Διδάσκων:
Ζορκάδης (Χ)

Γεωργίου Χάρης, ΑΜ:4
e-mail: csst9328@cs.uoi.gr

Μακρής Ηλίας. ΑΜ:ΧΧ
e-mail: csst93XX@cs.uoi.gr

Παπαδόπουλος Δημήτρης, ΑΜ:ΧΧ
e-mail: csst9337@cs.uoi.gr

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Εισαγωγική μελέτη θεμάτων ασφάλειας σε περιβάλλον κατανεμημένων πληροφοριακών συστημάτων

Τμήμα Πληροφορικής
Ιωάννινα, Μάιος 1997

Εισαγωγή

Μερικές απειλές για την ασφάλεια των κατανεμημένων συστημάτων είναι προφανείς. Για παράδειγμα σε πολλούς τύπους τοπικών δικτύων είναι εύκολο να δημιουργηθεί ένα πρόγραμμα που να κρατά αντίγραφα των μηνυμάτων που ανταλλάσονται μεταξύ των διαφόρων μερών.

Ένα τέτοιο πρόγραμμα μπορεί να εκτελεστεί σε έναν υπολογιστή που είναι ήδη συνδεδεμένος στο δίκτυο ή σε έναν που διεισδύει σε αυτό μέσα από ένα άλλο σημείο σύνδεσης. Άλλες απειλές είναι πιο έξυπνες, όπως ένα πρόγραμμα που μπορεί να εγκατασταθεί σε ένα file server και να κρατά αντίγραφα εμπιστευτικών πληροφοριών που αποθηκεύουν εκεί οι clients.

Για να εξασφαλισθούμε απέναντι σε τέτοιες απειλές πρέπει να υιοθετήσουμε πολιτικές για ασφάλεια που να έχουν σχεδιαστεί για να εξασφαλίσουν την ασφάλεια των δραστηριοτήτων του συστήματος και μηχανισμοί ασφάλειας πρέπει να αναπτυχθούν για να υλοποιήσουν αυτές τις πολιτικές. Όπως το κλείδωμα μιας πόρτας δεν εξασφαλίζει την ασφάλεια ενός κτιρίου εκτός, αν υπάρχει μια πολιτική χρησιμοποίησής της, έτσι και οι μηχανισμοί για την ασφάλεια που θα δούμε δεν εξασφαλίζουν από μόνοι τους την ασφάλεια ενός συστήματος εκτός αν υπάρχουν πολιτικές για την χρησιμοποίηση τους.

Η διάκριση μεταξύ πολιτικών και μηχανισμών ασφαλείας είναι χρήσιμη για την σχεδίαση ασφαλών συστημάτων, αλλά συχνά είναι δύσκολο να είμαστε σίγουροι ότι κάποιοι μηχανισμοί ασφάλειας εφαρμόζουν πλήρως τις επιθυμητές πολιτικές. Παρακάτω περιγράφεται ένα σενάριο για την προετοιμασία των θεμάτων για τις εξετάσεις σε ένα πανεπιστήμιο. Αυτό το παράδειγμα περιλαμβάνει μια σωστή πολιτική ασφάλειας και μηχανισμούς ασφάλειας που ακούγονται σωστοί.

Έστω ότι ένα κατανεμημένο σύστημα χρησιμοποιείται για την αποθήκευση και μετάδοση των θεμάτων. Τα θέματα θα αποθηκευθούν σε έναν file server, θα εκτυπωθούν σε έναν print server και θα μεταδοθούν από το δίκτυο στους σταθμούς εργασίας των εξεταστών. Πώς μπορεί να εξασφαλιστεί ότι δεν είναι εκτεθειμένα σε μη εξουσιοδοτημένη πρόσβαση;

Θα πρέπει να καταφύγουμε σε μηχανισμούς προστασίας για να διαπιστώνουμε τις πραγματικές ταυτότητες των χρηστών ή των διεργασιών που ζητάνε πρόσβαση στα θέματα. Οι πολιτικές ασφάλειας μπορούν να είναι οι εξής:

- Τα θέματα μπορούν να δούν μόνο τα μέλη του συμβουλίου των εξεταστών.
- Κάθε θέμα μπορεί να αλλάξει μόνο από τον εξεταστή που είναι υπεύθυνος γι αυτό το θέμα.

Εάν τα θέματα ετοιμάζοντα με το χέρι θα μπορούσαν να χρησιμοποιηθούν μέθοδοι για προστασία όπως ιδιωτικά γραφεία, υπογραφές και άλλα. Το συμβούλιο των εξεταστών θα μπορούσε να διαπιστώσει οτι τα θέματα ετοιμάστηκαν σύμφωνα με αυτές τις πολιτικές. Ακόμα όμως και έτσι το συμβούλιο δεν μπορεί να είναι σίγουρο ότι αυτές οι πολιτικές δεν έχουν παραβιαστεί, για παράδειγμα αν κάποιος χρησιμοποιούσε ένα αντικλείδι ή ένα τηλεσκόπιο.

Πώς μπορούν οι χρήστες ενός συστήματος να είναι σίγουροι ότι οι επιλεγμένοι μηχανισμοί ασφάλειας υλοποιούν την πολιτική ασφάλειας; Για το σκοπό αυτό έχουν αναπτυχθεί φορμαλιστικές αποδείξεις, που αποδεικνύουν ότι οι μηχανισμοί ασφαλείας και οι υλοποιήσεις τους εφαρμόζουν σωστά την πολιτική. Τεχνικές αποδείξεων για την ασφάλεια υπολογιστικών συστημάτων είναι αντικείμενο έρευνας.

Η μελέτη αυτή παρουσιάζει και ομαδοποιεί τις κυριότερες απειλές για τα κατανεμημένα συστήματα. Δεν ορίζονται συγκεκριμένες πολιτικές ασφάλειας εφόσον αυτές εξαρτώνται απο τις ανάγκες των χρηστών και των ιδιοκτητών των συστημάτων. Για παράδειγμα οι ανάγκες για ασφάλεια μιας τράπεζας ή ενός κυβερνητικού κτιρίου είναι διαφορετικές από τις ανάγκες μιας μικρής ομάδας ανθρώπων που εργάζονται μαζί.

Οι διαχειριστές και οι χρήστες ευαίσθητων σε θέματα ασφάλειας υπολογιστικών συστημάτων πρέπει να είναι σίγουροι όσο περισσότερο είναι δύνατόν ότι οι μηχανισμοί ασφάλειας που περιλαμβάνουν υλοποιούν σωστά τις πολιτικές ασφάλειας. Αντίθετα, πέρα από την καταστροφή ή απώλεια πληροφοριών από παραβιάσεις, παράπονα μπορούν να διατυπωθούν ενάντια στον διαχειριστή ενός συστήματος που δεν είναι ασφαλές. Για να αποφύγει τέτοια παράπονα, ο διαχειριστής πρέπει να είναι σε θέση να αποδείξει ότι το σύστημα είναι ασφαλές ή να κρατάει κάποιο λογαριασμό για όλες τις ενέργειες σε ένα χρονικό διάστημα. Ένα κοινό πρόβλημα είναι με τις μηχανές αυτόματης συναλλαγής. Οι διάφορες τράπεζες λένε ότι δεν υπάρχει δυνατότητα παραβίασης αυτών των συστημάτων και ότι τα διάφορα συστήματα αυτού του τύπου είναι ασφαλή. Θα μπορούσαν αυτό να το αποδείξουν πιο εύκολα αν πράγματι αυτά τα συστήματα ήταν ασφαλή.

Για να διαπιστώσουν την καταλληλότητα των μηχανισμών προστασίας, οι σχεδιαστές του συστήματος πρέπει πρώτα να δημιουργήσουν μία λίστα με τις απειλές και να δείξουν πώς αυτές αποτρέπονται από τους μηχανισμούς ασφάλειας. Καμιά λίστα από απειλές δεν μπορεί να είναι πλήρης, οπότε πρέπει να χρησιμοποιηθούν και μέθοδοι ελέγχου σε ευαίσθητες εφαρμογές για να αποφευχθούν παραβιάσεις. Αυτός ο έλεγχος μπορεί να βασιστεί σε ένα λογαριασμό κάποιων ευαίσθητων ενεργειών με λεπτομέρειες για τους χρήστες και τις εξουσίες τους.

Πρέπει να χρησιμοποιήσουμε τον όρο αντικείμενο ή μέρος (principal) για να αναφερθούμε στους παράγοντες που προσπελαύνουν πληροφορία ή πόρους σε ένα κατανεμημένο σύστημα. Ένα αντικείμενο είναι είτε ένα πρόσωπο είτε μία διεργασία. Στο μοντέλο ασφάλειας που θα αναπτύξουμε κάθε αντικείμενο έχει ένα όνομα που είναι ανάλογο με τα ονόματα των χρηστών που υπάρχουν σε ένα κεντρικοποιημένο σύστημα και ένα μυστικό κλειδί, που είναι ανάλογο με ένα συνθηματικό. Κάθε αντικείμενο μπορεί να αποκτήσει πρόσβαση σε πόρους. Το κατά πόσο είναι εξουσιοδοτημένοι να το κάνουν αυτό εξαρτάται από τα ονόματα τους και από την δυνατότητα κάθε server να διαπιστώνει την πραγματική ταυτότητα ενός αντικειμένου.

Απειλές

Για να δημιουργήσουμε ένα σύστημα που είναι πραγματικά ασφαλές πρέπει να ομαδοποιήσουμε τις απειλές και τις μεθόδους για την υλοποίηση τους.

- Διαρροή (Leaking): Η συλλογή πληροφοριών απο μη εξουσιοδοτημένους λήπτες.
- Ανακάτεμα (Tampering): Η μη εξουσιοδοτημένη αλλαγή πληροφορίας.
- Κλέψιμο πόρων (Resource stealing): Μη εξουσιοδοτημένη χρησιμοποίηση πόρων του συστήματος.
- Βανδαλισμός (Vandalism): Επέμβαση σε κάποια λειτουργία του συστήματος χωρίς κέρδος για τον δράστη.

Μέθοδοι επίθεσης

Για να παραβιαστεί ένα σύστημα με οποιοδήποτε από τους παραπάνω τρόπους χρειάζεται να υπάρχει πρόσβαση στο σύστημα. Στα κατανεμημένα συστήματα, οι

υπολογιστές βρίσκονται πάνω σε ένα δίκτυο που επιτρέπει την εγκατάσταση ιδεατών καναλιών επικοινωνίας.

Οι μέθοδοι για την πραγματοποίηση παραβιάσεων εξαρτώνται από το αν αποκτάται πρόσβαση σε υπάρχοντα κανάλια επικοινωνίας ή δημιουργούνται κανάλια που συμπεριφέρονται σαν συνδέσεις σε ένα principal με κάποια εξουσία. Αυτές περιλαμβάνουν:

- *Κρυφάκουσμα (Eavesdropping)*: Η απόκτηση αντιγράφων μηνυμάτων χωρίς εξουσιοδότηση. Αυτό μπορεί να γίνει είτε αποκτώντας μηνύματα κατευθείαν από ένα δίκτυο είτε εξετάζοντας αποθηκευμένη πληροφορία που δεν φυλάγεται σωστά. Παράδειγμα, στο Internet ένας σταθμός εργασίας μπορεί να θέσει την διεύθυνσή του ώστε να είναι ίδια με καποιου άλλου υπολογιστή στο δίκτυο και να λαμβάνει έτσι τα μηνύματα που αναφέρονται σε εκείνον.

- *Μεταμφίεση (Masquerading)*: Στέλνοντας ή λαμβάνοντας μηνύματα χρησιμοποιώντας την ταυτότητα ενός άλλου principal. Αυτό μπορεί να γίνει αποκτώντας την ταυτότητα και και το συνθηματικό κάποιου άλλου principal.

- *Ανακάτεμα μηνυμάτων (Message tampering)*: Κατακρατώντας μηνύματα και αλλάζοντας το περιεχόμενο τους πριν αυτά περάσουν στον προορισμό τους. Αυτό είναι δύσκολο να γίνει σε ένα δίκτυο όπως το Ethernet όπου τα μηνύματα ακούγονται από όλους τους υπολογιστές, αλλά είναι πολύ εύκολο να γίνει σε store-and-forward δίκτυα.

- *Επανάληψη (Relaying)*: Αποθηκεύοντας μηνύματα και στέλνοντας τα αργότερα, για παράδειγμα, αφού έχει ανακληθεί η εξουσιοδότηση για την χρησιμοποίηση ενός πόρου. Δεν μπορεί να αντιμετωπιστεί με απλή κρυπτογράφηση αφού μια τέτοιου είδους παραβίαση μπορεί να γίνει κι αν ακόμα τα μηνύματα δεν μπορουν να διαβαστούν απο τον δράστη.

Διείσδυση

Για να εξαπολύσει τέτοιου είδους επιθέσεις, ο επιτιθέμενος πρέπει να έχει πρόσβαση στο σύστημα για να τρέξει το πρόγραμμα που υλοποιεί την απειλή. Γι'αυτό η περισσότερες επιθέσεις γίνονται απο τους νόμιμους χρήστες ενός συστήματος που χρησιμοποιούν την δικαιοδοσία τους για να εκτελέσουν τέτοια

προγράμματα. Αν υπάρχουν μηχανισμοί για την πρόσβαση και τον έλεγχο της ταυτότητας των χρηστών, δεν θα μπορέσουν να πάνε πολύ μακριά, αλλά είναι για τους διαχειριστές να εγγυηθούν ότι αυτό θα συμβαίνει πάντα.

Για μη νόμιμους χρήστες μια απλή μέθοδος διείσδυσης είναι με το μαντέυουν συνθηματικά ή να χρησιμοποιούν προγράμματα για «σπάσιμο» συνθηματικών. Αυτού του είδους οι επιθέσεις μπορούν να αποφευχθούν με την χρησιμοποίηση καλά επιλεγμένων συνθηματικών.

Σε αντίθεση με αυτές τις ευθείς μορφές διείσδυσης, υπάρχουν διάφορες πιο έξυπνες μέθοδοι που είναι αρκετά γνωστές εξαιτίας της δημοσιότητας που γνώρισαν επιτυχημένες επιθέσεις που χρησιμοποίησαν αυτές τις μεθόδους. Αυτές περιλαμβάνουν:

- *Ιός (Virus)*. Είναι ένα προγράμμα που προσκολάται σε ένα νόμιμο πρόγραμμα και εγκαθίσταται στο περιβάλλον του στόχου όποτε τρέξει το πρόγραμμα που το «φιλοξενεί». Αφού ένα πρόγραμμα τέτοιου είδους εγκατασταθεί, υλοποιεί τις εγκληματικές του πράξεις όποτε θέλει, συνήθως σε μία συγκεκριμένη ημερομηνία. Όπως λέει και το όνομα του, μία απο τις ενέργειες του είναι να αντιγράφεται και να προσκολάται σε όλα τα προγράμματα που βρίσκει στο περιβαλλον του στόχου. Μετακινείται από μηχανή σε μηχανή μαζί με το πρόγραμμα που το «φιλοξενεί», είτε μέσω του δικτύου είτε μέσω της μεταφοράς της φυσικής αποθήκευσης (floppy disks). Υπάρχουν πολλά γνωστά παραδείγματα για συστήματα προσωπικών υπολογιστών (PC).

- *Σκουλίκι (Worm)*: Ένα πρόγραμμα που εκμεταλλεύεται ευκολίες για να τρέχει διεργασίες σε μακρινά συστήματα. Τέτοια προγράμματα μπορούν να δημιουργηθούν τυχαία όπως και από σκοπιμότητα: Το Internet worm εκμεταλλεύτηκε ένα συνδυασμό από τύχαία και σκόπιμα χαρακτηριστικά για να τρέξει προγράμματα από μακριά σε BSD UNIX συστήματα.

- *Δούρειος ίππος (Trojan horse)*. Ένα πρόγραμμα που, ενώ εξωτερικά φαίνεται να κάνει κάτι κάλο, εσωτερικά κάνει και μια δεύτερη «ύπουλη» ενέργεια. Το πιο κοινό παράδειγμα είναι το «spoof login» που, ενώ δεν διαφέρει στην «όψη» από ενα κοινό login-validation πρόγραμμα, στην πραγματικότητα αποθηκεύει την είσοδο του χρήστη σε ένα αρχείο για κατοπινή παράνομη χρήση. Ένα τέτοιο πρόγραμμα μπορεί να τρέχει σε

ένα workstation που δεν παράκολουθείται τόσο συχνά και να προσομοιώνει την συμπεριφορά μιας μηχανής που κανείς δεν έχει κάνει login.

Τα ονόματα των παραπάνω μεθόδων έχουν πάρει κάποια δημοσιότητα, αλλα πρεπει να υπογραμμιστεί ότι δεν είναι όλα τα προγράμματα αυτών των είδών καταστροφικά και στην πραγματικότητα το worm έχει επιτυχημένα χρησιμοποιηθεί ως ένας μηχανισμός για την κατανομή υπολογιστικών εργασιών σε κατανεμημένα συστήματα.

Ένα συμπέρασμα από την παραπάνω συζήτηση για τις απειλές και τις μεθόδους επίθεσης είναι ότι για να παράγουμε ένα ασφαλές κατανεμημένο σύστημα, πρέπει να σχεδιάσουμε τα συστατικά του συστήματος (για παράδειγμα, clients και servers) με την υπόθεση ότι τα άλλα μέρη (άνθρωποι ή μηχανές) είναι αναξιόπιστα μέχρι της αποδείξεως του αντιθέτου.

Δυστυχως, όμως, είναι αδύνατον να σχεδιάσουμε ένα σύστημα που να μην έχει αξιόπιστα συστατικά. Για το λόγο αυτό σχεδιάζουμε ένα σύστημα που το ελάχιστο των συστατικών του να είναι αξιόπιστα. Ο Lampson αναφέρεται σε αυτό ως «trusted computing base».

Δοθέντος μίας ελάχιστης εμπιστευτικής βάσης, μπορούμε να σχεδιάσουμε ασφαλείς servers. Η ασφάλεια αυτών των servers μπορεί να επιτευχθεί με έναν συνδυασμό φυσικού ελέγχου και ασφαλών καναλιών επικοινωνίας προστατευόμενων με επαλήθευση (authentication) και κρυπτογράφηση.

Μπορούμε, λοιπόν, τώρα να συνοψίσουμε την παραπάνω συζήτηση για τις απειλές της ασφάλειας σε κατανεμημένα συστήματα.

Οι απειλές για την ασφάλεια σε κατανεμημένα συστήματα προέρχονται από το γεγονός ότι τα διάφορα επικοινωνιακά κανάλια είναι τρωτά σε διάφορες επιθέσεις. Πρέπει να θεωρήσουμε ότι κάθε εποικινονιακό κανάλι σε όλα τα επίπεδα του υλικού και του λογισμικού είναι επικίνδυνα για τέτοιες απειλές.

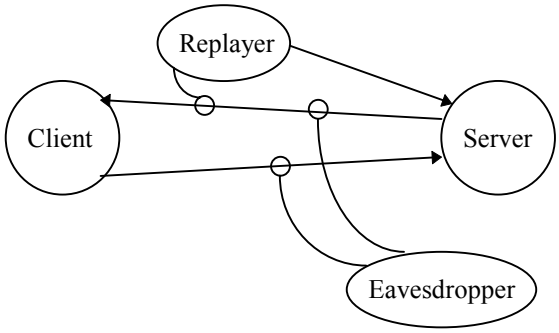
Οι διάφοροι παραβάτες (άνθρωποι ή προγράμματα) δεν αναγνωρίζονται εύκολα, οπότε πρέπει να υιοθετήσουμε μία όψη του κόσμου που δεν εμπνέει εμπιστοσύνη. Πρέπει, όμως, να ξεκινήσουμε από κάποια αξιόπιστα συστατικά ώστε να φτιάξουμε ένα χρήσιμο σύστημα. Ένας τρόπος είναι να θεωρήσουμε τα πάντα που επικοινωνούν αναξιόπιστα μέχρι να αποδειχτεί το αντίθετο. Η αξιοπιστία των άλλων

μερών που επικοινωνούν πρέπει να έχει αποδειχτεί όποτε χρησιμοποιείται ένα επικοινωνιακό κανάλι.

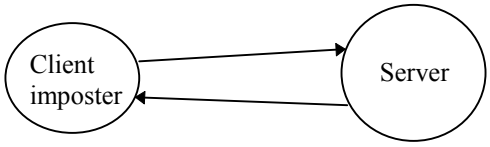
Οι μηχανισμοί που θα χρησιμοποιηθούν για την υλοποίηση της ασφάλειας πρέπει να έχουν την εγκυρότητα ενός προτύπου. Για παράδειγμα, τα ασφαλή επικοινωνιακά πρωτόκολλα και οι υλοποιήσεις τους σε λογισμικό πρέπει να αποδεικνύονται σωστά για όλες τις δυνατές ακολουθίες μηνυμάτων.

Σενάρια

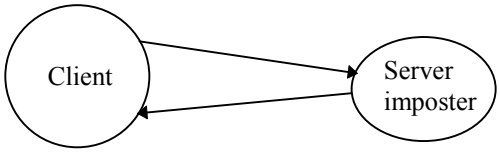
Το παρακάτω σχήμα δείχνει έναν αριθμό σεναρίων για παραβιάσεις της ασφάλειας στην επικοινωνία client-server. Στην πρώτη περίπτωση, η επικοινωνία ανάμεσα σε έναν νόμιμο client και σε έναν νόμιμο server είναι τρωτή στο κρυφάκουσμα που μπορεί να έχει ως αποτέλεσμα την διαρροή ιδιωτικών πληροφοριών και την αντιγραφή των μηνυμάτων από κρυφακουστές. Στη δεύτερη περίπτωση, ένας νόμιμος server είναι τρωτός σε ψεύτικους clients, που μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε υπηρεσίες του server και να αλλάξουν την κατάσταση του server ή να αποκτήσουν ελεύθερη πρόσβαση σε κάθε ιδιωτική πληροφορία που κρατείται στο server. Ένας νόμιμος server είναι τρωτός σε επαναλήψεις των μηνυμάτων που έχουν σταλθεί νωρίτερα από νόμιμους clients ώστε να αλλάξει η κατάσταση του server π.χ να επανακτήσει την ισορροπία σε ενός λογαριασμού σε μία τράπεζα κι αν ακόμα έχουν γίνει αναλήψεις στην διάρκεια της ημέρας ή απλά να υπερφορτώσει τον server. Τέλος, στην τρίτη περίπτωση, παρουσιάζεται πώς ένας νόμιμος client είναι τρωτός σε ψεύτικους servers. Ένας ψεύτικος server μπορεί να αποκτήσει πρόσβαση σε ιδιωτική πληροφορία και μπορεί να ξεγελάσει τον client ώστε αυτός να πιστέψει τις αιτούμενες συναλλαγές. Για παράδειγμα να χρεώσει έναν λογαριασμό σε τράπεζα έχει γίνει χωρίς όμως να έχει γίνει πραγματικά.



(α)



(β)



(γ)

ΣΧΗΜΑ - XXX

Εισηγήσεις για την ασφάλεια σε ένα client-server σύστημα

Για να αποφευχθούν παραβιάσεις του προηγούμενου τύπου, πρέπει:

- Να ασφαλίσουμε τα διάφορα επικοινωνιακά κανάλια ώστε να αποφύγουμε το κρυφάκουσμα.
- Να σχεδιάσουμε clients και servers που βλέπουν ο ένας τον άλλο με αμοιβαία καχυποψία και να εκτελούν τις κατάλληλες ανταλλαγές μηνυμάτων (πρωτόκολλο αυθεντικοποίησης) για να επιτευχθον τα εξής:

    1. Οι servers πρέπει να είναι ικανοποιημένοι ότι οι clients ενεργούν εκ μέρους των principals που ισχύρίζονται.

    2. Οι clients πρέπει να είναι ικανοποιημένοι ότι οι servers που παρέχουν κάποιες υπηρεσίες είναι οι αυθεντικοί servers γι'αυτές τις υπηρεσίες.

- Να εγγυηθούμε ότι η επικοινωνία είναι φρέσκια για να αποφύγουμε παραβιάσεις μέσω κατακράτησης των μυνημάτων.

Οι μηχανισμοί ασφάλειας για κατανεμημένα συστήματα στηρίζονται σε τρείς τεχνικές: κρυπτογραφία, αυθεντικοποίηση και έλεγχος πρόσβασης.

Κρυπτογραφία

Η κρυπτογράφηση των μηνυμάτων διαδραματίζει τρεις ρόλους στην ανάπτυξη ασφαλών συστημάτων:

- Χρησιμοποιείται για να κρύψει ιδιωτική πληροφορία όπου είναι εκθετημένη σε μέρη του συστήματος όπως επικοινωνιακά κανάλια, που είναι τρωτά σε κρυφάκουσμα και ανακάτεμα μηνυμάτων. Η χρήση της κρυπτογράφησης αντιστοιχεί στην παραδοσιακή χρήση της στις στρατιωτικές και μυστικές υπηρεσίες. Εκμεταλλεύεται το γεγονός ότι ένα μήνυμα κρυπτογραφείται με ένα συγκεκριμένο κλειδί κρυπτογράφησης μπορεί να κρυπτογραφηθεί μόνο από έναν λήπτη που ξέρει το αντίστροφο κλειδί.

- Χρησιμοποιείται για υποστήριξη μηχανισμών για αυθεντικοποίηση της επικοινωνίας μεταξύ δύο principals. Ένα principal που αποκρυπτογραφεί ένα μήνυμα χρησιμοποιώντας ένα συγκεκριμένο αντίστροφο κλειδί μπορεί να υποθέσει ότι το μήνυμα είναι πραγματικό εάν περιλαμβάνει κάποια αναμενόμενη τιμή. Είναι απίθανο να αποκρυπτογραφήσει ένα μήνυμα με κάποιο άλλο κλειδί και έτσι ο λήπτης του μηνύματος μπορεί να υποθέσει ότι ο αποστολέας κατέχει το κατάλληλο κρυπτογραφικό κλειδί. Έτσι αν τα κλειδιά κρατούνται ιδιωτικά, μία επιτυχημένη αποκρυπτογράφηση αυθεντικοποιεί ότι το μύνημα που αποκρυπτογραφείται έρχεται από τον κατάλληλο αποστολέα.

- Χρησιμοποιείται για να υλοποιήσει έναν μηχανισμό που λέγεται «ψηφιακή υπογραφή». Αυτός ο μηχανισμός προσομοιώνει τον ρόλο των συμβατικών υπογραφών, πιστοποιώντας σε ένα τρίτο μέρος ότι ένα μήνυμα είναι ένα αυθεντικό αντίγραφο κάποιου που παρήχθηκε απο ένα συγκεκριμένο μέρος. Η δυνατότητα να οριστούν ψηφιακές υπογραφές εξαρτάται από το αν υπάρχει κάτι που μπορεί να κάνει μόνο ο αποστολέας. Αυτό μπορεί να επιτευχθεί απο ένα τρίτο αξιόπιστο μέρος που έχει αποδείξεις για την ταυτότητα του αιτούμενου, να κρυπτογραφήσει το μήνυμα ή για πιο ευκολία να κρυπτογραφήσει μια σύντομη μορφή του μηνύματος που λέγεται περίληψη και είναι ανάλογη με ένα άθροισμα ελέγχου. Το αποτέλεσμα ενεργεί σαν μία υπογραφή που συνοδεύει το μήνυμα. Μπορεί να αποδειχθεί από κάθε λήπτη ρωτώντας το ίδιο αξιόπιστο μέρος να ξανακρυπτογραφήσει το μήνυμα. Αν τα αποτελέσματα συμφωνούν, η υπογραφή έχει επιβεβαιωθεί.

Μηχανισμοί αυθεντικοποίησης

Σε κεντρικοποιημένα συστήματα πολλαπλών χρηστών η ταυτότητα του χρήστη μπορεί να επιβεβαιωθεί με ένα συνθηματικό στην αρχή κάθε συνόδου. Αυτή η προσέγγιση ακολουθείται εξαιτίας του ελέγχου που ασκεί ο πυρήνας του συστήματος πάνω στους πόρους, εμποδίζοντας όλες τις απόπειρες να δημιουργηθούν νέες συνόδοι που συμπεριφέρονται σαν άλλοι χρήστες. Τέτοιος, όμως, βαθμός κεντρικού ελέγχου στους πόρους ενός συστήματος είναι δύσκολος, αν όχι αδύνατος, σε ένα κατανεμημένο σύστημα.

Στα κατανεμημένα συστήματα, η αυθεντικοποίηση είναι η μέθοδος για την απόδειξη των πραγματικών ταυτοτήτων των εξυπηρετητών και των εξυπηρετούμενων. Ο μηχανισμός για να το αποδείξει χρησιμοποιεί την κατοχή των κρυπτογραφικών κλειδιών. Εάν ένα μέρος κατέχει το κατάλληλο κρυπτογραφικό κλειδί, τότε λέμε ότι το μέρος αυτό έχει την ταυτότητα που ισχυρείζεται.

Οι μηχανισμοί για αυθεντικοποίηση πέρνουν την μορφή μιας «υπηρεσίας αυθεντικοποίησης». Οι υπηρεσίες για αυθεντικοποίηση χρησιμοποιούν την χρήση της κρυπτογράφησης για να εγγυθούν την ασφάλεια. Προνοούν για την δημιουργία, αποθήκευση και κατανομή όλων των κρυπτογραφικών κλειδιών που χρειάζονται σε ένα κατανεμημένο σύστημα περισσότερο γνωστή ως υπηρεσία κατανομής κλειδιών.

Στην συνέχεια θα περιγράψουμε τις αρχές πάνω στις οποίες στηρίζονται η αυθεντικοποίηση και η δημιουργία κλειδιών. Θα συζητήσουμε την αποτελεσματικότητα τους στην θεωρία και στην πράξη, χρησιμοποιώντας ως μελέτη τον Kerberos, την πιο πολυχρησιμοποιημένη υλοποίηση.

Μηχανισμοί ελέγχου πρόσβασης

Οι μηχανισμοί ελέγχου πρόσβασης επιχειρούν να εγγυθούν ότι η πρόσβαση στους διάφορους πόρους είναι διαθέσιμοι μόνο σε αυτούς τους χρήστες που είναι εξουσιοδοτημένοι για αυτό το σκοπό.

Οι μηχανισμοί ελέγχου πρόσβασης υπάρχουν μόνο σε μη κατανεμημένα συστήματα πολλαπλών χρηστών. Στο UNIX και σε άλλα συστήματα πολλαπλών χρηστών, τα αρχεία είναι οι πιο απαραίτητοι μοιράσιμοι πόροι, και ένας μηχανισμός ελέγχου έχει αναπτυχθεί για να επιτρέψει σε κάθε χρήστη να διατηρεί κάποια ιδιωτικά αρχεία. Ένας πολύ καλός μηχανισμός για να ελέγχει την πρόσβαση σε αρχεία

υπάρχει στο UNIX, βασισμένος στις λίστες ελέγχου πρόσβασης. Μηχανισμοί για έλεγχο πρόσβασης συζητούνται στη συνέχεια.

Το παρακάτω σχήμα εικονογραφεί τον τρόπο με τον οποίο οι μηχανισμοί ασφάλειας που εξετάστηκαν στις προηγούμενες παραγράφους αλληλεπιδρούν με την υλοποίηση των πολιτικών ασφάλειας.

Πολιτικές Ασφάλειας
(Security policies)

Μηχανισμοί Ελέγχου Πρόσβασης
(Access control mechanisms)

Συναρτήσεις Κρυπτογράφησης
(Encryption functions)

Αυθεντικοποίηση και Υπηρεσίες Διανομής Κλειδιών
(Authentication and key distribution services)

ΣΧΗΜΑ - XXX

Το κύριο μέρος της μελέτης αυτής θα επικεντρωθεί στην περιγραφή, την ανάλυση, την υλοποίηση και την επικύρωση των μηχανισμών ασφάλειας.

ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

1. ΕΙΣΑΓΩΓΗ

Η προσέγγιση της ασφάλειας ενός Πληροφοριακού Συστήματος είναι δυνατό να γίνει με πολλούς και διαφορετικούς τρόπους. Η προσέγγιση, όμως, της κρυπτογραφίας ως βασική στρατηγική φαίνεται να είναι η πιο αποτελεσματική, εξαιτίας δύο χαρακτηριστικών:

- Θεωρητικά, η επιλογή ενός κρυπτογραφικού συστήματος είναι η μόνη που έχει τη δυνατότητα παροχής «απόλυτης εξασφάλισης».
- Η μελέτη κρυπτογραφικών συστημάτων μπορεί να προσφέρει μια εξαιρετικά μεγάλη ποικιλία τεχνικών που έχουν πεδίο εφαρμογής σε κάθε συγκεκριμένο πρόβλημα.

Η βασική ανάγκη που δημιούργησε την ανάπτυξη της κρυπτογραφίας είναι η ανάγκη εξασφάλισης της διαχείρησης της εξουσίας. Η αποκλειστικότητα της κτήσης κάποιας συγκεκριμένης πληροφορίας σε μια συγκεκριμένη χρονική στιγμή είναι δυνατό να εξασφαλίσει στους γνώστες της κάποια «δικαιώματα» ή δυνατότητες που δεν έχουν αυτοί που τις αγνοούν. Χαρακτηριστικό παράδειγμα αποτελεί η ανάγκη ασφαλών επικοινωνιών μεταξύ στρατιωτικών κέντρων διοίκησης σε εμπόλεμη περίοδο.

Τα μέρη που επιθυμούν να ανταλλάξουν κάποιον όγκο πληροφοριών χαρακτηρίζονται ως «πομπός» (αποστολέας) και «δέκτης» (παραλήπτης), ανάλογα με την κατεύθυνση μετάδοσης της πληροφορίας. Η πληροφορίες μεταδίδονται διαμέσου ενός φυσικού μέσου επικοινωνίας, που μπορεί να είναι τεχνικό (επικοινωνιακή σύνδεση) ή φυσικό (αγγελιοφόρος). Σε κάθε περίπτωση, η ανάγκη μεσολάβησης ενός μέσου επικοινωνίας για την μετάδοση και στη συνέχεια την επιβεβαίωση παραλαβής του μηνύματος δημιουργεί αβεβαιότητα σχετικά με την ακεραιότητα, την εγκυρότητα και την εμπιστευτικότητα των πληροφοριών που διακινούνται. Ο μοναδικός τρόπος εξασφάλισης των παραπάνω είναι ο μετασχηματισμός του αρχικού μηνύματος από τον πομπό κατά τέτοιο τρόπο, ώστε μονάχα ο επιθυμητός δέκτης να είναι σε θέση να κατανοήσει την αρχική πληροφορία. Η μελέτη σχετικά με την εφικτότητα και τις τεχνικές που εξασφαλίζουν τις παραπάνω απαιτήσεις (εως κάποιο βαθμό) αποτελούν αντικείμενο της κρυπτογραφίας. Η αντίστροφη διαδικασία, όπου κάποιος δέκτης αναδημιουργεί το αρχικό μήνυμα, είτε

επειδή γνωρίζει τη μέθοδο είτε επειδή την εντοπίζει με ειδικές τεχνικές, ονομάζεται κρυπτανάλυση.

Παρά τη γενικότητα του προβλήματος, οι εφαρμογές της κρυπτογραφίας εως σήμερα περιορίζονται κυρίως στη χρήση σε διπλωματικές και στρατιωτικές επικοινωνίες, όμως υπάρχουν αρκετές περιπτώσεις όπου η κρυπτογραφία (και ειδικότερα η κρυπτανάλυση), υποστήριξε σημαντικά επιστημονικά επιτεύγματα. Αναφέρονται, ως παραδείγματα, η αποκρυπτογράφηση της ιερογλυφικής γραφής (Chambollion, 1822) και της Γραμμικής Β' (Ventris, 1952), καθώς και η δυνατότητα εκτίμησης της αυθεντικότητας ενός έργου τέχνης.

Η ανάπτυξη της κρυπτογραφίας στηρίχθηκε αρχικά σε εμπειρικές μεθόδους, για να θεμελιωθεί αργότερα από εργασίες στο πεδίο της Θεωρίας Πληροφοριών του Shannon. Η σημερινή μορφή της οφείλεται κυρίως στις εργασίες των Diffie, Hellman, Denning και άλλων επιστημόνων που ασχολήθηκαν με αυτό τον τομέα.

2. Η ΚΡΥΠΤΟΓΡΑΦΙΑ ΩΣ ΕΦΑΡΜΟΓΗ ΤΗΣ ΘΕΩΡΙΑΣ ΤΗΣ ΠΟΛΥΠΛΟΚΟΤΗΤΑΣ

Παρακάτω εισάγονται μερικές απαραίτητες έννοιες για την ανάλυση και τη θεωρητική μελέτη της κρυπτογραφίας ως εφαρμογή της θεωρίας της πολυπλοκότητας.

Ένα Σύστημα Μυστικότητας (Secrecy System) δημιουργείται όταν δύο ή περισσότερα μέρη που επιθυμούν να επικοινωνήσουν συμφωνούν στην καθιέρωση ενός πρωτοκόλλου, με βάση το οποίο μόνο αυτά τα μέρη θα έχουν τη δυνατότητα να γνωρίζουν το περιεχόμενο της επικοινωνίας τους. Σε περίπτωση που και ο φορέας (medium) του μηνύματος είναι απρόσιτος σε μη εξουσιοδοτημένα μέρη, τότε το σύστημα ονομάζεται Συγκαλυμμένο Σύστημα (Concealed System).

Υποσύνολο των Συγκαλυμμένων Συστημάτων αποτελούν τα Συστήματα Κενού Κρυπτοποιητή (Null Cipher Systems), όπου στα μηνύματα που μεταδίδονται με συμβατικό τρόπο μόνο ένα μέρος τους έχει πραγματική σημασία, ενώ το υπόλοιπο αποτελεί «κέλυφος» για την εξασφάλιση των αρχών του Συστήματος Μυστικότητας. Σε τέτοια συστήματα είναι φανερό ότι κανένα μαθηματικό μοντέλο κρυπτανάλυσης δεν είναι αποτελεσματικό στη γενική περίπτωση.

Τα Συστήματα Μυστικότητας είναι διακριτά, αφού κάθε μήνυμα (m) αποτελεί πεπερασμένη ακολουθία συμβόλων από ένα επίσης πεπερασμένο σύνολο Σ. Κάθε Σύστημα Μυστικότητας αποτελείται από δύο μέρη. Το πρώτο είναι το «σχήμα κρυπτογράφησης» (E) και το δεύτερο είναι το «σχήμα αποκρυπτογράφησης» (D). Το σχήμα κρυπτογράφησης χρησιμοποιείται για να μετασχηματίσουμε το αρχικό μήνυμα m στο αντίστοιχο κρυπτογραφημένο E(m), ενώ το σχήμα D μετασχηματίζει το κρυπτογραφημένο μήνυμα E(m) στο αρχικό D(E(m))=m. Η τελευταία ισότητα αποτελεί τη σημαντικότερη ιδιότητα κάθε Συστήματος Μυστικότητας. Το κρυπτογραφημένο μήνυμα E(m) ονομάζεται «κρυπτομήνυμα» (ciphertext, cryptogram).

Οι τεχνικές που χρησιμοποιούνται για την υλοποίηση του γενικού μοντέλου που προτάθηκε παραπάνω βασίζονται στο μοντέλο που πρότεινε ο Shannon σε εργασία του, όπου αναφέρεται διεξοδικά στη Θεωρία Επικοινωνίας (Communication Theory). Σύμφωνα με το μοντέλο του Shannon, κάθε σχήμα κρυπτογράφησης μπορεί να θεωρηθεί ως γενικευμένη συνάρτηση:

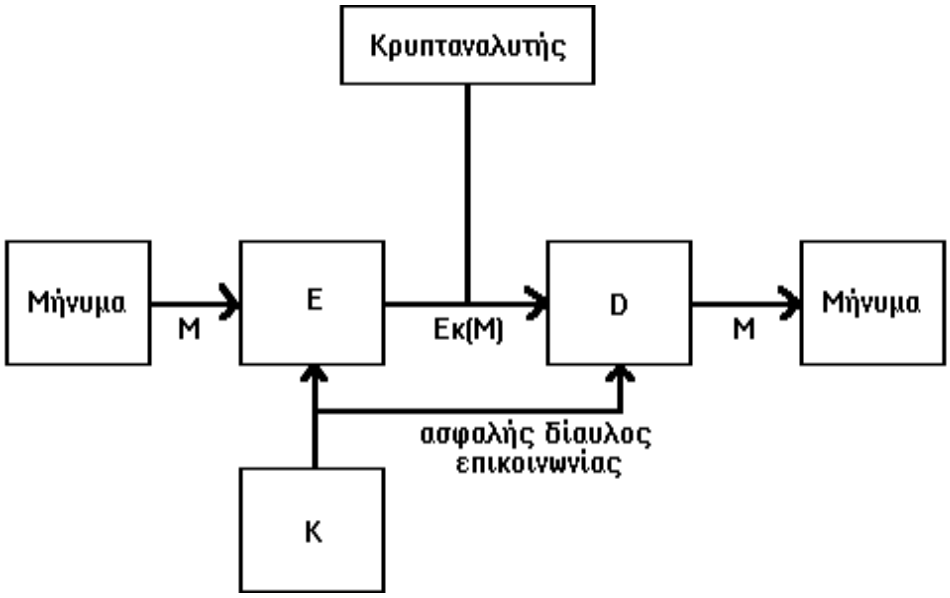
$$E : K \times M \rightarrow C$$

όπου: K είναι το σύνολο των κλειδιών, M είναι το σύνολο των μηνυμάτων και C το σύνολο των κρυπτογραφημένων μηνυμάτων. Το σχήμα αποκρυπτογράφησης μπορεί να οριστεί εντελώς ανάλογα, ως γενικευμένη συνάρτηση:

$$D : K \times C \rightarrow M$$

Υπό άλλη οπτική γωνία, κάθε σχήμα E μπορεί να θεωρηθεί ως σύνολο συναρτήσεων κρυπτογράφησης Ei, από το οποίο επιλέγεται κάθε φορά μία, ανάλογα με το κλειδί. Έτσι, αν το κλειδί είναι το k, τότε η συνάρτηση κρυπτογράφησης είναι η Ek. Αντίστοιχα, το σχήμα D αποτελεί το σύνολο των συναρτήσεων αποκρυπτογράφησης Di και για κλειδί k η συνάρτηση αποκρυπτογράφησης είναι η Dk. Παρατηρούμε ότι υπό αυτή την έννοια, ανεξάρτητα από την επιλογή του κλειδιού, ισχύει η σχέση: $D_i(E_i(m)) = m$.

Θα πρέπει να σημειωθεί ότι στο μοντέλο αυτό απαιτείται η γνώση του κλειδιού k και από τα δύο μέρη, και μάλιστα η απόκτηση του κλειδιού πρέπει να γίνει μέσω ασφαλούς διαύλου επικοινωνίας και όχι μέσω του διαύλου που χρησιμοποιείται για την αποστολή μηνυμάτων, που δεν θεωρείται ασφαλής.



Σχήμα XXX : Μοντέλο κρυπτογράφησης κατά Shannon (secret-key)

Θέλοντας να αξιολογήσουμε τις διάφορες τεχνικές κρυπτογράφησης, θεωρούμε ότι κάθε υποψήφιος κρυπταναλυτής:

- έχει πλήρη γνώση των σχημάτων E και D
- διαθέτει απεριόριστη υπολογιστική ισχύ
- μπορεί να λάβει οποιοδήποτε κρυπτογραφημένο μήνυμα.

Με βάση τα δεδομένα αυτά, υπάρχουν δύο πιθανά σενάρια κρυπτανάλυσης:

- έχοντας διαθέσιμο το $E_k(m)$, απαιτείται η αναδημιουργία του m
- έχοντας διαθέσιμα διαφορετικά $E_k(m)$, απαιτείται ο εντοπισμός του k.

Επειδή τα Συστήματα Μυστικότητας θεωρούνται πεπερασμένα, αυτό σημαίνει ότι τα σύνολα K και M πρέπει να είναι «αρκετά μεγάλα», έτσι ώστε να εξασφαλίζουν την δυσκολία κρυπτανάλυσης και στα δύο πιθανά σενάρια που προαναφέρθηκαν. Ο βαθμός ασφάλειας ενός κρυπτοσυστήματος καθορίζεται από το ποσοστό της πληροφορίας που μπορεί να ανακτηθεί από το κρυπτογραφημένο μήνυμα, χρησιμοποιώντας τεχνικές κρυπτανάλυσης. Στην περίπτωση όπου δεν είναι δυνατή η

ανάκτηση κανενός ποσοστού της αρχικής πληροφορίας από την κρυπτανάλυση του κρυπτογραφήματος, τότε το κρυπτοσύστημα θεωρείται «απόλυτα ασφαλές».

3. ΕΠΙΠΕΔΑ ΚΡΥΠΤΑΣΦΑΛΕΙΑΣ

Στο μοντέλο Shannon υποθέτουμε ότι κάποιος πιθανός κρυπταναλυτής μπορεί να γνωρίζει τόσο το σχήμα κρυπτογράφησης E, όσο και το σχήμα αποκρυπτογράφησης D. Είναι επίσης σε θέση να λαμβάνει κρυπτογραφημένα μηνύματα που αποστέλονται διαμέσου του κοινού μέσου επικοινωνίας. Αυτό που δεν γνωρίζει είναι το αντίστοιχο κλειδί για κάθε κρυπτόγραμμα.

Η προσβολή ενός μηνύματος με τη βοήθεια μόνο κρυπτογραμμάτων ονομάζεται «προσβολή επιπέδου 1». Παράδειγμα μιας τέτοιας προσβολής αποτελεί η παθητική υποκλοπή ενός κρυπτογραφημένου μηνύματος.

Στην περίπτωση όπου ο υποτιθέμενος κρυπταναλυτής έχει στη διάθεσή του τόσο το αρχικό όσο και το κρυπτογραφημένο μήνυμα σε αντιπαραβολή, τότε έχουμε «προσβολή επιπέδου 2». Παράδειγμα μιας τέτοιας προσβολής είναι ο συνδυασμός παθητικής υποκλοπής κρυπτογραφημένου κειμένου και παράλληλα κατοχή και αντιπαράθεση του αρχικού (μη κρυπτογραφημένου) κειμένου.

Τέλος, υπάρχει περίπτωση ο κρυπταναλυτής να είναι νόμιμος (ή όχι) χρήστης του κρυπτογραφικού συστήματος, έχοντας έτσι απεριόριστο πλήθος ζευγαριών αρχικού και κρυπτογραφημένου μηνύματος. Στην περίπτωση αυτή έχουμε «προσβολή επιπέδου 3».

Με βάση τα παραπάνω είναι δυνατό να οριστεί το «επίπεδο κρυπτασφάλειας» ενός Συστήματος Μυστικότητας. Έτσι, κάθε κρυπτογραφικό σύστημα το οποίο είναι «απρόσβλητο» (immune) από προσβολές επιπέδου-i, διαθέτει «κρυπτασφάλεια επιπέδου-I». Για παράδειγμα, ένα κρυπτογραφικό σύστημα που εφαρμόζει γραμμικούς μετασχηματισμούς στα δεδομένα αποτελεί κρυπτοσύστημα με κρυπτασφάλεια επιπέδου 1, αλλά δεν μπορεί να προσφέρει κρυπτασφάλεια επιπέδου 2, γιατί σε περίπτωση προσβολής επιπέδου 2 είναι δυνατή η εφαρμογή μεθόδων επίλυσης γραμμικών μετασχηματισμών για την αποκάλυψη όλων των παραμέτρων (μηνύματα ή/και κλειδιά).

Στην πράξη κανένα κρυπτοσύστημα δεν θεωρείται «επαρκώς ασφαλές», αν δεν μπορεί να προσφέρει κρυπτασφάλεια επιπέδου 2. Το επίπεδο αυτό απελευθερώνει το χρήστη του συστήματος από την ανάγκη διατήρησης της μυστικότητας των μηνυμάτων που έχουν ήδη κρυπτογραφηθεί και μεταδοθεί.

4. ΜΕΘΟΔΟΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Η εξελικτική πορεία των κρυπτοσυστημάτων ανέδειξε ως κομβικά σημεία δύο παραμέτρους: τον αλγόριθμο κρυπτογράφησης και το κλειδί της κρυπτογράφησης. Σύμφωνα με τις δύο αυτές παραμέτρους, τα υπάρχοντα κρυπτογραφικά συστήματα μπορούν να ταξινομηθούν σε δύο κύριες κατηγορίες:

- κρυπτοσυστήματα ενός («ιδιωτικού») κλειδιού ή αλλιώς Συμμετρικά συστήματα
- κρυπτοσυστήματα πολλών («δημόσια γνωστών») κλειδιών ή αλλιώς Ασύμμετρα συστήματα.

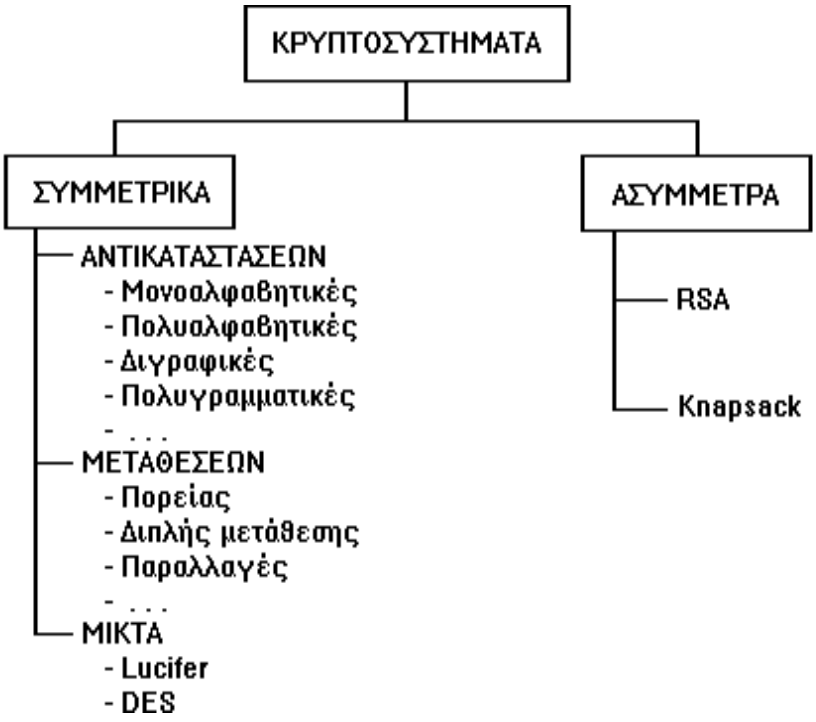
Όπως είναι φανερό, η ασφάλεια των συμμετρικών κρυπτοσυστημάτων εξαρτάται κατά κύριο λόγο από τη δυνατότητα διαφύλαξης της μυστικότητας του μοναδικού κλειδιού που χρησιμοποιείται από τον πομπό και από τον δέκτη. Αντίθετα, στα ασύμμετρα κρυπτοσυστήματα η ασφάλεια στηρίζεται στη φύση της διαδικασίας που ακολουθείται, σύμφωνα με την οποία το κλειδί αποτελείται από δύο επιμέρους κλειδιά, από τα οποία το ένα είναι δημόσια γνωστό και το άλλο άγνωστο (ιδιωτικό).

Τα συμμετρικά κρυπτοσυστήματα είναι, γενικά, πιο διαδεδομένα από τα ασύμμετρα και μπορούν να διαχωριστούν στις εξής επιμέρους κατηγορίες:

- κρυπτοσυστήματα («συμβατικών») αντικαταστάσεων
- κρυπτοσυστήματα μεταθέσεων
- μικτά κρυπτοσυστήματα

Στα συμμετρικά κρυπτοσυστήματα ανήκει και μια ιδιάιτερη κατηγορία συστημάτων, γνωστών ως «κρυπτοσυστημάτων λεξικού κρυπτογράφησης». Στα συστήματα αυτά το κλειδί που χρησιμοποιείται αποτελείται από ολόκληρο το λεξικό (πίνακας) κρυπτογράφησης, το οποίο παραμένει χρονικά αναλλοίωτο. Λόγω της

δυσκολίας διατήρησης και τροποποίησης του λεξικού κρυπτογράφησης, κρυπτοσυστήματα αυτού του τύπου χρησιμοποιούνται ελάχιστα σήμερα.



Σχήμα XXX : Ταξινόμηση των κυριότερων κατηγοριών κρυπτοσυστημάτων

4.1 ΣΥΜΜΕΤΡΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

Όπως αναφέρθηκε παραπάνω, τα συμμετρικά κρυπτοσυστήματα στηρίζονται στη λειτουργία ενός αλγορίθμου κρυπτογράφησης που χρησιμοποιεί κάποιο κλειδί, διαφορετικό για κάθε κρυπτογράφηση, το οποίο είναι γνωστό μόνο στον πομπό και στο «νόμιμο» δέκτη του μηνύματος. Το κλειδί αυτό είναι ακριβώς ένα κάθε φορά και η γνώση του είναι η αναγκαία και ικανή συνθήκη που επιτρέπει την αποκρυπτογράφηση του κρυπτογράμματος, μια και ο αλγόριθμος κρυπτογράφησης θεωρείται δημόσια γνωστός.

Τα πιο συνηθισμένα από τα πρότυπα που ακολουθούν τη βασική αυτή φιλοσοφία είναι αυτά που στηρίζονται σε μεθόδους αντικατάστασης, μετάθεσης ή συνδυασμό των δύο τεχνικών, στα περιεχόμενα του αρχικού μηνύματος.

4.1.1 Μέθοδοι αντικατάστασης

Σύμφωνα με αυτή τη μέθοδο, κάθε σύμβολο του μηνύματος αντικαθιστάται από ένα ή περισσότερα άλλα σύμβολα, σύμφωνα με κάποιο αλγόριθμο. Η αντικατάσταση είναι δυνατό να γίνει χρησιμοποιώντας σύμβολα που δεν εμφανίζονται στο αλφάβητο Μ των μηνυμάτων. Οι πιο διαδεδομένες μέθοδοι αντικατάστασης παρουσιάζονται παρακάτω.

4.1.1.i Μονοαλφαβητικές μέθοδοι

Στη μέθοδο αυτή υπάρχουν δύο αλφάβητα. Το αλφάβητο Μ στο οποίο είναι γραμμένο το αρχικό μήνυμα και το αλφάβητο C στο οποίο μετασχηματίζεται το μήνυμα, δηλαδή το αλφάβητο των κρυπτογραμμάτων. Τα δύο αυτά αλφάβητα μπορούν να ταυτίζονται, όμως κάτι τέτοιο δεν είναι υποχρεωτικό (όπως στην περίπτωση των μεθόδων μετάθεσης). Απαραίτητη προϋπόθεση, όμως, παραμένει η απαίτηση και τα δύο αλφάβητα να περιέχουν το ίδιο πλήθος στοιχείων έτσι ώστε η αντικατάσταση να ορίζεται καλά. Το αλφάβητο Μ ονομάζεται αλφάβητο επικοινωνίας και το C ονομάζεται αλφάβητο μετάδοσης.

Η μονοαλφαβητική μέθοδος στηρίζεται στην 1:1 αντιστοίχιση μεταξύ των στοιχείων των δύο αλφάβητων. Δημιουργείται, δηλαδή, μια «1 προς 1» (και «επί») απεικόνιση των στοιχείων του Μ στο C, με βάση μια συνάρτηση που λαμβάνει υπόψη ως παράμετρο το κλειδί k.

Παράδειγμα μιας τέτοιας μεθόδου αποτελεί το παρακάτω σχήμα:

Αλφάβητο επικοινωνίας Μ: {A,B,C,D,E}

Αλφάβητο μετάδοσης C: {1,2,3,4,5}

Κλειδί k=παράμετρος ολίσθησης

Έτσι, για αρχικό μήνυμα m=AABD και κλειδί k=2, το κρυπτογράφημα υπολογίζεται ολισθάινοντας (μετατοπίζοντας) το αλφάβητο C δεξιά (κατά σύμβαση) κατά δύο θέσεις και αντιστοιχώντας τα γράμματα του m ένα προς ένα στο νέο αλφάβητο C'. Έτσι, το κρυπτογραφημένο μήνυμα είναι: E(m)=3341 .

Η μονοαλφαβητική μέθοδος αναλύεται σχετικά εύκολα. Στην περίπτωση που τα μηνύματα είναι κείμενα και είναι γνωστή η συχνότητα χρήσης των γραμμάτων για τη χρησιμοποιούμενη γλώσσα, τότε είναι δυνατή η αποκρυπτογράφηση μηνυμάτων χωρίς την γνώση του κλειδιού.

Ένα απλό παράδειγμα μονοαλφαβητικής μεθόδου αποτελεί ο ιστορικά γνωστός αλγόριθμος του Καίσαρα. Ο αλγόριθμος αυτός αντικαθιστά κάθε σύμβολο του Λατινικού αλφάβητου με το αντίστοιχο σύμβολο που βρίσκεται μετατοπισμένο κατά ορισμένες θέσεις. Στην πραγματικότητα ο αλγόριθμος αντιστοιχεί τα γράμματα του Λατινικού αλφάβητου στους ακεραιους 1 εως 26, και στη συνέχεια προσθέτοντας +3 και παίρνοντας το υπόλοιπο της ακέραιας διάιρεσης με το 26 (ώστε να μπορεί να γίνει η αντιστοίχιση ξανά στα γράμματα), αντικαθιστά κάθε γράμμα με αυτό που βρίσκεται τρεις θέσεις "μετά". Ο μετασχηματισμός αυτός μπορεί, βέβαια, να γενικευθεί για μετατόπιση κατά κάποιον ακέραιο k (αλγόριθμος Καίσαρα: k=3).

Γενικά, για ένα αλφάβητο επικοινωνίας Μ με (μ) στοιχεία η μονοαλφαβητική μέθοδος προσφέρει Ν=μ! πιθανά σχήματα αντικατάστασης.

4.1.1.ii Πολυγραμματικές μέθοδοι

Η μέθοδος αυτή παρουσιάζει σημαντικές ομοιότητες με την προηγούμενη. Η μοναδική διαφορά είναι ότι κάθε σύμβολο του αλφάβητου επικοινωνίας Μ αντικαθιστάται από περισσότερα του ενός σύμβολα από το αλφάβητο μετάδοσης C. Αυτό σημαίνει αυτόματα ότι τα Μ και C δεν έχουν το ίδιο πλήθος στοιχείων. Στις πολυαλφαβητικές μεθόδους το αλφάβητο μετάδοσης C αποτελείται από κάποιο κατάλληλο πίνακα συμβόλων, στον οποίο όμως θα πρέπει να διασφαλίζεται η μοναδικότητα της σχέσης αντικατάστασης, ώστε να είναι δυνατή η αποκρυπτογράφηση.

Παράδειγμα μιας τέτοιας πολυγραμματικής αντικατάστασης είναι η παρακάτω:

	α	β	γ	δ	ε
1	A	B	C	D	E
2	F	G	H	I	J

Με βάση τον παραπάνω πίνακα αντικατάστασης, το μήνυμα: m=AABD κρυπτογραφείται ως: E(m)=α1α1β1δ1 . Το κλειδί στην περίπτωση αυτή είναι το ζεύγος των λέξεων-κλειδιών «α β γ δ ε» και «1 2», οι οποίες καθορίζουν (έμμεσα) τον

τρόπο αντικατάστασης. Η αντικατάσταση αυτή αποτελεί παράδειγμα δι-αλφαβητικής μεθόδου.

4.1.1.iii N-γραφικές μέθοδοι

Οι δύο προηγούμενες μέθοδοι είναι «μονογραφικές», με την έννοια ότι ένα μόνο σύμβολο του αλφάβητου επικοινωνίας αντικαθιστάται από ένα ή περισσότερα σύμβολα του αλφάβητου μετάδοσης. Έτσι, οι μέθοδοι που ανήκουν στις παραπάνω κατηγορίες είναι ευπαθείς στην κρυπτανάλυση με βάση τις συχνότητες εμφανίσεως των συμβόλων. Οι N-γραφικές μέθοδοι ασχολούνται με την αντικατάσταση συμβόλων κατά ν-άδες, έτσι ώστε να εξαλειφθούν παρόμοια προβλήματα. Οι ν-άδες μπορούν να αποτελούνται από δυάδες (διγραφική), τριάδες (τριγραφική), κ.ο.κ.

Από πρώτη άποψη φάινεται πως για την υλοποίηση μιας N-γραφικής μεθόδου αντικατάστασης για αλφάβητο επικοινωνίας M, απαιτείται η κατασκευή ενός |M|x|M| πίνακα όπου περιέχονται όλες οι δυνατές ν-άδες συμβόλων. Παρόλα αυτά, είναι δυνατή η χρήση πίνακα μικρότερης διάστασης, όπως προτείνεται από το σύστημα Playfair. Σύμφωνα με το σύστημα αυτό είναι δυνατή η χρήση ενός πίνακα διαστάσεων μόνο 5x5 για την υλοποίηση μιας διγραφικής αντικατάστασης. Πιο συγκεκριμένα, αν (π) ένας συνδυασμός (permutation) στο σύνολο αλφαβήτων επικοινωνίας: M^{μ}, όπου: M^{μ}=MxMx...xM (μ φορές), τότε:

$$E(M) = E(X_1X_2...X_{\nu\mu}) = \pi(X_1...X_{\mu}) \times \pi(X_{\mu+1}...X_{2\mu}) \times ... \times \pi(X_{\nu\mu-\mu+1}...X_{\nu\mu})$$

Συνεπώς, υπάρχουν: $|M_{\mu}|$! συνδυασμοί ομάδων συμβόλων. Κάθε τέτοια ομάδα συμβόλων απαρτίζει ένα μ-γράφημα.

Με τις N-γραφικές μεθόδους τα κρυπτογραφημένα μηνύματα διασφαλίζονται απέναντι σε προσπάθεια κρυπτανάλυσης με βάση τις συχνότητες εμφάνισης των συμβόλων. Μια τέτοια ανάλυση μπορεί να γίνει μόνο σε επίπεδο ν-γραμμάτων, δηλαδή συχνότητα εμφάνισης ομάδων των (N) συμβόλων. Κάτι τέτοιο είναι εφικτό για N=2 και N=3, αφού μπορούν εύκολα να υπολογιστούν οι συχνότητες χρήσης διγραμμάτων και τριγραμμάτων για κάποια συγκεκριμένη γλώσσα. Θεωρώντας τις N-γραφικές μεθόδους από Μαθηματική σκοπιά, αποδεικνύεται πως το M αποτελεί μοναδιαίο δακτύλιο και όλοι οι συνδυασμοί ομάδων συμβόλων είναι: $O(|M|_{\kappa})$, $\kappa=\mu^2$. Παρόμοιες μέθοδοι κρυπτογράφησης μελετήθηκαν διεξοδικά για πρώτη φορά από τον L.S.Hill το 1926.

4.1.1.iv Πολυαλφαβητικές μέθοδοι

Η μέθοδος αυτή εφαρμόζεται με τη βοήθεια πολλαπλού αλφάβητου μετάδοσης και σύμφωνα με προκαθορισμένο πρωτόκολλο διαδικασιών. Η πιο γνωστή μορφή της χρησιμοποιεί τον λεγόμενο πίνακα Vigenere, που είναι ένας |M|x|M| πίνακας συμβόλων αντικατάστασης. Σύμφωνα με τη μέθοδο αυτή για να κρυπτογραφηθεί ένα μήνυμα θεωρούμε ότι τα σύμβολα που το αποτελούν βρίσκονται στην πρώτη γραμμή πάνω από τον πίνακα, ενώ τα σύμβολα που αποτελούν το κλειδί βρίσκονται στην πρώτη στήλη αριστερά από τον πίνακα. Τα αντίστοιχα σύμβολα αντικατάστασης βρίσκονται στο σημείο «τομής» της γραμμής και της στήλης που ορίζει το τρέχον σύμβολο του μηνύματος και το τρέχον σύμβολο του κλειδιού. Αν το μήκος του κλειδιού είναι μικρότερο από το μήκος του μηνύματος (όπως συμβαίνει συνήθως), τότε το κλειδί επαναλαμβάνεται κατά μήκος της στήλης μέχρι να καλυφθεί όλος ο πίνακας.

Η μέθοδος αυτή βασίζεται στο εξής μαθηματικό σχήμα:

Αν: $M=X_0X_1...X_v$ το μήνυμα, όπου $X_i \varepsilon \Sigma=\{1,2,...,\mu\}$ και $K=Y_0Y_1..Y_{\kappa-1}$ το κλειδί, όπου $Y_i \varepsilon \Sigma$,

τότε: το κρυπτογραφημένο μήνυμα έχει τη μορφή:

$E_\kappa(M) = X_0'X_1'...X_v'$, όπου: $X_i' = (X_i + Y_{(i) \bmod (\kappa)}) \bmod (\mu)$

Ο αλγόριθμος αυτός πιστευόταν ασφαλής ως το 1863, οπότε ο F.Kasiski δημοσίευσε ένα γενικό αλγόριθμο λύσης. Η πιο ενδιαφέρουσα παραλλαγή του αλγόριθμου του Vigenere είναι αυτή στην οποία το κλειδί δεν επαναλαμβάνεται, ώστε να καλύψει όλο το μήκος του μεταδιδόμενου μηνύματος, αλλά έχει μήκος ίσο με το μήκος του μηνύματος. Στην περίπτωση αυτή το χρησιμοποιούμενο κλειδί είναι μέρος ενός κειμένου περισσότερο, παρά μιας σημειοσειράς. Το κλειδί αυτό λέγεται «τρέχον κλειδί» (running key) και θα μπορούσε να λαμβάνεται από μια εγκυκλοπαίδεια ή θα μπορούσε να δημιουργείται από κάποιο μετασχηματισμό του ίδιου του μηνύματος. Για παράδειγμα, το κλειδί θα μπορούσε να είναι μια μετάθεση του αρχικού μηνύματος, το οποίο στη συνέχεια θα χρησιμοποιούνταν για την κρυπτογράφηση του ίδιου του μηνύματος. Όμως, και για την περίπτωση όπου χρησιμοποιείται κλειδί μήκους ίσο με το μήκος του μηνύματος, ο Kerckhoffs παρουσίασε το 1883 μια γενικευμένη λύση του αλγορίθμου.

Ο αμερικανός μηχανικός G.S.Vernam πρότεινε το 1926 τη χρήση ψευδοτυχαίων κλειδιών. Στο βαθμό που ο αλγόριθμος παραγωγής του κλειδιού δημιουργεί πραγματικά τυχαία κλειδιά, τότε σύμφωνα με το μοντέλο του Shannon η μέθοδος αυτή είναι «απόλυτα ασφαλής». Σε αυτή την περίπτωση το κλειδί χρησιμοποιείται μία φορά και μόνο. Χάρη σε αυτές τις δυνατότητες η μέθοδος χρησιμοποιείται αρκετά σήμερα, με μείωση του μήκους του χρησιμοποιούμενου κλειδιού. Η μείωση αυτή, βέβαια, αναιρεί το χαρακτηρισμό του κρυπτοσυστήματος ως «απόλυτα ασφαλούς».

4.1.2 Μέθοδοι μετάθεσης

Σύμφωνα με αυτές τις μεθόδους το αλφάβητο επικοινωνίας Μ απεικονίζεται στο αλφάβητο μετάδοσης C, το οποίο ταυτίζεται με το Μ. Είναι δηλαδή μια «1 προς 1» απεικόνιση του Μ στον ευατό του. Αυτή η απαίτηση είναι και το κύριο σημείο διαφοροποίησης από τις μεθόδους αντικατάστασης. Μερικές από τις πιο χαρακτηριστικές μεθόδους μετάθεσης παρουσιάζονται συνοπτικά παρακάτω.

4.1.2.i Μετάθεση καθορισμένης πορείας

Σύμφωνα με αυτή τη μέθοδο το μήνυμα διατάσσεται κατά τέτοιο τρόπο, ώστε να σχηματίζει ένα «ορθογώνιο». Στη συνέχεια αναδιατάσσεται σύμφωνα με κάποια καθορισμένη πορεία κίνησης, που διατρέχει όλα τα σύμβολα του «ορθογωνίου» κατά καθορισμένη πορεία. Για παράδειγμα,από το αρχικό μήνυμα, το οποίο έχει τοποθετηθεί «κατά γραμμές» στο ορθογώνιο, θα μπορούσε να δημιουργηθεί το κρυπτογραφημένο παίρνοντας το μήνυμα που σχηματίζεται «διαβάζοντας» το ορθογώνιο κατά στήλες. Η αποκρυπτογράφηση γίνεται ακολουθώντας την αντίθετη πορεία.

Για την σωστή αποκρυπτογράφηση του κρυπτογραφήματος είναι αναγκαία η αποστολή των διαστάσεων του ορθογωνίου μαζί με το μεταδιδόμενο μήνυμα. Πρόβλημα, όμως, δημιουργείται στην περίπτωση που το μήκος του μηνύματος δεν αρκεί για να καλύψει όλο το «εμβαδό» του ορθογωνίου. Στην περίπτωση αυτή, οι υπόλοιπες θέσεις θα πρέπει να συμπληρώνονται με κάποιο καθορισμένο σύμβολο, ενώ μαζί με τις διαστάσεις του ορθογωνίου θα πρέπει να αποστέλεται και το μήκος του πραγματικού μηνύματος (χωρίς τους προστιθέμενους χαρακτήρες), ώστε να είναι δυνατή η σωστή αποκωδικοποίηση του μηνύματος. Η αντιμετώπιση παρόμοιων

περιπτώσεων, καθώς και η μετάδοση επιπλέον συμβόλων κάνει την μέθοδο αυτή προβληματική στην εφαρμογή της.

4.1.2.ii Μέθοδος πολλαπλής μετάθεσης

Αποτελεί επέκταση της προηγούμενης μεθόδου. Το μήνυμα κρυπτογραφείται όπως περιγράφηκε παραπάνω περισσότερες από μία φορές, χρησιμοποιώντας το ίδιο ή διαφορετικό κλειδί, δηλαδή τις ίδιες ή διαφορετικές διαστάσεις ορθογωνίου.

4.1.2.iii Παραλλαγές

Αυτές οι μέθοδοι βασίζονται στην ίδια φιλοσοφία με αυτή της πολλαπλής μετάθεσης. Το μήνυμα κρυπτογραφείται με την ίδια τεχνική σε πολλά επίπεδα, όμως τώρα σε κάθε επίπεδο χρησιμοποιείται διαφορετικό «σχήμα», για παράδειγμα τρίγωνο. Έτσι, κάθε επίπεδο διαφοροποιείται από το προηγούμενο όχι μόνο στο κλειδί (διαστάσεις), αλλά και στον τρόπο κρυπτογράφησης (σχήμα) που χρησιμοποιείται.

4.1.3 Μέθοδοι λεξικού κρυπτογράφησης

Η μέθοδος αυτή καλείται από ορισμένους (H.F.Gaines) ως η «ευγενής των κρυπτοσυστημάτων». Για την υλοποίησή της απαιτείται η ύπαρξη ενός λεξικού (code book), στο οποίο υπάρχουν όλες οι λέξεις, μερικές φράσεις που χρησιμοποιούνται συχνά στο αλφάβητο επικοινωνίας, καθώς και οι αντίστοιχές τους στο αλφάβητο μετάδοσης. Για παράδειγμα, στο λεξικό αυτό υπάρχουν εγγραφές όπως:

Αλφάβητο Επικοινωνίας (M)	**Αλφάβητο Μετάδοσης (C)**
"THE"	2310, 2144, 4279
"MEETING PLACE"	6511
"ATHENS"	4896
"COMPUTER"	2546, 7600

Η λειτουργία της μεθόδου, όπως είναι φανερό, βασίζεται στην αντικατάσταση κάθε λέξης ή φράσης από μία από τις αντίστοιχες που υπάρχουν στο λεξικό. Σημειώνεται ότι κάποιες από τις λέξεις ή φράσεις που χρησιμοποιούνται συχνότερα είναι δυνατό να αντιστοιχεί σε περισσότερες της μιας κρυπτογραφημένες «λέξεις». Το γεγονός αυτό κάνει δυσκολότερη την κρυπτανάλυση με μεθόδους ανάλυσης συχνότητας.

Το κυριότερο μειονέκτημα της μεθόδου είναι η μεγάλη δυσκολία εφαρμογής της, λόγω της μικρής ταχύτητας κρυπτογράφησης ενός κειμένου, καθώς και της δυσκολίας επιλογής και μεταβολής του απαιτούμενου κλειδιού, δηλαδή ολόκληρου του λεξικού. Αυτός είναι και ο λόγος που σήμερα χρησιμοποιείται σε σχετικά περιορισμένη έκταση. Από την άλλη πλευρά, το σημαντικότερο πλεονέκτημα είναι ότι κρυπταναλύεται εξαιρετικά δύσκολα, ιδιαίτερα αν οι συχνότερα εμφανιζόμενες λέξεις και φράσεις κρυπτογραφούνται με περισσότερους από έναν πιθανούς τρόπους. Αυτό οφείλεται κυρίως στο ότι η μέθοδος δεν βασίζεται σε κάποιο φορμαλιστικό σχήμα που μπορεί να προσσεγγιστεί από κάποιο μαθηματικό μοντέλο.

4.1.4 Μικτές μέθοδοι

Το ενδιαφέρον για μικτές μεθόδους κρυπτογράφησης βασίζεται στη γνωστή εργασία του Shannon: «Communication Theory of Secrecy Systems» (1949). Στην εργασία αυτή ο Shannon εισήγαγε την έννοια του μικτού μετασχηματισμού. Η έννοια αυτή βασίζεται στην ιδέα διαδοχικών γινομένων των προηγούμενων μετασχηματισμών. Με την ίδια επίσης εργασία προτάθηκαν για πρώτη φορά οι έννοιες της «σύγχυσης» και της «διάχυσης», με σκοπό την αποτελεσματικότερη σχεδίαση αλγορίθμων κρυπτογράφησης.

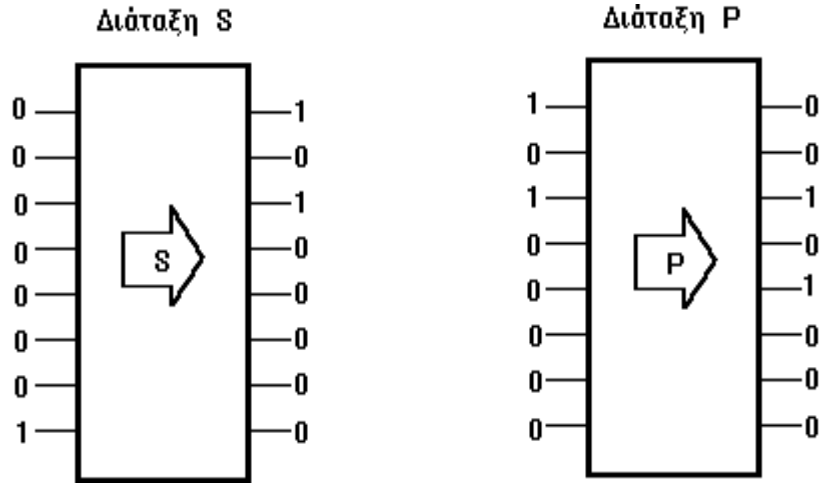
Ένα μικτό κρυπτογραφικό σύστημα αποτελείται στην πράξη από διαδοχικούς συνδυασμούς «διατάξεων S» και «διατάξεων P». Οι διατάξεις αυτές αποτελούνται από ηλεκτρονικά κυκλώματα ή προσομοιώσεις τους, με τη βοήθεια των οποίων υλοποιούνται τόσο η αντικατάσταση («σύγχυση») όσο και τη μετάθεση («διάχυση») των συμβόλων του μεταδιδόμενου μηνύματος.

Κάθε διάταξη S εκτελεί ένα γραμμικό ή μη γραμμικό μετασχηματισμό αντικατάστασης, απαιτώντας (για είσοδο των N bits) 2^N εσωτερικούς αποδέκτες, που να μπορούν να συνδυαστούν κατά N! διαφορετικούς συνδυασμούς. Για παράδειγμα, μια διάταξη S με είσοδο των 5 bits μπορεί να κρυπτογραφήσει ένα αλφάβητο των 32

συμβόλων. Τότε οι πιθανές συνδέσεις των συμβόλων θα ήταν 32!, αλλά το σύστημα θα μπορούσε να κρυπταναλυθεί με ανάλυση συχνότητας χρησιμοποιούμενων συμβόλων. Η αδυναμία αυτή δεν είναι εγγενής του συστήματος, αλλά σχετίζεται με το μικρό αριθμό εισόδων και εξόδων (μόνο 32). Αν, για παράδειγμα, ο αριθμός εισόδων ήταν 128, τότε ο κρυπταναλυτής θα είχε να αντιμετωπίσει 2^{128} πιθανούς συνδυασμούς, αριθμός αποθαρρυντικός για ανάλυση συχνότητας. Μια τέτοια, όμως, συσκευή θα απαιτούσε την ύπαρξη 2^{128} εσωτερικών συνδέσεων, κάτι που είναι τεχνολογικά ανέφικτο σήμερα.

Η λύση στο παραπάνω πρόβλημα μπορεί να δοθεί με τη χρήση διατάξεων P. Οι διατάξεις αυτές είναι ηλεκτρονικά κυκλώματα που υλοποιούν τη μετάθεση των συμβόλων του μεταδιδόμενου μηνύματος. Μια διάταξη P που έχει N εισόδους μπορεί να δώσει δυνατότητα επιλογής μεταξύ N! κλειδιών. Η κατασκευή διατάξεων P ακόμη κει με N=128 εισόδους είναι τεχνολογικά εφικτή.

Παρόλα αυτά, με τη χρήση μιας εξειδικευμένης τεχνικής είναι δυνατό να βρεθεί το κλειδί κρυπτογράφησης σε διάταξη P με μόνο N-1 δοκιμές, πράγμα που καθιστά τη χρησιμοποίηση διατάξεων P και μόνο, αναποτελεσματική. Αντίθετα, η συνδυασμένη εφαρμογή διατάξεων S και P αποδεικνύεται ιδιαίτερα αποτελεσματική, λόγω της αντικατάστασης (S) και της μη-γραμμικότητας της μετάθεσης (P). Τα σύμβολα του αρχικού μηνύματος, περνώντας μέσα από τη διάταξη S αντικαθίστανται, ενώ στη συνέχεια περνώτας μέσα από τη διάταξη P μετατίθενται και μετακινούνται από τις προηγούμενες θέσεις τους. Τα χαρακτηριστικά αυτά, σε συνδυασμό με το γεγονός ότι μπορούν να εφαρμοστούν πολλαπλά επίπεδα διατάξεων S και P με διαφορετικά κλειδιά στο καθένα, κάνουν την κρυπτανάλυση ενός τέτοιου κρυπτοσυστήματος εξαιρετικά δύσκολη.



Σχήμα XXX : Διάταξη S και διάταξη P

Δύο από τα πιο διαδεδομένα μικτά κρυπτοσυστήματα είναι το Lucifer και το DES, τα οποία περιγράφονται στη συνέχεια.

4.1.4.i Σύστημα Lucifer

Το σύστημα αυτό αναπτύχθηκε από την εταιρία IBM και χρησιμοποιεί διατάξεις P με N=64 ή N=128 εισόδους (bits) και διατάξεις S με N=4 εισόδους. Στο σύστημα αυτό ενυπάρχει και η δυνατότητα χρήσης ατομικού κλειδιού, για την περίπτωση που πολλοί χρήστες έχουν πρόσβαση και χρησιμοποιούν το ίδιο σύστημα. Η δυνατότητα χρήσης ατομικού κλειδιού υλοποιείται με την εισαγωγή στο σύστημα δύο καταστάσεων S_0 και S_1 για κάθε διάταξη S. Η ενεργοποίηση της μιας ή της άλλης υπο-διάταξης γίνεται από το προσωπικό κλειδί. Έτσι, για κάθε λογικό "1" στο κλειδί ενεργοποιείται η μονάδα 1 της διάταξης στην αντίστοιχη θέση, ενώ για κάθε λογικό "0" στο κλειδί ενεργοποιείται η μονάδα 0 της διάταξης.

4.1.4.ii Σύστημα DES (Data Encryption Standard)

Το σύστημα DES, παρά τις διαφωνίες και τις αμφισβητήσεις σχετικά με το επίπεδο ασφάλειας που προσφέρει σήμερα, αποτελεί το πιο διαδεδομένο μικτό κρυπτοσύστημα ιδιωτικού κλειδιού. Λόγω της σπουδαιότητάς του θα παρουσιαστεί αναλυτικά σε επόμενη ενότητα.

4.2 ΑΣΥΜΜΕΤΡΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

Ένα σημαντικό μειονέκτημα των συμμετρικών μεθόδων είναι ότι το χρησιμοποιούμενο κλειδί πρέπει να διανέμεται με εξαιρετική προσοχή, αφού πρέπει να διατηρείται μυστικό. Αυτό είναι φυσικό γιατί, ενώ ένα κρυπτογραφημένο μήνυμα μπορεί να μεταδίδεται διαμέσου ανασφαλών γραμμών επικοινωνίας, τα κλειδιά πρέπει να μεταδίδονται μόνο διαμέσου ασφαλών γραμμών. Το μειονέκτημα αυτό αντιμετωπίζεται από τα λεγόμενα ασύμμετρα κρυπτοσυστήματα με τη βοήθεια αλγορίθμων "δημόσιου κλειδιού" (public key cryptosystems). Τα συστήματα αυτά παρουσιάστηκαν για πρώτη φορά στο Stanford University από τους Martin Hellman, Ralph Merkle και Whitfield Diffie (1976).

Σε αυτούς τους αλγορίθμους το κρυπτογραφημένο μήνυμα μεταδίδεται μαζί με το κλειδί της κρυπτογράφησης, το οποίο είναι κοινά γνωστό. Αυτό που είναι άγνωστο είναι το κλειδί της αποκρυπτογράφησης, το οποίο είναι γνωστό μόνο στο (νόμιμο) δέκτη του μηνύματος.

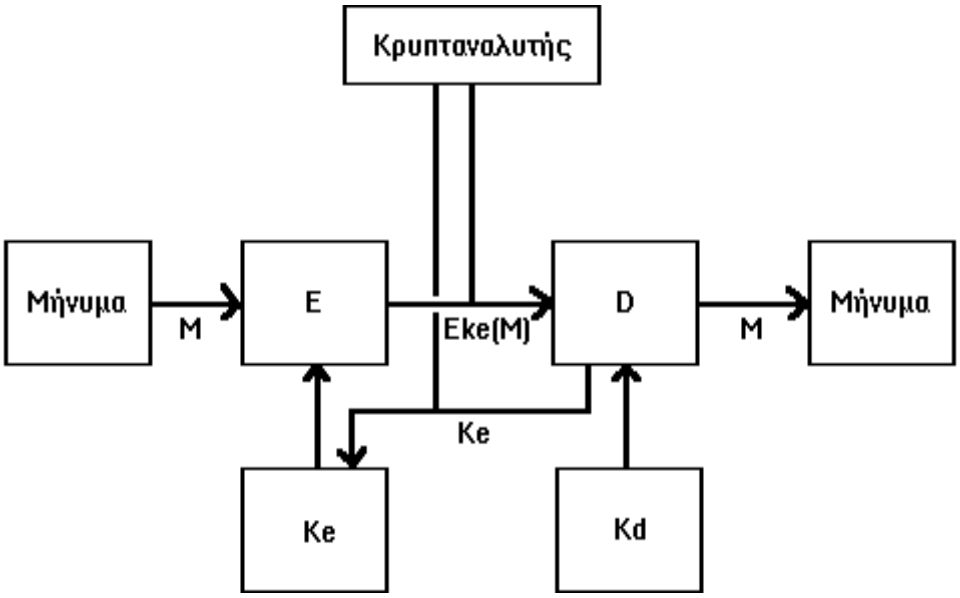
Η διαδικασία που ακολουθείται είναι η εξής:

α) Ο παραλήπτης δημιουργεί δύο κλειδιά. Το κλειδί της κρυπτογράφησης και το κλειδί της αποκρυπτογράφησης.

β) Το κλειδί της κρυπτογράφησης γίνεται γνωστό σε όλους τους χρήστες του κρυπτοσυστήματος με τη βοήθεια ενός κοινού καταλόγου.

γ) Όποιος επιθυμεί να στείλει κάποιο μήνυμα σε κάποιον αποδέκτη βρίσκει το κλειδί κρυπτογράφησης από τον κατάλογο, το χρησιμοποιεί και στέλνει το κρυπτογραφημένο μήνυμα.

δ) Ο αποδέκτης χρησιμοποιεί το κλειδί αποκρυπτογράφησης, το οποίο μόνο αυτός γνωρίζει, και αναγνωρίζει το περιεχόμενο του μηνύματος.



Σχήμα 4 : Κρυπτοσυστήματα δημόσιου κλειδιού (public-key cryptosystems)

Η μέθοδος αυτή απορρίπτει την ανάγκη ύπαρξης ασφαλούς γραμμής επικοινωνίας για την ανταλλαγή των κλειδιών, κάτι πολύ σημαντικό σε συστήματα πολλαπλών χρηστών, μια και σε παρόμοια συστήματα είναι δύσκολο να εξασφαλιστεί ασφαλής επικοινωνία για όλους τους συνδυασμούς χρηστών (αποστολέας/παραλήπτης).

Το μαθηματικό υπόβαθρο της μεθόδου αυτής είναι το εξής:

Υποθέτουμε ότι υπάρχουν δύο οικογένειες συναρτήσεων, οι {Εκ : κεΚ} και {Dκ : κεΚ}, τέτοιες ώστε:

α) οι τιμές των συναρτήσεων Εκ και Dκ να υπολογίζονται εύκολα

β) γνωρίζοντας την Εκ, αλλά όχι το κ, είναι "δύσκολο" να υπολογιστεί η Dκ

γ) γνωρίζοντας το κ, είναι "εύκολο" να κατασκευάσουμε τις Εκ και Dκ .

Υποθέτουμε, επίσης, ότι υπάρχει ένας δημόσια γνωστός κατάλογος που είναι προσπελάσιμος από κάθε χρήστη του κρυπτοσυστήματος. Κάθε νέος χρήστης επιλέγει ένα κλειδί (κ), με βάση το οποίο (και μέσω της ιδιότητας (γ)) μπορεί να κατασκευάσει τις δύο συναρτήσεις Εκ και Dκ. Στη συνέχεια "ανακοινώνει" μέσω του κοινού καταλόγου μόνο τη συνάρτηση Εκ (αλγόριθμο κρυπτογράφησης), αλλά όχι την Dκ , και το κλειδί κ. Όταν κάποιος άλλος χρήστης επιθυμεί να αποστείλει σε αυτόν κάποιο μήνυμα, τότε εντοπίζει από τον κατάλογο την Εκ του συγκεκριμένου χρήστη και την χρησιμοποιεί για να κρυπτογραφήσει το μήνυμα (κάτι που γίνεται εύκολα με βάση την ιδιότητα (α)).

Συνεπώς, το όλο πρόβλημα ανάγεται στην ύπαρξη συναρτήσεων κρυπτογράφησης Εκ , για τις οποίες οι αντίστοιχες συναρτήσεις αποκρυπτογράφησης Dκ δεν μπορούν να υπολογιστούν εύκολα. Οι συναρτήσεις αυτού του είδους ονομάζονται "μονόδρομες συναρτήσεις" (one-way functions). Αν Φ είναι μια μονόδρομη συνάρτηση και υπάρχουν οι απαραίτητες πληροφορίες για τον υπολογισμό της αντίστροφης Φ-1 όταν είναι γνωστό το κλειδί (κ), τότε η Φ λέγεται "επισφαλής συνάρτηση" (trap-door function). Άρα, η αποτελεσματικότητα των μεθόδων δημόσιου κλειδιού εξαρτώνται από την ύπαρξη επισφαλών συναρτήσεων.

Η καλύτερη προσσέγγιση, με βάση τις παραπάνω παρατηρήσεις, είναι διαμέσου της Θεωρίας της Πολυπλοκότητας. Από τις τρεις ιδιότητες-απαιτήσεις, αναγνωρίζονται εύκολα:

α) οι εύκολα υπολογίσιμες συναρτήσεις (Εκ και Dκ)

β) η κλάση P των ντετερμινιστικών συναρτήσεων που υπολογίζονται σε πολυωνυμικό χρόνο

γ) οι δύσκολα υπολογίσιμες συναρτήσεις (υπολογισμός της Dκ από την Εκ), οι οποίες δεν ανήκουν στην κλάση P.

Μια ευρύτατα χρησιμοποιούμενη συνάρτηση που χρησιμοποιείται ως συνάρτηση κρυπτογράφησης Εκ είναι το "υπόλοιπο ακέραιας διαίρεσης": Εκ = (μ) mod (κ) . Η συνάρτηση αυτή ικανοποιεί και τις τρεις παραπάνω ιδιότητες και έχει την ιδιότητα να

μετατρέπει συνεχείς συναρτήσεις (πεδίο τιμών) σε ασυνεχείς, δυσκολεύοντας έτσι την κρυπτανάλυση.

Στην εργασία των Diffie και Hellman δεν προτείνεται κάποιο συγκεκριμένο κρυπτοσύστημα. Δύο ευρύτατα διαδεδομένα ασύμμετρα κρυπτοσυστήματα αυτού του τύπου είναι το πολύ γνωστό RSA και το σύστημα Knapsack, τα οποία παρουσιάζονται στη συνέχεια.

4.2.1 Μέθοδοι Knapsack

Γενικά

Οι Merkle-Hellman ανάπτυξαν έναν αλγόριθμο κρυπτογράφησης βασιζόμενο στο "πρόβλημα του σάκου". Σύμφωνα με το τελευταίο, δεδομένων ενός συνόλου ακεραίων και ενός αθροίσματος-στόχου, ζητείται ενό υποσύνολο του αρχικού συνόλου, τέτοιο ώστε το άθροισμα των στοιχείων του να είναι το δεδομένο άθροισμα-στόχος. Φορμαλιστικά, έχουμε:

Δοθέντος ενός συνόλου $S = \{c_1, c_2, \ldots, c_n\}, c_i \geq 0$ *και ενός στόχου* T, *υπάρχει διάνυσμα επιλογής* $V = \{v_1, v_2, \ldots, v_n\}, v_i \in \{1,0\}$ *τέτοιο ώστε* $\sum_{i=1}^{n} c_i * v_i = T$;

Για πράδειγμα, αν S={4,7,1,12,10}, για το στόχο T=17 υπάρχει λύση, αφού 17=4+1+12. Δηλαδή ο στόχος επιτυγχάνεται χρξσιμοποιώντας ως διάνυσμα επιλογής το V={1,0,1,1,0}. Αντίθετα, για T=25 δεν υπάρχει λύση.

Το πρόβλημα του σάκου είναι NP-πλήρες. Αυτό δηλώνει ότι η λύση του ίσως απαιτεί χρόνο εκθετικό σε σχέση με το μέγεθος του προβλήματος, δηλαδή το πλήθος των ακεραίων στο σύνολο S.

Η ιδέα πίσω από την πρόταση των Merkle-Hellman είναι η κωδικοποίηση ενός δυαδικού μηνύματος ως μία λύση σε κάποιο πρόβλημα σάκου. Δηλαδή, το αρχικό μήνυμα θεωρείται ως το σύνολο V και παράγεται μία ακολουθία από αθροίσματα-

στόχους με δεδομένο ένα σύνολο ακεραίων S. Το πλήθος των στοιχείων του S (του "σάκου") καθορίζει και το block των bits που θα χρησιμοποιούνται για να παραχθεί το άθροισμα, όπως φαίνεται και στο ακόλουθο παράδειγμα:

{Σχήμα 3.5}

Ένας σάκος δηλώνεται ως ένα διάνυσμα από ακέραιους όρους, στο οποίο η σειρά των όρων έχει μεγάλη σημασία. Στην πράξη υπάρχουν δύο "σάκοι", ένας απλός , για τον οποίο υπάρχει ένας γρήγορος αλγόριθμος (γραμμικός χρόνος), και ένας δύσκολος, που είναι αποτέλεσμα μετατροπής των όρων του αρχικού (απλού) σάκου. Η μετατροπή είναι τέτοια, ώστε η λύση με τους όρους του ενός είναι λύση και για τον άλλο. Με αυτήν την μετατροπή δίνεται η δυνατότητα σε εξουσιοδοτημένους χρήστες να λύσουν το πρόβλημα εύκολα. Έτσι το γενικό πρόβλημα είναι NP-πλήρες, αλλά υπάρχει και μια παραλλαγή του που έχει μια πολύ γρήγορη λύση.

Η μέθοδος κρυπτογράφησης

Η μέθοδος κρυπτογράφησης Merkle-Hellman είναι ένα κρυπτοσύστημα δημόσιου κλειδιού. Δηλαδή, κάθε χρήστης έχει ένα δημόσιο κλειδί, που μπορεί να το διαθέσει σε οποιονδήποτε, καθώς και ένα ιδιωτικό κλειδί. Το δημόσιο κλειδί είναι ένα σύνολο ακεραίων για κάποιο πρόβλημα σάκου. Το ιδιωτικό κλειδί είναι ένας "απλός σάκος" που λύνει το ίδιο πρόβλημα με το δημόσιο κλειδί.

Με τον όρο "απλός σάκος" εννοούμε μία ακολουθία ακεραίων όπου κάθε όρος είναι μεγαλύτερος από το άθροισμα όλων των προηγούμενων:

$$a_k \rangle \sum_{j=1}^{k-1} a_j \qquad (1)$$

Για παράδειγμα, το {1,4,11,17,38,73} είναι ένας τέτοις σάκος. Για τέτοιες ακολουθίες το πρόβλημα του σάκου είναι πολύ εύκολο, αφού είναι προφανές αν κάποιος όρος της ακολουθίας ανήκει στο άθροισμα ή όχι. Κανένας συνδυασμός όρων μικρότερων από έναν συγκεκριμένο δεν δίνει άθροισμα ίσο με το συγκεκριμένο όρο. Έτσι, το 17 είναι μεγαλύτερο από 1+4+11 (=16). Αν το άθροισμα-στόχος είναι μεγαλύτερο ή ίσο με το 17, το 17 ή κάποιος μεγαλύτερος όρος πρέπει να ανήκει στο άθροισμα.

Η συμβολή των Merkle-Hellman ήταν ο σχεδιασμός μιας τεχνικής μετατροπής ενός απλού σάκου σε έναν κοινό. Το μυστικό είναι η αλλαγή των όρων με έναν μη προφανή αλλά αντιστρέψιμο τρόπο.

Με δεδομένο έναν απλό σάκο $S = \{s_1, s_2, \ldots, s_n\}$ επιλέγουμε έναν πολλαπλασιαστή w και ένα modulo n. Το modulo πρέπει να είναι μεγαλύτερο από τον μεγαλύτερο όρο s_n. Ο πολλαπλασιαστής δεν πρέπει να έχει κοινούς παράγοντες με το modulo. Ένας εύκολος τρόπος για αυτό είναι να επιλεγεί ως modulo ένας πρώτος αριθμός, αφού κανένας μικρότερος αριθμός δεν θα έχει κοινούς παράγοντες με αυτόν. Στη συνέχεια, αντικαθιστούμε κάθε όρο s_i του απλού σάκου με τον όρο

$$h_i = w * s_i \bmod n$$

Έτσι το $H = \{h_1, h_2, \ldots, h_n\}$ είναι ο "δύσκολος σάκος". Για παράδειγμα, αρχίζοντας με το S={1,2,4,9} και επιλέγοντας w=15 και n=17 έχουμε:

1*15 mod 17 = 15 mod 17 = 15

2*15 mod 17 = 30 mod 17 = 13

4*15 mod 17 = 60 mod 17 = 9

9*15 mod 17 = 135mod 17 = 16

Το σύνολο που προκύπτει είναι το H={15,13,9,16}.

Το γεγονός ότι το w και το n είναι πρώτοι μεταξύ τους, εξασφαλίζει ότι υπάρχει ο αντίστροφος του w στο mod n. Η ιδιότητα αυτή χρησιμοποιείται στην αποκρυπτογράφηση, όπως θα δειχτεί παρακάτω.

Για S={1,2,4,9} και H={15,13,9,16} το μήνυμα P = 0100101110100101 θα κωδικοποιηθεί με το H, αφού χωριστεί σε blocks των 4 bits (όσο και ο πληθάριθμος των S και H):

$[0,1,0,0] * [15,13,9,16] = 13$
$[1,0,1,1] * [15,13,9,16] = 40$
$[1,0,1,0] * [15,13,9,16] = 24$
$[0,1,0,1] * [15,13,9,16] = 29$

Το αρχικό μήνυμα κρυπτογραφείται ως τους ακέραιους 13, 40, 24, 29 χρησιμοποιώντας το δημόσιο κλειδί H={15,13,9,16}.

Η μέθοδος αποκρυπτογράφησης

Ο νόμιμος παραλήπτης του μηνύματος γνωρίζει τον απλό σάκο και τις τιμές των w και n που χρησιμοποιήθηκαν για την μετατροπή του σε δύσκολο δημόσιο κλειδί. Ο παραλήπτης υπολογίζει την τιμή του $_{w^{-1}}$ έτσι ώστε $w*w^{-1} = 1 \bmod n$. Στο προηγούμενο παράδειγμα $15^{-1} \bmod 17$ είναι το 8, αφού 15*8 mod 17 = 120 mod 17 = (17*7) + 1 = 1.

Δεδομένου ότι το δύσκολο κλειδί H παρήχθει από το εύκολο S και μάλιστα $H = w*S \bmod n$, κρυπτογραφημένο μήνυμα C είναι: $C = H*P = w*S*P \bmod n$. Για την αποκρυπτογράφηση είναι απαραίτητο να πολλαπλασιαστεί το C με το $_{w^{-1}}$, αφού $C = H * P = w * S * P \bmod n$. Για να παράγει το αρχικό μήνυμα P, ο παραλήπτης θα πρέπει να λύσει το απλό πρόβλημα του σάκου με σάκο το S και στόχο το $w^{-1}*C_i$ για κάθε ακέραιο-κωδικό C_i. Αφού $w^{-1}*C_i = w^{-1}*S*P_i \bmod n$, η λύση για το στόχο $w^{-1}*C_i$ είναι το block P_i, δηλαδή το αρχικό μήνυμα.

Για παράδειγμα, η αποκρυπτογράφηση του μηνύματος 13, 40, 24, 29, που παρήχθη με χρήση του δημόσιου κλειδιού H={15,13,9,16}, ξεκινάει με πολλαπλασισμό όλων των ακέραιων-κωδικών με το 8 mod n, αφού $15^{-1} \bmod 17 = 8$.

$13*8 = 104 \bmod 17 = 2$
$40*8 = 320 \bmod 17 = 14$
$24*8 = 192 \bmod 17 = 5$
$29*8 = 232 \bmod 17 = 11$

Το κάθε ένα από τα παραπάνω αποτελέσματα αποτελεί στόχο για το απλό πρόβλημα σάκου με σάκο το ιδιωτικό κλειδί S={1,2,4,9}. Έτσι, για καθέναν από τους νέους στόχους το διάνυσμα επιλογής είναι:

Στόχος	**Διάνυσμα επιλογής**	**Αιτιολόγηση**

2	0100	2=2
14	1011	14=1+4+9
5	1010	5=1+4
11	0101	11=2+9

Με αυτήν τη μέθοδο το μήνυμα που ανακτάται είναι το P = 0100101110100101, δηλαδή το αρχικό μήνυμα που στάλθηκε.

Πρακτική εφαρμογή και αδυναμίες του αλγορίθμου Merkle-Hellman

Στην πράξη, το n επιλέγεται να είναι 100 με 200 bits. Αν το n είναι 200 bits, τα s_i συνήθως επιλεγονται να απέχουν μεταξύ τους περίπου κατά 2^{200}. Έτσι υπάρχουν περίπου 200 όροι στο σάκο και κάθε ένας από αυτούς είναι μεταξύ 200 και 400 bits. Ακριβέστερα, το s_0 επιλέγεται ώστε $1 \le s_0 < 2^{200}, 2^{200} \le s_1 < 2^{201}, 2^{201} \le s_2 < 2^{202}$ κ.ό.κ., έτσι ώστε να υπάρχουν περίπου 2^{200} επιλογές για κάθε s_i.

Η ακολουθία των s_i μπορεί να παραχθεί με χρήση τυχαίων αριθμών, έστω r_i, αρκεί αυτοί να είναι μεταξύ 0 και 2^{200}. Τότε κάθε όρος του σάκου μπορεί να υπολογιστεί ως εξής:

$s_i = 2^{200+i-1} + r_i$ για i=1,2,...,m

Για τόσο μεγάλους όρους στο S και στο H είναι ακατόρθωτο να δοκιμαστούν όλες οι πιθανές τιμές των s_i ώστε να αποκαλυφθεί το S με δεδομένο το H και το C.

Παρ'όλα αυτά, ένας που θα θελήσει να σπάσει τον κώδικα δε χρειάζεται να λύσει το βασικό "πρόβλημα του σάκου", αφού η κρυπτογράφηση βασίζεται πάνω σε ειδικά επιλεγμένες περιπτώσεις του προβλήματος. Έχει δειχθεί ότι αν είναι γνωστή η τιμή του modulo n, μπορεί να είναι δυνατό να καθοριστεί ο απλός σάκος (το ιδιωτικό κλειδί). Ο τρόπος με τον οποίο επιτυγχάνεται κάτι τέτοιο περιγράφεται σε γενικές γραμμές παρακάτω.

Αρχικά, αφού όλοι οι όροι του δημόσιου κλειδιού είναι γνωστοί, είναι απλό να καθοριστούν ποια είναι η αντιστοιχία με τους όρους του ιδιωτικού κλειδιού. Έστω ότιh_0 και h_1είναι οι δύο πρώτοι όροι του δημόσιου κλειδιού που αντιστοιχούν με τους s_0 και s_1του ιδιωτικού κλειδιού.

Αν $p = h_0/h_1 \bmod n$, τότε αφού $h_0 = w*s_0 \bmod n$ και $h_1 = w*s_1 \bmod n$ ισχύει:

$$p = (w*s_0)/(w*s_1) = s_0/s_1 \bmod n$$

Δεδομένης έτσι του λόγου p ορίζουμε την ακολουθία

$$\Delta = p \bmod n, 2*p \bmod n, 3*p \bmod n, ..., k*p \bmod n, ..., 2^m * p \bmod n$$

Για κάποιο k, kκαι s_1 θα αλληλοαναιρούν το mod n, δηλαδή $k*(1/s_1) = 1 \bmod n$. Τότε , $k*p \bmod n = k*s_0*1/s_1 \bmod n = s_0 \bmod n = s_0$. Είναι λογικό να ανεμένει κανείς ότι το s_0 θα είναι το μικρότερο στοιχείο της Δ. Εφόσων το s_0 γίνει γνωστό, είναι απλό να καθοριστεί το w, μετά το w^{-1} και καθένα από τα s_i.

Ένα ακόμη μειονέκτημα του αλγορίθμου έχει ανακαλυφθεί. Αυτή η μέθοδος αποκάλυψης του κώδικα προσπαθεί να καθορίσει το w και το n μόνο από τα h_i.

Το μέγεθος του n κατά προσέγγιση μπορεί να εκτιμηθεί από το γεγονός ότι πρέπει να είναι μεγαλύτερο από κάθε h_i, αφού τα τελευταία έχουν αναχθεί σε mod n. Παρ'όλα αυτά το n δεν θα είναι σημαντικά μεγαλύτερο από το μέγιστο h_i, αφού όλοι οι όροι του δημόσιου κλειδιού αναμένεται να είναι ομοιόμορφα κατανεμημένοι μεταξύ 1 και n.

Ας υποθέσουμε ότι προσπαθούμε να μαντέψουμε το w. Επαναληπτικά θα δοκιμάζαμε διάφορες τιμές $\tilde{w} = 1,2,3,....$ Η γραφική παράσταση του $\tilde{w}*h_i \bmod n$ ως συνάρτηση του $\tilde{w}$ θα αυξάνει σταθερά μέχρι το $\tilde{w}*h_i$ γίνει μεγαλύτερο του n. Στο σημείο αυτό η γραφική παράσταση θα παροθσιάσει μια ασυνέχεια και θα πάρει μια μικρή τιμή. Οι τιμές των $\tilde{w}*h_i$ θα ανακάμψουν στη συνέχεια καθώς το $\tilde{w}$ θα αυξάνει μέχρι το $\tilde{w}*h_i$ ξεπεράσει και πάλι το n. Έτσι δημιουργείται μια "πριονωτή" μορφή, όπου η κλίση κάθε "δοντιού" είναι το h_i.

{Σχήμα 3.7}

Η ζητούμενη τιμή $\tilde{w}$=w βρίσκεται σε ένα από τα σημεία ασυνέχειας της παραπάνω γραφικής παράστασης. Για όλα τα h_i η γραφική παράσταση έχει την ίδια μορφή. Για να εντοπίσουμε το w κάνουμε σε ένα γράφημα τις γραφικές παραστάσεις των $\tilde{w} * h_i \bmod n$ για $h_i = h_1, h_2, \ldots$. Το w θα βρίσκεται σε ένα από τα σημεία όπου όλες οι γραφικές παραστάσεις είναι ασυνεχείς και πέφτουν από μια μεγάλη τιμή σε μια μικρή, όπως φαίνεται και στο Σχ.3.8. Έτσι το πρόβλημα προσδιορισμού του w ανάγεται στην εύρεση του σημείου όπου όλες οι ασυνέχειες συμπίπτουν.

Η ακριβής διαδικασία στην πράξη είναι λίγο πιο δύσκολη από αυτήν που περιγράφηκε. Η τιμή του n αντικαθίσταται από έναν πραγματικό αριθμό N. Αφού το n και N είναι άγνωστα, οι γραφικές παραστάσεις κλιμακώνονται διαιρώντας με N και μετά προσεγγίζοντας με διαδοχικές τιμές του πραγματικού $\tilde{w}/N$ στην συνάρτηση $(\tilde{w}/N) * h_i \bmod 1.0$. Ευτυχώς, αυτό ανάγεται στην επίλυση ενός γραμμικού συστήματος ανισοτήτων. Αυτό το πρόβλημα λύνεται σε πολυωνυμικό χρόνο. Επομένως, το πρόβλημα του σάκου των Merkle-Hellman μπορεί να σπάσει σε λογικό χρονικό διάστημα.

Συμπεράσματα

Η παραπάνω λύση προφανώς δεν εφαρμόζεται και στο γενικό πρόβλημα του σάκου. Εφαρμόζεται μόνο σε ειδικές περιπτώσεις του γενικού προβλήματος που παρήχθησαν από ακολουθίες με την ιδιότητα (1) μετά από πολλαπλασιασμό με κάποια σταθερά και κατόπιν διαίρεση. Άρα, το βασικό πρόβλημα του σάκου παραμένει ως έχει: μόνο μια περιορισμένη μορφή του έχει λυθεί. Αυτό υποδεικνύει ότι ένα κρυπτοσύστημα βασιζόμενο σε ένα δύσκολο πρόβλημα δεν είναι κατ'ανάγκην τόσο δύσκολο να λυθεί όσο και το βασικό πρόβλημα.

Αφότου έγινε γνωστό ότι ο κώδικας των Merkle-Hellman έσπασε, έχουν μελετηθεί και προταθεί διάφορες παραλλαγές. Σήμερα, τέτοιες μέθοδοι κρυπτογράφησης δεν δείχνουν ασφαλείς για μια εφαρμογή η οποία είναι πιθανό να δεχτεί μια συντονισμένη επίθεση παραβίαση της ασφάλειας. Ο αλγόριθμος Merkle-Hellman ή κάποια παραλλαγή του θα αρκούσε για ορισμένες περιπτώσεις. Παρ'όλα αυτά, επειδή είναι αρκετά πολύπλοκος να χρησιμοποιηθεί, η μέθοδος Merkle-Hellman δεν συνιστάται συχνά.

4.2.2 Μέθοδος RSA

Η μέθοδος αυτή αποτελεί την πιο διαδεδομένη μέθοδο δημόσιου κλειδιού σήμερα και μαζί με τη μέθοδο DES τα κρυπτοσυστήματα με την πιο ευρεία χρήση. Λόγω της σπουδαιότητάς του, η μέθοδος RSA θα παρουσιαστεί ναναλυτικά σε επόμενη παράγραφο.

4.3 Μέθοδος DES

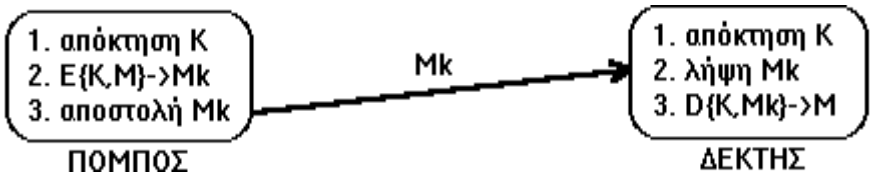
Η μέθοδος DES ανήκει στη γενικότερη κατηγορία μεθόδων "ιδιωτικού κλειδιού". Οι μέθοδοι κρυπτογράφησης αυτού του τύπου χρησιμοποιήθηκαν αιώνες πριν την ανακάλυψη του ηλεκτρονικού υπολογιστή. Η εφαρμογή τους σε συστήματα υπολογιστών πρόσφεραν τη δυνατότητα χρησιμοποίησης μεγαλύτερων κλειδιών και πιο πολύπλοκων αλγορίθμων κρυπτογράφησης. Ανάλογη, όμως, δυνατότητα προσφέρεται και σε πιθανή προσπάθεια κρυπτανάλυσης παρόμοιων μεθόδων. Μια και κάποιος υποτιθέμενος κρυπταναλυτής θεωρείται πως έχει στη διάθεσή του συστήματα της ίδιας (ή μεγαλύτερης) υπολογιστικής ισχύς, οι δύο παράμετροι (κλειδιά, αλγόριθμοι) θα πρέπει να επιλεχθούν με εξαιρετική προσοχή, ώστε να εξασφαλίσουν το βαθμό ασφάλειας τέτοιων κρυπτοσυστημάτων. Το σύστημα DES αποτελεί σήμερα τον κυριότερο αντιπρόσωπο αυτής της κατηγορίας κρυπτοσυστημάτων.

4.3.1 Γενικά

Το μήνυμα κρυπτογραφείται χρησιμοποιώντας κάποιο αλγόριθμο κρυπτογράφησης, οποίος χρησιμοποιεί το κλειδί. Τόσο ο αποστολέας, όσο και ο παραλήπτης γνωρίζουν τον αλγόριθμο αυτό (ή τον αντίστροφο, για την αποκρυπτογράφηση). Στο σημείο αυτό θα πρέπει να τονιστεί ότι οι αλγόριθμοι αυτοί πρέπει να είναι δημόσια γνωστοί, οπότε η ασφάλεια της μεθόδου θα πρέπει να εξαρτάται αποκλειστικά και μόνο από την μυστικότητα του κλειδιού, και όχι από την μυστικότητα του αλγορίθμου.

Η μέθοδος Data Encryption Standard (DES - National Bureau of Standards, 1977) αναπτύχθηκε από την εταιρία IBM ως αναβαθμισμένη έκδοση του ήδη υπάρχοντος συστήματος Lucifer και αργότερα υιοθετήθηκε ως εθνικό πρότυπο στις Ηνωμένες Πολιτείες Αμερικής για τη μετάδοση μη διαβαθμισμένων εγγράφων σε κυβερνητικές υπηρεσίες , καθώς και για εμπορικές εφαρμογές. Στο πρότυπο αυτό η συνάρτηση κρυπτογράφησης απεικονίζει ομάδες των 64 bits από το αρχικό μήνυμα σε 64 bits κρυπτογραφημένου μηνύματος, χρησιμοποιώντας κλειδί μήκους 56 bits. Ο αλγόριθμος υλοποιεί 16 στάδια κρυπτογράφησης, τα οποία καθορίζονται έμμεσα από το κλειδί, στα οποία τα δεδομένα προς κρυπτογράφηση υπόκεινται σε ολίσθηση κατά bits (bit-rotated) σε βαθμό που καθορίζει το κλειδί και στη συνέχεια σε μετασχηματισμό τριών επιπέδων ανεξάρτητο του κλειδιού.

Πριν την υιοθέτηση του σχήματος DES ως προτύπου διεξήχθησαν δύο συναντήσεις εμπειρογνωμόνων όπου εξετάστηκαν οι πιθανές αδυναμίες του αλγορίθμου, κυρίως σε ό,τι αφορά το μήκος του κλειδιού και στην αποφυγή επισφαλών συναρτήσεων στην κατασκευή των διατάξεων S.



Σχήμα 5 : Πρωτόκολλο λειτουργίας σχημάτων ιδιωτικού κλειδιού (secret-key)

4.3.2 Ανάλυση του αλγορίθμου

Στη γενική μορφή του το σχήμα DES αποτελείται από μια διάταξη S, όπως αυτή περιγράφηκε αναλυτικά παραπάνω στα συμμετρικά κρυπτοσυστήματα. Επειδή, όμως, δεν είναι δυνατό να υλοποιηθεί με 64 εισόδους/εξόδους, υποδιαιρείται σε 8 επιμέρους διατάξεις S των 6 εισόδων και 4 εξόδων. Επίσης, χρησιμοποιούνται 8 ψηφία ελέγχου (parity bits). Σε κάθε στάδιο κρυπτογράφησης το μήνυμα διαχωρίζεται σε δύο ισομήκη τμήματα Li και Ri , όπου ο δείκτης i συμβολίζει το στάδιο επεξεργασίας (i=1,2,...,16).

Αρχικά το μήνυμα αλλοιώνεται σύμφωνα με κάποια καθορισμένη αρχική μετάθεση. Στη συνέχεια υφίσταται την αλλοίωση που επιβάλλει ο αλγόριθμος κρυπτογράφησης, σε κάθε ένα από τα στάδια επεξεργασίας.

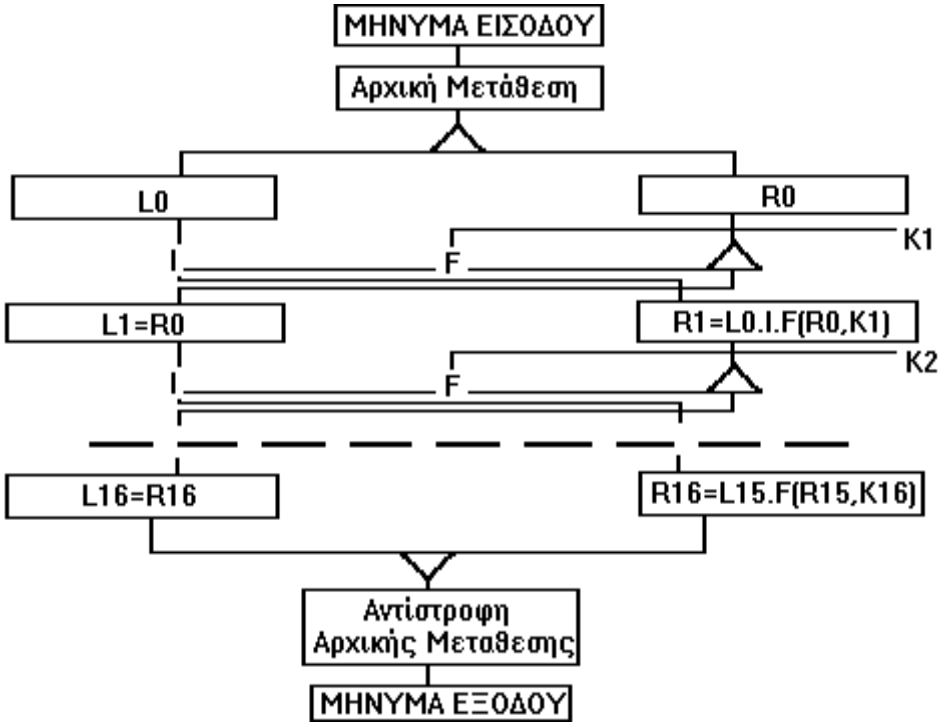
Πριν την εφαρμογή του αλγορίθμου σε κάθε στάδιο, το τμήμα Ri-1 διευρύνεται ώστε να καταλαμβάνει 48 bits, ενώ στη συνέχεια υπολογίζεται το αποτέλεσμα της πράξης XOR μεταξύ του εκτεταμένου Ri-1 και του κλειδιού Ki . Μετά το μήνυμα διασπάται σε 8 ομάδες των 6 bits, οι οποίες συμβολίζονται ως: B1B2...B8 , ενώ ισχύει η σχέση: E(Ri-1) XOR Ki = B1B2...B8 . Κάθε ομάδα Bi , που αποτελείται από 6 bits, χρησιμοποιείται στη συνέχεια ως είσοδος σε μια διάταξη αντικατάστασης S, η

οποία επιστρέφει έξοδο των 4 bits. Οι ομάδες των 4 bits συνενώνονται και το μήνυμα των 32 bits που δημιουργείται αλλοιώνεται από τη μετάθεση που επιφέρει μια διάταξη P. Έτσι, το μήνυμα που επιστρέφει η συνάρτηση κρυπτογράφησης F σε κάθε στάδιο επεξεργασίας, είναι:

F (Ri-1 , Ki) = P (S (Bi1Bi2...Bi8))

Το αρχικό κλειδί K αποτελείται από 64 bits, εκ των οποίων τα 8 είναι bits ελέγχου. Τα χρήσιμα 56 bits, που απομονώνονται με ένα μετασχηματισμό μετάθεσης στο αρχικό κλειδί, διαχωρίζονται σε δύο τμήματα των 28 bits το καθένα. Τα τμήματα αυτά στη συνέχεια ολισθαίνουν αριστερά και επαυξάνονται με κατάλληλους μετασχηματισμούς, για να δημιουργήσουν τα κλειδιά Ki , τα οποία αποτελούνται από 48 bits και χρησιμοποιούνται στα αντίστοιχα στάδια επεξεργασίας. Τα αποτελέσματα του κάθε σταδίου συνδυάζονται χρησιμοποιώντας λογικές πράξεις "αποκλειστικής διάζευξης" (XOR) μεταξύ των τμημάτων Li και Ri .

Τέλος, το μήνυμα μετασχηματίζεται σύμφωνα με την αντίστροφη (της αρχικής) μετάθεση. Ας σημειωθεί ότι το ίδιο σχήμα χρησιμοποιείται τόσο στην κρυπτογράφηση, όσο και στην αποκρυπτογράφηση του μηντυματος. Αυτό επιτυγχάνεται τροποποιώντας κατάλληλα το τελευταίο στάδιο επεξεργασίας ώστε να μην πραγματοποιεί αντιμετάθεση μεταξύ των τμημάτων Li και Ri .



Σχήμα 6 : Γενική λειτουργία κρυπτοσυστήματος τύπου DES

4.3.3 Αξιολόγηση και σχόλια

Αν και η μέθοδος γενικά είναι κάπως χρονοβόρα σε κοινά υπολογιστικά συστήματα, ο άλγόριθμος έχει υλοποιηθεί σε κυκλώματα VLSI υψηλής ταχύτητας (τάξεως 109 bps) τα οποία μπορούν εύκολα να προσαρμοστούν σε συστήματα επικοινωνιών.

Κρυπτοσυστήματα αυτού του τύπου χρησιμοποιούνται σήμερα ευρύτατα και δεν έχουν αναφερθέι μέχρι τώρα επιτυχείς προσπάθειες κρυπτανάλυσής τους. Παρόλα αυτά, οι καθηγητές Diffie και Hellman διατύπωσαν την άποψη πως το σχετικά μικρό μήκος κλειδιού (56 bits) δεν είναι αρκετό για να διασφαλίσει το σύστημα απέναντι σε μια συστηματική προσπάθεια κρυπτανάλυσης με υπολογιστή μεγάλης ισχύος. Σε

περίπτωση, δηλαδή, που ήταν διαθέσιμα κάποια ζεύγη αρχικών/κρυπτογραφημένων μηνυμάτων, θα ήταν δυνατή η ανακάλυψη του κλειδιού με διαδοχική δοκιμή όλων των πιθανών συνδυασμών. Μια τέτοια προσπάθεια θα απαιτούσε κατά μέσο όρο: 256 = 7x1016 δοκιμές. Υπολογίστηκε πως ακόμη και για τα δεδομένα εκείνης της εποχής (1977) το κόστος αγοράς και συντήρησης ενός υπολογιστικού συστήματος ικανού για ένα τέτοιο εγχείρημα δεν ήταν εκτός της πραγματικότητας, υπολογισμοί που επιβεβαιώθηκαν και αργότερα (1981). Έτσι, διατυπώθηκε η απόψη πως το μήκος του κλειδιού θα έπρεπε να επεκταθεί στα 112 bits, κάτι που δεν έχει γίνει ακόμη αποδεκτό. Επίσης, έχει ζητηθεί επίμονα η άρση της διαβάθμισης της τεχνολογίας σχεδιασμού των διατάξεων S του σχήματος DES, έτσι ώστε να είναι δυνατή η αξιολόγησή τους από τη διεθνή ερευνητική κοινότητα.

4.4 Μέθοδος RSA

Η μέθοδος κρυπτογράφησης RSA αποτελεί σήμερα την πιο διαδεδομένη παραλλαγή του ευρύτερου σχήματος "δημόσιου κλειδιού" (public key). Το όνομά της προέρχεται από τα αρχικά των τριών ερευνητών που τη θεμελίωσαν - R.Rivest, A.Shamir, L.Adleman (Massachusetts Institute of Technology, 1978). Είναι επίσης γνωστός και με το όνομα "Σχήμα MIT".

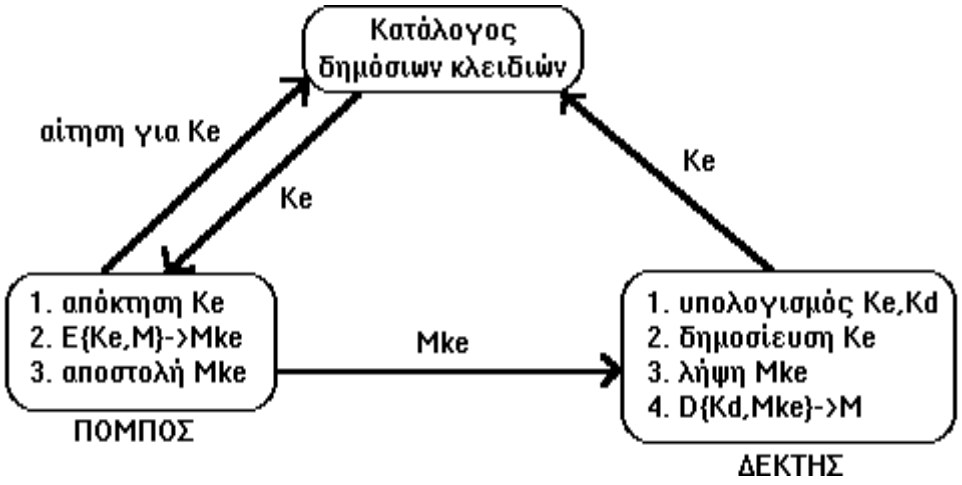
4.4.1 Γενικά

Η ασφάλεια κρυπτοσυστημάτων αυτού του τύπου βασίζεται στη χρησιμοποίηση γινομένων δύο πολύ μεγάλων πρώτων αριθμών (της τάξεως τουλάχιστον 10100 ο καθένας) και στο γεγονός ότι η ανάλυση τόσο μεγάλων αριθμών σε γινόμενο πρώτων παραγόντων είναι τόσο δαπανηρή υπολογιστικά, ώστε θεωρείται πρακτικά αδύνατη.

Το κλειδί σε αυτή τη μέθοδου αποτελείται από μια τετράδα θετικών ακέραιων αριθμών: κ = {p,q,e,d}. Οι αριθμοί (p) και (q) είναι δύο πολλοί μεγάλοι πρώτοι αριθμοί, ενώ οι αριθμοί (e) και (d) υπολογίζονται από αυτούς ως εξής. Ορίζουμε το γινόμενο: (p-1)x(q-1) = Φ(N) , όπου N = p x q . Η συνάρτηση Φ(N) ονομάζεται "ολοκληρωτική συνάρτηση του Euler" και ορίζεται για κάθε αριθμό N ο οποίος είναι γινόμενο δύο πρώτων αριθμών. Τότε:

α) ο αριθμός (d) ορίζεται να είναι οποιοσδήποτε θετικός ακέραιος που είναι πρώτος ως προς τον Φ(N), δηλαδή να μην έχουν κοινούς παράγοντες.

β) ο αριθμός (e) ορίζεται να είναι οποιοσδήποτε θετικός ακέραιος που είναι πολλαπλασιαστικό αντίστροφο της πράξης: (d) mod (Φ(N)), δηλαδή ισχύει: e x d = 1 mod Φ(N) . Αυτό σημαίνει ότι το (e) είναι ο μικρότερος (κατά σύμβαση) αριθμός στην ακολουθία: { Φ(N)+1 , 2Φ(N)+1 , ... } ο οποίος διαιρείται με το (d).



Σχήμα 7 : Πρωτόκολλο λειτουργίας σχημάτων δημόσιου κλειδιού (public-key)

4.4.2 Ανάλυση του αλγορίθμου

Με βάση τα παραπάνω αποδεικνύεται ότι ισχύει η σχέση: Dκ (Eκ (M)) = M , που επιβεβαιώνει ότι τα σχήματα Eκ και Dκ αποτελούν σχήματα κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα. Αρχικά, παρατηρούμε ότι ισχύει:

(1) Dκ (Eκ (M)) = Dκ (Me) = (Me)d = Mi*Φ(N)+1 mod N , για κάποιο i>0 , βάσει του ορισμού του γινομένου e x d όπως έγινε παραπάνω. Από το θεώρημα του Fermat προκύπτει ότι αν M<>0 mod p , τότε: Mp-1 = 1 mod p , συνεπώς: Mi*Φ(N)+1 = M mod p , μια και ο αριθμός p-1 διαιρεί το Φ(N).

Αν επίσης ισχύει: M = 0 mod p , τότε: Mi*Φ(N)+1 = mod p . Άρα, η ιδιότητα αυτή ισχύει για κάθε M. Όμοια έχουμε για: Mi*Φ(N)+1 = M mod q . Από αυτές τις διαπιστώσεις προκύπτει ότι:

(2) Mi*Φ(N)+1 = M mod (p x q) , για κάθε M .

Από τι σχέσεις (1) και (2) προκύπτει τελικά ότι:

Dκ (Eκ (M)) = ((M) mod (p x q)) mod (N) = M

, σχέση που αποδεικνύει το ζητούμενο.

Υποθέτοντας ότι το μήνυμα M που πρόκειται να κρυπτογραφηθεί αποτελείται από μια ακολουθία από bits, τότε το μήνυμα διαχωρίζεται σε ομάδες των log2N bits η κάθε μία, όπου N = p x q . Με τη μορφή αυτή, κάθε ομάδα παριστάνει έναν θετικό ακέραιο αριθμό στο διάστημα: [0 , N-1] . Το κρυπτογραφημένο μήνυμα Eκ(M) = C προκύπτει από την ύψωση στην δύναμη (e) του "αριθμού" M και την εφαρμογή (στο αποτέλεσμα) της πράξης "mod N". Η αποκρυπτογράφηση προκύπτει, αντίστοιχα, από την ύψωση του C στη δύναμη (d) και την εφαρμογή της πράξης "mod N". Συνοπτικά, ισχύουν οι σχέσεις:

α) Eκ(M) = Me mod N = C (κρυπτογράφηση)

β) Dκ(C) = Cd mod N = M (αποκρυπτογράφηση)

Το σχήμα RSA έχει μια ακόμα ενδιαφέρουσα ιδιότητα:

Eκ (Dκ (M)) = Dκ (Eκ (M)) = M

Τα σχήματα Εκ και Dκ αποτελούν μεταθέσεις (permutations) επί του συνόλου: Σ = {1,2,...,N-1} . Από την τετράδα των αριθμών {p,q,e,d} που απαρτίζουν το κλειδί K, οι αριθμοί {p,q,d} μπορούν να θεωρηθούν ως το ιδιωτικό κλειδί, ενώ ο αριθμός (e) αποτελεί το δημόσια γνωστό κλειδί κρυπτογράφησης.

Σαν παράδειγμα εφαρμογής της μεθόδου αναφέρεται η παρακάτω περίπτωση κρυπτογράφησης ενός τμήματος κειμένου χρησιμοποιώντας το σχήμα RSA. Για ευκολία, οι χρησιμοποιούμενοι αριθμοί είναι πολύ μικροί σε σχέση με αυτούς που χρησιμποποιούνται σε μια πραγματική εφαρμογή.

Έστω ότι το κείμενο είναι κωδικοποιημένο σε χαρακτήρες των 7 bits. Αυτό σημαίνει ότι: N=27=128 . Όμως, ο αριθμός 128 δεν μπορεί να αναλυθεί σε γινόμενο δύο (μόνο) πρώτων παραγόντων, οπότε ως N επιλέγεται κάποιος αριθμός μεγαλύτερος από 128. Έστω ότι: p=13 και q=17 . Τότε: N=13x17=221 , Φ(N)=12x16=192 και επιλέγεται επίσης: d=5 . Για την εύρεση του (e) αρκεί να επιλυθεί η εξίσωση: e x d = 1 mod Φ(N) . Αυτό σημαίνει ότι το (e) είναι ο μικρότερος (κατά σύμβαση) αριθμός στην ακολουθία: A = { Φ(N)+1 , 2Φ(N)+1 , ... } που διαιρείται με το (d). Άρα, εδώ έχουμε: A = { 1, 193, 385, ... } , οπότε επειδή το 385 διαιρείται με το d=5 , επιλέγεται: e = 385/5 = 77 . Έτσι, λοιπόν, για την κρυπτογράφηση ενός M, ισχύει:

Εκ(M)=Εκ(e,N,M)=C=(M77)mod(221)

, ενώ για την αποκρυπτογράφηση:

Dκ(C)=Dκ(d,N,C)=(C5)mod(221)=M

4.4.3 Θέματα υλοποίησης

Είναι γνωστό ότι η ύψωση του M στη δύναμη (e) απαιτεί το πολύ: 2 x log2e πολλαπλασιασμούς. Επειδή, όμως, ο υπολογισμός χρησιμοποιεί και την πράξη "mod" ο χρόνος που απαιτείται τελικά είναι ανάλογος του O(log22N). Αν ο αριθμός (e) επιλεγεί να είναι e<N , τότε ο χρόνος που απαιτείται είναι ανάλογος του O(log23N). Ο χρήστης καλείται να ορίσει μια τετράδα αριθμών {p,q,e,d} ως κλειδί της

κρυπτογράφησης. Η πρόταση των ερευνητών που δημιούργησαν τον αλγόριθμο RSA προτείνουν να χρησιμοποιηθεί αριθμός N της τάξεως των 600 bits (τουλάχιστον), συνεπώς κάθε ένας από τους (p) και (q) μπορούν να θεωρηθούν τάξεως 300 bits αντίστοιχα. Για την επιλογή τους χρησιμοποιείται γεννήτρια τυχαίων αριθμών και τελικά επιλέγονται δύο τυχαίοι αριθμοί οι οποίοι είναι πρώτοι μεταξύ τους.

Για τον εντοπισμό ενός πρώτου αριθμού χρησιμοποιούνται ταχείς αλγόριθμοι. Παρόλα αυτά, για να εντοπιστεί ένας πρώτος αριθμός με βάση τις παραπάνω παραμέτρους, απαιτούνται κατά μέσο όρο: 0.5xloge2600-100 αναζητήσεις, ένας αρκετά μεγάλος αριθμός δοκιμών. Για τον εντοπισμό κάποιο (d) πρώτο ως προς το Φ(N) αρκεί η τυχαία επιλογή κάποιου πρώτου αριθμού μεγαλύτερου από το max{p,q}. Στη συνέχεια, με βάση τα (d) και Φ(N) θα πρέπει να υπολογιστεί ο αριθμός (e).

Επειδή ισχύει: e x d = 1 mod Φ(N) , για κάποιο ακέραιο (μ) θα ισχύει:

(3) e x d + μ x Φ(N) = Μ.Κ.Δ.{d,Φ(N)} = 1

Εφαρμόζοντας τον εκτεταμένο Ευκλείδιο αλγόριθμο στα (d) και Φ(N) μπορούν να υπολογίστουν τις τιμές των (e) και (μ), ώστε να ικανοποιείται η σχέση (3). Είναι προτιμότερο ο αριθμός (d) να επιλεγεί έτσι ώστε ο αριθμός (e) να είναι μεγαλύτερος του log2N. Αυτό εξασφαλίζει ότι το κρυπτογραφημένο μήνυμα Εκ(Μ) υφίσταται κάποια πρόσθετη εξασφάλιση για Μ>1 .

4.4.4 Αξιολόγηση και σχόλια

Το σχήμα RSA, όπως προαναφέρθηκε, βασίζεται στη δυσκολία επίλυσης του προβλήματος ανάλυσης ενός μεγάλου αριθμού σε γινόμενο πρώτων παραγόντων. Δεν έχει (ακόμα) διατυπωθεί απόδειξη που να επιβεβαιώνει πως το πρόβλημα αυτό είναι NP-Complete, όμως όλοι οι γνωστοί αλγόριθμοι αντιμετώπισής του απαιτούν μη πολυωνυμικούς χρόνους. Ένας από τους ταχύτερους αλγορίθμους αυτού του τύπου είναι ο προτεινόμενος από τον R.Scroeppel, ο οποίος απαιτεί αριθμό βημάτων της τάξης: O((logN)logN / loglogN). Για παράδειγμα, αν υποθέσουμε ότι κάθε βήμα

απαιτεί για την εκτέλεσή του 1 msec = 10-6 sec , τότε ο αλγόριθμος χρειάζεται 2 x 109 χρόνια (!) για νε παραγοντοποιήσει έναν αριθμό αποτελούμενο από 600 bits. Το 1978 ο R.Rivest κατέληξε στο συμπέρασμα ότι η παραγοντοποίηση ενός αριθμού της τάξης του 10200, χρησιμοποιώντας τον αποδοτικότερο αλγόριθμο παραγοντοποίησης και σύστημα με υπολογιστική ισχύ 1 MIPS (Million Instructions Per Second - εκατομμύρια εντολές το δευτερόλεπτο), θα απαιτούσε περισσότερα από 4 δισεκατομμύρια χρόνια (4x109). Από τότε μέχρι σήμερα έχουνε αναπτυχθεί υπολογιστικά συστήματα με πολλαπλάσια υπολογιστική ισχύ, όμως η υπολογιστική πολυπλοκότητα του προβλήματος αυτού παραμένει τόσο μεγάλη, ώστε εξασφαλίζει το βαθμό ασφάλειας του κρυπτοσυστήματος.

Ο αλγόριθμος RSA, με κάποια τροποποίηση στη διαδικασία κρυπτογράφησης και αποστολής μηνυμάτων, να συνδυάσει την κρυπτογράφηση μαζί με την αυθεντικοποίηση των μηνυμάτων. Συνεπώς, το σχήμα αυτό παρουσιάζει αρκετά πλεονεκτήματα έναντι άλλων μεθόδων, αν και πιθανή απόδειξη ότι ο αλγόριθμος δεν ανήκει στην NP-Complete κλάση προβλημάτων (συνεπώς υπάρχει αλγόριθμος κρυπτανάλυσής του σε πολυωνυμικό χρόνο) θα επιφέρει σοβαρές αμφισβητήσεις για το βαθμό ασφάλειας που προσφέρει.

4.5 Σύγκριση μεθόδων ιδιωτικού και δημόσιου κλειδιού

Η σύγκριση των μεθόδων ιδιωτικού (secret-key) και δημόσιου κλειδιού (public-key) σχετικά με τα πλεονεκτήματα και το μειονεκτήματα της κάθε μιας, μπορεί να επικεντρωθεί σε τρία κύρια σημεία: το βαθμό ασφάλειας που προσφέρουν, την ευκολία χρήσης και την απόδοση.

Όσο αφορά το βαθμό ασφάλειας, με κατάλληλη επιλογή κλειδιών και αλγορίθμων κρυπτογράφησης, και οι δύο μέθοδοι θεωρούνται "επαρκώς ασφαλείς" στον ίδιο βαθμό, μια και δεν έχει αναφερθεί περίπτωση επιτυχούς κρυπτανάλυσης σε καμία από τις δύο.

Παρόλα αυτά, οι μέθοδοι δημόσιου κλειδιού είναι γενικά ευκολότερες στη χρήση, μια και η εξάλειψη της ανάγκης ύπαρξης ασφαλούς διαύλου επικοινωνίας για την ανταλλαγή κλειδιών (περίπτωση ιδιωτικών κλειδιών). Φυσικά, η ανάγκη σωστής αναγνώρισης του νόμιμου πομπού υπάρχει και στην περίπτωση της μεθόδου δημόσιου κλειδιού (η αναγνώριση γίνεται αυτόματα σε περίπτωση ιδιωτικού κλειδιού).

Από την άλλη πλευρά, η απόδοση των αλγορίθμων ιδιωτικού κλειδιού είναι κατά πολύ μεγαλύτερη από αυτή των αντίστοιχων αλγορίθμων ιδιωτικού κλειδιού. Αυτό οφείλεται στη φύση και τα ιδιαίτερα χαρακτηριστικά της κάθε μεθόδου, κυρίως όσο αφορά την τεχνική εξασφάλισης του βαθμού ασφάλειας του κάθε κρυπτοσυστήματος. Ο παρακάτω πίνακας παρουσιάζει μια πρακτική σύγκριση των αλγορίθμων RSA (pyblic-key) και DES (secret-key), τους σημαντικότερους αντιπροσώπους της κάθε κατηγορίας. Οι δοκιμές με υλοποίηση σε λογισμικό (software) βασίζονται σε υπολογιστικό σύστημα με επεξεργαστή Intel 286/8MHz με ισχύ 0.5 MIPS. Ο αλγόριθμος δημόσιου κλειδιού έγινε με βάση τμήματα μήκους 500 bits, ενώ ο αλγόριθμος ιδιωτικού κλειδιού χρησιμοποιεί πίνακα μεγέθους 64 Kbytes για κάθε κλειδί. Φυσικά, τα νούμερα είναι εντελώς ενδεικτικά και δείχνουν μόνο τις διαφορές στην απόδοση ως τάξη μεγέθους (όπου είναι δυνατό να γίνει μια τέτοια σύγκριση).

Αλγόριθμος	Υλοποίηση software (bps)	Υλοποίηση hardware (bps)
RSA (public-key)		
Εκ(X)	0.5 x 103	220 x 103
Dκ(X)	32 x 103	(δεν υπάρχει)

DES (secret-key)

Εκ(X)/Dκ(X)	400 x 103	1.2 x 109

Σε πραγματικές εφαρμογές, συχνά χρησιμοποιείται κάποιο σύνθετο σχήμα που συνδυάζει τις δύο παραπάνω μεθόδους. Ένα τυπικό παράδειγμα τέτοιου σχήματος χρησιμοποιεί αλγορίθμους δημόσιου κλειδιού για την αποστολή ενός ιδιωτικού κλειδιού, που χρησιμοποιείται για την κρυπτογράφηση μηνύματος. Το σύνθετο αυτό σχήμα, σε συνδυασμό με την ύπαρξη κατάλληλης "υπηρεσίας αυθεντικοποίησης" (authentication service), μπορεί να υλοποιήσει τον ασφαλή δίαυλο ανταλλαγής ιδιωτικών κλειδιών στον ίδιο τον -κοινό ("ανασφαλή")- δίαυλο επικοινωνίας. Το πρόβλημα αυτό ανάγεται στο πρόβλημα κατασκευής εξυπηρέτη αυθεντικοποίησης (authentication server), την διανομή κλειδιών (key distribution), τη χρήση ψηφιακών υπογραφών (digital signatures), κτλ.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από τις τεχνικές που αναφέρθηκαν είναι φανερό ότι η Κρυπτογραφία παρέχει ένα ευρύ φάσμα δυνατοτήτων, που επεκτείνονται από την απλή προστασία ενός αρχείου ή προγράμματος, μέχρι την υιοθέτηση ενός προτύπου γενικής χρήσης. Η επιλογή μιας συγκεκριμένης μεθόδου εξαρτάται από τις απαιτήσεις σε ασφάλεια, το περιβάλλον στο οποίο καλείται να λειτουργήσει και φυσικά από τις δυνατότητες του υπάρχοντος εξοπλισμού. Ακόμα και σχετικά απλές μέθοδοι, όπως η μέθοδος της αντικατάστασης, μπορεί να καλύψει τις απαιτήσεις ενός (ελάχιστα απαιτητικού) περιβάλλοντος. Αντίθετα, η υιοθέτηση ενός προτύπου, όπως το DES και το RSA, απαιτεί προσεκτική εκτίμηση μιας σειράς παραγόντων, που δεν είναι απαραίτητα πάντα τεχνικοί.

Δεδομένου ότι η μαθηματική υποδομή που απαιτείται για την κρυπτανάλυση ενός κρυπτογραφικού σχήματος είναι αρκετά ευρεία, τόσο σε έκταση όσο και σε βάθος, δεν φαίνεται πιθανό ότι -ακόμη και απλές μέθοδοι- μπορούν εύκολα να κρυπταναλυθούν. Επιπλέον, δεν υπάρχουν (τουλάχιστον υπό τη μορφή ευρεία διαδεδομένων εφαρμογών) κάποια πακέτα λογισμικού με παραμετρικές κρυπταναλυτικές δυνατότητες. Σημαντικό είναι το γεγονός ότι, ενώ τόσο για σχήματα τύπου DES όσο και RSA, δεν υπάρχουν μαθηματικές αποδείξεις που να βεβαιώνουν ότι τα σχήματα αυτά είναι ασφαλή, δεν έχουν αναφερθεί ποτέ επιτυχημένες προσπάθειες κρυπτανάλυσής τους. Ένας αποδεκτός "δείκτης" της ασφάλειας που προσφέρουν είναι ο χρόνος "αντοχής" τους σε κρυπταναλυτικές προσπάθειες. Για το σύστημα DES, για παράδειγμα, η εταιρία IBM ισχυρίζεται ότι έχει αφιερώσει 17 ανθρωπο-χρόνια κρυπταναλυτικών προσπαθειών, χωρίς αποτέλεσμα.

Αυθεντικοποίηση και κατανομή κλειδιών

Τα δύο προβλήματα της αυθεντικοποίησης και της ασφαλούς κατανομής των κλειδιών γίνονται με μία υπηρεσία, η οποία συζητήται σε αυτήν την ενότητα.

Έχει γίνει βελτίωση τα προηγούμενα χρόνια πάνω στην θεωρία και πράξη της αυθεντικοποίησης. Σε αυτήν την ενότητα θα περιγράψουμε το μοντέλο ενός server αυθεντικοποίησης κατά Needlham και Schroeder. Στην επόμενη ενότητα θα περιγράψουμε την υπηρεσία αυθεντικοποίησης Kerberos το οποίο έχει υλοποιηθεί στο MIT χρησιμοποιώντας ως βάση του το μοντέλο των Needlham και Schroeder.

Οι Neeedlham και Schroeder πρώτοι πρότειναν μια λύση στην αυθεντικοποίηση και την κατανομή κλειδιών που βασίζεται σε έναν server αυθεντικοποίησης που προμηθεύει με κλειδιά τους clients. Η δουλειά ενός server αυθεντικοποίησης είναι να αναπτύξει έναν ασφαλή τρόπο για ζεύγη διεργασιών να πάρουν κλειδιά.Για να το κάνει αυτό, θα πρέπει να επικοινωνήσει με τους clients χρησιμοποιώντας κρυπτογραφημένα μυνήματα. Οι Neeedlham και Schroeder περιγράφουν δύο πρωτόκολλα για ασφαλούς server αυθεντικοποίησης,χρησιμοποιώντας για τον ένα μυστικά κλειδιά και για τον άλλο δημόσια κλειδιά.

Κατά Neeedlham και Schroeder με μυστικά κλειδιά. Σε αυτό το μοντέλο, μία διεργασία που δουλεύει εκ μέρους ενός A που θέλει να έχει ασφαλή επικοινωνία με κάποια άλλη διεργασία που δουλεύει εκ μέρους ενός B μπορεί να αποκτήσει ένα κλειδί γι' αυτόν τον σκοπό. Το πρωτόκολλο περιγράφεται για δύο διεργασίες A και B, αλλά σε συστήματα client-server, ο A συνήθως θα είναι ένας client που θα στέλνει μία ακολουθία αιτήσεων σε κάποιο server B. Το κλειδί προμηθεύεται στον A σε δύο μορφές, μία που μπορεί να χρησιμοποιήσει ο A για να κρυπτογραφήσει τα μηνύματα που στέλνει στον B και ένα που μπορεί να μεταδώσει με ασφάλεια στον B. (Το τελευταίο είναι κρυπτογραφημένο με ένα κλειδί που ξέρει μόνο ο B και όχι ο A, έτσι ώστε ο B μπορεί να το αποκρυπτογραφήσει και το κλειδί δεν γίνεται γνωστό κατά την μετάδωση.)

Ο server αυθεντικοποίησης περιλαμβάνει έναν πίνακα που περιλαμβάνει ένα όνομα και ένα μυστικό κλειδί για κάθε principal που είναι γνωστό στο σύστημα.Το μυστικό κλειδί χρησιμοποιείται μόνο για να αυθεντικοποιήσει client διεργασίες στον

server αυθεντικοποίησης και να μεταδώσει μηνύματα με ασφάλεια ανάμεσα σε client διεργασίες και τον server αυθεντικοποίησης. Δεν δίνεται ποτέ σε τρίτα μέρη και μεταδίδεται μέσω του δικτύου το πολύ μία φορά, όταν δημιουργείται. (Ιδανικά, ένα κλειδί πρέπει να μεταδίδεται με άλλους τρόπους, όπως με το χαρτί ή προφορικά, για να αποφευχθεί οπιαδήποτε έκθεση στο δίκτυο.) Ένα μυστικό κλειδί είναι ισοδύναμο με ένα συνθηματικό που χρησιμοποίείται για να αυθεντικοποιεί τους χρήστες σε κεντρικοποιημένα συστήματα. Για τους ανθρώπους το όνομα που κρατείται από τον server αυθεντικοποίησης είναι τα "user name" τους και ως κλειδί το συνθηματικό τους. Και τα δύο προμηθεύονται από τον χρήστη, από αιτήσεις των client διεργασιών που λειτουργούν εκ μέρους του.

Σχηματοποιούμε τα μηνύματα που ανταλλάσονται σύμφωνα με το πρωτόκολλο Neeedlham και Schroeder μυστικού κλειδιού στο σχήμα 16.6 , χρησιμοποιώντας τον συμβολισμό {}K που χρησιμοποιήθηκε πριν για να δείξει την κρυπτογράφηση με το κλειδί K. Ο server αυθεντικοποίησης είναι ο S.

Επικεφαλίδα Μήνυμα Παρατηρήσεις

1.A->S: A,B,NA Ο A ζητάει απο τον S να τον προμηθεύσει με ένα κλειδί για την επικοινωνία με τον B.

2.S->A: {NA,B,KAB,{KAB,A}KB}KA Ο S επιστρέφει ένα μήνυμα κρυπτογραφημένο με το μυστικό κλειδί του A, που περιλαμβάνει ένα πρόσφατα υπολογισμένο κλειδί KAB, και ένα εισιτήριο κρυπτογραφημένο με το μυστικό κλειδί του B. Το nonce δείχνει ότι το μήνυμα στάλθηκε προς απάντηση στο προηγούμενο. Ο A πιστεύει ότι ο S έστειλε το μήνυμα γιατί μόνο ο S ξέρει το μυστικό κλειδί του A.

3.A->B: {KAB,A}KB Ο A στέλνει το εισιτήριο στον B.

4.B->A: {NB}KAB Ο B αποκρυπτογραφεί το κλειδί και χρησιμοποιεί το νέο κλειδί KAB για να κρυπτογραφήσει κάποιο άλλο nonce NB.

5.A->B: {NB-1}KAB Ο A αποδυκνύει στον B οι είναι ο αποστολέας του προηγούμενου μηνύματος επιστρέφοντας έναν σύμφωνο μετασχηματισμό του NB.

Συμβολισμός:

A: Το όνομα του μέρους της διεργασίας που αρχίζει την επικοινωνία.

B: Το όνομα του συντρόφου του A στην επικοινωνία.

KA: Το μυστικό κλειδί του A (password).

KB: Το μυστικό κλειδί του B (password).

KAB: Το μυστικό κλειδί για την επικοινωνία ανάμεσα στο A και στο B.

NA: Το nonce που δημιουργείται από τον A.

{M}K: Το μήνυμα M που κρυπτογραφείται με το κλειδί K.

Το πρωτόκολλο βασίζεται στην δημιουργία και μετάδοση των κουπονιών από τον server αυθεντικοποίησης. Ένα κουπόνι είναι ένα κρυπτογραφημένο μήνυμα που περιλαμβάνει ένα μυστικό κλειδί για χρήση στην επικοινώνία μεταξύ A και B.

Ένα nonce είναι μία ακέραια τιμή που περιλαμβάνεται σε ένα μήνυμα για να διαπιστωθεί πόσο καινούργιο είναι. Τα nonces χρησιμοποιούνται μόνο μία φορά και δημιουργούνται όταν ζητούνται. Παράδειγμα, τα nonces μπορούν να δημιουργηθούν σαν μία ακολουθία από ακέραιες τιμές ή διαβάζοντας το ρολόι της μηχανής που στέλνει.

Αν το πρωτόκολλο συμπληρώνεται ικανοποιητικά , και τα δύο μέρη A και B μπορούν να είναι σίγουρα, ότι κάθε μήνυμα που λαμβάνουν και έχει κρυπτογραφηθεί με το KAB στέλνεται από τον άλλο, και ότι κάθε μήνυμα που στέλνουν και έχει κρυπτογραφηθεί με το KAB μπορεί να το καταλάβει μόνο το άλλο μέρος ή ο S (που πρέπει να είναι αξιόπιστος). Αυτό συμβαίνει γιατί τα μόνα μηνύματα που έχουν σταλεί και περιλαμβάνουν το KAB έχουν κρυπτογραφηθεί είτε με το μυστικό κλειδί του A είτε με το μυστικό κλειδί του B.

Υπάρχει μία αδυναμία σε αυτό το πρωτόκολλο στο ότι ο B δεν έχει κανένα λόγο να πιστέψει ότι το μήνυμα 3 είναι καινούργιο. Κάποιος που καταφέρνει να αποκτήσει το κλειδί KAB και να φτιάξει ένα αντίγραφο του κλειδιού και του αυθεντικοποιητή (τα οποία και τα δύο μπορεί να έχουν μείνει σε μία εκτεθημένη τοποθεσία αποθήκευσης εξαιτίας μιας απροσεξίας ή ενός αποτυχημένου client που τρέχει υπό την δικαιοδοσία του A), μπορεί να τα χρησιμοποιήσει για να κάνει μία παράνομη ανταλλαγή με τον B, προσποιούμενος τον A. Σήμερα οι Neeedlham και Schroeder δεν συμπεριλαμβάνουν αυτήν την πιθανότητα στην λίστα των απειλών

τους αν και πρέπει. Αυτή η αδυναμία μπορεί να ξεπεραστεί με μία σφραγίδα χρόνου που προστείθεται στο μήνυμα 3 το οποίο γίνεται: {KAB,A,t}KB. Ο Β αποκρυπτογραφεί αυτό το μήνυμα και ελέγχει αν το t είναι πρόσφατο. Αυτή είναι η λύση που υιοθετείται απο τον Kerberos.

Neeedlham και Schroeder με δημόσια κλειδιά: Τα δημόσια κλειδιά πρέπει να καταεμηθούν από έναν αξιόπιστο server κατανομής κλειδιών για να αποφευχθούν επιθέσεις. Όταν αποκτά ένα δημόσιο κλειδί για χρήση στην επικοινωνία με τον Β, ο Α ελπίζει ότι πράγματι αποκτά το δημόσιο κλειδί του Β και όχι κάποιο άλλο κλειδί που στέλνεται από κάποιον που προσπειήται τον Β.

Το πρωτόκολλο των Neeedlham και Schroeder για αυθεντικοποίηση με δημόσια κλειδιά περιγράφεται στο σχήμα 16.7.

Επικεφαλίδα Μήνυμα Παρατηρήσεις

1.A->S: A,B Ο Α ζητάει το δημόσιο κλειδί του Β από τον S.

2.S->A: {PKB,B}SKS Ο S στέλνει το δημόσιο κλειδί του Β στο Α, κρυπτογραφημένο χρησιμοποιώντας το μυστικό του κλειδί. Το μήνυμα κρυπτογραφείται για να εξασφαλίσει ότι δεν ανακαστευτεί κάποιος με αυτό.Ο Α (και οποιοσδήποτε άλλος) μπορούν να αποκρυπτογραφήσουν το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του server, PKS.

3.A->B: {NA,A}PKB Ο Α στέλνειένα μήνυμα που περιέχει ένα nonce στον Β, κρυπτογραφημένο με το δημόσιο κλειδί του Β. Μόνο ο Β μπορεί να το αποκρυπτογραφήσει για να πάρει το όνομα του Α.

4.B->S: B,A Ο Β ζητάει το δημόσιο κλειδί του Α από τον S.

5.S->B: {PKA,A}SKS Ο S στέλνει το δημόσιο κλειδί του Α στον Β, κρυπτογραφημένο με το μυστικό κλειδί του.

6.B->A: {NA,NB}PKA Ο Β στέλνει στον Α ένα ζευγάρι από nonces κρυπτογραφημένεα με το δημόσιο κλειδί του Α.

7.A->B: {NB}PKB Ο Α στέλνει το nonce που μόλις έλαβε, κρυπτογραφημένο με το δημόσιο κλειδί του Β, αποδεικνύοντας ότι η επικοινωνία είναι καινούργια και ότι

είναι πράγματι ο Α που επικοινωνεί (από την στιγμή που μόνο ο Α μπορεί να αποκρυπτογραφήσει το Μήνυμα 6)

Πρόσθετοι συμβολισμοί:

PKA Το δημόσιο κλειδί του Α

PKB Το δημόσιο κλειδί του Β

PKS Το δημόσιο κλειδί του S

SKS Το μυστικό κλειδί του S

Μια αδυναμία του πρωτοκόλλου βρέθηκε από τους Barrows, Abadi και Neeedlham χρησιμοποιώντας την λογική που ανέπτυξαν για να αναλύσουν τις ιδιότητες των πρωτοκόλλων αυθεντικοποίησης. Αυτή η αδυναμία είναι ότι το Α και το Β πρέπει να πιστέψουν ότι τα δημόσια κλειδιά που λαμβάνουν από τον S είναι καινούργια. Δεν υπάρχει προστασία ενάντια στην κατακράτηση παλιών μηνυμάτων. Αυτό μπορεί να αντιμετωπιστεί προσθέτοντας σφραγίδες χρόνου στα μηνύματα 2 και 5.

Ψηφιακές υπογραφές

Τα κείμενα όπως τα συμβόλαια υπογράφονται όταν γράφονται και μετά μεταδίδονται στα άλλα μέρη. Οι υπογραφές επιτρέπουν σε οποιοδήποτε πρόσωπο που λαμβάνει ένα κείμενο να διαπιστώσει ότι το κείμενο έχει πράγματι από τον υπογράφοντα και ότι δεν έχει αλλάξει. Η υπογραφή χαρακτηρίζει τον υπογράφοντα.

Οι υπογραφές παρέχουν μόνο μία μη πλήρη λύση σε αυτές τις απαιτήσεις:

. Πλαστογραφημένες υπογραφές είναι δύσκολο να βρεθούν αν δεν υπάρχουν κάποια πρότυπα για να τις συγκρύνουμε. Ακόμα όμως και τότε μπορεί να μην βρεθούν.

. Μία υπογραφή δεν μπορεί να εμποδίσει την τροποποίηση ενός κειμένου.

. Αυτός που υπογράφει μπορεί τυχαία να υπογράψει ή και να εξαναγκαστεί να το κάνει.

. Υπογραφές μαρτύρων προσθέτονται συχνά σε ένα κείμενο για να κάνουν πιο έγκυρη την κύρια υπογραφή, αλλά μπορούν να υποφέρουν από ανάλογη αδυναμία.

Παρόλα αυτά, οι υπογραφές χρησιμοποιούνται ευρέως για ταυτοποίηση στα συμβατικά κείμενα. Μία υπογραφή δείχνει ότι το κείμενο δημιουργήθηκε εν γνώση

αυτού που υπογράφει και ότι δεν έχει αλλάξει. Οι υπογραφές όμως δεν εφαρμόζονται

στα κείμενα που δημιουργούνται σε υπολογιστές. Ας δούμε πως μπορούν αυτές οι

ιδιότητες να επιτευχθούν σε τέτοια κείμενα.

Σε υπολογιστικά συστήματα, κείμενα ή μηνύματα μπορούν να προτυποποιηθούν

με την ταυτότητα ενός αντικειμένου, μεταδιδόμενα σε άλλο. Συχνά είναι απαραίτητο

ότι κάθε παραλήπτης μπορεί να διαπιστώσει ότι αυτός που ισχειρίζεται ότι

δημιούργησε το κείμενο είναι ο αληθινός δημιουργός του, ότι το κείμενο δεν έχει

αλλάξει και ότι ο δημιουργός δεν μπορεί να το αποκυρήξει.

Εν συντομία, προτείνεται μία ψηφιακή υπογραφή. Οι δύο έννοιες (ψηφιακή

και συμβατική υπογραφή) διαφέρουν στο ότι όταν μία υπογραφή προστίθεται σε ένα

ηλεκτρονικό κείμενο, είναι δυνατόν για έναν που λαμβάνει ένα αντίγραφο του

μηνύματος από κάθε πηγή να διαπιστώσει ότι το κείμενο στάλθηκε αρχικά από αυτόν

που το υπογράφει, και ότι δεν έχει αλλάξει κατά την μεταφόρά.

Ένα ηλεκτρονικό κείμενο ή μήνυμα Μ μπορεί να υπογραφεί από κάποιον Α

κρυπτογραφόντας ένα αντίγραφο του Μ με ένα κλειδί ΚΑ και προσθέτοντας το απλό Μ

και τον ταυτοποιητή του Α. Το υπογεγραμένο κείμενο περιλαμβάνει το <M,A,{M}KA>.

Ο σκοπός της πρόσθεσης της υπογραφής στο κείμενο είναι να επιτραπεί στον καθένα

που παραλαμβάνει το κείμενο να επαληθεύσει ότι το κείμενο πράγματι προήλθε από

τον Α και ότι τα περιεχόμενα του Μ δεν έχουν αλλάξει.

Ο τρόπος για την επιβεβαίωση της υπογραφής εξαρτάται από το αν

χρησιμοποιείθηκε κρυπτογράφηση με μυστικό ή δημόσιο κλειδί. Παρακάτω

περιγράφουμε και τους δύο τρόπους.

Για να μειώθεί το μέγεθος της υπογραφής για μεγάλα κείμενα,

χρησιμοπείται μία συνάτηση περίληψης D που παράγει μία χαρακτηριστική τιμή που

μοναδικά ταυτοποιεί το μήνυμα που υπογράφεται. Η χαρακτηριστική τιμή είναι μία

σταθερού μήκους συμβολοσειρά που υπολογίζεται από το μήνυμα όπως και ένα

άθροισμα ελέγχου ή μία συνάρτηση κατακερματισμού. Πρέπει να σχεδιαστούν

προσεκτικά για να εγγυώνται ότι για οποιαδήποτε διαφορετικά μηνύματα Μ και Μ', η

D(M) είναι διαφορετική από την D(M'). Μία τέτοια συνάρτηση γνωστή ως MD5 έχει

σχεδιαστεί γι'αυτό το σκοπό και προτείνεται από τον Rivest για χρήση στο ασφαλές

mail και σε άλλες εφαρμογές στο Internet. Ο Mitchell εξετάζει τις τεχνικές των

ψηφιακών υπογραφών σε βάθος, με μία χρήσιμη συζήτηση για συναρτήσεις digest.

Ψηφιακές υπογραφές με δημόσια κλειδιά. Είναι πολύ απλό να παράγουμε το

επιθημητό αποτέλεσμα χρησιμοποιώντας δημόσια κλειδιά. Ο δημιουργός Α του

μηνύματος M μπορεί να το υπογράψει προσθέτοντας σε αυτό ένα αντίγραφο του D(M)

κρυπτογραφημένο με το μυστικό κλειδί KAprivate και στέλνοντας το σε άλλο μέρος.

Ο παραλήπτης, και όποιος άλλος λάβει το μήνυμα, μπορεί να επιβεβαιώσει την

υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του A για να αποκρυπτογραφήσει την

υπογραφή, για να λάβει το D(M) και να το συγκρίνει με τον δικό του υπολογισμό

του D(M). Έτσι δεν ανακατεύεται κάποιος server, εκτός από κάποιον server

κατανομής κλειδιών που προμηθεύει σε καθέναν το δημόσιο κλειδί του A που δεν το

έχει ήδη. Το πρωτόκολλο αν ο A στέλνει το υπογεγραμένο κείμενο στον B που με την

σειρά του ελέγχει την υπογραφή είναι:

Επικεφαλίδα Μήνυμα Παρατηρήσεις

1.A->B: M,A,{D(M)}KAprivate Ο A στέλνει το αυθεντικό μήνυμα και την υπογραφή

στον B.

2.B->S: A Ο B ζητάει το δημόσιο κλειδί του A από τον S.

3.S->B: A,KApublic Ο S δίνει το δημόσιο κλειδί του A, KApublic. Ο B το

χρησιμοποιεί για να αποκρυπτογραφήσει την υπογραφή που λαμβάνεται στο Μήνυμα 1

και το συγκρίνει με μία πρόσφατα υπολογισμένη τιμή του D(M).

Ψηφιακές υπογραφές με μυστικά κλειδιά. Οι Needlham και Schroeder περιέγραψαν

μία ψηφιακή υπογραφή που βασίζεται στην υπηρεσία ταυτοποίησης που περιγράφεται

στα προηγούμενα κεφάλαια. Παρακάτω περιγράφουμε τα βήματα του πρωτοκόλλου που

πρότειναν κι όπου ο Α στέλνει ένα υπογεγραμένο μήνυμα Μ στον Β χρησιμοποιώντας

μυστικά κλειδιά:

Επικεφαλίδα Μήνυμα Παρατηρήσεις

1.A->S: A,{D(M)}KA Ο Α υπολογίζει την περίληψη του μηνύματος D(M)

κρυπτογραφεί το D(M) με το μυστικό κλειδί του Α και το στέλνει στο server

ταυτοποίησης.

2.S->A: {A,D(M),t}KS Ο server φτιάχνει ένα υπογεγραμένο και χρονολογημένο

πιστοποιητικό της υπογραφής του Α φτιάχνοντας ένα κείμενο που περιλαμβάνει το

όνομα του Α, το D(M) και μία χρονο-σφραγίδα t και το κρυπτογραφεί με το μυστικό

του κλειδί. Στέλνει το αποτέλεσμα ως πιστοποιητικό στον Α.

3.A->B: M,{A,D(M),t}KS Ο Α στέλνει το αυθεντικό μήνυμα και το πιστοποιητικό σε

ένα μήνυμα στον Β.

4.B->S: B,{A,D(M),t}KS Ο Β σώζει ένα αντίγραφο του μηνύματος και του

πιστοποιητικού και στέλνει το πιστοποιητικο στον S για αποκρυπτογράφηση.

5.S->B: {A,D(M),t}KB Ο S αποκρυπτογραφεί το πιστοποιητικό. Τότε χρησιμοποιεί

το μυστικό κλειδί του Β για να κρυπτογραφήσει το αποτέλεσμα και το στέλνει στο

Β, όπου αποκρυπτογραφείται.

Από αυτό το στάδιο, ο Β έχει δύο πράγματα. Το μήνυμα που έλαβε από τον Α, που περιλαμβάνει το όνομα του Α και το κείμενο του μηνύματος, και το πιστοποιητικό, Α, D(M). Χρησιμοποιεί την συνάρτηση περίληψης για να υπολογίσει την τιμή του D(M) από το κείμενο του μηνύματος και το συγκρίνει με την τιμή που έλαβε από τον S. Αν ταιριάζουν τότε ο Β μπορεί να είναι σίγουρος ότι το μήνυμα είναι αυτό που στην πραγματικότητα δημιουργήθηκε από τον Α και ότι ο Α δεν θα το αποκυρήξει γιατί:

. Ο S επιβεβαιώνει την υπογραφή του Α στο βήμα 2. Ο χρήστης Β εμπιστεύεται τον S και έχει ένα μήνυμα απο τον S ότι η υπογραφή του Α επιβεβαιώθηκε.

. Θα ήταν δύσκολο για τον Α να ισχυριστεί ότι η υπογραφή του έχει πλαστογραφηθεί, γιατί ο Β έχει ένα αντίγραφο ενός πιστοποιητικού που μπορεί να ελεγχθεί από τον S. Ο Α δεν μπορεί να ισχυριστεί ότι ο Β έχει πλαστογραφήσει το πιστοποιητικό γιατί ο Β δεν ξέρει το μυστικό κλειδί του S.

Μελέτη: Kerberos

Ο Kerberos είναι ένα πρωτόκολλο αυθεντικοποίησης που βασίζεται στο πρωτόκολλο Needlham και Scroeder με μυστικά κλειδιά. Έχει αναπτυχθεί στο MIT για να εξασφαλίσει μια σειρά από ευκολίες για αυθεντικοποίηση και ασφάλεια για χρήση στο πανεπιστημιακό δίκτυο Athena και άλλα ανοιχτά συστήματα. Το πρωτόκολλο Kerberos έχει υποστεί μια σειρά από επαναλήψεις και επαυξήσεις από την εμπειρία και την επίδραση από οργανισμούς χρηστών και η πιο πρόσφατη έκδοση που θα περιγράψουμε εδώ είναι γνωστή ως έκδοση 5. Χρησιμοποιείται ευρύτατα στο MIT και αλλού για να εξασφαλίσει ασφαλή πρόσβαση στο NFS, στο Andrew File System και πολλές άλλες εφαρμογές. Το Open Software Foundation's Distributed Computing Environment και σε πρόσφατες εκδόσεις του Andrew File System (έκδοση 3 και μετά) περιλαμβάνει μια ολοκληρωμένη υλοποίηση του Kerberos.

Το σχήμα δείχνει την αρχιτεκτονική της διεργασίας. Το Kerberos έχει τρία είδη αντικειμένων για ασφάλεια:

Εισιτήριο: ένα κουπόνι που δίνεται από τον client από τον Kerberos για να παρουσιαστεί σε έναν συγκεκριμένο server, αποδεικνύοντας ότι ο αποστολέας έχει πρόσφατα αυθεντικοποιηθεί από τον Kerberos. Τα εισιτήρια περιλαμβάνουν έναν χρόνο λήξεως και ένα νεοδημιούργητο κλειδί συνόδου για χρήση από τον client και τον server.

Αυθεντικοποιητής: ένα κουπόνι που δημιουργείται από έναν client και στέλνεται σε έναν server για να αποδείξει την ταυτότητα του χρήστη και την εγκυρότητα κάθε επικοινωνίας με έναν server. Ένας αυθεντικοποιητής μπορεί να χρησιμοποιηθεί μόνο μία φορά. Περιλαμβάνει το όνομα του client και μία σφραγίδα χρόνου και κρυπτογραφείται με το κατάλληλο κλειδί συνόδου.

Κλειδί συνόδου: ένα μυστικό κλειδί που δημιουργείται τυχαία από τον Kerberos και δίνεται σε έναν client για χρήση όταν επικοινωνεί με έναν συγκεκριμένο server. Η κρυπτογράφηση δεν είναι υποχρεωτική για όλες τις επικοινωνίες με servers: Το κλειδί συνόδου χρησιμοποιείται για την κρυπτογράφηση της επικοινωνίας

με αυτούς τους servers που το απαιτούν και για την κρυπτογράφηση όλων των αυθεντικοποιητών.

Οι client διεργασίες πρέπει να κατέχουν ένα εισιτήριο και ένα κλειδί συνόδου για κάθε server που χρησιμοποιούν. Δεν θα ήταν λογικό να δίνουμε ένα νέο εισιτήριο για κάθε αλληλεπίδραση client-server, έτσι τα περισσότερα κλειδιά δίνονται στους clients με διάρκεια ζωής κάποιων ωρών έτσι ώστε να χρησιμοποιηθούν για μία αλληλεπίδραση με έναν συγκεκριμένο server μέχρι να λήξουν.

Ένας Kerberos server είναι γνωστός ως ένα Κέντρο Κατανομής Κλειδιών (KDC στα αγγλικά). Κάθε KDC προσφέρει μία Υπηρεσία Αυθεντικοποίησης (AS) και μία Υπηρεσία Παροχής Εισιτηρίων (TGS). Στο login, οι χρήστες αυθεντικοποιούνται από την Υπηρεσία Αυθεντικοποίησης, χρησιμοποιώντας μια δικτυακή και ασφάλη παραλλαγή της μεθόδου του password, και η client διεργασία που ενεργεί εκ μέρους του χρήστη προμηθεύεται με ένα εισιτήριο παροχής εισιτηρίων και ένα κλειδί συνόδου για την επικοινωνία με το TGS. Η αρχική client διεργασία και τα παιδιά της μπορούν να χρησιμοποιείσουν το εισιτήριο παροχής εισιτηρίων για να αποκτήσουν εισιτήρια και κλειδιά συνόδων για συγκεκριμένες υπηρεσίες από το TGS.

Το πρωτόκολλο Needlham και Scroeder έχει ακολουθηθεί στενά στο Kerberos, με χρόνους τιμών (ακέραιοι που παριστούν μια ημερομηνία) που χρησιμοποιούνται για nonces. Αυτό εξυπηρετεί δύο σκοπούς:

. να προφυλαχθούμε από κατακρατήσεις παλιών μηνυμάτων ή την επαναχρησιμοποίηση παλιών εισιτηρίων που κάθονται στην μνήμη μηχανών απ'όπου ο εξουσιοδοτημένος χρήστης έχει βγέι (τα nonces χρησιμοποιούνται για να πετύχουν αυτό το σκοπό στο πρωτόκολλο Needlham και Scroeder).

. να βάλουμε μια διάρκεια ζωής στα εισιτήρια, επιτρέποντας στο σύστημα να ανακαλέσει τα δικαιώματα χρηστών όταν παύουν να είναι εξουσιοδοτημένοι χρήστες του συστήματος.

Παρακάτω περιγράφουμε λεπτομερειακά το πρωτόκολλο Kerberos, χρησιμοποιώντας τον συμβολισμό που ορίζεται στην συνέχεια. Πρώτα περιγράφουμε το πρωτόκολλο με το οποίο ο client αποκτά ένα κλειδί και ένα κλειδί συνόδου για πρόσβαση στο TGS.

Ένα εισιτήριο στο Kerberos έχει μια σταθερή τιμή εγκυρότητας που αρχίζει στον χρόνο t1 και τελειώνει στον χρόνο t2. Το εισιτήριο για έναν client για πρόσβαση στον server S παίρνει την μορφή:

{C,S,t1,t2,KCS}KS

στο οποίο θα αναφερόμαστε ως:

{ticket(C,S)}KS

Το όνομα του client συμπεριλαμβάνεται στο εισιτήριο για να αποφευχθεί πιθανή χρήση από απατεώνες, όπως θα δούμε αργότερα. Οι αριθμοί στα μηνύματα αντιστοιχούν σ'αυτούς στο σχήμα 16.8. Παρατηρήστε ότι το μήνυμα 1 δεν είναι κρυπτογραφημένο και δεν συμπεριλανβάνει το password του C. Περιλαμβάνει ένα nonce που χρησιμοποιείται για να ελέγξει την εγκυρότητα της απάντησης.

Επικεφαλίδα	Μήνυμα	Παρατηρήσεις
1.C->A: Αίτηση για εισιτήριο από TGS	C,T,n	Ο client C ζητάει από τον server αυθεντικοποίησης A του Kerberos να τον εφοδιάσει με ένα κλειδί για επικοινωνία με την υπηρεσία παροχής εισιτηρίων T.
2.A->C: Κλειδί συνόδου και εισιτήριο από το TGS	{KCT,N}KC, {ticket(C,T)}KT	περιλαμβάνει C, T, t1, t2, KCT Ο A επιστρέφει ένα μήνυμα που περιλαμβάνει ένα εισιτήριο κρυπτογραφημένο με το μυστικό του κλειδί και ένα κλειδί συνόδου για τον C για χρησιμοποίηση με το T. Ο συνυπολογισμός του nonce που κρυπτογραφείται με το KC δείχνει ότι το μήνυμα έρχεται από τον παραλήπτη του μηνύματος 1, που πρέπει να ξέρει το KC.

Συμβολισμός:

A: Όνομα της υπηρεσίας αυθεντικοποίησης του Kerberos.

T: Όνομα της υπηρεσίας παροχής κλειδιών του Kerberos.

C: Όνομα του client.

n: Ένα nonce.

t: Μία χρονο-σφραγίδα.

t1: Αρχική τιμή της εγκυρότητας του κλειδιού.

t2: Τελική τιμή της εγκυρότητας του κλειδιού.

Το μήνυμα 2 είναι ρίσκο γιατί δίνει στον αιτούμενο πληροφορία που είναι μόνο χρήσιμη εαν ξέρει το μυστικό κλειδί του C, KC. Κάποιος απατεώνας που θέλει να προσποιηθεί τον C στέλνοντας το μήνυμα 1 δεν μπορεί να πάει μακρύτερα, από την στιγμή που δεν μπορεί να αποκρυπτογραφήσει το μήνυμα 2. Για μέρη που είναι χρήστες, το KC είναι μία παραλλαγή των password των χρηστών. Οι client θα παρακινήσει τον χρήστη να πληκτρολογήσει το password του και θα προσπαθήσει να κρυπτογραφήσει το μήνυμα 2 με αυτό. Αν ο χρήστης δώσει το σωστό password, ο client λαμβάνει το κλειδί συνόδου KCT και ένα έγκυρο κλειδί για την υπηρεσία παροχής εισιτηρίων, αν όχι, λαμβάνει σκουπίδια. Οι servers έχουν μυστικά κλειδιά από μόνοι τους, που είναι γνωστά μόνο στις σχετικές server διεργασίες και στον server αυθεντικοποίησης.

Όταν ένα έγκυρο εισιτήριο λαμβάνεται από την υπηρεσία αυθεντικοποίησης, ο client μπορεί να το χρησιμοποιήσει για να επικοινωνίσει με την υπηρεσία παροχής εισιτηρίων για να λάβει εισιτήρια για άλλους servers όσες φορές θέλει μέχρι να λήξει το εισιτήριο. Έτσι για να λάβει ένα εισιτήριο για καθε server S, ο C δημιουργεί έναν ταυτοποιητή, κρυπτογραφημένο με το KCT στην μορφή:

{C,t}KCT

στο οποίο θα αναφερόμαστε ως:

{auth(C)}KCT

και στέλνει μία αίτηση στο T:

3.C->T: Αίτηση για εισιτήριο για την υπηρεσία S {auth(C)}KCT, {ticket(C,T)}KT, S, n Ο C ζητάει απο τον server παροχής εισιτηρίων να τον εφοδιάσει με ένα εισιτήριο για την επικοινωνία με έναν άλλο server S.

4.T->C: Εισιτήριο για υπηρεσία {KCS,n}KCT, {ticket(C,S)}KS Ο T ελέγχει το εισιτήριο .Αν είναι έγκυρο, ο T δημιουργεί ένα νέο τυχαίο κλειδί KCS και το επιστρέφει με ένα εισιτήριο για τον S (κρυπτογραφημένο με το μυστικό κλειδί του server KS).

Ο C είναι τότε έτοιμος να στείλει αιτήσεις στον S:

5.C->S: Αίτηση για υπηρεσία {auth(C)}KCS, {ticket(C,S)}KS, request, n Ο C στέλνει το εισιτήριο στον S με έναν νεοδημιούργητο αυθεντικοποιητή για τον Cκαι μία αίτηση. Η αίτηση κρυπτογραφείται με το KCS αν θέλουμε ασφάλεια για τα δεδομένα.

Για να είναι σίγουρος ο client για την αυθεντικότητα του server, ο S πρέπει να επιστρέψει το nonce στον C.

6.S->C: Αυθεντικοποίηση του server {n}KCS (Προαιρετικό): Ο S στέλνει το nonce ston C που κρυπτογραφείται με το KCS.

Στο σχήμα 16.9 δείχνουμε το πρωτόκολλο γραφικά χρησιμοποιώντας σκιασμένα κουτιά για να σημειώσουμε τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται.

Εφαρμογή του Kerberos.Το Kerberos αναπτύχθηκε για χρήση στο Project Athena στο MIT ένα πανεπιστημιακό δίκτυο για προπτυχιακή εκπαίδευση με πολλούς σταθμούς εργασίας και servers που παρείχε μια υπηρεσία σε περισσότερους από 5000 χρήστες. Το περιβάλλον είναι τέτοιο ώστε ούτε η αξιοπιστία των clients ούτε η ασφάσλεια του δικτύου και των μηχανών που προσέφεραν υπηρεσίες στο δίκτυο μπορούσε να εξασφαλισθεί. Π.χ, οι σταθμοί εργασίας δεν προστατεύονταν από την

εγκατάσταση προγραμμάτων και οι servers (άλλων από τον Kerberos server) δεν ήταν απαραίτητα ασφαλείς ενάντια στην φυσική παρέμβαση στο configuration του λογισμικού τους.

Το Kerberos παρέχει ιδεατά όλη την ασφάλεια στο σύστημα Athena. Χρησιμοποιείται για να αυθεντικοποιεί χρήστες και άλλα αντικείμενα. Οι περισσότεροι από τους servers που τρέχουν στο δίκτυο έχουν επεκταθεί για να συμπεριλάβουν ένα εισιτήριο για κάθε client στην αρχή κάθε αλληλεπίδρασης client-server. Αυτοί περιλαμβάνουν αποθήκευση αρχείων (NFS και Andrew File System), e-mail, απομακρυσμένο login και εκτύπωση. Τα password των χρηστών είναι γωστά μόνο στον χρήστη και την υπηρεσία αυθεντικοποίησης του Kerberos. Οι υπηρεσίες έχουν μυστικά κλειδιά που είναι γνωστά μόνο στο Kerberos και τους servers που παρέχουν την υπηρεσία.

Θα περιγράψουμε τον τρόπο με τον οποίο το Kerberos κάνει την αυθεντικοποίηση των χρηστών κατά το login και την χρησιμοποίηση του για την επαύξηση της ασφάλειας του NFS.

Login με το Kerberos. Όταν ένας χρήστης logs σε έναν σταθμό εργασίας, το login πρόγραμμα στέλνει το όνομα του χρήστη στην υπηρεσία αυθεντικοποίησης του Kerberos. Αν ο χρήστης είναι άγνωστος σε αυτήν την υπηρεσία, αυτή απαντά με ένα κλειδί συνόδου και ένα nonce που έχει κρυπτογραφηθεί με το password του χρήστη και ένα εισιτήριο για το TGS. Το πρόγραμμα για login επιχειρεί να αποκρυπτογραφήσει το κλειδί συνόδου και το nonce χρησιμοποιώντας το password που πληκτρολόγησε ο χρήστης στην προτροπή του password. Αν το password είναι σωστό, το login πρόγραμμα λαμβάνει το κλειδί συνόδου και το nonce. Αυτό ελέγχει το nonce και αποθηκεύει το κλειδί συνόδου για επόμενη χρήση όταν επικοινωνεί με το TGS. Σε αυτό το σημείο, το login πρόγραμμα μπορεί να σβήσει το password του χρήστη από την μνήμη του, απ'την στιγμή που το εισιτήριο χρησιμοποιείται για να αυθεντικοποιήσει τον χρήστη. Μία login σύνοδος αρχίζει τότε για τον χρήστη στον σταθμό εργασίας. Σημειώστε ότι το password του χρήστη δεν είναι εκτεθιμένο για κρυφάκουσμα στο δίκτυο, αφού παραμένει στον σταθμό εργασίας και σβήνεται από την μνήμη αμέσως μετά την είσοδο του.

Προσπελαύνοντας servers με το Kerberos. Όποτε ένα πρόγραμμα που τρέχει σε έναν σταθμό εργασίας χρειάζεται να προσπελάσει κάποια νέα υπηρεσία, ζητάει ένα

εισιτήριο για την υπηρεσία από την υπηρεσία παροχής εισιτηρίων. Π.χ, όταν ένας χρήστης θέλει να κάνει login σε κάποιον μακρινό υπολογιστή, η εντολή rlogin παίρνει ένα εισιτήριο από την υπηρεσία παροχής εισιτηρίων του Kerberos για να προσπελάσει την υπηρεσία rlogind. Η εντολή rlogin στέλνει το εισιτήριο μαζί με έναν νέο αυθεντικοποιητή σε μία αίτηση στην rlogind διεργασία του υπολογιστή που θέλει να κάνει login. Το πρόγραμμα rlogind αποκρυπτογραφεί το εισιτήριο με το μυστικό κλειδί της υπηρεσίας του rlogin και ελέγχει την εγκυρότητα του εισιτηρίου. Οι μηχανές των servers πρέπει να φροντίσουν να αποθηκεύσουν τα μυστικά κλειδιά σε μέρη που δεν μπορούν να τα προσπελάσουν παρείσακτοι.

Τότε το πρόγραμμα rlogind χρησιμοποιεί το κλειδί συνόδου που συμπεριλαμβάνεται στο εισιτήριο για να αποκρυπτογραφήσει τον αυθεντικοποιητή και ελέγχει ότι ο αυθεντικοποιητής είναι καινούργιος. Αν το πρόγραμμα rlogind είναι ικανοποιημένο ότι το εισιτήριο και ο αυθεντικοποιητής είναι έγκυροι, δεν υπάρχει ανάγκη για έλεγχο του ονόματος και του password του χρήστη.

NFS με τον Kerberos. Οι σταθμοί εργασίας δεν είναι αξιόπιστοι και όλα τα συστήματα αρχείων προσπελαύνονται από έναν file server. Όταν ένας χρήστης κάνει log σε έναν σταθμό εργασίας, ο αρχικός του (home) κατάλογος προσαρτάται χρησιμοποιώντας το NFS. Ομοίως, το σύστημα αρχείων προσαρτάται από έναν file server. Αυτό επιτρέπει στο χρήστη να δουλεύει με τα αρχεία που είναι προσβάσιμα από τα σημεία προσάρτησης. Το NFS φυσικά χρησιμοποιεί τους γνωστούς ελέγχους που ξέρουμε από το UNIX για να ελέγχει την πρόσβαση, αλλά αυτό εξαρτάται από την γνώση για την πραγματική ταυτότητα του χρήστη, κάτι που δεν εγγυάται το NFS.

Μία λύση γι'αυτό είναι να αλλάξουμε την φύση αυτών που ζητάει το NFS ώστε να είναι ένα εισιτήριο και ένας αυθεντικοποιητής σύμφωνα με το Kerberos. Εφόσον όμως το NFS δεν αποθηκεύει την προηγούμενη κατάσταση του κάθε αίτηση στο NFS θα πρέπει να περιλαμβάνει αυτά τα στοιχεία. Αυτό όμως είναι πολύ δαπάνηρό σε χρόνο που χρειάζεται για τις απαραίτητες κρυπτογραφήσεις.

Έτσι, υιοθετείται μία υβριδική λύση κατά την οποία ο NFS server παραλαμβάνει πληροφορία για αυθεντικοποίηση των χρηστών μόνο όταν προσαρτόνται οι αρχικοί κατάλογοι και τα root συστήματα αρχείων. Σε κάθε αίτηση για προσπέλαση αρχείου , ο server ελέγχει τον identifier του χρήστη και την διεύθηνση του αποστολέα και επιτρέπει την πρόσβαση αν ταιριάζουν με αυτά που αποθηκεύθηκαν στον server την ώρα της προσάρτησης. Αυτή η προσέγγιση

ελαχιστοποιεί το κόστος και είναι ασφαλής αν μόνο ένας χρήστης κάθε στιγμή μπορεί να κάνει log σε ένα workstation, πράγμα που ισχύει στο MIT.

Σημειώστε όμως ότι οι αιτήσεις και οι απαντήσεις μεταξύ του NFS server και των clients δεν κρυπτογραφούνται και η επανάληψη μπορεί να χρησιμοποιειθεί για να σταλούν δεδομένα σε ένα τρίτο μέρος που θα έχει μπεί νόμιμα στο σύστημα.

Υλοποίηση του Kerberos. Το Kerberos έχει υλοποιηθεί ως ένας server που τρέχει σε μία ασφαλή μηχανή. Ένα σύνολο από βιβλιοθήκες προβλεπονται για χρήση από εφαρμογές clients και υπηρεσίες. Χρησιμοποιείται ο αλγόριθμος DES, αλλά αυτό έχει υλοποιηθεί σαν μία ξεχωριστή μονάδα που μπορεί εύκολα να αντικατασταθεί.

Η υπηρεσία Kerberos είναι στρωματωποιημένη. Ο κόσμος είναι διαιρεμένος σε ξεχωριστά domains που λέγονται realms, καθένα με τον δικό του Kerberos server. Τα περισσότερα αντικείμενα είναι καταχωρημένα σε ένα realm, αλλά οι servers παροχής εισιτηρίων είναι καταχωρημένοι σε όλα τα realms. Τα διάφορα αντικείμενα μπορούν να αυθεντικοποιήσουν τους εαυτούς τους σε servers άλλων realms μέσω των τοπικών τους servers παροχής εισιτηρίων.

Σε ένα απλό realm, μποούν να είναι πολλοί servers ταυτοποίησης, οι οποίοι έχουν αντίγραφα της ίδιας βάσης ταυτοποίησης. Η βάση ταυτοποίησης επαναλαμβάνεται με μία απλή τεχνική master-slave. Οι αλλαγές γίνονται στο κύριο αντίγραφο από μία απλή υπηρεσία Διαχείρισης Βάσης του Kerberos (KDBM) που τρέχει μόνο στην κύρια μηχανή. Το KDBM χειρίζεται αιτήσεις από χρήστες για αλλαγή των password τους και αιτήσεις από διαχειριστές για την πρόσθεση ή την διαγραφή αντικειμένων και την αλλαγή των password τους.

Για να το κάνει διαφανές στους χρήστες, η διάρκεια ζωής των εισιτηρίων του TGS πρέπει να είναι τόσο μεγάλη όσο η μεγαλύτερη σύνοδος χρήστη, ώστε να μην έχουμε απόρριψη αιτήσεων εξαιτίας εισιτηρίων που έχουν λήξει. Πρακτικά, τα εισιτήρια έχουν διάρκεια ζωής περίπου 12 ώρες.

Κριτικές του Kerberos. Το πρωτόκολλο για την έκδοση 5 του Kerberos που περιγράφτηκε προηγουμένως περιλαμβάνει μεγάλες βελτιώσεις που σχεδιάστηκαν εξαιτίας κριτικών των παλιότερων εκδόσεων. Κάποιες από τις κριτικές των Bellovin και Merritt είναι πάνω σε λειτουργικά θέματα που δεν επηρεάζουν άμεσα την ασφάλεια του Kerberos αν χρησιμοποιηθεί στο περιβάλλον για το οποίο σχεδιάστηκε.

Η πιο σπουδαία κριτική τους είναι ότι στην έκδοση 4 του Kerberos τα nonces που χρησιμοποιούνται στους ταυτοποιητές υλοποιούνται ως χρονο-σφραγίδες και η προστασία ενάντια στην επανάληψη των ταυτοποιητών εξαρτάται απο τον συγχρονισμό των clients και των servers. Ακόμα, αν το πρωτόκολλο συγχρονισμού χρησιμοποιείται για να φέρει τα ρολόγια των clients και των servers σε χαλαρό συγχρονισμό, πρέπει από μόνο του να είναι ασφαλές ενάντια σε επιθέσεις.

Η περιγραφή του πρωτοκόλλου για την έκδοση 5 επιτρέπει στα nonces στους ταυτοποιητές να υλοποιηθούν σαν χρονο-σφραγίδες ή σαν αριθμοί ακολουθιών. Και στις δύο περιπτώσεις, οι servers πρέπει να κρατάνε μία λίστα των nonces που λήφθηκαν πρόσφατα από κάθε client για να ελεγχθούν ότι δεν επαναλήφθηκαν. Αυτή είναι μία ασυνήθιστη υλοποίηση και είναι δύσκολο για τους servers να εγγυθούν σε περίπτωση αποτυχίας. Ο Kehne δημοσίευσε μία βελτίωση στο πρωτόκολλο του Kerberos που δεν εξαρτάται από τα ρολόγια συγχρονισμού.

Οι κριτικές των Burrows, Abadi και Needlham προέρχονται από την ανάλυση του προηγούμενου πρωτοκόλλου του Kerberos (έκδοση 4) χρησιμοποιώντας την δικιά τους λογική της ταυτοπειήσης. Τα συμπεράσματα τους περιείχαν μια κριτική για τον συγχρονισμό των ρολογιών clients και servers όπως και οι προηγούμενοι και ένα σχόλιο ότι η χρήση της διπλής κρυπτογράφησης σε κάποια μηνύματα δεν προσέφερε τίποτα και ήταν δαπανηρός. Η τελευταία κριτική λαμβάνεται υπόψη στην έκδοση 5 που δεν περιλαμβάνει καμία διπλή κρυπτογράφηση.

Τελειώνοντας, σημειώνουμε ότι η ασφάλεια στο Kerberos εξαρτάται από τις διάρκειες ζωής των εισιτηρίων. Η διάρκεια ζωής πρέπει να επιλεχθεί αρκετά μεγάλη ώστε να αποφεύγει διακοπές της υπηρεσίας, αλλά και αρκετά μικρή ώστε να σιγουρευτούμε ότι οι χρήστες που έχουν βγει δεν χρησιμοποιούν πόρους για περισσότερο από μία μικρή περίοδο.