, την αποφυγή προστριβών μεταξύ των συμμετεχόντων μερών, καθώς και την εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα.

4.7.2. **Τύποι ψηφιακών πιστοποιητικών**

- **Client SSL certificates:** χρησιμοποιούνται για την αναγνώριση χρηστών από εξυπηρετητές μέσω SSL.
- **Server SSL certificates:** χρησιμοποιούνται για την αναγνώριση των εξυπηρετητών από πελάτες μέσω SSL.
- **S/MIME certificates:** χρησιμοποιούνται για την κρυπτογράφηση και την υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- **Object – signing certificates:** χρησιμοποιούνται για την αναγνώριση υπογεγραμμένου κώδικα σε Java, Javascript, καθώς και των άλλων τύπων αρχείων.
- **CA certificates:** χρησιμοποιούνται για την αναγνώριση Αρχών Πιστοποίησης.

Τα πιστοποιητικά χαρακτηρίζονται ακόμη και από το είδος της πληροφορίας που περιέχουν. Υπάρχουν:

- **Πιστοποιητικά ταυτότητας,** που ταυτοποιούν μια οντότητα.
- **Πιστοποιητικά χαρακτηριστικών,** που περιγράφουν τις ιδιότητες μιας οντότητας, όπως κάποιο δικαίωμα προσπέλασης ή τη συμμετοχή της σε μια ομάδα χρηστών.

4.7.3. **Αρχές Πιστοποίησης:** Επιβεβαιώνουν τις ταυτότητες των χρηστών και εκδίδουν τα αντίστοιχα πιστοποιητικά. Μια αρχή πιστοποίησης μπορεί να είναι:

- Είτε ένας έμπιστος τρίτος φορέας (Trusted Third Party –TTP)
- Είτε να λειτουργεί στα πλαίσια ενός οργανισμού.

Μια αρχή πιστοποίησης είναι ένας οργανισμός που λειτουργεί με ασφάλεια κάτω από αυστηρές προδιαγραφές με σκοπό τη δημιουργία και διανομή ψηφιακών πιστοποιητικών. Κάθε αρχή πρέπει θεωρητικά να συμμετέχει σε μια ευρύτερη Υποδομή Δημόσιου Κλειδιού, συνήθως ιεραρχικής δομής, όπου οι ανώτερες αρχές πιστοποιούν τις κατώτερες. Σε κάθε χώρα μπορεί να υπάρχουν μια ή περισσότερες Αρχές Πιστοποίησης, συνήθως κατά περιοχή εφαρμογής (τράπεζες, υγεία, παιδεία).

Το πρότυπο X.509 προτείνει τη σύσταση ιεραρχιών Αρχών Πιστοποίησης με σκοπό την κάλυψη των αναγκών πιστοποίησης μεγάλων οργανισμών και γεωγραφικών περιοχών. Στην κορυφή κάθε ιεραρχίας βρίσκεται η Αρχή – ρίζα. Το πιστοποιητικό της ΑΠ – ρίζας είναι υπογεγραμμένο από την ίδια. Οι ΑΠ που βρίσκονται κάτω από τη ρίζα έχουν τα πιστοποιητικά τους υπογεγραμμένα από τη ρίζα. Τα πιστοποιητικά των ΑΠ κατώτερων επιπέδων υπογράφονται από τις ΑΠ των αμέσως ανώτερων επιπέδων.

Κατά την αυθεντικοποίηση ενός χρήστη από έναν άλλο μπορεί να μεσολαβεί ένας μεταβλητός αριθμός από Αρχές Πιστοποίησης. Αυτό σημαίνει ότι όταν ένας αποστολέας θέλει να στείλει ένα μήνυμα σε έναν παραλήπτη που πιστοποιείται από μια άλλη Αρχή πρέπει να επαληθεύσει την ταυτότητα όλων των Αρχών που μεσολαβούν μέχρι να αποκτήσει το πιστοποιητικό του παραλήπτη.

ΚΕΦΑΛΑΙΟ ΠΕΜΠΤΟ

ΑΡΧΕΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΚΑΙ ΠΙΣΤΟΠΟΙΗΤΙΚΑ SERVER

5.1. Αρχές πιστοποίησης (Certifications Authorities)

Οι αρχές πιστοποίησης είναι οι οντότητες της Υποδομής Δημόσιου Κλειδιού που εκδίδουν τα πιστοποιητικά. Κάθε αρχή πιστοποίησης χρησιμοποιεί μία ή περισσότερες αρχές καταχώρισης για τη μεταβίβαση των αιτήσεων των συνδρομητών στην αρχή πιστοποίησης.

Η Ιεραρχία της Υπηρεσίας Πιστοποίησης αποτελείται από τις παρακάτω οντότητες:

5.1.1. **Κεντρική Αρχή Πιστοποίησης (Root Certification Authority, GRNET-ROOT-CA),** η οποία εκδίδει αποκλειστικά ψηφιακά πιστοποιητικά για υφιστάμενες Αρχές Πιστοποίησης που πιθανά λειτουργούν σε άλλα ακαδημαϊκά ιδρύματα ή σε άλλους οργανισμούς και δεν εκδίδει πιστοποιητικά για τελικές οντότητες. Το πιστοποιητικό της GRNET-ROOT-CA έχει διάρκεια ισχύος 20 έτη.

5.1.2. **Υφιστάμενες Αρχές Πιστοποίησης,** που πιθανά λειτουργούν σε διοικητικές μονάδες του ΕΔΕΤ ή σε άλλα ιδρύματα που συμμορφώνονται και υιοθετούν πλήρως την παρούσα Δήλωση Διαδικασιών Πιστοποίησης. Τα πιστοποιητικά των Υφιστάμενων Αρχών Πιστοποίησης έχουν διάρκεια ισχύος έως 4 έτη. Αρχικά λειτουργούν οι υφιστάμενες Αρχές Πιστοποίησης για τις οντότητες που ανήκουν διοικητικά στο ΕΔΕΤ (GRNET-SUBSCRIBERS-CA και GRNET-SERVERS-CA) οι οποίες εκδίδουν πιστοποιητικά χρήστες και συσκευές του ΕΔΕΤ, αλλά όχι για τελικούς χρήστες άλλων ιδρυμάτων. Εφόσον ζητηθεί η έκδοση ψηφιακών πιστοποιητικών από το ΕΔΕΤ για τελικές οντότητες άλλων Ιδρυμάτων, θα δημιουργούνται οι αντίστοιχες υφιστάμενες ΑΠ για κάθε Ίδρυμα (<ΙΔΡΥΜΑ>-SUBSCRIBERS-CA και <ΙΔΡΥΜΑ>-SERVERS-CA) οι οποίες θα εκδίδουν τα σχετικά πιστοποιητικά. Η λειτουργία αυτών των ΑΠ είναι δυνατό να αναληφθεί είτε από το ΕΔΕΤ με τη μορφή outsourcing είτε από το ίδιο το Ίδρυμα.

5.1.3. **Δια-πιστοποιούμενες Αρχές Πιστοποίησης (Cross-Certified CAs)**, είναι Αρχές Πιστοποίησης άλλων Ιδρυμάτων ή Οργανισμών με τις οποίες η Υπηρεσία Πιστοποίησης του ΕΔΕΤ έχει συνάψει σχέσεις λειτουργικές, πολιτικές και εμπιστοσύνης, έτσι ώστε οι εγγραφόμενοι των δύο ΑΠ να εμπιστεύονται διαφανώς τα πιστοποιητικά της απέναντι ΑΠ.

5.2. Χρήση των Πιστοποιητικών

Κατάλληλες χρήσεις των πιστοποιητικών:

Τα πιστοποιητικά μπορούν να χρησιμοποιηθούν μόνο για ακαδημαϊκούς και ερευνητικούς σκοπούς, σε όλες τις δικτυακές υπηρεσίες και εφαρμογές στις οποίες το

απαιτούμενο επίπεδο ασφάλειας είναι ίσο ή χαμηλότερο από αυτό της διαδικασίας έκδοσης των πιστοποιητικών.

Ενδεικτικές εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν τα ψηφιακά πιστοποιητικά που εκδίδονται από την Υπηρεσία είναι οι εξής:

5.2.1. **Στην υπογραφή ενός ηλεκτρονικού εγγράφου από ένα φυσικό πρόσωπο** με τη χρήση του ψηφιακού πιστοποιητικού του και κατά προτίμηση με τη χρήση μιας 'ασφαλούς διάταξης δημιουργίας υπογραφής' (π.χ. smart card), ώστε να εξασφαλίζονται τουλάχιστον τα παρακάτω χαρακτηριστικά: 1) η αυθεντικότητα της προέλευσης (authenticity), 2) η ακεραιότητα του υπογεγραμμένου κειμένου (integrity), δηλαδή ότι το περιεχόμενό του δεν έχει τροποποιηθεί από τη στιγμή της υπογραφής του και 3) η δέσμευση του υπογράφοντα ως προς το περιεχόμενο του εγγράφου και η μη άρνηση της υπογραφής του (non-repudiation).

5.2.2. **Στην υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου,** για την εξασφάλιση της αυθεντικότητας της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αποστολέα και για όλες τις ιδιότητες που περιγράφηκαν στην παράγραφο 5.2.1. Επιπλέον μπορούν να χρησιμοποιηθούν για την αποστολή 'ασφαλών αποδείξεων παραλαβής μηνυμάτων' (non-repudiation of receipt).

5.2.3. **Στην ισχυρή απόδειξη της ταυτότητας (Strong Authentication)**, ενός φυσικού προσώπου ή μιας συσκευής κατά την επικοινωνία τους με άλλες οντότητες, εξασφαλίζοντας επιπλέον χαρακτηριστικά ασφάλειας, ισχυρότερα από αυτά που παρέχει η κλασική μέθοδος πρόσβασης με συνθηματικό χρήστη.

5.2.4. **Στην κρυπτογράφηση εγγράφων και μηνυμάτων,** με την χρήση του δημοσίου κλειδιού κάποιας οντότητας, εξασφαλίζοντας ότι μόνο ο επιδιωκόμενος παραλήπτης και κάτοχος του αντίστοιχου ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει και να διαβάσει το έγγραφο ή το μήνυμα.

5.2.5. **Στην πιστοποίηση άλλων παρόχων υπηρεσιών πιστοποίησης**, είτε πρόκειται για υφιστάμενες Αρχές Πιστοποίησης (Subordinate CAs), είτε πρόκειται για παροχή επιπλέον υπηρεσιών πιστοποίησης, όπως για παράδειγμα η χρονοσήμανση, οι συμβολαιογραφικές πράξεις και η μακροπρόθεσμη ασφαλής αποθήκευση δεδομένων.

5.2.6. **Στην υλοποίηση ασφαλών δικτυακών πρωτοκόλλων,** όπως τα SSL, secure DNS, IPSec κλπ.

5.3. Υποχρεώσεις των αρχών πιστοποίησης

Η αρχή πιστοποίησης είναι υπεύθυνη για την έκδοση και τη διαχείριση των πιστοποιητικών. Συγκεκριμένα, οι Αρχές Πιστοποίησης του ΕΔΕΤ δεσμεύονται:

- Να παρέχουν και να συντηρούν την υποδομή που απαιτείται για την σύσταση μιας ιεραρχίας πιστοποίησης για την ελληνική ακαδημαϊκή και ερευνητική κοινότητα, σύμφωνα με τις Διαδικασίες Πιστοποίησης που περιγράφονται στο έγγραφο αυτό.
- Να υλοποιούν και να συντηρούν τις απαιτήσεις ασφαλείας σύμφωνα με τα όσα ορίζονται στις σχετικές παραγράφους του παρόντος εγγράφου.

- Να αποδέχονται ή να απορρίπτουν αιτήσεις για έκδοση πιστοποιητικών σύμφωνα με τα όσα ορίζονται στις σχετικές παραγράφους του παρόντος εγγράφου.
- Να συντηρούν ένα χώρο αποθήκευσης ευρείας πρόσβασης για την αποθήκευση των πιστοποιητικών και των Λιστών Ανάκλησης Πιστοποιητικών. Οι πληροφορίες αυτές θα πρέπει να δημοσιοποιούνται μέσω ευρέως χρησιμοποιούμενων πρωτοκόλλων του παγκόσμιου ιστού, όπως HTTP, FTP και LDAP.
- Να ανακαλούν πιστοποιητικά όταν συντρέχουν λόγοι ή μετά από αίτημα του υποκειμένου ενός πιστοποιητικού.
- Να διατηρούν τις Λίστες Ανάκλησης Πιστοποιητικών πρόσφατα ενημερωμένες.
- Να διαχειρίζονται εμπιστευτικά όλες τις προσωπικές πληροφορίες που παρέχονται από τους εγγραφόμενους στην Υπηρεσία Πιστοποίησης.
- Να ενημερώνουν άμεσα το τεχνικό προσωπικό των υφιστάμενων ΑΠ, για έκθεση, απώλεια, δημοσιοποίηση, τροποποίηση, ή μη εγκεκριμένη χρήση του μυστικού κλειδιού των ΑΠ.
- Να διασφαλίζουν ότι όλα τα θέματα αναφορικά με τις υπηρεσίες που παρέχουν, όλες οι λειτουργίες που εκτελούνται και το σύνολο της υποδομής συμμορφώνονται με την παρούσα Δήλωση Διαδικασιών Πιστοποίησης.

5.4. Διαφορετικά Είδη Πιστοποιητικών

Υπάρχουν τέσσερις τύποι ψηφιακών πιστοποιητικών σε χρήση στο Internet:

- **Πιστοποιητικά Αρχών Πιστοποίησης (Certification authority certificates):** Αυτά τα πιστοποιητικά περιλαμβάνουν το δημόσιο κλειδί της αρχής πιστοποίησης, και είτε το όνομα της CA είτε το όνομά της συγκεκριμένης υπηρεσίας που πιστοποιεί. Μπορούν να υπογραφτούν από μόνα τους ή αλλιώς να υπογραφτούν από άλλη CA. Αυτά συνηθίζεται να πιστοποιούν άλλα είδη πιστοποιητικών.
- **Πιστοποιητικά Server (Server certificates):** Αυτά τα πιστοποιητικά περιλαμβάνουν το δημόσιο κλειδί ενός SSL Server, το όνομα του οργανισμού που τρέχει τον Server, το όνομα της Internet διεύθυνσης του και το δημόσιο κλειδί του server.
- **Προσωπικά πιστοποιητικά (Personal certificates):** Αυτά τα πιστοποιητικά περιλαμβάνουν το όνομα ενός ατόμου και άλλες πληροφορίες, όπως την ηλεκτρονική διεύθυνση του ατόμου, την ταχυδρομική διεύθυνση του, ή οτιδήποτε άλλο.
- **Πιστοποιητικά εκδοτών λογισμικού (Software Publisher certificates):** Αυτά τα πιστοποιητικά χρησιμοποιούνται για να υπογράφουν προγράμματα που πρόκειται να διανεμηθούν.

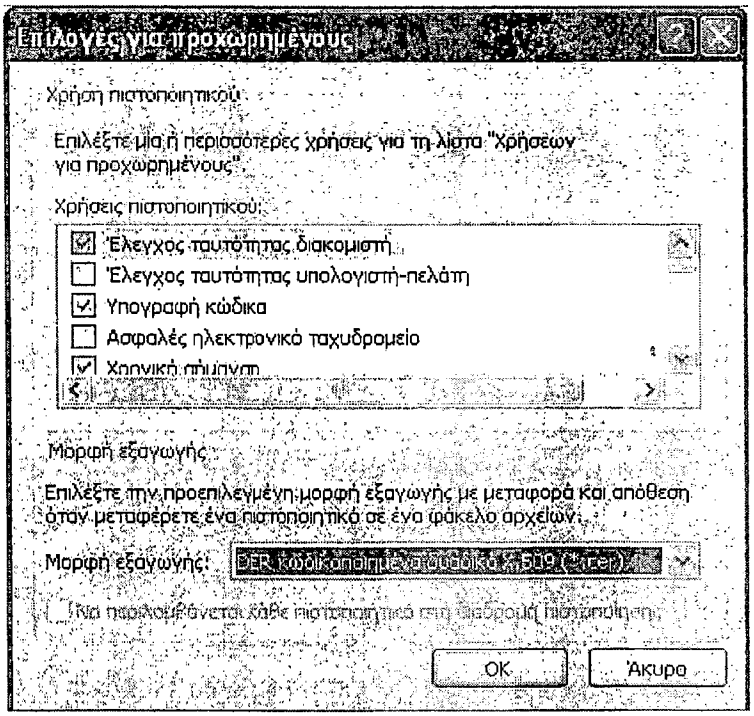
5.4.1. **Πιστοποιητικά Αρχών Πιστοποίησης:** Ένα πιστοποιητικό μιας αρχής πιστοποίησης είναι ένα πιστοποιητικό που περιλαμβάνει το όνομα και το δημόσιο κλειδί της αρχής πιστοποίησης. Αυτά τα πιστοποιητικά μπορούν να υπογραφτούν από μόνα τους (self-signed). Αυτό σημαίνει ότι η αρχή

πιστοποίησης μας λέει ότι το κλειδί της είναι καλό, και εμείς πρέπει να το εμπιστευτούμε. Αλλιώς, αυτά μπορούν να υπογραφτούν από μια άλλη αρχή. Επίσης, οι αρχές μπορούν να διασταυρώνουν η μια με την άλλη την πιστότητα των κλειδιών τους ή ακόμα και να υπογράφει η μια της άλλης τα κλειδιά.

Τα πιστοποιητικά αυτά διανέμονται με την προοπτική να τα εμπιστευτούμε όπως είναι, αυτό φαίνεται από το γεγονός ότι ενσωματώνονται απευθείας στους web browsers.

5.4.2. **Πιστοποιητικά Server:** Κάθε SSL server πρέπει να έχει ένα SSL πιστοποιητικό server. Όταν ένας browser συνδέεται σε ένα web server χρησιμοποιώντας το SSL πρωτόκολλο, ο server στέλνει στον browser το δημόσιο κλειδί του σε ένα X.509 v3 πιστοποιητικό. Το πιστοποιητικό χρησιμοποιείται για να αποδείξει την ταυτότητα του server και για να διανέμει το δημόσιο κλειδί του server, το οποίο χρησιμοποιείται για να κρυπτογραφήσει την αρχική πληροφορία που στέλνεται στον server από τον client.

Στην εικόνα 5.1 φαίνεται ένα πιστοποιητικό Server:



Εικόνα 5.1

5.5. Απόκτηση Πιστοποιητικού για ένα Server

Για να αποκτήσουμε ένα πιστοποιητικό για τον server μας, χρειαζόμαστε να ακολουθήσουμε τα παρακάτω βήματα:

- Δημιουργία ενός RSA δημόσιου / προσωπικού ζεύγους κλειδιών χρησιμοποιώντας ένα πρόγραμμα που θα το προμηθευτούμε από τον πωλητή του server.
- Αποστολή του δημόσιου κλειδιού, το διακεκριμένο και το κοινό όνομα στην αρχή πιστοποίησης που επιθυμούμε να χρησιμοποιήσουμε. Η αποστολή συνήθως γίνεται με την χρήση e-mail.

- Ακολουθούμε την διαδικασία πιστοποίησης της CA. Συμπλήρωση διαφόρων στοιχείων στο web site της CA, αποστολή εγγράφων με e-mail / fax ή και με ταχυδρομείο. Επίσης μπορεί να χρειαστεί να πληρώσουμε και την CA.
- Αναμονή για την επεξεργασία της αίτησης από την CA. Όταν η CA πειστεί ότι η αίτηση πληρή τις προϋποθέσεις, θα εκδώσει ένα πιστοποιητικό αποτελούμενο από το δημόσιο κλειδί μας, το διακεκριμένο όνομα μας, άλλες πληροφορίες, και την ψηφιακή υπογραφή του. Η αποστολή συνήθως γίνεται με την χρήση e-mail.
- Εγκατάσταση του κλειδιού χρησιμοποιώντας ένα πρόγραμμα που θα το προμηθευτούμε από τον πωλητή του server.

5.6. Περίοδοι χρήσης των δημόσιων και ιδιωτικών κλειδιών

Η διάρκεια χρήσης των ζευγών των κρυπτογραφικών κλειδιών προσδιορίζεται από την αντίστοιχη περίοδο ισχύος του σχετικού ψηφιακού πιστοποιητικού. Η μέγιστη διάρκεια χρήσης των κλειδιών ορίζεται σε 20 έτη για ΑΠ ρίζας, σε 5 έτη για ενδιάμεση ΑΠ και σε 2 έτη για πιστοποιητικά τελικών χρηστών και συσκευών. Η διάρκεια χρήσης σε κάθε περίπτωση θα πρέπει να αποφασίζετε σε συνάρτηση με το μέγεθος των κλειδιών και με τις τρέχουσες τεχνολογικές εξελίξεις στο χώρο της κρυπτογραφίας, έτσι ώστε να εξασφαλίζεται το βέλτιστο επίπεδο ασφάλειας αλλά και αποτελεσματικότητας χρήσης.

ΚΕΦΑΛΑΙΟ ΕΚΤΟ

ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΑΠΟ ΤΗΝ ΜΕΡΙΑ ΤΟΥ ΧΡΗΣΤΗ

Σε αυτό το κεφάλαιο θα δούμε πως τα ψηφιακά πιστοποιητικά μπορούν να πιστοποιήσουν την ταυτότητα ενός ατόμου.

6.1. Client Πιστοποιητικά

Ένα client πιστοποιητικό είναι ένα ψηφιακό πιστοποιητικό το οποίο είναι σχεδιασμένο για να πιστοποιεί την ταυτότητα ενός ατόμου. Όπως και με τα πιστοποιητικά των Web sites, τα client πιστοποιητικά συνδέουν ένα συγκεκριμένο όνομα με ένα συγκεκριμένο μυστικό κλειδί. Αυτά εκδίδονται από τις αρχές πιστοποίησης (CAs).

Τα client πιστοποιητικά έχουν πολλές χρήσεις και οφέλη:

- Τα ψηφιακά πιστοποιητικά μπορούν να απομακρύνουν την ανάγκη της απομνημόνευσης των usernames και των passwords. Απλά υπογράφουμε με την ψηφιακή υπογραφή μας οποτεδήποτε εισβάλουμε σε περιορισμένο χώρο.
- Αντί να αναπτύσσουν μια μεγάλη διασκορπισμένη βάση δεδομένων, οι οργανισμοί μπορούν απλά να χρησιμοποιούν ένα ψηφιακό πιστοποιητικό εκδομένο από μια ειδική CA σαν απόδειξη ιδιότητας μέλους στον οργανισμό αυτό.
- Είναι δυσκολότερο για μια ομάδα ατόμων να μοιραστούν ένα μόνο ψηφιακό ID από ότι είναι να μοιραστούν ένα ζεύγος username – password. Αυτό συμβαίνει επειδή η υπογραφή του ονόματος μας με ένα ψηφιακό πιστοποιητικό απαιτεί πρόσβαση σε ένα μυστικό κλειδί. Αυτό είναι επειδή υπάρχουν τεχνικά εμπόδια στο να μπορούν να μοιράζονται κοινά μυστικά κλειδιά οι χρήστες μεταξύ τους, και επειδή ίσως οι χρήστες να είναι απρόθυμοι να μοιράζονται ένα μυστικό κλειδί που είναι χρήσιμο για περισσότερες από μια εφαρμογές.
- Επειδή τα ψηφιακά πιστοποιητικά περιέχουν ένα δημόσιο κλειδί (που ανήκει στον ιδιοκτήτη του πιστοποιητικού), εμείς μπορούμε να χρησιμοποιήσουμε κάποιου το ψηφιακό πιστοποιητικό για να του στείλουμε κρυπτογραφημένο e-mail.
- Τα πιστοποιητικά που δείχνουν την ηλικία ενός προσώπου μπορούν να χρησιμοποιηθούν για περιορισμούς σε πονηρού περιεχομένου δεδομένα ή και chat groups.
- Τα πιστοποιητικά που δείχνουν το φύλο ενός προσώπου μπορούν να χρησιμοποιηθούν για την ελεύθερη πρόσβαση σε χώρους μόνο για άνδρες, ή μόνο για γυναίκες.

Δημιουργώντας ισχυρά συστήματα αναγνώρισης της ταυτότητας των χρηστών, τα πιστοποιητικά βοηθούν για την εξασφάλιση της ανωνυμίας. Επίσης είναι περισσότερο αποτελεσματικά και από τα «cookies». Ένα cookie απλώς αφήνει ένα ίχνος, που έχει να κάνει με τα σημεία από τα οποία εμείς περάσαμε στην επίσκεψη μας σε ένα web site. Ένα ψηφιακό πιστοποιητικό από την άλλη πλευρά, αφήνει πίσω το όνομα μας, την ηλεκτρονική μας διεύθυνση, ή και άλλες πληροφορίες αναγνώρισης ταυτότητας οι οποίες έχουν την δυνατότητα να ξαναγυρίσουν σε εμάς και να μας δώσουν πληροφορίες για την ταυτότητα του site που επισκεφτήκαμε.

Επειδή τα πιστοποιητικά ελαχιστοποιούν την ανωνυμία, μερικοί χρήστες του Internet είναι αντίθετοι στη χρήση τους, βασιζόμενοι στο ότι αυτά εκθέτουν την μυστικότητα του χρήστη. Αυτό κάνουν, αυτός είναι και ο σκοπός που δημιουργήθηκαν άλλωστε. Όπως κατασκευάζονται, τα πιστοποιητικά δεν στέλνονται ποτέ από έναν web browser χωρίς την γνώση και την άδεια του χρήστη. Επίσης, δεν περιέχουν πληροφορίες που είναι άγνωστες στον χρήστη.

Είναι αλήθεια ότι ένα σημαντικό στοιχείο ενός ολοκληρωμένου συστήματος διακυβέρνησης είναι η έκδοση καρτών απόδειξης ταυτότητας, και η ύπαρξη μεγάλων προστίμων όταν ο πολίτης δεν είναι σε θέση να αποδείξει την ταυτότητά του όταν του ζητηθεί. Αυτές οι κάρτες απόδειξης ταυτότητας, βοηθούν στην εδραίωση μιας δυνατής κοινωνίας με άτομα υπεύθυνα για τις πράξεις τους.

6.2. Απόδειξη ταυτότητας ιδιώτη

Πρόσωπο που αιτείται την έκδοση πιστοποιητικού: Ανάλογα με τις διαδικασίες ταυτοποίησης του αιτούντος, όπως περιγράφονται στη συνέχεια, καθορίζονται δύο κλάσεις πιστοποιητικών φυσικών προσώπων:

6.2.1. **USERS - SECURE:** Ασφαλής ταυτοποίηση με φυσική παρουσία και εμφάνιση αποδεκτού επίσημου εγγράφου που αποδεικνύει την ταυτότητα του αιτούντος.

Η αρχή καταχώρισης εκχωρεί τον έλεγχο της ταυτότητας σε υπηρεσίες των φορέων στους οποίους ανήκουν οι συνδρομητές και χρησιμοποιεί τρόπους πιστοποίησης ταυτότητας του χρήστη που διατίθενται από τους φορείς για να εκτελέσει τον έλεγχο ταυτότητας. Οι συνεργαζόμενοι φορείς είναι υποχρεωμένοι να έχουν πιστοποιήσει την ταυτότητα του χρήστη από κάποιο επίσημο έγγραφο που φέρει τη φωτογραφία του δικαιούχου (π.χ. αστυνομική ταυτότητα, διαβατήριο, δίπλωμα οδήγησης, φοιτητική ταυτότητα) και το οποίο θεωρείται αναγνωρισμένο από τον οικείο φορέα. Εναλλακτικά, η ίδια η ΑΚ του ΕΔΕΤ μπορεί να εκτελέσει την παραπάνω διαδικασία ταυτοποίησης του αιτούντος.

Εφόσον ο οικείος φορέας του χρήστη, σύμφωνα με την πολιτική του, έχει ήδη εκτελέσει διαδικασία φυσικής ταυτοποίησης του χρήστη στο παρελθόν (π.χ. για την εκχώρηση κωδικού πρόσβασης ή λογαριασμού e-mail) τότε δεν είναι απαραίτητη η επανάληψη της διαδικασίας, αλλά θεωρείται αρκετή μία τυπική επιβεβαίωση της αίτησης μέσω της πιστοποιημένης διεύθυνσης ηλεκτρονικής αλληλογραφίας.

Τα πιστοποιητικά αυτής της κλάσης περιέχουν ένα επιπλέον πεδίο οργανωτικής μονάδας (OU) στο πεδίο του αντικειμένου με τιμή 'Users-Secure Class – Personal Identity Verified'.

6.1.1. **USERS - BASE:** Βασική ταυτοποίηση μόνο μέσω e-mail ή και υπηρεσίας ευρετηρίου, χωρίς απαίτηση φυσικής παρουσίας.

Σε αυτή την περίπτωση δεν πραγματοποιείται ασφαλής έλεγχος της ταυτότητας του φυσικού προσώπου. Η έκδοση του πιστοποιητικού γίνεται είτε με απλή σύγκριση των στοιχείων του αιτούντος με τα στοιχεία που τηρούνται στην υπηρεσία καταλόγου του οικείου φορέα, είτε με απλή ανταλλαγή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Ο έλεγχος ταυτότητας από υπηρεσία καταλόγου προτιμάται από τον έλεγχο ταυτότητας μέσω υπηρεσίας ηλεκτρονικού ταχυδρομείου.

Στον έλεγχο ταυτότητας μέσω υπηρεσίας καταλόγου, ο συνδρομητής πρέπει να εισάγει το μυστικό κωδικό που έχει αποκτήσει στην υπηρεσία καταλόγου από τον οικείο φορέα του, ώστε να αποκτήσει δικαίωμα αποστολής της αίτησης πιστοποίησης, μέσω σχετικής ιστοσελίδας ή άλλης εφαρμογής.

Στον έλεγχο ταυτότητας μέσω υπηρεσίας ηλεκτρονικού ταχυδρομείου, αποστέλλεται στην διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη μήνυμα με σύνδεσμο σε ιστοσελίδα και μυστικό κωδικό πρόσβασης. Ζητείται από τον συνδρομητή να συνδεθεί στη συγκεκριμένη σελίδα για να επιβεβαιωθεί ότι κατέχει πρόσβαση στη διεύθυνση ηλεκτρονικού ταχυδρομείου.

Η κλάση πιστοποιητικών USERS - BASE δεν παρέχει τα εχέγγυα ασφαλούς ταυτοποίησης του υποκειμένου του πιστοποιητικού, και δεν μπορεί να χρησιμοποιηθεί σε περιπτώσεις όπως η μη - άρνηση υπογραφής ή η ασφαλής αυθεντικοποίηση χρήστη. Η χρήση αυτής της κλάσης πιστοποιητικών προτείνεται για δοκιμαστικούς μόνο λόγους.

Τα πιστοποιητικά αυτής της κλάσης περιέχουν ένα επιπλέον πεδίο οργανωτικής μονάδας (OU) στο πεδίο του αντικειμένου με τιμή 'Users-Base Class – Personal Identity NOT Verified'.

6.3. Πιστοποιητικό συσκευής

Το άτομο που δηλώνει υπεύθυνος για τη λειτουργία και τη συμμόρφωση της συσκευής στην πολιτική πιστοποίησης, πρέπει να είναι συνδρομητής πιστοποιητικού που έχει εκδοθεί από ΑΠ η οποία συμμορφώνεται με τη «Πολιτική Πιστοποίησης του ΕΔΕΤ».

Ο συνδρομητής συμπληρώνει την αίτηση για έκδοση πιστοποιητικού σε σελίδα όπου πρέπει να αυθεντικοποιηθεί παρουσιάζοντας το προσωπικό πιστοποιητικό του. Δεν επιτρέπεται η έκδοση πιστοποιητικού για συσκευή φορέα διαφορετικού από τον φορέα στον οποίο ανήκει ο υπεύθυνός του.

6.4. Αιτήματα ανάκλησης

Ισχύουν όσα περιγράφονται παραπάνω. Επιπλέον, η ΑΠ και ο συνδρομητής συμφωνούν κατά την παραλαβή του πιστοποιητικού, μυστικό κωδικό ανάκλησης του πιστοποιητικού. Ο συνδρομητής μπορεί να αιτηθεί την ανάκληση του πιστοποιητικού του μέσω κατάλληλης web διεπαφής, με τη χρήση του μυστικού κωδικού ανάκλησης.

Εναλλακτικά, μπορεί να ζητηθεί ανάκληση πιστοποιητικού με τηλεφωνική επικοινωνία του εγγραφόμενου με την αρμόδια Αρχή Πιστοποίησης και θα πρέπει να ακολουθήσει επιβεβαίωση της ταυτότητάς του.

6.5. Έλεγχοι τεχνικής ασφάλειας

- **Δημιουργία ζεύγους κλειδιών:** Τα κλειδιά της ΑΠ δημιουργούνται από λογισμικό το οποίο είναι εγκατεστημένο στην ΑΠ. Πρέπει να ελέγχεται κατά το χρόνο δημιουργίας των κλειδιών ύπαρξη πληροφοριών για σφάλματα του λογισμικού ή του υλικού που χρησιμοποιείται, που αφορούν τη δημιουργία κλειδιών.

  Τα κλειδιά των εγγραφόμενων δημιουργούνται από το υλικό και το σχετικό λογισμικό στην πλευρά των εγγραφόμενων και παραμένουν κάτω από τον απόλυτο έλεγχο του υποκειμένου, σε όλη τη διάρκεια της ισχύος τους.

- **Παράδοση ιδιωτικού κλειδιού σε οντότητα:** Δεν επιτρέπεται η δημιουργία κλειδιών από οποιαδήποτε οντότητα για λογαριασμό του εγγραφόμενου ή άλλης οντότητας ούτε από την ΑΠ για λογαριασμό των εγγραφόμενων. Δεν επιτρέπεται η παράδοση του ιδιωτικού κλειδιού του εγγραφόμενου σε οποιαδήποτε τρίτη οντότητα.

- **Παράδοση δημόσιου κλειδιού συνδρομητή στην αρχή πιστοποίησης:** Ο εγγραφόμενος υποβάλλει στην αρχή καταχώρισης το δημόσιο κλειδί του μέσω δομημένης αίτησης για έκδοση πιστοποιητικού. Η αίτηση είναι υπογεγραμμένη με το σχετικό ιδιωτικό κλειδί. Η ΑΚ επαληθεύει την ορθότητα της υπογραφής και συμπεραίνει ότι ο αιτών κατέχει πράγματι το σχετικό με την αίτηση ιδιωτικό κλειδί.

- **Παράδοση του δημόσιου κλειδιού της αρχής πιστοποίησης στους χρήστες:** Η ΑΠ παρέχει μηχανισμούς για την ασφαλή παράδοση του ψηφιακού πιστοποιητικού της το οποίο περιέχει το δημόσιο κλειδί της όταν αυτό ζητείται από ενδιαφερόμενες οντότητες. Οι ενδιαφερόμενοι αποστέλλουν αίτηση με ηλεκτρονικό ταχυδρομείο. Η ΑΠ αποστέλλει με ταχυδρομείο σε μαγνητικό μέσο το πιστοποιητικό της, το οποίο εμπεριέχει το δημόσιο κλειδί της. Εναλλακτικά, το πιστοποιητικό της ΑΠ δημοσιοποιείται μέσω ασφαλούς ιστοσελίδας, της οποίας η ταυτότητα πιστοποιείται από διαφορετική έμπιστη τρίτη οντότητα.

6.6. Μεγέθη κλειδιών

Το ελάχιστο επιτρεπτό μέγεθος κλειδιού εγγραφόμενου είναι 512bits για την περίπτωση προσωπικού πιστοποιητικού κλάσης 'USERS - BASE', 1024bits για τις περιπτώσεις προσωπικού πιστοποιητικού κλάσης 'USERS - SECURE' και για πιστοποιητικά συσκευών, 2048bits για πιστοποιητικά Αρχών Πιστοποίησης και 1024bits για όλες τις υπόλοιπες περιπτώσεις (π.χ. πιστοποιητικά για χρήση code-signing ή timestamping).

Σκοπός χρήσης των κλειδιών (ως προς το αντίστοιχο πεδίο του X.509): Οι σκοποί χρήσης ενός κλειδιού αναφέρονται στο σχετικό βασικό πεδίο και στη σχετική επέκταση του πιστοποιητικού τύπου X.509 v3. Οι αναφερόμενοι σκοποί χρήσης του πιστοποιητικού δεν είναι περιοριστικοί (π.χ. μη κρίσιμη επέκταση πιστοποιητικού) αλλά 'προτεινόμενοι'. Ο έλεγχος συμμόρφωσης με τους επιτρεπόμενους σκοπούς χρήσης γίνεται κατά την κρίση των βασιζόμενων μερών.

ΚΕΦΑΛΑΙΟ ΕΒΔΟΜΟ

PGP (Pretty Good Privacy)

Το λογισμικό Pretty Good Privacy (PGP), το οποίο σχεδιάστηκε από τον Phill Zimmerman, είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας για λειτουργικά συστήματα όπως τα MS DOS, Unix, VAX / VMS και για άλλες πλατφόρμες. Το PGP επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο και την ταυτότητα σε συνδυασμό με την ευκολία λειτουργίας.

7.1. Τι είναι το PGP

Διασφάλιση του απορρήτου σημαίνει ότι μόνο αυτός για τον οποίο προορίζεται ένα μήνυμα είναι ικανός και να το διαβάσει. Πιστοποίηση της ταυτότητας σημαίνει ότι μηνύματα που φαίνεται πως έχουν προέλθει από κάποιο άτομο μπορούν να έχουν προέλθει μόνο από αυτό το άτομο.

Ευκολία λειτουργίας σημαίνει ότι η διασφάλιση του απόρρητου και πιστοποίησης της ταυτότητας παρέχονται χωρίς την πολυπλοκότητα της διαχείρισης κλειδιών η οποία σχετίζεται με τη συμβατική κρυπτογραφία. Δεν είναι αναγκαία ασφαλή κανάλια για την ανταλλαγή κλειδιών μεταξύ χρηστών κάτι που κάνει το PGP πολύ ευκολότερο στη χρήση από κάθε άλλο αντίστοιχο πακέτο. Αυτό συμβαίνει διότι το PGP είναι βασισμένο σε μια δυναμική νέα τεχνολογία που καλείται κρυπτογράφηση "δημοσίων κλειδιών" (public key).

Το PGP συνδυάζει την ευκολία του RSA κρυπτοσυστήματος δημοσίων κλειδιών με την ταχύτητα της συμβατικής κρυπτογράφησης, περιλήψεις μηνυμάτων για ψηφιακές υπογραφές, συμπίεση δεδομένων πριν την κρυπτογράφηση, καλός εργονομικός σχεδιασμός και υψηλού επιπέδου διαχείριση κλειδιών. Επιπλέον το PGP εκτελεί τις λειτουργίες των δημοσίων κλειδιών γρηγορότερα από τα περισσότερα αντίστοιχα προγράμματα. Το PGP είναι κρυπτογράφηση δημοσίων κλειδιών για τις μάζες.

Σήμερα εάν η κυβέρνηση θελήσει να παραβιάσει το απόρρητο των πολιτών πρέπει να καταβάλλει ένα συγκεκριμένο ποσό χρημάτων και εργασίας για να υποκλέψει και να διαβάσει το συμβατικό ταχυδρομείο και να ακούσει ή να υποκλέψει τηλεφωνικές συνομιλίες. Αυτός ο τρόπος της παρακολούθησης δεν είναι πρακτικός σε μεγάλο επίπεδο. Αυτό συμβαίνει μόνο σε σημαντικές περιπτώσεις όπου φαίνεται ότι αξίζει.

Όλο και μεγαλύτερο ποσοστό από τις ιδιωτικές μας επικοινωνίες δρομολογείται μέσω ηλεκτρονικών καναλιών. Το ηλεκτρονικό ταχυδρομείο σταδιακά αντικαθιστά το συμβατικό ταχυδρομείο. Τα μηνύματα e-mail είναι πολύ εύκολο να υποκλέπτουν και να περάσουν από διαδικασία ανίχνευσης βάσει καθορισμένων λέξεων - κλειδιών (keywords). Αυτό μπορεί να γίνει εύκολα, αυτόματα και χωρίς να πέσει στην αντίληψη κανενός σε μεγάλο επίπεδο. Οι διεθνείς συνδέσεις βρίσκονται ήδη κάτω από μια τέτοια διαδικασία παρακολούθησης από την NSA.

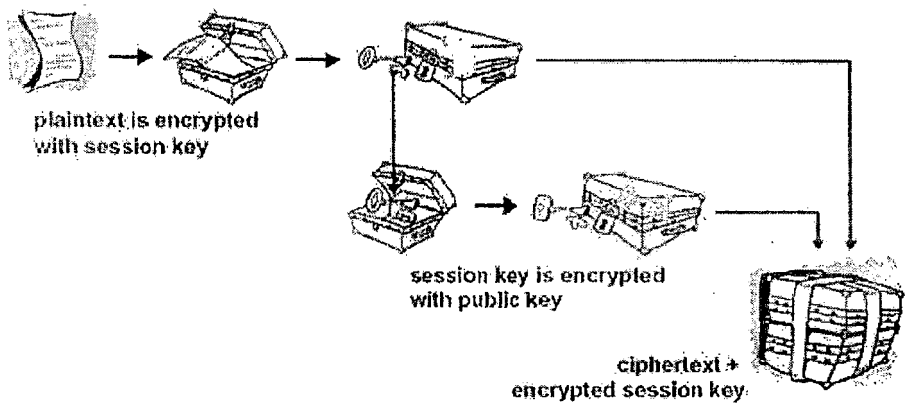
Κινούμαστε προς ένα μέλλον όπου οι υπολογιστές διεθνώς θα ενώνονται με δίκτυα οπτικών ινών υψηλής χωρητικότητας. Το e-mail θα είναι κάτι το αυτονόητο για όλους

και όχι η καινοτομία που θεωρείται σήμερα. Οι κυβερνήσεις θα προστατεύουν το e-mail των πολιτών με πρωτόκολλα σχεδιασμένα από τις ίδιες. Πιθανότατα οι περισσότεροι άνθρωποι θα συμβιβαστούν με αυτή τη λύση αλλά ίσως μερικοί προτιμήσουν να πάρουν τα δικά τους μέτρα ασφάλειας.

7.2. Λειτουργία του PGP

Για να κατανοήσουμε τη λειτουργία του PGP θα πρέπει να αναφέρουμε λίγα λόγια πάνω στην ορολογία που χρησιμοποιείται. Ας θεωρήσουμε ότι θέλει κάποιος να στείλει ένα μήνυμα αλλά δεν θέλει να το διαβάσει κανένας άλλος εκτός από τον παραλήπτη. Μπορεί να το κρυπτογραφήσει με τη χρήση ενός κλειδιού το οποίο θα πρέπει να χρησιμοποιηθεί στην αποκρυπτογράφηση του μηνύματος από τον παραλήπτη του - τουλάχιστον έτσι δουλεύει η συμβατική κρυπτογραφία ενός κλειδιού.

Στην εικόνα 7.1 φαίνεται η λειτουργία του PGP:



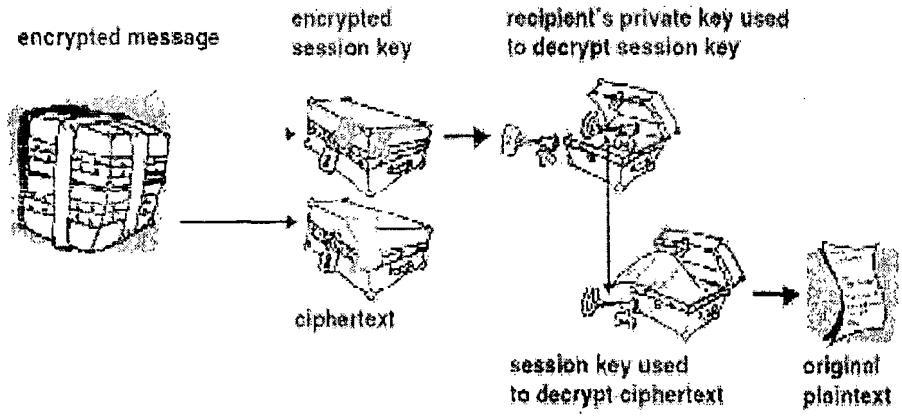
Εικόνα 7.1

Στα συμβατικά κρυπτοσυστήματα, όπως το DES, ένα και μόνο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αυτό σημαίνει ότι το κλειδί θα πρέπει να μεταδοθεί αρχικά μέσα από ένα ασφαλές κανάλι έτσι ώστε και τα δυο μέρη να το γνωρίζουν προτού αρχίσει η αποστολή κρυπτογραφημένων μηνυμάτων μέσω ασφαλών καναλιών. Αυτό δεν είναι και τόσο βολικό διότι αν έχεις ένα ασφαλές κανάλι για να ανταλλάζεις κλειδιά τότε τι χρειάζεσαι την κρυπτογραφία;

Στα κρυπτοσυστήματα δημοσίων κλειδιών ο καθένας έχει δυο συμπληρωματικά κλειδιά. Ένα που δίδεται δημόσια (public key) και ένα μυστικό (secret key ή private key). Το κάθε κλειδί ξεκλειδώνει τον κώδικα που το άλλο φτιάχνει. Η γνώση του δημοσίου κλειδιού δεν βοηθάει στην εξαγωγή του αντίστοιχου μυστικού κλειδιού. Το δημόσιο κλειδί μπορεί να διατεθεί σε ένα δίκτυο επικοινωνιών. Αυτό το πρωτόκολλο παρέχει διασφάλιση του απόρρητου χωρίς την ανάγκη ύπαρξης ασφαλών καναλιών, όπως απαιτεί η συμβατική κρυπτογραφία.

Ο καθένας μπορεί να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη ενός μηνύματος για να κρυπτογραφήσει ένα μήνυμα προς αυτό το άτομο ενώ ο παραλήπτης μπορεί να χρησιμοποιήσει με τη σειρά του το αντίστοιχο μυστικό κλειδί για να αποκρυπτογραφήσει το μήνυμα. Κανένας άλλος εκτός από τον παραλήπτη δεν μπορεί να το αποκρυπτογραφήσει διότι κανένας άλλος δεν έχει πρόσβαση στο μυστικό κλειδί - ακόμη και το άτομο που κρυπτογράφησε το μήνυμα.

Στην εικόνα 7.2 φαίνεται η αποκρυπτογράφηση του PGP:



Εικόνα 7.2

Επίσης παρέχεται η υπηρεσία πιστοποίησης του μηνύματος. Το μυστικό κλειδί του αποστολέα μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση του μηνύματος άρα και για την υπογραφή του. Έτσι δημιουργείται μια ψηφιακή υπογραφή του μηνύματος την οποία ο παραλήπτης ή οποιοσδήποτε άλλος μπορεί να ελέγξει χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα για να την αποκρυπτογραφήσει. Αυτό αποδεικνύει ότι ο αποστολέας ήταν ο πραγματικός δημιουργός του μηνύματος και ότι το μήνυμα δεν αλλοιώθηκε από κάποιον άλλον διότι μόνο ο αποστολέας έχει στην κατοχή του το μυστικό κλειδί που έφτιαξε την υπογραφή. Η πλαστογράφηση ενός υπογεγραμμένου μηνύματος δεν είναι εφικτή και ο αποστολέας δεν μπορεί μετά να απαρνηθεί την υπογραφή του.

Αυτές οι δυο διαδικασίες μπορούν να συνδυαστούν για την παροχή τόσο διασφάλισης του απόρρητου όσο και πιστοποίησης της ταυτότητας αφού μπορεί κάποιος πρώτα να υπογράψει ένα μήνυμα με το μυστικό κλειδί του και μετά να το κρυπτογραφήσει με το δημόσιο κλειδί του παραλήπτη. Ο παραλήπτης αντιστρέφει αυτά τα βήματα αποκρυπτογραφώντας πρώτα το μήνυμα με το μυστικό κλειδί του και κατόπιν ελέγχοντας την ψηφιακή υπογραφή που περιέχεται σε αυτό με το δημόσιο κλειδί του αποστολέα. Αυτές οι διαδικασίες γίνονται αυτόματα από το λογισμικό του παραλήπτη.

Επειδή ο αλγόριθμος της κρυπτογράφησης δημοσίων κλειδιών είναι πολύ πιο αργός από τη συμβατική κρυπτογράφηση ενός κλειδιού η κρυπτογράφηση επιτυγχάνεται καλύτερα με τη χρήση μιας υψηλής ποιότητας γρήγορου αλγόριθμου συμβατικής κρυπτογράφησης ενός κλειδιού για την κρυπτογράφηση του μηνύματος. Το αρχικό μη κρυπτογραφημένο μήνυμα καλείται "απλό κείμενο". Σε μια διαδικασία αόρατη στο χρήστη ένα προσωρινό τυχαίο κλειδί, το οποίο έχει δημιουργηθεί μόνο για τη συγκεκριμένη φορά, χρησιμοποιείται για να κρυπτογραφηθεί συμβατικά το αρχείο "απλό κείμενο". Μετά το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για να κρυπτογραφηθεί αυτό το προσωρινό κλειδί. Αυτό το συμβατικά δημιουργημένο κλειδί μιας φοράς (session key) το οποίο έχει κρυπτογραφηθεί και με τη διαδικασία του δημόσιου κλειδιού αποστέλλεται μαζί με το κρυπτογραφημένο κείμενο (κρυπτοκείμενο) στον παραλήπτη. Ο παραλήπτης χρησιμοποιεί το δικό του μυστικό κλειδί για να ανακτήσει το session key και μετά χρησιμοποιεί αυτό κλειδί για να τρέξει τον γρήγορο συμβατικό αλγόριθμο ενός κλειδιού έτσι ώστε να αποκρυπτογραφήσει το κρυπτοκείμενο.

Τα δημόσια κλειδιά φυλάσσονται σε ξεχωριστά πιστοποιητικά κλειδιών (key certificates) τα οποία περιλαμβάνουν την ταυτότητα του ιδιοκτήτη τους (το όνομα του ιδιοκτήτη), μια σφραγίδα χρόνου που δείχνει πότε το ζεύγος των κλειδιών δημιουργήθηκε και τέλος το ίδιο το υλικό του κλειδιού. Τα πιστοποιητικά δημοσίων κλειδιών περιλαμβάνουν το υλικό των δημοσίων κλειδιών ενώ τα πιστοποιητικά των μυστικών κλειδιών περιλαμβάνουν το υλικό των μυστικών κλειδιών. Κάθε μυστικό κλειδί κρυπτογραφείται επιπλέον με τον κωδικό του σε περίπτωση που κλαπεί. Ένα αρχείο κλειδιών ή ένα μπρελόκ κλειδιών (key ring) περιέχει ένα ή περισσότερα από αυτά τα πιστοποιητικά κλειδιών. Τα δημόσια μπρελόκ περιέχουν τα δημόσια πιστοποιητικά κλειδιών ενώ τα ιδιωτικά μπρελόκ περιέχουν τα ιδιωτικά πιστοποιητικά κλειδιά.

Τα κλειδιά χαρακτηρίζονται από ένα "key id" (ταυτότητα κλειδιού) η οποία είναι μια συντομογραφία του δημόσιου κλειδιού (τα 64 λιγότερο σημαντικά bits του δημοσίου κλειδιού). Όταν αυτή η ταυτότητα παρουσιάζεται μόνο τα 32 λιγότερο σημαντικά bits δίνονται για επιπλέον ελαχιστοποίηση του όγκου της ταυτότητας. Καθώς πολλά κλειδιά μπορεί να μοιράζονται το ίδιο user id (ταυτότητα χρήστη), για πρακτικούς λόγους κανένα κλειδί δεν μοιράζεται το ίδιο key id με κανένα άλλο.

Το PGP χρησιμοποιεί τις περιλήψεις μηνυμάτων (message digests) για να δημιουργήσει υπογραφές. Μια περίληψη μηνύματος είναι μια κρυπτογραφικά πολύ δυνατή μονόδρομη (hash) συνάρτηση 128 bit του μηνύματος. Είναι κάτι ανάλογο με το "check sum" ή CRC κώδικα ελέγχου στο ότι αντιπροσωπεύουν συμπαγώς το μήνυμα και χρησιμοποιούνται για την ανίχνευση αλλαγών σε αυτό. Αντίθετα βέβαια με το CRC είναι υπολογιστικά αδύνατο για κάποιον επιτιθέμενο να φτιάξει ένα υποκατάστατο μήνυμα το οποίο θα μπορούσε να παράγει την ίδια περίληψη μηνύματος. Η περίληψη μηνύματος κρυπτογραφείται με το μυστικό κλειδί και έτσι σχηματίζει την ψηφιακή υπογραφή.

Τα κείμενα υπογράφονται με την εισαγωγή στην αρχή τους ψηφιακών πιστοποιητικών υπογραφών οι οποίες περιέχουν το key id του κλειδιού που χρησιμοποιήθηκε για την υπογραφή τους, μια υπογεγραμμένη με το μυστικό κλειδί περίληψη του κειμένου και μια χρονική σφραγίδα της δημιουργίας της υπογραφής. Το key id χρησιμοποιείται από τον παραλήπτη για την ανεύρεση του δημόσιου κλειδιού του αποστολέα έτσι ώστε να ελέγξει την ψηφιακή υπογραφή. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το δημόσιο κλειδί του αποστολέα και το user id του στο μπρελόκ δημοσίων κλειδιών που έχει στην κατοχή του ο παραλήπτης.

Τα κρυπτογραφημένα αρχεία περιέχουν στην αρχή τους το key id του δημοσίου κλειδιού που χρησιμοποιήθηκε στην κρυπτογράφησή τους. Ο παραλήπτης χρησιμοποιεί αυτό το key id για την ανεύρεση του μυστικού κλειδιού που απαιτείται για την αποκρυπτογράφηση του μηνύματος. Το λογισμικό του παραλήπτη αναζητεί αυτόματα το απαραίτητο μυστικό κλειδί αποκρυπτογράφησης στο μπρελόκ μυστικών κλειδιών του παραλήπτη.

Αυτοί οι δυο τύποι μπρελόκ κλειδιών είναι η κύρια μέθοδος της αποθήκευσης και διαχείρισης των δημόσιων και ιδιωτικών κλειδιών. Αντί να κρατάμε ξεχωριστά κλειδιά σε ξεχωριστά αρχεία κλειδιών τα μαζεύουμε σε μπρελόκ κλειδιών έτσι ώστε να διευκολύνουμε την αυτόματη ανεύρεσή τους είτε με τη χρήση του key id είτε με τη χρήση του user id. Κάθε χρήστης διατηρεί το δικό του ζεύγος μπρελόκ. Ένα ξεχωριστό δημόσιο κλειδί αποθηκεύεται προσωρινά σε ένα ξεχωριστό αρχείο μόνο για το χρόνο που χρειάζεται για την αποστολή του σε κάποιο φίλο ο οποίος κατόπιν θα το προσθέσει στο δικό του μπρελόκ κλειδιών.

7.3. Εκδώσεις του PGP

7.3.1. **PGP 1.x (Ιούνιος, 1991):** Παρόλο που χρησιμοποιούσε τον αλγόριθμο δημόσιου κλειδιού RSA για την κρυπτογράφηση, το σχέδιο κρυπτογράφησης του είναι τελείως ασύμβατο με νεώτερες εκδόσεις.

Οι δυνατότητες παραγωγής κλειδιού ήταν:

- 288 bits – περιστασιακή χρήση, γρήγορη αλλά λιγότερο ασφαλής.
- 512 bits – εμπορική χρήση, μέτρια ταχύτητα, καλή ασφάλεια.
- 992 bits – στρατιωτική χρήση, πολύ αργή, υψηλότερη ασφάλεια.

Λειτουργικά Συστήματα: Μόνο DOS και SunOs

Κλειδιά: Χρησιμοποιεί και παράγει μόνο RSA κλειδιά

Κατασκευαστής: Philip Zimmerman (PPGS)

7.3.2. **PGP 2.x:** Αυτές οι εκδόσεις PGP χρησιμοποιούσαν RSA τεχνολογία κρυπτογράφησης για να παράγουν άσπαστα κλειδιά.

Κλειδιά: Διαβάζουν και γράφουν μόνο RSA κλειδιά εκτός από την έκδοση 2.6.4 που διαβάζει και γράφει DH κλειδιά. Από τη 2.3 άλλαξε σταδιακά ο τρόπος που υπογράφονταν τα μηνύματα. Οι πριν τις 2.3 υπογραφές αναγνωρίζονται από την 2.3 ως 4.5 αλλά με κάποια δυσκολία. Η PGP 5 προσπαθεί να εξαλείψει τις υπογραφές αυτές.

7.3.3. **PGP 2.4.x (PPGS ή Viacrypt):** Πρώτη που δημιουργήθηκε από την Viacrypt.

7.3.4. **PGP 2.6.x (PPGS):** Είναι πολύ διάσημες μέχρι σήμερα και διατίθενται για μη – εμπορική χρήση.

- PGP 2.6.3g (US Guerilla Version) (Noel Bell): Χρησιμοποιεί και παράγει RSA κλειδιά 4096 bits.
- PGP 2.6.3ig (International Guerilla version): Συμβατή με την 2.5 και μεταγενέστερες, τρέχει σε μηχανές 286 και 386.
- PGP 2.6.3uin (Georg Bauer): RSA κλειδιά 8192 bits.
- PGP 2.6.3CKT: Κατασκευάστηκε από την Cyber – Knights Templar και χρησιμοποιεί τεράστια RSA κλειδιά.
- PGP 2.6.3ia-multi03: Υποστηρίζει κάποιους αλγόριθμους cipher και μπορεί να δουλέψει με υπογραφές DSS / DH.
- PGP 2.6.4: Δουλεύει σε αντίθεση με τις προηγούμενες εκδόσεις όταν εισάγουμε κλειδιά DSS / DH ή κλειδιά με υπογραφές DSS / DH.

7.3.5. **PGP 4.0 (Viacrypt):** Η έκδοση αυτή χρησιμοποιεί κλειδιά μονής – συνάρτησης που χρησιμοποιούνται τόσο για υπογραφή όσο και για κρυπτογράφηση / αποκρυπτογράφηση. Δεν ήταν κλειδιά γενικού σκοπού όπως αυτά που παρήγαγαν οι προηγούμενες εκδόσεις. Έτσι κάποιος μέσα σε μια εταιρία μπορεί να δημιουργήσει και να δώσει ένα κλειδί στην εταιρία για να διαβάσει τα μηνύματα αλλά η εταιρία δεν μπορεί να πλαστογραφήσει την υπογραφή του υπαλλήλου. Τα μηνύματα που

κρυπτογραφήθηκαν με μονής – συνάρτησης κλειδιά δεν αναγνωρίζονται από τις άλλες παλαιότερες εκδόσεις PGP.

7.3.6. **PGP 4.5:** Υποστηρίζει μόνο RSA κλειδιά και επιπλέον διαθέτει plugs-ins για Netscape 3 και Eudora 3.x.

7.3.7. **PGP 5.0:** Η έκδοση αυτή του PGP καθιέρωσε την χρήση των κλειδιών DH. Οι περισσότερες πλατφόρμες του μπορούν να διαβάσουν τα κλειδιά των εκδόσεων 2.x.

Υπάρχουν 4 προσωπικές εκδόσεις:

- Η δωρεάν έκδοση του MIT χρησιμοποιεί αλλά δεν παράγει RSA κλειδιά.
- Η εμπορική του έκδοση χρησιμοποιεί και παράγει κλειδιά RSA και DH.
- Η έκδοση plug-in για Eudora παρέχει μηδενική υποστήριξη για RSA κλειδιά: δεν επιτρέπει ούτε δημιουργία ούτε χρήση.
- Η αναβαθμισμένη έκδοση για PGP παρέχει την δυνατότητα για δημιουργία και χρήση κλειδιών RSA τουλάχιστον μέχρι την έκδοση 5.3.

7.3.8. **OPEN PGP:** Χρησιμοποιεί σαν βάση την έκδοση PGP 5.x. Οι τεχνολογίες που χρησιμοποιεί είναι οι εξής:

- Ψηφιακές Υπογραφές
- Κρυπτογράφηση
- Συμπίεση
- Μετατροπή Radix-64

Το Open PGP χρησιμοποιεί δύο μεθόδους κρυπτογράφησης για να παρέχει εμπιστευτικότητα – συμμετρική και μη συμμετρική. Με την συμμετρική κρυπτογραφείται το αντικείμενο με έναν συμμετρικό αλγόριθμο κρυπτογράφησης. Κάθε συμμετρικό κλειδί χρησιμοποιείται μόνο μια φορά. Ένα νέο «κλειδί συνόδου» δημιουργείται σαν τυχαίος αριθμός για κάθε μήνυμα. Αφού χρησιμοποιείται μια και μόνο φορά το νέο κλειδί ενσωματώνεται στο μήνυμα και διαβιβάζεται μαζί με αυτό. Προκειμένου να προστατευτεί το «κλειδί συνόδου» κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη.

7.3.9. **PGP 6.0 (NAI):** Αρχικά η NAI εξέδωσε 5 εκδόσεις.

- PGP Desktop Security 6.0.0 DH
- PGP Desktop Security 6.0.0 RSA Add-on
- PGP Personal Privacy 6.0.0 DH
- PGP Personal Privacy 6.0.0 RSA Add-on
- PGP Freeware 6.0.0 DH

Όλες οι εκδόσεις διαβάζουν και παράγουν DH κλειδιά ενώ υπάρχουν ορισμένες που δεν παράγουν αλλά μόνο διαβάζουν κλειδιά RSA. Η NAI έδωσε μεγάλο βάρος στην φιλικότητα προς τον χρήστη π.χ. στις 6.0.x με

την επιλογή "Use Current Window" μπορείς να κρυπτογραφήσεις ένα μήνυμα απευθείας από το πλαίσιο εργασίας σου χωρίς να χρειαστεί να το αποκόψεις να το κρυπτογραφήσει και να το επικολλήσει.

7.3.10. **PGP 6.5:** Τον Απρίλιο του 1999 η NAI εξέδωσε το PGP Desktop Security 6.5 για τα Windows NT ενώ αργότερα για άλλες πλατφόρμες (Win95/98, Macintosh).

Αλλαγές:

- Το PGPNet προστατεύει TCP/IP συνδέσεις, χρησιμοποιεί τα IKE and IPsec internet πρότυπα και δουλεύει με υλικό και λογισμικό με τα ίδια πρότυπα.
- Αυτό – αποκρυπτογράφηση αρχείων για την αποστολή τους σε χρήστες που δεν χρησιμοποιούν PGP.
- Επικύρωση X.509 και CA.
- Προγραμματισμένη εξάλειψη των διαγραμμένων αρχείων από το σκληρό δίσκο για μεγαλύτερη ασφάλεια.
- Ειδικά κουμπιά, όπως για παράδειγμα για την επιλογή "Use Current Window" των εκδόσεων 6.0.

7.3.11. **PGP 7.0 (PGP, Inc):** Κλειδιά: Οι εκδόσεις 7.0.x διαβάζουν και παράγουν RSA και DH κλειδιά.

Χαρακτηριστικά:

- Πολλές ευκολίες για την υποστήριξη του PGP σε επιχειρήσεις. Βελτιωμένη multi – user υποστήριξη για Windows NT/2000.
- Προσωπικό Firewall, προσωπικό σύστημα ανίχνευσης διείσδυσης, Virtual Private Networking.
- Νέα δομή κλειδιού RSA ώστε να υποστηρίζεται το κλειδί ADK (Additional Decryption Key) – "RSA Legacy" key format.
- Επανάκτηση κλειδιού από χαμένα passphrases απαντώντας σε 5 ερωτήσεις που μόνο ο χρήστης γνωρίζει.
- Αρκετές προσθήκες σχετικά με τα πιστοποιητικά X.509.
- Υποστήριξη Twofish.
- Κρυπτογράφηση για ICQ.
- Διάφορες προσθήκες PGPdisk.

7.3.12. **PGP 7.1:** Χαρακτηριστικά

- Βελτιωμένες ικανότητες firewall
- Βελτιωμένες ικανότητες VPN
- Υποστήριξη για αρχεία μεγαλύτερα από 2.5 gigabytes.

7.3.13. **PGP 8.0 (PGP, Inc):** Windows and Mac versions, με 4 μορφές:

- PGP Freeware
- PGP Personal

- PGP Desktop
- PGP Enterprise

7.4. Πρότυπα PGP

- PGP Message Exchange Formats [RFC1991]
- MIME Security with Pretty Good Privacy (PGP)
- OpenPGP Message Format [RFC2440]
- MIME Security with OpenPGP [RFC3156]

7.5. Επίδοση του PGP

Το PGP κρατάει στοιχεία για το ποια από τα δημόσια κλειδιά που έχουμε στην κατοχή μας είναι πιστοποιημένα με υπογραφές που εμπιστευόμαστε. Το μόνο που εμείς πρέπει να κάνουμε είναι να πούμε στο PGP ποιους εμπιστευόμαστε σαν μεσάζοντες και να πιστοποιήσουμε τα κλειδιά τους με το δικό μας. Το PGP αναλαμβάνει από εκεί και πέρα να κρίνει αυτόματα κάποιο δημόσιο κλειδί ως έγκυρο ή όχι.

Πρέπει να διασφαλίσουμε ότι κανένας δεν πρόκειται να αλλοιώσει το μπρελόκ με τα κλειδιά μας. Ο έλεγχος ενός νέου υπογεγραμμένου δημοσίου κλειδιού πρέπει να εξαρτάται ολοκληρωτικά από την ακεραιότητα των κλειδιών τα οποία ήδη έχουμε στο μπρελόκ μας και τα οποία φυσικά εμπιστευόμαστε. Πρέπει να διατηρούμε συνεχή φυσικό έλεγχο των μπρελόκ δημοσίων κλειδιών μας σε κάποιο PC εκτός δικτύου όπως ακριβώς θα κάναμε και με το μυστικό κλειδί μας. Επιπλέον πρέπει να κρατάμε ένα αντίγραφο του δημόσιου και μυστικού κλειδιού μας σε κάποιο προστατευμένο μέσο όπου αποκλείεται ποτέ να τα σβήσουμε κατά λάθος. Από τη στιγμή κατά την οποία το δημόσιο κλειδί μας χρησιμοποιείται ως ο τελικός κριτής για την πιστοποίηση ή μη όλων των άλλων κλειδιών του μπρελόκ είναι σημαντική για την ασφάλεια όλου του συστήματος η διασφάλισή του. Το PGP μπορεί αυτόματα να συγκρίνει το δημόσιο κλειδί μας με ένα αντίγραφό του σε κάποιο προστατευμένο φυσικό μέσο.

Το PGP γενικά θεωρεί ότι διατηρούμε το σύστημά μας, τα μπρελόκ και το PGP ασφαλές σε φυσικό επίπεδο. Εάν κάποιος έχει πρόσβαση στο σκληρό δίσκο του συστήματός μας τότε θεωρητικά μπορεί να αλλοιώσει το ίδιο το PGP έτσι ώστε αυτό να αδυνατεί να ανιχνεύσει οποιαδήποτε αλλοιώσει σε άλλα κλειδιά.

Ένας ακόμα τρόπος να προστατεύσουμε ολόκληρο το μπρελόκ με τα κλειδιά μας είναι να το υπογράψουμε ολόκληρο με το μυστικό μας κλειδί. Βέβαια θα έπρεπε πάλι να έχουμε κάπου αλλού προστατευμένο ένα αντίγραφο του δημοσίου κλειδιού μας για να είμαστε σε θέση να ελέγξουμε την υπογραφή μας. Όπως είναι φυσικό δεν μπορούμε να βασιστούμε στο δημόσιο κλειδί μας, που βρίσκεται στο μπρελόκ, για τον έλεγχο της υπογραφής μας διότι αυτό είναι μέρος αυτού που πάμε να προστατέψουμε.

Παράρτημα Α – Βιβλιογραφία

Παρακάτω αναφέρω τις ιστοσελίδες που επισκέφτηκα στο Internet και τα βιβλία που συμβουλεύτηκα για την συγγραφή αυτής της πτυχιακής.

Υλικό που άντλησα από Web Sites.

Cryptography

- http://eos.uom.gr/~kaklaman/book/Chapters/C11/Cryptography%20and%20its%20products%204.htm
- http://eos.uom.gr/~kaklaman/book/Chapters/C11/C11Header.htm

Dimanast

- http://www.dimanast.gr/modules/news/article.php?storyid=13

Security Manager - Protection

- http://www.securitymanager.gr/protection_email_93.html

LerosNet

- http://www.lerosnet.gr/index-9.html

Wikipedia - SSL

- http://en.wikipedia.org/wiki/SSL

Certificates – Ψηφιακά Πιστοποιητικά

- http://noc.auth.gr/services/personal/certificates/index.html

Ψηφιακές Υπογραφές

- http://www.in.gr/Articles/Article.asp?ArticleId=67351&CurrentTopId=67168&IssueTitle=RAM+144

Microsoft – Security S/MIME

- http://office.microsoft.com/el-gr/assistance/HP052495551032.aspx
- http://www.microsoft.com/resources/howtotell/el-gr/coa.mspx
- http://www.microsoft.com/hellas/athome/security/email/smime.mspx

Grnet - Πιστοποιητικά και Αρχές πιστοποίησης

- http://www.ca.grnet.gr/documents/CPS.html#_Toc83618418

Epmhs - PGP

- http://www.epmhs.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/pgp.htm

Go-Online

- http://www.go-online.gr/ebusiness/specials/article.html?article_id=715

Υλικό που άντλησα από Βιβλία

- Τίτλος Βιβλίου: Ασφάλεια Πληροφοριακών Συστημάτων /Διδάσκων: Καραγιάννης Γιώργος / Διδακτικές σημειώσεις / Έκδοση: Σεπτέμβριος 2003