7 ΔΙΑΧΕΙΡΙΣΗ ΚΛΕΙΔΙΩΝ

7.1. Εισαγωγή

Το σημείο αναφοράς της ασφάλειας ενός κρυπτοσυστήματος είναι οι ειδικές ποσότητες πληροφορίας που ονομάζουμε κλειδιά. Σε ένα καλά σχεδιασμένο κρυπτοσύστημα, η ασφάλειά του εξαρτάται αποκλειστικά από τα κλειδιά (αρχή του Kerchoff). Επομένως, η σωστή διαχείριση των κλειδιών συνιστά ενέργειες ζωτικής σημασίας για την ασφάλεια της επικοινωνίας δύο ή περισσοτέρων μελών.

Η διαχείριση κλειδιών αποτελείται από τη δημιουργία, διανομή, εγκατάσταση, χρήση, ανανέωση, ανάκληση, φύλαξη και καταστροφή κλειδιών. Εκτός από την καταστροφή των κλειδιών, όλες οι άλλες ενέργειες διαχείρισης μπορούν να περιλαμβάνουν κρυπτογραφικές τεχνικές.

ΟΡΙΣΜΟΣ 7.1 – Η ***κρυπτοπερίοδος*** ενός κλειδιού είναι ο χρόνος ο οποίος περιλαμβάνει τη δημιουργία, διανομή και χρήση ενός κλειδιού.

Η κρυπτοπερίοδος ενός κλειδιού εξαρτάται από τις ακόλουθες παραμέτρους:

- Μήκος του κλειδιού. Η κρυπτοπερίοδος αυξάνει με το μήκος του κλειδιού. Εφόσον το μήκος του κλειδιού είναι ένας από τους παράγοντες που επηρεάζουν την αποτελεσματικότητα της εξαντλητικής αναζήτησης, έπεται ότι η εξέλιξη της τεχνολογίας μειώνει την κρυπτοπερίοδο ενός κλειδιού με συγκεκριμένο μέγεθος.
- Ευαισθησία του απλού κειμένου ως προς την εμπιστευτικότητα. Όταν οι πληροφορίες που ανταλλάσσονται μεταξύ δύο ή περισσότερων μελών έχουν υψηλές απαιτήσεις εμπιστευτικότητας, τότε είναι επιθυμητό το κλειδί να αλλάζει συχνότερα, για να περιορίζει τη συλλογή πληροφοριών του
  αντιπάλου κάτω από το ίδιο κλειδί, το οποίο μπορεί να οδηγήσει σε επιτυχή κρυπτανάλυση. Επιπλέον, η τυχόν ανακάλυψη ενός κλειδιού θα αποκαλύψει μικρότερο τμήμα του απλού κειμένου.
- Τύπος του κλειδιού, όπως θα εξετάσουμε στην επόμενη παράγραφο.

- Κρυπτοσύστημα. Για δεδομένο μέγεθος κλειδιού, διαφορετικά κρυπτοσυστήματα έχουν και διαφορετική κρυπτοπερίοδο. Ισοδύναμα, για δεδομένη κρυπτοπερίοδο αντιστοιχούν διαφορετικά μήκη κλειδιών σε διαφορετικά κρυπτοσυστήματα. Κλασσικά παραδείγματα είδαμε στα προηγούμενα κεφάλαια, όπου τα μεγέθη των κλειδιών μεταξύ συμμετρικών και ασύμμετρων κρυπταλγόριθμων έχουν διαφορές τάξης μεγέθους μεγαλύτερες του 10.

ΟΡΙΣΜΟΣ 7.2 – Το σύνολο των διαδικασιών που αποτελείται από τη διαδικασία δημιουργίας ενός κλειδιού, τη διανομή του, τη χρήση του και την αντικατάστασή του, ονομάζεται ***κύκλος ζωής*** του κλειδιού.

7.2. Τύποι κλειδιών

Τα κλειδιά ταξινομούνται ανάλογα με τον τύπο του κρυπταλγόριθμου και ανάλογα με τη χρήση για την οποία προορίζονται.

Ανάλογα με τον τύπο του κρυπταλγόριθμου, τα κλειδιά χωρίζονται σε τρεις κατηγορίες:

- μυστικό κλειδί, το οποίο ορίζεται σε συμμετρικό κρυπτοσύστημα. Το μυστικό κλειδί θα πρέπει να βρίσκεται στην κατοχή όλων των μελών που επικοινωνούν χρησιμοποιώντας συμμετρική κρυπτογραφία.
- δημόσιο κλειδί, το οποίο ορίζεται σε ασύμμετρο κρυπτοσύστημα. Το δημόσιο κλειδί είναι το κλειδί εκείνο το οποίο αναφέρεται σε κάποιο μέλος με το οποίο είναι επιθυμητή η επικοινωνία. Το δημόσιο κλειδί είναι γνωστό σε όλους.
- ιδιωτικό κλειδί, το οποίο ορίζεται σε ασύμμετρο κρυπτοσύστημα. Το ιδιωτικό κλειδί συνδέεται κρυπτογραφικά με το δημόσιο κλειδί και είναι γνωστό σε ένα μόνο μέλος.

Ανάλογα με τη χρήση για την οποία προορίζονται τα παραπάνω κλειδιά, διακρίνουμε τους ακόλουθους τύπους:

- κλειδί συνόδου (session key), το οποίο χρησιμοποιείται για την κρυπτογράφηση για μόνο μία περίοδο επικοινωνίας. Μετά το τέλος της επικοινωνίας, το κλειδί καταστρέφεται. Σε επόμενη περίοδο επικοινωνίας, δημιουργείται νέο κλειδί συνόδου.
- κλειδί τερματικού (terminal key). Στην περίπτωση που το κλειδί συνόδου δεν καταστρέφεται, αλλά χρησιμοποιείται για περισσότερες από μία επικοινωνίες ενός μέλους, τότε το κλειδί αυτό ονομάζεται κλειδί τερματικού.
- κύριο κλειδί (master key). Συνήθως ένα μέλος στην πράξη κατέχει πολλά κλειδιά συνόδου και κλειδιά τερματικού. Προκειμένου να απλουστευθεί η διαχείριση των κλειδιών, χρησιμοποιείται το κύριο κλειδί. Έτσι κατά την αποθήκευση των κλειδιών, αυτά κρυπτογραφούνται με το κύριο κλειδί, οπότε ο έλεγχος της ασφαλούς αποθήκευσης εξαρτάται από μία και μόνον

ποσότητα, το κύριο κλειδί. Επίσης, το κύριο κλειδί μπορεί να χρησιμοποιηθεί για τη δημιουργία κλειδιού τερματικού, ή κλειδιού συνόδου.

Οι παραπάνω τύποι κλειδιών έχουν διαφορετικές κρυπτοπεριόδους. Το κλειδί συνόδου ονομάζεται και βραχυπρόθεσμο κλειδί (short term key) και έχει τη μικρότερη κρυπτοπερίοδο από τους τρεις τύπους κλειδιών. Αντίθετα, το τερματικό κλειδί και το κύριο κλειδί είναι μακροπρόθεσμα κλειδιά (long term keys), με μεγαλύτερες κρυπτοπεριόδους. Μεταξύ των δύο αυτών κλειδιών, το κύριο κλειδί έχει μεγαλύτερη κρυπτοπερίοδο, αφού χρειάζεται για την αποθήκευση των υπολοίπων κλειδιών.

Η ύπαρξη των διαφορετικών τύπων κλειδιών με βάση τον προορισμό χρήσης τους, οφείλεται σε πρακτικούς λόγους. Όπως τονίζουμε κατ' επανάληψη σε αυτό το βιβλίο, η κρυπτογραφία δε λύνει τα προβλήματα, αλλά τα μετασχηματίζει σε μορφές όπου η διαχείριση του προβλήματος είναι αποτελεσματικότερη και ευκολότερη. Είδαμε ότι προστατεύοντας μια συγκριτικά μικρή ποσότητα πληροφορίας που ονομάζουμε «κλειδί», μπορούμε με τη χρήση της κρυπτογραφίας να προστατεύσουμε μια κατά πολύ μεγαλύτερη σε μέγεθος πληροφορία, το «απλό κείμενο». Αντίστοιχα, με τη διαχείριση των κλειδιών, χρησιμοποιούμε κλειδιά για να προστατεύσουμε άλλα κλειδιά. Η ανάγκη αυτή δημιουργήθηκε λόγω της ύπαρξης πολλών κλειδιών σε ένα σύστημα επικοινωνίας. Το πρόβλημα του τετραγώνου που παρουσιάσαμε στο Κεφάλαιο 1, είναι ένα ενδεικτικό παράδειγμα όπου απαιτείται μεγάλος αριθμός κλειδιών για εμπιστευτική επικοινωνία.

7.3. Ο αντίπαλος

Ο αντίπαλος και το κλειδί ίσως είναι οι δύο έννοιες με τη μεγαλύτερη αλληλεξάρτηση στην κρυπτογραφία και γενικότερα στην ασφάλεια της πληροφορίας. Ο αντίπαλος ανάλογα με τις ευκαιρίες που έχει μπορεί να επιτεθεί σε όλες τις διαδικασίες διαχείρισης κλειδιών, από τη δημιουργία, μέχρι και την καταστροφή των κλειδιών. Ο κύριος στόχος του αντιπάλου είναι η ανακάλυψη των κλειδιών ενός κρυπτογραφικού συστήματος επικοινωνίας. Ενδεικτικά, αναφέρουμε επιμέρους στόχους του αντιπάλου:

- ανακάλυψη του κυρίως κλειδιού. Η ανακάλυψη του κυρίως κλειδιού δημιουργεί και τα περισσότερα και μεγαλύτερα προβλήματα. Πέραν του γεγονότος ότι ο αντίπαλος με την ανακάλυψη του κυρίως κλειδιού ανακαλύπτει αυτόματα και όλα τα επιμέρους κλειδιά τα οποία είναι υπό την προστασία του κυρίως κλειδιού, δημιουργούνται και επιπλέον θέματα στην αντικατάσταση του κλειδιού. Η αντικατάσταση του κυρίως κλειδιού πολλές φορές περιλαμβάνει φυσικές διαδικασίες οι οποίες απαιτούν χρόνο και επιπλέον προσπάθεια. Για παράδειγμα, στις μηχανές ATM των τραπεζών, το κυρίως κλειδί γίνεται πάντοτε με αυστηρές διαδικασίες που περιλαμβάνουν φυσική παρουσία υπαλλήλων.
- ανακάλυψη του κλειδιού συνόδου. Φαινομενικά, η ανακάλυψη ενός κλειδιού συνόδου μπορεί να είναι ενέργεια μικρού ρίσκου. Ωστόσο, υπάρχουν

συστήματα όπου η ανακάλυψη ενός κλειδιού συνόδου οδηγεί και στην ανακάλυψη προηγούμενων κλειδιών, ή ακόμη και στην ανακάλυψη του πηγαίου κυρίως κλειδιού, από το οποίο προήλθε το κλειδί συνόδου.

- ανακάλυψη των παλαιών κλειδιών. Παρόμοια με τον προηγούμενο στόχο, η μη σωστή καταστροφή των κλειδιών μπορεί να προσδώσει πλεονεκτήματα στον αντίπαλο ο οποίος μπορεί να τα εκμεταλλευτεί και να αποκρυπτογραφήσει τόσο μηνύματα τα οποία στάλθηκαν στο παρελθόν με το παλιό κλειδί, όσο και να ανακαλύψει μεταγενέστερα κλειδιά.

Με βάση τους παραπάνω στόχους, ορίζουμε την έννοια της τέλειας μυστικότητας «προς τα εμπρός» και «προς τα πίσω».

ΟΡΙΣΜΟΣ 7.3 – Ένα κρυπτογραφικό σύστημα επικοινωνίας κατέχει ***τέλεια μυστικότητα προς τα εμπρός*** (perfect forward secrecy), όταν η ανακάλυψη ενός από τα μακροπρόθεσμα κλειδιά, δεν συνεπάγεται ανακάλυψη των κλειδιών συνόδου.

ΟΡΙΣΜΟΣ 7.4 – Ένα κρυπτογραφικό σύστημα επικοινωνίας κατέχει ***τέλεια μυστικότητα προς τα πίσω*** (perfect backward secrecy), όταν η ανακάλυψη ενός κλειδιού συνόδου, δεν συνεπάγεται ανακάλυψη των μακροπρόθεσμων κλειδιών.

Όταν το κρυπτογραφικό σύστημα δεν κατέχει τέλεια μυστικότητα προς τα εμπρός και προς τα πίσω, τότε σε περίπτωση που ο αντίπαλος ανακαλύψει οποιοδήποτε από τα κλειδιά συνόδου, μπορεί αυτόματα να ανακαλύψει και όλα τα μελλοντικά κλειδιά συνόδου. Λέμε τότε ότι το σύστημα είναι ευπαθές σε ***επίθεση γνωστού κλειδιού*** (known-key attack).

7.4. Εδραίωση κλειδιών

Με τον όρο «εδραίωση κλειδιών» (key establishment) εννοούμε το σύνολο των μηχανισμών που εκτελούνται προκειμένου να αποκτήσουν τα επικοινωνούντα μέλη τα απαιτούμενα κλειδιά για κρυπτογραφική επικοινωνία. Οι μηχανισμοί εδραίωσης κλειδιών περιλαμβάνουν τη δημιουργία, μεταφορά και εγκατάσταση κλειδιών, και αναφέρονται περισσότερο στα κλειδιά συνόδου. Οι μηχανισμοί εδραίωσης κλειδιών οι οποίοι είναι κρυπτογραφικής φύσης, αποτελούν τα πρωτόκολλα εδραίωσης κλειδιών (key establishment protocols).

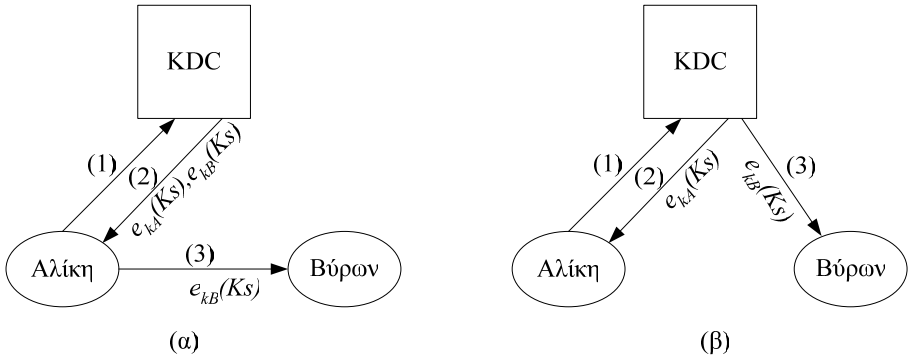
7.4.1. Εδραίωση κλειδιών σε συμμετρικά κρυπτοσυστήματα

Οι δύο βασικές αδυναμίες στην εδραίωση κλειδιών σε ένα συμμετρικό κρυπτοσύστημα είναι η ανάγκη ασφαλούς καναλιού για τη μεταφορά των κλειδιών, και ο αυξημένος αριθμός απαιτούμενων κλειδιών, ο οποίος είναι ανάλογος του τετραγώνου των μελών. Οι αδυναμίες αυτές αντιμετωπίζονται με την εισαγωγή δύο νέων οντοτήτων στο μοντέλο επικοινωνίας: το Κέντρο Διανομής Κλειδιών (Key Distribution Centre, KDC) και το Κέντρο Μετάφρασης Κλειδιών (Key Translation Centre, KTC).

Τα KDC και KTC αποτελούν λύσεις ***συγκεντρωτικής διαχείρισης κλειδιών*** (centralized key management) και βασίζονται στην ακόλουθη αρχή. Εφόσον δεν πραγματοποιείται επικοινωνία μεταξύ όλων των μελών με όλους, δεν είναι απαραίτητο να ανταλλαχθούν n^2 κλειδιά, όπου n ο αριθμός των μελών του συστήματος. Αντίθετα, μπορούν αρχικά να διανεμηθούν (μέσω ασφαλών καναλιών) μόνον n κλειδιά, μεταξύ κάποιου έμπιστου μέλους με τα υπόλοιπα μέλη. Όταν κάποιο μέλος επιθυμεί να επικοινωνήσει με κάποιο άλλο μέλος, δημιουργείται ένα κρυπτογραφικά ασφαλές κανάλι, με τη βοήθεια του έμπιστου μέλους, το οποίο λειτουργεί ως KDC, ή KTC, ανάλογα με το μοντέλο επικοινωνίας.

Κέντρο Διανομής Κλειδιών, KDC

Στην περίπτωση του KDC, η δημιουργία του κλειδιού συνόδου πραγματοποιείται από το KDC. Οι δύο εναλλακτικές λύσεις όπου εμπλέκεται το KDC φαίνονται στο Σχήμα 7.1.



Σχήμα 7.1 – KDC με (α) ενδιάμεση και (β) άμεση επικοινωνία.

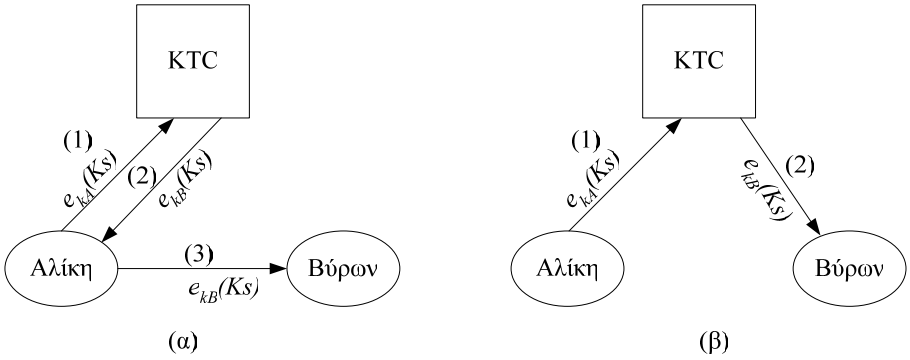
Σύμφωνα με την πρώτη εναλλακτική (Σχήμα 7.1α), η Αλίκη επικοινωνεί με το KDC (1) και αιτείται κλειδί συνόδου για να επικοινωνήσει με τον Βύρωνα. Το KDC δημιουργεί το κλειδί συνόδου *ks* και το κρυπτογραφεί με το κλειδί *kA* το οποίο το μοιράζεται με την Αλίκη, και με το κλειδί *kB* το οποίο το μοιράζεται με τον Βύρωνα, παράγοντας δύο κρυπτοκείμενα, $e_{kA}(ks)$ και $e_{kB}(ks)$. Στη συνέχεια το KDC στέλνει τα δύο κρυπτοκείμενα στην Αλίκη (2). Η Αλίκη με τη σειρά της στέλνει το κρυπτοκείμενο $e_{kB}(ks)$ στον Βύρωνα. Τέλος, η Αλίκη και ο Βύρων αποκρυπτογραφούν ο καθένας το αντίστοιχο κρυπτοκείμενο και αποκτούν το κλειδί συνόδου *ks*.

Σύμφωνα με τη δεύτερη εναλλακτική (Σχήμα 7.1β), η Αλίκη ξεκινά και πάλι την επικοινωνία (1), στέλνοντας την αίτηση κλειδιού συνόδου στο KDC για να επικοινωνήσει με τον Βύρωνα. Το KDC δημιουργεί ένα κλειδί συνόδου και το κρυπτογραφεί χωριστά με το κλειδί της Αλίκης και του Βύρωνα, όπως και στην προηγούμενη περίπτωση. Στη συνέχεια στέλνει τα κρυπτογραφημένα κλειδιά χω-

ριστά στην Αλίκη (2) και στον Βύρωνα (3). Τέλος, η Αλίκη και ο Βύρων αποκρυπτογραφούν το κρυπτοκείμενο που έλαβαν και ανακτούν το κλειδί συνόδου.

Κέντρο Μετάφρασης Κλειδιών, ΚΤC

Στην περίπτωση του ΚΤC, το κλειδί συνόδου δημιουργείται από το μέλος το οποίο ξεκινά την επικοινωνία. Οι δύο εναλλακτικές για τη διανομή και εγκατάσταση του κλειδιού συνόδου είναι παρόμοιες με αυτές του KDC, όπως φαίνεται στο Σχήμα 7.2.



Σχήμα 7.2 ΚΤC με (α) ενδιάμεση και (β) άμεση επικοινωνία.

Σύμφωνα με το μοντέλο της ενδιάμεσης επικοινωνίας (Σχήμα 7.2α), η Αλίκη δημιουργεί ένα κλειδί συνόδου *ks* και το κρυπτογραφεί με το κλειδί το οποίο το μοιράζεται με το ΚΤC. Στη συνέχεια στέλνει το κρυπτογραφημένο κλειδί $e_{kA}(ks)$ στο ΚΤC (1) μαζί με το όνομα του Βύρωνα. Το ΚΤC «μεταφράζει» το κλειδί συνόδου που έλαβε, αποκρυπτογραφώντας το με το κλειδί *kA* και κρυπτογραφώντας το με το κλειδί *kB*. Στη συνέχεια, το ΚΤC στέλνει το κρυπτογραφημένο κλειδί στην Αλίκη (2), η οποία με τη σειρά της το μεταβιβάζει στον Βύρωνα (3). Τέλος, ο Βύρων αποκρυπτογραφεί το κρυπτογραφημένο κλειδί συνόδου που έλαβε.

Το μοντέλο της άμεσης επικοινωνίας (Σχήμα 7.2β), είναι ίδιο με το μοντέλο της ενδιάμεσης επικοινωνίας, μέχρι το στάδιο όπου το ΚΤC μεταφράζει το κλειδί συνόδου από την Αλίκη στον Βύρωνα. Στη συνέχεια, το ΚΤC στέλνει το κρυπτογραφημένο κλειδί απ' ευθείας στον Βύρωνα, χωρίς τη μεσολάβηση της Αλίκης.

Ανάλυση των KDC και ΚΤC

Στο εξής θα αναφερόμαστε στα KDC και ΚΤC ως «Κεντρο», εκτός και αν υπάρχει ανάγκη για διαφοροποίηση. Το βασικό πλεονέκτημα από τη χρήση των Κέντρων είναι η ανάγκη αποθήκευσης περιορισμένου αριθμού μακροπρόθεσμων κλειδιών. Πιο συγκεκριμένα, το κάθε μέλος απαιτείται να αποθηκεύει ένα και μόνο κλειδί, αυτό το οποίο το μοιράζεται με το Κέντρο, ενώ το Κέντρο θα πρέπει να αποθηκεύσει *n* κλειδιά.

Ωστόσο, η εξάρτηση της ασφάλειας του συστήματος από μια οντότητα όπως το Κέντρο, επιφυλάσσει κινδύνους. Πρώτον, το Κέντρο θεωρείται έμπιστο. Γενικά όταν αναφερόμαστε σε εμπιστοσύνη, ένα ορθά σχεδιασμένο μοντέλο εμπιστοσύνης θα πρέπει να ελαχιστοποιεί τον αριθμό των οντοτήτων οι οποίες θεωρούνται έμπιστες. Στο συγκεκριμένο μοντέλο του Κέντρου, από τις n+1 οντότητες οι οποίες συμμετέχουν, απαιτείται να αποδίδεται εμπιστοσύνη μόνον σε μία οντότητα. Σε περίπτωση που ένα μοντέλο απαιτεί εμπιστοσύνη σε πολλά μέλη, η πιθανότητα κατάρρευσης της ασφάλειας του συστήματος αυξάνεται, διότι αυξάνονται οι ευκαιρίες προσβολής από τον αντίπαλο, ο οποίος μπορεί να είναι και κάποιο από τα μέλη.

Η υπόθεση της έμπιστης οντότητας δεν είναι νέα έννοια. Για παράδειγμα, μια τράπεζα λαμβάνει εμπιστοσύνη από τους πελάτες της. Οι πελάτες της τράπεζας από την άλλη εμπιστεύονται τη συγκεντρωτική διαχείριση των χρημάτων τους από την τράπεζα, προς χάριν αποτελεσματικότερης διαχείρισης ρίσκου. Συνεπώς, η εισαγωγή της έμπιστης οντότητας σε ένα μοντέλο επικοινωνίας είναι πολλές φορές αναπόφευκτη.

Έτσι, η υπόθεση της έμπιστης οντότητας εισάγει νέες απειλές και νέους κινδύνους. Στην περίπτωση που ο αντίπαλος εκθέσει την ασφάλεια ενός από τα μέλη, τότε προσβάλλεται η επικοινωνία του συγκεκριμένου μέλους. Όμως, στην περίπτωση που ο αντίπαλος εκθέσει την ασφάλεια της έμπιστης οντότητας, τότε θα καταρρεύσει η ασφάλεια όλου του συστήματος. Έτσι, τα μοντέλα με Κέντρα που παρουσιάσαμε στις προηγούμενες παραγράφους θα πρέπει να προστατευθούν περαιτέρω με πρόσθετους μηχανισμούς, προκειμένου να μειωθεί το ρίσκο στο βαθμό εκείνον, ώστε να δικαιολογηθεί η χρήση των μοντέλων με Κέντρα.

Προτού προχωρήσουμε στους μηχανισμούς προστασίας, θα εξετάσουμε τις απειλές που εμφανίζονται στα παραπάνω μοντέλα. Αρχικά απαιτείται η ανταλλαγή των μακροπρόθεσμων κλειδιών μεταξύ του Κέντρου με τα μέλη. Σε αυτό το σημείο οι απειλές είναι οι ίδιες με αυτές του μοντέλου επικοινωνίας δύο μελών με συμμετρική κρυπτογραφία. Απαιτείται δηλαδή ασφαλές κανάλι ώστε τα επικοινωνούντα μέλη να μοιράζονται το ίδιο μυστικό κλειδί, η μεταφορά του οποίου γίνεται με μη κρυπτογραφικά μέσα (π.χ. με κούριερ, αυτοπροσώπως, κτλ.).

Όπως είδαμε, στα μοντέλα με Κέντρα παίρνουν μέρος τρεις οντότητες, η Αλίκη, ο Βύρων και το Κέντρο. Η Αλίκη είναι το μέλος το οποίο εκτελεί το πρώτο βήμα στη διαδικασία εδραίωσης του κλειδιού συνόδου, και είναι εκείνη η οποία ξεκινά την επικοινωνία με το Κέντρο. Μεταξύ των τριών μελών, η επικοινωνία της Αλίκης με το Κέντρο ονομάζεται φάση ***απόκτησης κλειδιού*** (key acquisition), ενώ η επικοινωνία μεταξύ της Αλίκης και του Βύρωνα ονομάζεται φάση ***μεταφοράς κλειδιού*** (key transfer). Και στις δύο φάσεις η ποσότητα η οποία μεταφέρεται υπό την προστασία κρυπτογραφίας είναι το κλειδί συνόδου. Κατά τις φάσεις αυτές, η κρυπτογραφική υπηρεσία που παρέχεται είναι η εμπιστευτικότητα. Αυτό ισοδυναμεί με προστασία απέναντι σε παθητική επίθεση του αντιπάλου. Ο αντίπαλος έχει το ρόλο του υποκλοπέα ο οποίος παρακολουθεί και καταγράφει τα μηνύματα τα οποία ανταλλάσσονται μεταξύ των τριών.

Σε τυχόν ενεργητική επίθεση του αντιπάλου, τα προαναφερθέντα μοντέλα δεν μπορούν να διαφυλάξουν τόσο την εμπιστευτικότητα, όσο και την αυθεντικοποίηση των επικοινωνούντων μελών. Θα εξετάσουμε τις περιπτώσεις όπου ο αντίπαλος επιχειρεί επίθεση τόσο στη φάση απόκτησης, όσο και στη φάση μεταφοράς κλειδιού. Επίσης θεωρούμε ότι ο αντίπαλος μπορεί να είναι κάποιο από τα άλλα μέλη.

Κατά τη φάση απόκτησης του κλειδιού, ο αντίπαλος ελέγχει την επικοινωνία μεταξύ της Αλίκης και του Κέντρου. Στην περίπτωση του KDC, ο αντίπαλος μπορεί να προσποιηθεί ότι είναι το Κέντρο, και να αποστείλει στην Αλίκη κάποιο από τα περασμένα κλειδιά συνόδου. Με αυτόν τον τρόπο ελέγχει ποια κλειδιά συνόδου χρησιμοποιούνται, χωρίς να τα γνωρίζει. Η χρησιμοποίηση του ίδιου κλειδιού αποτελεί σημαντική πληροφορία, διότι ο αντίπαλος μπορεί στο μέλλον να ανακαλύψει το κλειδί και κατ' επέκταση θα μπορεί να αποκρυπτογραφήσει κρυπτοκείμενα περισσότερα της μιας συνόδου επικοινωνίας. Αντίστοιχα, ο αντίπαλος μπορεί να προσποιηθεί ότι είναι η Αλίκη και να ζητήσει κλειδί για επικοινωνία με τον Βύρωνα. Η προσποίηση επιτυγχάνεται με την επανάληψη κάποιου προηγούμενου μηνύματος που τυχόν έχει στείλει η Αλίκη στο Κέντρο.

Κατά τη φάση μεταφοράς του κλειδιού, ο αντίπαλος μπορεί να αποστείλει ένα από τα προηγούμενα κρυπτογραφημένα κλειδιά συνόδου τα οποία προορίζονται για την επικοινωνία μεταξύ του Βύρωνα και της Αλίκης. Εάν ο αντίπαλος έχει τη δυνατότητα να επαναμεταδίδει περασμένα κλειδιά, τότε έχει το κίνητρο να επιχειρήσει κρυπτανάλυση σε οποιοδήποτε από τα κλειδιά αυτά, με σκοπό να ελέγχει τις επικοινωνίες μεταξύ των άλλων μελών.

Στην περίπτωση του KTC, οι παραπάνω απειλές υφίστανται με ορισμένες τροποποιήσεις. Επειδή το κλειδί συνόδου δε δημιουργείται στο Κέντρο, οι απειλές δεν έχουν την ίδια ισχύ, αλλά είναι πιο αδύναμες. Για παράδειγμα, στην περίπτωση που ο αντίπαλος προσποιηθεί ως το Κέντρο και απαντήσει στην αίτηση της Αλίκης με ένα από τα προηγούμενα κλειδιά, η επίθεσή του θα γίνει αντιληπτή μετά από ορισμένη ποσότητα ανταλλαγής μηνυμάτων μεταξύ της Αλίκης και του Βύρωνα.

Ωστόσο, εάν η Αλίκη έχει επικοινωνήσει στο παρελθόν με τον αντίπαλο, τότε ο αντίπαλος μπορεί να αναπτύξει μια πιο πολύπλοκη αλλά και πιο αποτελεσματική επίθεση ως εξής. Αν θεωρήσουμε ότι οι ταυτότητες των μελών είναι αριθμοί κάποιου καθορισμένου μεγέθους, τότε ο αντίπαλος μπορεί να καταγράψει και να απομονώσει το μήνυμα το οποίο στάλθηκε από την Αλίκη στο Κέντρο, τα οποίο περιείχε την ταυτότητα του αντιπάλου. Σε νέα αίτηση επικοινωνίας της Αλίκης με τον Βύρωνα, ο αντίπαλος καταγράφει το μήνυμα που στέλνεται από την Αλίκη στο Κέντρο. Στη συνέχεια ο αντίπαλος αντικαθιστά το τμήμα της νέας αίτησης της Αλίκης με τη δικιά του ταυτότητα, όπως την είχε καταγράψει από την προηγούμενη επικοινωνία. Το αποτέλεσμα θα είναι το Κέντρο να μεταφράσει το κλειδί συνόδου μεταξύ της Αλίκης και του Βύρωνα και να το κρυπτογραφήσει με το κλειδί του αντιπάλου. Έτσι ο αντίπαλος μπορεί και αυτός να αποκρυπτογραφήσει το κρυπτογραφημένο κλειδί συνόδου και να υποκλέψει όλη την επικοινωνία μεταξύ της Αλίκης και του Βύρωνα.

Είναι φανερό από τα παραπάνω παραδείγματα επιθέσεων ότι η κύρια αδυναμία των Κέντρων είναι η έλλειψη αυθεντικοποίησης των μηνυμάτων, η οποία αφήνει ελεύθερες τις ενεργές επιθέσεις επανάληψης παλαιών μηνυμάτων. Τα πρωτόκολλα εδραίωσης κλειδιών που μπορούν να αμυνθούν στις παραπάνω επιθέσεις, αποβλέπουν στην προσθήκη αυθεντικοποίησης των μηνυμάτων που ανταλλάσσονται, τόσο κατά τη φάση απόκτησης, όσο και κατά τη φάση μετάδοσης του κλειδιού συνόδου.

Χαρακτηριστικά πρωτοκόλλων εδραίωσης κλειδιού

Τα σύγχρονα πρωτόκολλα εδραίωσης κλειδιού περιλαμβάνουν επιπλέον ποσότητες πληροφορίας, οι οποίες συνεισφέρουν στην αντιμετώπιση των ενεργών επιθέσεων του αντιπάλου. Οι ποσότητες αυτές είναι:

- χρονοσφραγίδα (timestamp). Η χρονοσφραγίδα αποτελείται από την ημερομηνία, ώρα, λεπτά, δευτερόλεπτα και σε ορισμένες περιπτώσεις και από δέκατα ή εκατοστά του δευτερολέπτου και εκφράζει τη χρονική στιγμή που εκτελείται μια ενέργεια του πρωτοκόλλου, η οποία μπορεί να είναι κάποια (κρυπτογραφική) πράξη ή μετάδοση πληροφορίας. Η χρονοσφραγίδα απαιτεί στην πράξη έμπιστο εξυπηρετητή (server) χρονοσφραγίδας, ο οποίος εξυπηρετεί αιτήσεις δημιουργίας χρονοσφραγίδων.
- μοναδικός αριθμός (nonce). Ο μοναδικός αριθμός πολλές φορές αντικαθιστά τη χρονοσφραγίδα και είναι ένας τυχαίος αριθμός ο οποίος δεν εμφανίζεται σε μελλοντική εκτέλεση του πρωτοκόλλου και προσδίδει μοναδικότητα στα μηνύματα τα οποία ανταλλάσσονται. Είναι σημαντικό ο αριθμός αυτός να μην είναι προβλέψιμος από τον αντίπαλο. Ο μοναδικός αριθμός συνυπολογίζεται στις κρυπτογραφικές πράξεις και έτσι δεσμεύεται κρυπτογραφικά με τα αντίστοιχα μηνύματα, με αποτέλεσμα να μειώνονται οι βαθμοί ελευθερίας δράσης του αντιπάλου.

Όλες οι πληροφορίες εμπλέκονται στα πρωτόκολλα εδραίωσης κλειδιών με τη μορφή μηνυμάτων, τα οποία ανταλλάσσονται μεταξύ των μελών του μοντέλου επικοινωνίας. Τα πρωτόκολλα χωρίζονται σε δύο βασικές κατηγορίες, ανάλογα με την φύση ανταλλαγής των μηνυμάτων:

- πρωτόκολλα μίας φοράς (one pass). Τα πρωτόκολλα μίας φοράς έχουν χαμηλή πολυπλοκότητα σε ανταλλαγή μηνυμάτων και χαρακτηρίζονται από τη μονόδρομη επικοινωνία μεταξύ των επικοινωνούντων μελών. Τα μοντέλα των Κέντρων που παρουσιάσαμε παραπάνω αποτελούν πρωτόκολλα μίας φοράς.
- πρωτόκολλα πρόκλησης-απόκρισης (challenge-response). Τα πρωτόκολλα αυτά παρουσιάζουν υψηλή σχετικά πολυπλοκότητα στην ανταλλαγή μηνυμάτων, αλλά συγχρόνως μπορούν να προσφέρουν ισχυρότερη αυθεντικοποίηση από τα πρωτόκολλα μίας φοράς. Ο μικρότερος αριθμός μηνυμά-

των επικοινωνίας είναι δύο, αλλά στην πράξη είναι σύνηθες να ανταλλάσσονται τρία μηνύματα.

Πρωτόκολλα μίας φοράς

Μια απλή αναβάθμιση των πρωτοκόλλων του βασικού μοντέλου του KDC, περιλαμβάνει τη χρήση μοναδικού αριθμού ή χρονοσφραγίδας. Με αναφορά το μοντέλο του Σχήματος 7.1α, το πρωτόκολλο κατά την απόκτηση του κλειδιού αποτελείται από τα εξής βήματα:

$$\text{Αλίκη} \rightarrow \text{Κέντρο:} \quad (ID_A \,\|\, ID_B \,\|\, n_A) \qquad (1)$$

$$\text{Κέντρο} \rightarrow \text{Αλίκη:} \quad e_{kA}(n_A \,\|\, ID_B \,\|\, ks \,\|\, e_{kB}(ks \,\|\, ID_A)) \qquad (2)$$

όπου ID_A, ID_B οι ταυτότητες της Αλίκης και του Βύρωνα αντίστοιχα και n_A ο μοναδικός αριθμός που δημιουργήθηκε από την Αλίκη.

Αρχικά, η Αλίκη στέλνει στο Κέντρο την ταυτότητά της, την ταυτότητα του Βύρωνα και έναν μοναδικό αριθμό. Το βήμα αυτό δεν απαιτεί κρυπτογράφηση των στοιχείων αυτών. Η ταυτότητα της Αλίκης θα πρέπει να μην είναι κρυπτογραφημένη διότι στην αντίθετη περίπτωση το Κέντρο δε θα είναι σε θέση να επιλέξει το σωστό κλειδί για την αποκρυπτογράφηση. Συνεπώς, στην περίπτωση που είναι επιθυμητή η εμπιστευτικότητα σε αυτό το βήμα, μπορεί να κρυπτογραφηθεί μόνον η ταυτότητα του Βύρωνα και ο μοναδικός αριθμός. Ωστόσο, δεν προστίθεται ιδιαίτερη ασφάλεια κρυπτογραφώντας σε αυτό το στάδιο. Ο μοναδικός αριθμός στο μήνυμα της Αλίκης προστατεύει από την επαναχρησιμοποίηση του μηνύματος αυτού από τον αντίπαλο, παρόλο που ο αριθμός αυτός έχει γίνει γνωστός στον αντίπαλο. Βέβαια, απαραίτητη προϋπόθεση είναι να μην επαναληφθεί στο μέλλον ο αριθμός αυτός, αλλά και να μην μπορεί ο αντίπαλος να προβλέψει τους επόμενους μοναδικούς αριθμούς.

Κατά την απόκριση του Κέντρου, το μήνυμα που επιστρέφει στην Αλίκη είναι κρυπτογραφημένο με το κλειδί που μοιράζεται η Αλίκη και το Κέντρο. Κατά την αποκρυπτογράφηση, η Αλίκη μπορεί να ελέγξει αφενός την αυθεντικοποίηση του μηνύματος, εφόσον τα δύο πρώτα μέρη του αποκρυπτογραφημένου κειμένου είναι ο μοναδικός αριθμός και η ταυτότητα του Βύρωνα, και αφετέρου την επικαιρότητα του μηνύματος, σχετίζοντάς το με την αρχική αίτηση μέσω του κοινού μοναδικού αριθμού. Επομένως, ο συνδυασμός της κρυπτογραφημένης απάντησης του Κέντρου με το μοναδικό αριθμό, καθιστά σχεδόν αδύνατη την απόπειρα να προσποιηθεί ο αντίπαλος ότι είναι το Κέντρο.

Πρωτόκολλα πρόκλησης-απόκρισης

Η χρήση του πρωτοκόλλου μίας φοράς μπορεί να εξασφαλίσει την αυθεντικοποίηση του ενός από τα δύο επικοινωνούντα μέλη. Στο παραπάνω πρωτόκολλο, η Αλίκη είχε τη δυνατότητα να ελέγξει την αυθεντικότητα των μηνυμάτων που έλαβε από το Κέντρο και να ανιχνεύσει απόπειρες προσποίησης του αντιπάλου. Το αντί-

θετο κατά την επικοινωνία Αλίκης-Κέντρου δεν ήταν υποχρεωτικό. Στην περίπτωση όμως της επικοινωνίας μεταξύ της Αλίκης και του Βύρωνα, το κάθε μέλος επιθυμεί εξίσου διαβεβαίωση ότι τα μηνύματα που ανταλλάσσονται δεν προέρχονται από τις επαναληπτικές μεταδόσεις παλαιών μηνυμάτων του αντιπάλου.

Στο ακόλουθο πρωτόκολλο, η Αλίκη εκμεταλλεύεται τη γνώση του κλειδιού συνόδου και το χρησιμοποιεί ως μέσο αυθεντικοποίησης του Βύρωνα:

$$\text{Αλίκη} \rightarrow \text{Βύρων:} \quad n_A \,||\, e_{kB}(ks \,||\, ID_A) \qquad (1)$$
$$\text{Βύρων} \rightarrow \text{Αλίκη:} \quad n_B \,||\, e_{ks}(n_A) \qquad (2)$$
$$\text{Αλίκη} \rightarrow \text{Βύρων:} \quad e_{ks}(n_B) \qquad (3)$$

Η Αλίκη επιλέγει έναν μοναδικό αριθμό και τον στέλνει μαζί με το κρυπτογραφημένο κλειδί συνόδου (1) που έλαβε από το Κέντρο για τον Βύρωνα. Στη συνέχεια, εφόσον ο Βύρων γνωρίζει το κλειδί *kB*, μπορεί να αποκρυπτογραφήσει το κρυπτογραφημένο κλειδί συνόδου και να το χρησιμοποιήσει για να κρυπτογραφήσει τον μοναδικό αριθμό «πρόκληση» που έστειλε η Αλίκη. Ο κρυπτογραφημένος μοναδικός αριθμός στέλνεται στην Αλίκη μαζί με έναν νέο μοναδικό αριθμό (2) που επιλέγει ο Βύρων. Η κρυπτογράφηση του μοναδικού αριθμού n_A της Αλίκης με το κλειδί συνόδου αποδεικνύει ότι ο Βύρων γνωρίζει το κλειδί *kB*, διότι χωρίς τη γνώση αυτού δεν θα ήταν σε θέση να εκτελέσει κρυπτογράφηση με το κλειδί συνόδου *ks*. Στο τέλος του βήματος (2), η Αλίκη διαβεβαιώνεται ότι επικοινωνεί με τον Βύρωνα.

Κατά το βήμα (3), η Αλίκη ανταποδίδει την διαβεβαίωση στον Βύρωνα ότι γνωρίζει το σωστό κλειδί συνόδου. Αν το βήμα (3) είχε παραληφθεί, τότε το βήμα (1) θα μπορούσε να είχε εκτελεσθεί από τον αντίπαλο, ο οποίος θα μετέδιδε κάποιο κλειδί από προηγούμενη επικοινωνία της Αλίκης με τον Βύρωνα, ενώ ο Βύρων δε θα ήταν σε θέση να ανιχνεύσει την επέμβαση του αντιπάλου.

Αν και το παραπάνω πρωτόκολλο φαίνεται ασφαλές, η ασφάλειά του βασίζεται στο βραχυπρόθεσμο κλειδί συνόδου *ks*. Στην περίπτωση που ο αντίπαλος ανακτήσει το κλειδί αυτό, το πρωτόκολλο δεν θα έχει τη δυνατότητα να προσφέρει την απαραίτητη προστασία. Έτσι, είναι προτιμότερο η ασφάλεια να στηρίζεται στα μακροπρόθεσμα κλειδιά *kA*, *kB*. Τα μακροπρόθεσμα κλειδιά είναι από τη φύση τους πιο ανθεκτικά σε κρυπταναλυτικές επιθέσεις, θυσιάζοντας φυσικά ταχύτητα και οικονομία μεγέθους. Το πρωτόκολλο των Denning και Sacco χρησιμοποιεί χρονοσφραγίδες οι οποίες συνδέονται κρυπτογραφικά με το κλειδί *kB* του Βύρωνα με το Κέντρο:

$$\text{Αλίκη} \rightarrow \text{Κέντρο:} \quad ID_A \,||\, ID_B$$
$$\text{Κέντρο} \rightarrow \text{Αλίκη:} \quad e_{kA}(ks \,||\, ID_B \,||\, t_K \,||\, e_{kB}(ks \,||\, ID_A \,||\, t_K))$$
$$\text{Αλίκη} \rightarrow \text{Βύρων:} \quad e_{kB}(ks \,||\, ID_A \,||\, t_K)$$

όπου t_K η χρονοσφραγίδα η οποία δημιουργήθηκε από το Κέντρο. Στη συνέχεια μπορεί να ακολουθήσει πρωτόκολλο πρόκλησης-απόκρισης μεταξύ Αλίκης και Βύρωνα. Το πρωτόκολλο αυτό είναι ισχυρότερο από το προηγούμενο, καθώς ούτε η Αλίκη είναι σε θέση να στείλει παλιό κλειδί συνόδου στον Βύρωνα, επειδή η χρονοσφραγίδα είναι κρυπτογραφημένη με το κλειδί του Βύρωνα και η Αλίκη δεν έχει πρόσβαση σε αυτή.

Η χρονοσφραγίδα είναι μια ισχυρότατη πληροφορία που μπορεί να θωρακίσει τις επικοινωνίες από απειλές επανάληψης παλαιότερων μηνυμάτων, αλλά απαιτείται συγχρονισμός των ρολογιών των διαφορετικών συστημάτων, γεγονός το οποίο ανοίγει νέα μονοπάτια επίθεσης.

7.4.2. Περαιτέρω εδραίωση κλειδιών χωρίς τη συμμετοχή του Κέντρου

Η συμμετοχή του Κέντρου κατά την εδραίωση κλειδιών σε συμμετρικά κρυπτοσυστήματα είναι απαραίτητη, προκειμένου να αποκτήσουν δύο μέλη ένα κοινό μυστικό κλειδί συνόδου. Από τη στιγμή που τα δύο μέλη επιτύχουν να μοιρασθούν το μυστικό κλειδί, μπορούν να το χρησιμοποιήσουν για να δημιουργήσουν τα επόμενα κλειδιά συνόδου για μελλοντική επικοινωνία. Αυτό θα έχει σαν συνέπεια το αρχικό κλειδί συνόδου να μετατραπεί σε μακροπρόθεσμο κλειδί. Τα πρωτόκολλα τα οποία χρησιμοποιούν ένα αρχικό μυστικό κλειδί για να δημιουργήσουν επιπλέον κλειδιά ονομάζονται ***πρωτόκολλα παραγωγής κλειδιών*** (key derivation protocols). Η διαφορά των πρωτοκόλλων παραγωγής κλειδιών από τα πρωτόκολλα εδραίωσης κλειδιών είναι ότι στα πρωτόκολλα παραγωγής κλειδιών, το κλειδί που παράγεται εξαρτάται από το αρχικό κλειδί και δεν απαιτείται ασφαλές κανάλι επικοινωνίας. Στην περίπτωση των πρωτοκόλλων εδραίωσης κλειδιών, το αρχικό (μακροπρόθεσμο) κλειδί χρησιμοποιείται μόνο για να δημιουργήσει ασφαλές κανάλι επικοινωνίας.

Στη συνέχεια θα παρουσιάσουμε μηχανισμούς που χρησιμοποιούνται σε πρωτόκολλα παραγωγής κλειδιών.

Ενημέρωση κλειδιού με δείκτη

Έστω ότι η Αλίκη και ο Βύρων μοιράζονται ένα μυστικό κλειδί k. Η ενημέρωση κλειδιού (key update) με δείκτη επιτυγχάνεται με ένα και μόνο βήμα:

Αλίκη $\rightarrow$ Βύρων: r_A

όπου r_A ένας τυχαίος αριθμός, ο οποίος ονομάζεται ***δείκτης***. Ο δείκτης χρησιμοποιείται για να επιλεγεί το κλειδί από ένα σύνολο κλειδιών το οποίο ορίζεται από μια κρυπτογραφική συνάρτηση. Η κρυπτογραφική συνάρτηση θα πρέπει να αποτελείται από δύο εισόδους, από τις οποίες η μία είναι το κλειδί. Σύμφωνα με τις απαιτήσεις αυτές, η κρυπτογραφική συνάρτηση μπορεί να είναι:

- κρυπτογραφική πράξη κρυπτογράφησης ή αποκρυπτογράφησης συμμετρικού κρυπτοσυστήματος:

$$ks = e_k(r_A) \text{ ή } ks = d_k(r_A)$$

- μονόδρομη συνάρτηση hash με κλειδί:

$$ks = f_k(r_A)$$

Επειδή η κρυπτογραφική πράξη περιλαμβάνει στον υπολογισμό τη μυστική ποσότητα *k*, έπεται ότι μόνον η Αλίκη και ο Βύρων μπορούν να εκτελέσουν το βήμα το οποίο παράγει το κλειδί συνόδου *ks*.

Η ασφάλεια του κλειδιού εξαρτάται τόσο από την ασφάλεια που παρέχει η κρυπτογραφική πράξη, όσο και από τη μυστικότητα του κλειδιού *k*. Η ενημέρωση κλειδιού με δείκτη παρέχει μυστικότητα προς τα πίσω, αφού εάν ανακαλυφθεί το κλειδί *ks* από τον αντίπαλο, αυτός δεν μπορεί να ανακαλύψει το μακροπρόθεσμο κλειδί *k*. Αντίθετα, η ενημέρωση κλειδιού με δείκτη δεν παρέχει μυστικότητα προς τα εμπρός, διότι η ανακάλυψη του μακροπρόθεσμου κλειδιού δίνει τη δυνατότητα στον αντίπαλο να ανακτήσει όλα τα κλειδιά συνόδου που προήλθαν από το κλειδί *k*.

Η ενημέρωση κλειδιού μπορεί να βελτιωθεί με δύο τεχνικές. Η μια είναι να χρησιμοποιηθεί χρονοσφραγίδα αντί του τυχαίου αριθμού. Έτσι στην περίπτωση που η Αλίκη και ο Βύρων έχουν συγχρονισμένα ρολόγια, μπορούν να συμφωνήσουν να ενημερώνουν το κλειδί συνόδου υπολογίζοντας κατά συγκεκριμένα χρονικά διαστήματα νέα κλειδιά. Έτσι δεν απαιτείται η Αλίκη να στείλει το r_A στον Βύρωνα, καθώς ο Βύρων μπορεί να το παράγει από την ώρα του συστήματός του. Το μειονέκτημα της τεχνικής αυτής είναι ότι αν το κανάλι επικοινωνίας έχει καθυστερήσεις, τα κρυπτοκείμενα που θα φθάνουν στην Αλίκη και στον Βύρωνα και βρίσκονται κοντά στους χρόνους ενημέρωσης των κλειδιών, μπορεί να αποκρυπτογραφηθούν με το επόμενο κλειδί, ενώ έχουν κρυπτογραφηθεί με το προηγούμενο κλειδί.

Η δεύτερη τεχνική βελτίωσης είναι απαλλαγμένη από το παραπάνω μειονέκτημα, αλλά μπορεί να πραγματοποιηθεί μόνον στην περίπτωση που η κρυπτογραφική συνάρτηση είναι αντιστρέψιμη. Έστω ότι η κρυπτογραφική συνάρτηση που χρησιμοποιείται είναι η κρυπτογράφηση με κάποιον κρυπταλγόριθμο. Τότε η Αλίκη μπορεί να επιλέξει μια χρονοσφραγίδα και να το αποκρυπτογραφήσει. Το αποτέλεσμα θα είναι ο φαινομενικά τυχαίος αριθμός r_A :

$$r_A = d_k(t_A)$$

Όταν ο Βύρων παραλάβει τον αριθμό r_A και τον κρυπτογραφήσει, το κρυπτοκείμενο θα είναι ίσο με την ώρα της Αλίκης. Έτσι εκτελείται και αυθεντικοποίηση του μηνύματος. Δεν απαιτείται τα ρολόγια της Αλίκης και του Βύρωνα να είναι συγχρονισμένα. Ο Βύρων μπορεί να αποθηκεύσει την ώρα της Αλίκης που παρέλαβε και εκτελεί την επόμενη ενημέρωση, μόνον όταν η επόμενη ώρα της Αλίκης που θα παραλάβει είναι μεταγενέστερη από την προηγούμενη. Με αυτόν τον τρόπο, ο αντίπαλος δεν έχει τη δυνατότητα επιτυχούς επαναχρησιμοποίησης του r_A. Φυσικά το νέο κλειδί δεν μπορεί να είναι η κρυπτογράφηση του r_A, διότι αυτό όπως είδαμε

αντιστοιχεί στη χρονοσφραγίδα της Αλίκης την οποία μπορεί να μαντέψει με ευκολία ο αντίπαλος. Επομένως, απαιτείται και μια δεύτερη κρυπτογράφηση της χρονοσφραγίδας, για να προκύψει το νέο κλειδί.

Πρωτόκολλο ανταλλαγής κλειδιού με αυθεντικοποίηση

Το πρωτόκολλο ανταλλαγής κλειδιού με αυθεντικοποίηση (authenticated key exchange protocol) πραγματοποιεί τόσο αμοιβαία αυθεντικοποίηση (mutual authentication) των μελών, όσο και αυθεντικοποίηση του παραγόμενου κλειδιού συνόδου. Για την εκτέλεση του πρωτοκόλλου απαιτούνται δύο μακροπρόθεσμα κλειδιά k και k'. Η κρυπτογραφική συνάρτηση που περιλαμβάνεται στο πρωτόκολλο είναι κρυπτογραφική μονόδρομη hash με κλειδί (π.χ. μια MAC).

Τα βήματα του πρωτοκόλλου είναι τα εξής:

$$\text{Αλίκη} \rightarrow \text{Βύρων:} \quad n_A \tag{1}$$

$$\text{Βύρων} \rightarrow \text{Αλίκη:} \quad n_A \,||\, n_B \,||\, ID_A \,||\, ID_B \,||\, f_k(n_A \,||\, n_B \,||\, ID_A \,||\, ID_B) \tag{2}$$

$$\text{Αλίκη} \rightarrow \text{Βύρων:} \quad ID_A \,||\, n_B \,||\, f_{ks}(ID_A \,||\, n_B) \tag{3}$$

Αρχικά, η Αλίκη επιλέγει έναν μοναδικό αριθμό n_A και τον στέλνει στον Βύρωνα (1). Ο Βύρων με τη σειρά του επιλέγει έναν μοναδικό αριθμό n_B και τον στέλνει μαζί με τον αριθμό n_A της Αλίκης, τις ταυτότητές τους καθώς και τη σύνοψη όλων των στοιχείων αυτών, στην Αλίκη (2).

Η Αλίκη ελέγχει την αυθεντικότητα και την ακεραιότητα των στοιχείων που παρέλαβε με τη βοήθεια της μονόδρομης hash και του κλειδιού k. Το βήμα αυτό αποτελεί την αυθεντικοποίηση του Βύρωνα στην Αλίκη. Στη συνέχεια, η Αλίκη στέλνει την ταυτότητά της μαζί με τον αριθμό n_B του Βύρωνα καθώς και τη σύνοψη αυτών των δύο στον Βύρωνα (3).

Ο Βύρων εξακριβώνει ότι η σύνοψη που έλαβε από την Αλίκη είναι σωστή. Το βήμα αυτό αποτελεί την αυθεντικοποίηση της Αλίκης στον Βύρωνα. Τέλος, το κλειδί συνόδου μπορεί να υπολογισθεί από το κάθε μέλος χωριστά, με τη συμμετοχή του δεύτερου μακροπρόθεσμου κλειδιού:

$$ks = f_{k'}(n_B)\,.$$

Το παραπάνω πρωτόκολλο μπορεί να εκτελεσθεί με πολλές παραλλαγές. Για παράδειγμα, για οικονομία μεγέθους μηνυμάτων, μπορούν να παραλειφθούν οι μεταδόσεις των ποσοτήτων οι οποίες είναι ήδη γνωστές και στα δύο μέλη. Επίσης, η δημιουργία του κλειδιού συνόδου θα μπορούσε να προκύψει από τον μοναδικό αριθμό της Αλίκης, n_A.

7.4.3. Το πρωτόκολλο αυθεντικοποίησης Κέρβερος

Ο Κέρβερος είναι ένα σύστημα αυθεντικοποίησης μελών ενός δικτύου υπολογιστών. Τα μέλη μπορεί να είναι χρήστες ή και συστατικά του δικτύου όπως προσω-

πικοί υπολογιστές, εκτυπωτές, servers, κτλ. Ο Κέρβερος αναπτύχθηκε στο MIT και αποτελεί μέρος του project Athena. Εκτός από την αυθεντικοποίηση των μελών, ο Κέρβερος προσφέρει πληροφορίες ελέγχου πρόσβασης ενός χρήστη στους κατανεμημένους πόρους ενός δικτύου. Έχει υλοποιηθεί σε περιβάλλον Unix, και επίσης εκτελεί τις βασικές υπηρεσίες ασφάλειας των Windows 2000 της Microsoft.

Όσον αφορά την εδραίωση κλειδιών, ο Κέρβερος περιλαμβάνει ένα KDC, το οποίο αποτελεί την έμπιστη οντότητα στην αυθεντικοποίηση των χρηστών. Στο σημείο αυτό θα παρουσιάσουμε το πρωτόκολλο αυθεντικοποίησης ενός χρήστη σε κάποιον άλλον και δημιουργίας κλειδιού συνόδου μεταξύ αυτών.

Στον Κέρβερο ορίζονται οι εξής έννοιες πληροφοριών που διακινούνται μεταξύ των μελών:

$ticket_B = e_{kB}(ks, ID_A, L)$: «εισιτήριο», το οποίο το ζητά η Αλίκη μετά από αίτηση στο Κέντρο για επικοινωνία με τον Βύρωνα

L: χρόνος ζωής του εισιτηρίου. Ουσιαστικά η παράμετρος αυτή αποτελείται από την ημερομηνία λήξης του κλειδιού συνόδου και προαιρετικά από μια ημερομηνία έναρξης .

$authenticator = e_{ks}(ID_A, t_A, ks')$: δεδομένα αυθεντικοποίησης της Αλίκης στον Βύρωνα. Το ks' είναι, προαιρετικά, ένα επιπλέον κλειδί συνόδου το οποίο δημιουργήθηκε από την Αλίκη.

Το πρωτόκολλο αυθεντικοποίησης και εδραίωσης κλειδιού του Κέρβερου έχει ως εξής:

Αλίκη → Κέντρο:	$ID_A \parallel ID_B \parallel n_A$	(1)
Κέντρο → Αλίκη:	$ticket_B, e_{kA}(ks \parallel n_A \parallel L \parallel ID_B)$	(2)
Αλίκη → Βύρων:	$ticket_B, authenticator$	(3)
Βύρων → Αλίκη:	$e_{ks}(t_A, ks'')$	(4)

Αρχικά, η Αλίκη δημιουργεί έναν μοναδικό αριθμό n_A και τον στέλνει μαζί με την ταυτότητά της και την ταυτότητα του Βύρωνα στο Κέντρο (1). Στη συνέχεια, το Κέντρο δημιουργεί ένα κλειδί συνόδου *ks*, επιλέγει το χρόνο ζωής L του εισιτηρίου και δημιουργεί το εισιτήριο του Βύρωνα κρυπτογραφώντας το κλειδί συνόδου, την ταυτότητα της Αλίκης και το χρόνο ζωής. Η επιλογή του χρόνου ζωής του εισιτηρίου εξαρτάται από την πολιτική ασφάλειας της επιχείρησης όπου υλοποιείται ο Κέρβερος. Το εισιτήριο συνδέει κρυπτογραφικά το κλειδί συνόδου, την Αλίκη και τον Βύρωνα για μια χρονική περίοδο, καθιστώντας το ακατάλληλο για οποιαδήποτε άλλη χρήση με άλλα μέλη ή άλλον χρόνο από L.

Στη συνέχεια, το Κέντρο στέλνει το εισιτήριο μαζί με το κλειδί συνόδου, τον μοναδικό αριθμό που έλαβε από την Αλίκη, τη διάρκεια ζωής και την ταυτότητα

του Βύρωνα, κρυπτογραφημένα με το κλειδί που μοιράζεται με την Αλίκη (2). Εφόσον η Αλίκη δεν έχει πρόσβαση στα περιεχόμενα του εισιτηρίου, το Κέντρο την ενημερώνει για το κλειδί συνόδου και τη διάρκεια ζωής, στέλνοντας τις πληροφορίες αυτές κρυπτογραφημένες με το κλειδί kA.

Από το μήνυμα που παραλαμβάνει η Αλίκη από το Κέντρο έχει τη δυνατότητα να αποκρυπτογραφήσει μόνον το τμήμα εκείνο το οποίο δεν ανήκει στο εισιτήριο. Έτσι μπορεί να ανακτήσει το κλειδί ks, τη διάρκεια ζωής του εισιτηρίου L (και κατ' επέκταση του κλειδιού ks) και τον μοναδικό αριθμό n_A. Ο μοναδικός αριθμός χρησιμεύει και ως στοιχείο ταξινόμησης των αιτήσεων της Αλίκης στο Κέντρο, η οποία μπορεί να έχει στείλει περισσότερες από μία, προκειμένου να επικοινωνήσει με διαφορετικά μέλη. Χρησιμοποιώντας το κλειδί συνόδου ks, κρυπτογραφεί την ταυτότητά της μαζί με μια νέα χρονοσφραγίδα t_A, και ένα προαιρετικό δεύτερο κλειδί συνόδου ks', που μπορεί να μοιραστεί με τον Βύρωνα. Το κρυπτοκείμενο που προκύπτει αποτελεί τα δεδομένα αυθεντικοποίησης (authenticator) της Αλίκης προς τον Βύρωνα, το οποίο αποστέλλεται στον Βύρωνα μαζί με το εισιτήριο (3).

Μόλις ο Βύρων παραλάβει το εισιτήριο και το κρυπτοκείμενο αυθεντικοποίησης, αποκρυπτογραφεί το εισιτήριο για να ανακτήσει το κλειδί συνόδου ks, το χρόνο ζωής L και την ταυτότητα της Αλίκης ID_A. Αρχικά ελέγχει εάν το τοπικό του ρολόι είναι εντός των ορίων που καθορίζονται από το χρόνο ζωής L. Στην περίπτωση που η τοπική του ώρα είναι εντός των ορίων, ο Βύρων χρησιμοποιεί το κλειδί συνόδου ks για να αποκρυπτογραφήσει το κρυπτοκείμενο αυθεντικοποίησης. Από το κρυπτοκείμενο αυτό ανακτά την ταυτότητα της Αλίκης ID_A, τη χρονοσφραγίδα t_A και το δεύτερο κλειδί συνόδου ks', εάν υπάρχει. Στη συνέχεια, εκτελεί δύο επιπλέον ελέγχους. Κατά τον πρώτο έλεγχο, συγκρίνει την ταυτότητα της αυθεντικοποίησης με την ταυτότητα του εισιτηρίου. Οι δύο ταυτότητες θα πρέπει να συμπίπτουν και να είναι ίσες με την ταυτότητα της Αλίκης. Κατά τον δεύτερο έλεγχο, ο Βύρων εξετάζει την επικαιρότητα της χρονοσφραγίδας t_A, με βάση το τοπικό του ρολόι. Η χρονοσφραγίδα θεωρείται επίκαιρη και συνεπώς έγκυρη, αν η διαφορά του με την τοπική ώρα του Βύρωνα δεν ξεπερνά κάποιο καθορισμένο όριο. Το όριο αυτό καθορίζεται από την πολιτική ασφάλειας της επιχείρησης.

Τέλος, ο Βύρων κρυπτογραφεί τη χρονοσφραγίδα της Αλίκης με το κλειδί συνόδου ks και το κρυπτογραφημένο κείμενο αποστέλλεται στην Αλίκη (4). Προαιρετικά, ο Βύρων έχει τη δυνατότητα να δημιουργήσει ένα τρίτο κλειδί συνόδου ks'' και να το κρυπτογραφήσει μαζί με τη χρονοσφραγίδα. Η κρυπτογράφηση αυτή είναι η πράξη αυθεντικοποίησης του Βύρωνα στην Αλίκη. Κρυπτογραφώντας τη χρονοσφραγίδα της Αλίκης με το κλειδί συνόδου, ο Βύρων αποδεικνύει ότι γνωρίζει το σωστό κλειδί συνόδου.

Ανάλυση του πρωτοκόλλου Κέρβερος

Η ασφάλεια του Κέρβερου εξαρτάται κυρίως από δύο χαρακτηριστικά: από το χειρισμό του χρόνου και από τα μακροπρόθεσμα κλειδιά.

Η χρησιμοποίηση παραμέτρων που εξαρτώνται από το χρόνο, έχει πλεονεκτήματα και μειονεκτήματα. Ο ορισμός του χρόνου ζωής του εισιτηρίου αποβλέπει στην εξοικονόμηση μηνυμάτων από και προς το Κέντρο. Σε ένα δίκτυο υπάρχουν οντότητες οι οποίες επικοινωνούν με μεγάλη συχνότητα, όπως για παράδειγμα ένας εξυπηρετητής αρχείων (file server) με τα προγράμματα-πελάτες του, σε ένα κατανεμημένο σύστημα αρχείων. Σε ένα τέτοιο σύστημα, η συνεχής απαίτηση επικοινωνίας με το Κέντρο για την έκδοση των εισιτηρίων θα προκαλούσε, τόσο μεγάλη κίνηση στο δίκτυο, όσο και αυξημένο φόρτο εργασίας στο Κέντρο. Η χρησιμοποίηση του χρόνου ζωής του εισιτηρίου μειώνει εντυπωσιακά τις απαιτήσεις υπολογιστικής ισχύος του Κέντρου και αυξάνει επίσης την απόδοση του δικτύου.

Ωστόσο, η χρησιμοποίηση μεγάλων ορίων χρόνου ζωής καθιστά το σύστημα ευάλωτο σε επιθέσεις επαναχρησιμοποίησης. Το ρίσκο είναι αυξημένο στις υπηρεσίες εκείνες όπου ο χρήστης χρησιμοποιεί πόρους του δικτύου για μικρό χρονικό διάστημα, όπως για παράδειγμα, ο έλεγχος μηνυμάτων ηλεκτρονικού ταχυδρομείου και η αποστολή εγγράφων σε υπηρεσία εκτύπωσης. Υπό αυτές τις συνθήκες, ο αντίπαλος έχει το πλεονέκτημα να επαναχρησιμοποιήσει το εισιτήριο του χρήστη προκειμένου να αποκτήσει πρόσβαση στους πόρους που επιθυμεί. Συνεπώς, ο καθορισμός των ορίων του χρόνου ζωής του κλειδιού εξαρτάται από τα όρια ρίσκου που θεωρούνται ανεκτά, σύμφωνα με την πολιτική της επιχείρησης.

Από τεχνικής πλευράς, η χρησιμοποίηση παραμέτρων που εξαρτώνται από το χρόνο, απαιτεί υπηρεσίες συγχρονισμού της ώρας όλων των συστημάτων που συμμετέχουν στον Κέρβερο. Παρόλο που υπάρχουν πρωτόκολλα συγχρονισμού ώρας μεταξύ των συστημάτων, πολλά από αυτά δεν είναι κατάλληλα για χρήση σε πρωτόκολλα ασφάλειας όπως ο Κέρβερος, διότι δεν είναι σχεδιασμένα στο να αντιστέκονται σε επιθέσεις. Ο Κέρβερος και γενικότερα τα πρωτόκολλα που παρέχουν υπηρεσίες ασφάλειας και περιλαμβάνουν χρονικές παραμέτρους θα πρέπει να χρησιμοποιούν υπηρεσίες συγχρονισμού ώρας οι οποίες προσφέρουν αυθεντικοποίηση και ακεραιότητα.

Όσον αφορά τα μακροπρόθεσμα κλειδιά που μοιράζονται τα μέλη με το Κέντρο, για χάριν ευκολίας χρήσης τα κλειδιά αυτά παράγονται από κωδικούς πρόσβασης που πληκτρολογούν οι χρήστες για να συνδεθούν στο σύστημα. Επομένως, η ασφάλεια του Κέρβερου εκφυλίζεται στην ασφάλεια των κωδικών πρόσβασης και οι επιθέσεις του αντιπάλου σχετίζονται με τις μεθόδους ανάκτησης των κωδικών πρόσβασης που είναι η εξαντλητική αναζήτηση και η επίθεση λεξιλογίου (dictionary attack).

Οι παραπάνω επιθέσεις στα μακροχρόνια κλειδιά μπορούν να πραγματοποιηθούν σε όλα τα συστήματα όπου ο αντίπαλος έχει πρόσβαση στο κανάλι επικοινωνίας των μελών με το Κέντρο και μπορεί να υποκλέψει τα μηνύματα που διακινούνται. Σε ορισμένα δικτυακά λειτουργικά, ο αντίπαλος μπορεί να αναπτύξει πιο αποτελεσματικές επιθέσεις, εκμεταλλευόμενος συγκεκριμένες αδυναμίες του λειτουργικού συστήματος. Για παράδειγμα, αν το λειτουργικό σύστημα δεν μπορεί να παρέχει το απαιτούμενο βαθμό ασφάλειας κατά τη σύνδεση (login) του χρήστη στο σταθμό εργασίας, ο αντίπαλος μπορεί να υποκλέψει τον κωδικό πρόσβασης

καθώς αυτός πληκτρολογείται από το χρήστη. Σε μια τέτοια επίθεση, τα πρωτόκολλα του Κέρβερου δεν μπορούν να παρέχουν τις επιθυμητές κρυπτογραφικές υπηρεσίες ασφάλειας.

7.4.4. Εδραίωση κλειδιών χωρίς την ύπαρξη Κέντρων

Ο Shamir ανέπτυξε ένα πρωτόκολλο όπου δύο μέλη μπορούν να μοιρασθούν ένα κλειδί συνόδου χωρίς τη συμμετοχή Κέντρου, χωρίς την ύπαρξη ασφαλούς καναλιού και χωρίς την ύπαρξη μακροπρόθεσμου κλειδιού μεταξύ των μελών αυτών. Το πρωτόκολλο ανήκει στην κατηγορία πρωτοκόλλων εδραίωσης κλειδιών σε συμμετρικά κρυπτοσυστήματα, παρόλο που χρησιμοποιεί modular αριθμητική που συναντάται κατά κόρον στην ασύμμετρη κρυπτογραφία.

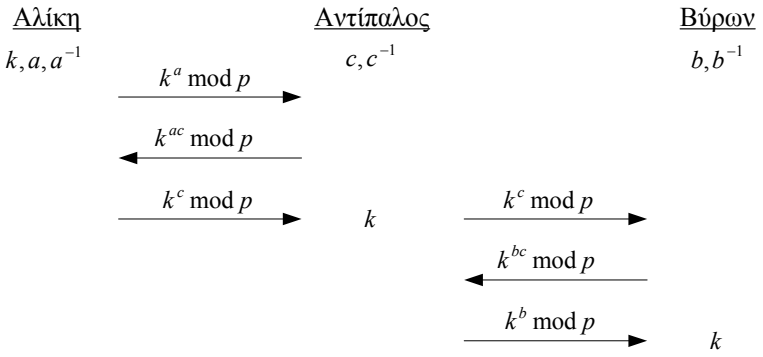
Το πρωτόκολλο του Shamir έχει ως εξής. Αρχικά η Αλίκη και ο Βύρων επιλέγουν δημόσια έναν πρώτο αριθμό p. Στη συνέχεια η Αλίκη και ο Βύρων επιλέγουν αντίστοιχα ακέραιους a και b, τέτοιους ώστε $0 < a, b < p–1$ με $\gcd(a, p–1) = \gcd(b, p–1) = 1$. Οι αριθμοί αυτοί κρατούνται μυστικοί. Η Αλίκη υπολογίζει τον αντίστροφο $a^{-1} \bmod p–1$, ενώ ο Βύρων υπολογίζει τον αντίστροφο $b^{-1} \bmod p–1$. Στη συνέχεια εκτελείται το εξής πρωτόκολλο:

Αλίκη → Βύρων:	$k^a \bmod p$	(1)
Βύρων → Αλίκη:	$(k^a)^b \bmod p$	(2)
Αλίκη → Βύρων:	$(k^{ab})^{a^{-1}} \bmod p$	(3)

Αρχικά, η Αλίκη επιλέγει ένα κλειδί συνόδου k, $0 < k < p–1$, το οποίο υψώνει στον μυστικό εκθέτη a και το στέλνει στον Βύρωνα (1). Στη συνέχεια ο Βύρων υψώνει το μήνυμα που έλαβε στο μυστικό εκθέτη b και στέλνει το αποτέλεσμα πίσω στην Αλίκη. Τέλος, η Αλίκη απομακρύνει τον μυστικό εκθέτη a, υψώνοντας το μήνυμα που έλαβε στον a^{-1} και στέλνει το αποτέλεσμα της πράξης στον Βύρωνα (3). Το μήνυμα που παραλαμβάνει ο Βύρων αντιστοιχεί στο κλειδί συνόδου υψωμένο στον μυστικό εκθέτη b. Έτσι ο Βύρων είναι σε θέση να απομακρύνει τον εκθέτη αυτόν και να ανακτήσει το κλειδί συνόδου k, υψώνοντας το μήνυμα στον b^{-1}.

Η ασφάλεια του πρωτοκόλλου βασίζεται στο πρόβλημα του διακριτού λογάριθμου. Ο αντίπαλος ο οποίος υποκλέπτει τα μηνύματα μεταξύ της Αλίκης και του Βύρωνα, για να ανακτήσει το κλειδί, θα πρέπει να βρει οποιοδήποτε από τα a και b. Αυτό ισοδυναμεί με τον υπολογισμό του διακριτού λογάριθμου του $k^a \bmod p$ ή $k^b \bmod p$.

Αν και το πρωτόκολλο του Shamir είναι ασφαλές σε παθητική επίθεση του αντιπάλου, είναι ευάλωτο σε ενεργητική επίθεση, όπου ο αντίπαλος έχει τη δυνατότητα να τροποποιεί τα μηνύματα. Η επίθεση που μπορεί να αναπτύξει ο αντίπαλος είναι γνωστή ως επίθεση του ενδιάμεσου ατόμου (man-in-the-middle attack), και παριστάνεται στο Σχήμα 7.3.



Σχήμα 7.3 Ενεργή επίθεση του ενδιάμεσου ατόμου στο πρωτόκολλο του Shamir

Ο αντίπαλος παρεμβάλλεται μεταξύ της Αλίκης και του Βύρωνα και εκτελεί το πρωτόκολλο με τον καθένα χωριστά. Έτσι η Αλίκη και ο Βύρων έχουν την εντύπωση ότι το πρωτόκολλο εκτελείται μεταξύ τους και μόνο μία φορά, αλλά στην πραγματικότητα εκτελείται δύο φορές, μία μεταξύ της Αλίκης και του αντιπάλου ο οποίος προσποιείται ότι είναι ο Βύρων, και μία μεταξύ του Βύρωνα και του αντιπάλου, ο οποίος προσποιείται ότι είναι η Αλίκη. Ο αντίπαλος είναι σε θέση να επιλέξει μυστικό ακέραιο c, όπως απαιτεί το πρωτόκολλο. Κατά την ολοκλήρωση του πρωτοκόλλου με την Αλίκη, ο αντίπαλος έχει στην κατοχή του το κλειδί συνόδου k, και αμέσως ξεκινά την εκτέλεση του πρωτοκόλλου με τον Βύρωνα. Με την ολοκλήρωση της εκτέλεσης του πρωτοκόλλου με τον Βύρωνα, ο αντίπαλος μπορεί να λειτουργήσει πλέον παθητικά ως υποκλοπέας και να ανακτά με επιτυχία την κρυπτογραφημένη συνομιλία μεταξύ της Αλίκης και του Βύρωνα.

Θεωρητικά η καθυστέρηση της επικοινωνίας της Αλίκης με τον Βύρωνα, λόγω της δεύτερης εφαρμογής του πρωτοκόλλου, θα μπορούσε να χρησιμοποιηθεί από την Αλίκη για να ανιχνεύσει την παρουσία και παρεμβολή του αντιπάλου. Όμως στην πράξη τα πρωτόκολλα εκτελούνται μεταξύ σταθμών εργασίας και διαρκούν ελάχιστο χρόνο, της τάξεως ορισμένων δευτερολέπτων. Πολλές φορές η καθυστέρηση λόγω της αυξημένης κίνησης του δικτύου μπορεί να είναι μεγαλύτερη από το χρόνο εκτέλεσης του πρωτοκόλλου, οπότε η Αλίκη δεν είναι σε θέση να διακρίνει αν η καθυστέρηση οφείλεται στην παρεμβολή του αντιπάλου ή όχι.

7.4.5. Εδραίωση κλειδιών σε ασύμμετρα κρυπτοσυστήματα

Η χρήση της ασύμμετρης κρυπτογραφίας μετέβαλλε δραματικά το τοπίο της διαχείρισης των κλειδιών. Η βασική αιτία που προώθησε την έρευνα της ασύμμετρης κρυπτογραφίας είναι το πρόβλημα του τετραγώνου στη διανομή και διαχείριση κλειδιών των συμμετρικών κρυπτοσυστημάτων.

Όπως και στην εδραίωση κλειδιών στα συμμετρικά κρυπτοσυστήματα, το μοντέλο επικοινωνίας μπορεί να περιλαμβάνει έμπιστη οντότητα. Ωστόσο, ο ρόλος

της έμπιστης οντότητας στα ασύμμετρα κρυπτοσυστήματα είναι εντελώς διαφορετικός από αυτόν στα συμμετρικά κρυπτοσυστήματα. Εδώ, η έμπιστη οντότητα δεν χρησιμοποιείται ως μέσο δημιουργίας ασφαλούς καναλιού επικοινωνίας για τη μεταφορά των κλειδιών. Εξάλλου στην ασύμμετρη κρυπτογραφία δεν απαιτείται ασφαλές κανάλι για τη μεταφορά των κλειδιών. Στην ασύμμετρη κρυπτογραφία, η έμπιστη οντότητα καλείται για να πιστοποιήσει την ταυτότητα των μελών ή γενικότερα να υποστηρίξει τις υπηρεσίες αυθεντικοποίησης των μελών και των μηνυμάτων που ανταλλάσσονται σε ένα μοντέλο επικοινωνίας. Έτσι, η έμπιστη οντότητα χρησιμοποιείται για να αποτρέψει τις επιθέσεις προσποίησης ταυτότητας, όπως είναι η επίθεση του ενδιάμεσου ατόμου.

Ανταλλαγή κλειδιών κατά Diffie και Hellman

Το πρωτόκολλο ανταλλαγής κλειδιών (key exchange protocol) των Diffie και Hellman (1976) είναι το πρώτο ασύμμετρο πρωτόκολλο εδραίωσης κλειδιού και η ασφάλειά του συνδέεται με το πρόβλημα του διακριτού λογάριθμου.

Το πρωτόκολλο των Diffie και Hellman είναι σχετικά απλό στην περιγραφή. Η Αλίκη και ο Βύρων επιλέγουν δημόσια έναν πρώτο αριθμό p και έναν γεννήτορα a του συνόλου $\boldsymbol{Z}_p^*$. Στη συνέχεια η Αλίκη και ο Βύρων επιλέγουν χωριστά από έναν κρυφό τυχαίο ακέραιο x και y αντίστοιχα, όπου $0 < x, y < p–1$ και εκτελούν το ακόλουθο πρωτόκολλο:

Αλίκη → Βύρων:	$a^x \bmod p$	(1)
Βύρων → Αλίκη:	$a^y \bmod p$	(2)

Το κλειδί συνόδου είναι το $a^{xy} \bmod p$. Για να υπολογισθεί το κλειδί αυτό, ο μεν Βύρων υψώνει την ποσότητα που παρέλαβε από την Αλίκη στον μυστικό εκθέτη y, ενώ η Αλίκη υψώνει την ποσότητα που παρέλαβε από τον Βύρωνα στον μυστικό εκθέτη x.

Ο αντίπαλος έχει γνώση των a, p, a^x, a^y και καλείται να ανακαλύψει τον a^{xy}. Αυτό μπορεί να επιτευχθεί με δύο τρόπους:

- εύρεση του διακριτού λογάριθμου του $a^x \bmod p$ με βάση τον a, το οποίο είναι υπολογιστικά αδύνατο για μεγάλο p.
- εύρεση του a^{xy}, υψώνοντας τον a^x σε διάφορους εκθέτες, έως ότου βρεθεί ο a^{xy}. Η καταλληλότητα της επίθεσης αυτής εξαρτάται από τη δυνατότητα του αντιπάλου να ελέγχει αν βρήκε το σωστό εκθέτη. Αυτή η επίθεση ισοδυναμεί με εξαντλητική αναζήτηση, η οποία θα πρέπει να είναι πρακτικά ανέφικτη.

ΠΑΡΑΔΕΙΓΜΑ 7.1 – Ανταλλαγή κλειδιών κατά Diffie και Hellman. Έστω $p = 257$ και $a = 11$. Η Αλίκη επιλέγει μυστικό εκθέτη $x = 52$. Ο Βύρων επιλέγει μυστικό εκθέτη $y = 121$.

Η Αλίκη υπολογίζει: $11^{52} \bmod 257 = 129$.

Ο Βύρων υπολογίζει $11^{121} \bmod 257 = 213$.

Στη συνέχεια η Αλίκη και ο Βύρων ανταλλάσσουν τα αποτελέσματα των υπολογισμών.

Η Αλίκη υπολογίζει: $k = 213^{52} \bmod 257 = 128$.

Ο Βύρων υπολογίζει $129^{121} \bmod 257 = 128$.

Υλοποίηση του πρωτοκόλλου Diffie και Hellman σε ελλειπτικές καμπύλες

Όπως παρουσιάσαμε στο Κεφάλαιο 6, το πρόβλημα του διακριτού λογάριθμου ορίζεται σε ελλειπτικές καμπύλες ως πρόβλημα εύρεσης του συντελεστή του βαθμωτού γινομένου ενός σημείου της ελλειπτικής καμπύλης, το οποίο διατηρεί την ιδιότητα του υπολογιστικά αδύνατου προβλήματος.

Το πρωτόκολλο των Diffie και Hellman σε ελλειπτικές καμπύλες εκφράζεται ως εξής. Η Αλίκη και ο Βύρων επιλέγουν δημόσια μια ελλειπτική καμπύλη:

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

και ένα στοιχείο γεννήτορα της καμπύλης $A = (x_1, y_1)$. Στη συνέχεια, η Αλίκη επιλέγει έναν μυστικό αριθμό x_a, τέτοιον ώστε $1 < x_a < p$. Παρόμοια, ο Βύρων επιλέγει έναν μυστικό αριθμό x_b, τέτοιον ώστε $1 < x_b < p$. Το πρωτόκολλο εκτελείται ως εξής:

Αλίκη → Βύρων: $x_a \cdot A \bmod p$ (1)

Βύρων → Αλίκη: $x_b \cdot A \bmod p$ (2)

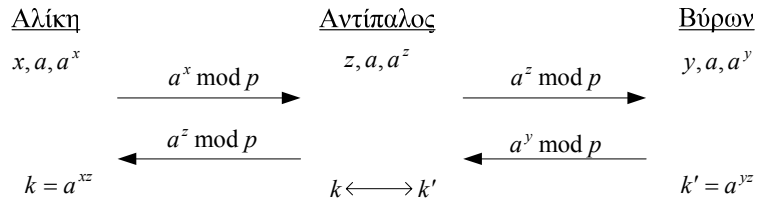
Το κοινό κλειδί συνόδου αντιστοιχεί στο στοιχείο της καμπύλης $x_a x_b A \bmod p$, το οποίο μπορούν να το υπολογίσουν ανεξάρτητα η Αλίκη και ο Βύρων.

Ο αντίπαλος γνωρίζει την ελλειπτική καμπύλη, το στοιχείο γεννήτορα A, καθώς και τα στοιχεία της καμπύλης $x_a A$ και $x_b A$ και καλείται να ανακαλύψει το κλειδί συνόδου ανακαλύπτοντας είτε το x_a είτε το x_b.

Ασφάλεια του πρωτοκόλλου Diffie και Hellman

Το πρωτόκολλο ανταλλαγής κλειδιών του Diffie και Hellman θεωρείται ότι βασίζεται στο πρόβλημα του διακριτού λογάριθμου. Αυτό σημαίνει ότι αν ανακαλυφθεί αλγόριθμος ο οποίος μπορεί να βρίσκει αποτελεσματικά το διακριτό αλγόριθμο ενός αριθμού ως προς κάποια βάση, τότε το πρωτόκολλο δεν θα είναι ασφαλές. Το αντίστροφο όμως δεν ισχύει, η μη ύπαρξη αποτελεσματικού αλγόριθμου δεν εγγυάται την ασφάλεια του πρωτοκόλλου.

Το πρωτόκολλο ανταλλαγής κλειδιών θεωρείται ασφαλές στην περίπτωση παθητικής επίθεσης, δηλαδή στην περίπτωση που ο αντίπαλος λειτουργεί ως υποκλοπέας και καταγράφει τα μηνύματα που ανταλλάσσονται μεταξύ της Αλίκης και του Βύρωνα. Ωστόσο στην περίπτωση ενεργητικής επίθεσης, το πρωτόκολλο δεν είναι ασφαλές. Έτσι το πρωτόκολλο υποπίπτει στην επίθεση του ενδιάμεσου ατόμου όπως φαίνεται στο Σχήμα 7.4.



Σχήμα 7.4 Επίθεση ενδιάμεσου ατόμου στο πρωτόκολλο Diffie και Hellman

Η αρχή της επίθεσης είναι η ίδια με αυτήν του πρωτοκόλλου του Shamir (§7.4.4). Ο αντίπαλος ο οποίος δεν είναι αντιληπτός από τα δύο μέλη, εισάγει τις δικές του παραμέτρους με τέτοιον τρόπο ώστε να ελέγχει τη δημιουργία του κλειδιού συνόδου. Η διαφορά εδώ με την επίθεση του πρωτοκόλλου του Shamir είναι ότι ο αντίπαλος κατά την ολοκλήρωση του πρωτοκόλλου δεν μπαίνει σε λειτουργία παθητικού υποκλοπέα, αλλά λειτουργεί ως αναμεταδότης των μηνυμάτων, μεταφράζοντας τα μηνύματα μεταξύ των κλειδιών k και k' τα οποία μοιράζεται αντίστοιχα με την Αλίκη και τον Βύρωνα χωριστά.

Συμμετοχή τρίτης οντότητας

Για να αντιμετωπιστεί η περίπτωση ενεργητικής επίθεσης, μια λύση είναι το μοντέλο επικοινωνίας να περιλάβει μια τρίτη οντότητα η οποία εκτελεί το ρόλο του δημόσιου καταλόγου (public directory). Σύμφωνα με το μοντέλο αυτό, η Αλίκη και ο Βύρων, καθώς και όλα τα επικοινωνούντα μέλη, δημοσιεύουν τον γεννήτορα a υψωμένο στο μυστικό τους εκθέτη. Ο γεννήτορας, καθώς και οι μυστικοί εκθέτες, είναι μακροχρόνιες παράμετροι και παραμένουν σταθεροί σε όλες τις επικοινωνίες, σε αντίθεση με το αρχικό πρωτόκολλο Diffie και Hellman όπου οι εκθέτες επιλέγονται κατά την έναρξη του πρωτοκόλλου.

Το κάθε μέλος έχει ασφαλή επικοινωνία με το δημόσιο κατάλογο. Αυτό μπορεί να γίνει με κάποιο κλειδί που μπορεί να μοιράζεται ο κατάλογος με το κάθε μέλος, ή με ψηφιακή υπογραφή. Στην περίπτωση που ο κατάλογος μοιράζεται μυστικό κλειδί με τα μέλη, το κλειδί αυτό θα χρησιμοποιείται στον υπολογισμό μιας συνάρτησης MAC, για να ελεγχθεί η αυθεντικότητα του μηνύματος. Συνοπτικά, το πρωτόκολλο που θα εκτελεσθεί είναι το εξής:

$$\text{Αλίκη} \rightarrow \text{Κατάλογος: } ID_A \parallel ID_B \qquad (1\alpha)$$

Κατάλογος → Αλίκη: $ID_B \| a^y \| h_{kA}(ID_B \| a^y)$ (2α)

Βύρων → Κατάλογος: $ID_B \| ID_A$ (1β)

Κατάλογος → Βύρων: $ID_A \| a^x \| h_{kB}(ID_A \| a^x)$ (2β)

Μπορούμε να παρατηρήσουμε ότι δεν πραγματοποιείται επικοινωνία μεταξύ της Αλίκης και του Βύρωνα για τη δημιουργία του κλειδιού συνόδου. Χωριστά η Αλίκη και ο Βύρων επικοινωνούν με τον κατάλογο για να προσκομίσουν το δημόσιο τμήμα του κλειδιού του ομότιμού τους προκειμένου να υπολογίσουν το κλειδί συνόδου. Η Αλίκη γνωρίζοντας τη μυστική ποσότητα x, λαμβάνει από τον κατάλογο το δημόσιο τμήμα του κλειδιού του Βύρωνα a^y και στη συνέχεια υπολογίζει το μυστικό κλειδί συνόδου $a^{yx} \bmod p$. Παρόμοια, ο Βύρων γνωρίζοντας τον μυστικό του εκθέτη y, λαμβάνει από τον κατάλογο το δημόσιο τμήμα της Αλίκης που χρειάζεται προκειμένου να υπολογίσει το μυστικό κλειδί συνόδου $a^{yx} \bmod p$.

Επειδή τα μηνύματα που ανταλλάσσονται μεταξύ των οντοτήτων δεν περιλαμβάνουν μυστικές ποσότητες, η κρυπτογράφηση δεν αρμόζει. Ωστόσο, η απειλή σε αυτήν την περίπτωση είναι η πληγή της αυθεντικότητας των μηνυμάτων. Έτσι χρησιμοποιείται η κρυπτογραφική μονόδρομη συνάρτηση MAC για να προσδώσει την απαραίτητη ακεραιότητα και αυθεντικοποίηση.

Πρωτόκολλο Σταθμού-σε-Σταθμό (Station to Station protocol, STS)

Το παραπάνω πρωτόκολλο προϋποθέτει διάθεση σύνδεσης με την τρίτη οντότητα και επιπλέον χρήση μυστικών κλειδιών για τον υπολογισμό της συνάρτησης MAC. Η συμμετοχή τρίτης οντότητας μπορεί να υλοποιηθεί με τεχνολογία ψηφιακών υπογραφών, με συνέπεια, η συμμετοχή της τρίτης οντότητας στο μοντέλο επικοινωνίας να είναι έμμεση, χωρίς να απαιτείται σύνδεση με αυτήν. Το πρωτόκολλο STS που θα περιγράψουμε στη συνέχεια, χρησιμοποιεί ψηφιακές υπογραφές σε ανταλλαγή κλειδιών Diffie και Hellman, αποτρέποντας παράλληλα επίθεση ενδιάμεσου ατόμου.

Αρχικά θεωρούμε ότι όλα τα μέλη έχουν στην κατοχή τους το δημόσιο κλειδί της τρίτης οντότητας. Έστω k_{eE} το κλειδί αυτό. Το πρωτόκολλο STS περιλαμβάνει τα ακόλουθα συστατικά:

e_k, συμμετρικός κρυπταλγόριθμος,

$(k_{eA}, k_{dA}), (k_{eB}, k_{dB})$, ζευγάρια δημόσιου / ιδιωτικού κλειδιού RSA της Αλίκης και του Βύρωνα αντίστοιχα,

h, κρυπτογραφική μονόδρομη συνάρτηση hash άνευ κλειδιού,

$s_{k_d}(m) \equiv (h(m))^{k_d} \pmod p$, συνάρτηση υπογραφής μηνύματος m.

Πριν από την εκτέλεση του κυρίως πρωτοκόλλου, η Αλίκη και ο Βύρων προσκομίζουν το δημόσιο κλειδί του ομότιμού τους. Αυτό μπορεί να γίνει είτε μέσω ενός

καταλόγου, είτε με ανταλλαγή μεταξύ των δύο μελών. Τα δημόσια κλειδιά είναι υπογεγραμμένα (πιστοποιημένα) από την τρίτη οντότητα. Στη συνέχεια εκτελείται το κυρίως πρωτόκολλο ανταλλαγής κλειδιών:

$$\text{Αλίκη} \rightarrow \text{Βύρων:} \quad a^x \bmod p \tag{1}$$

$$\text{Βύρων} \rightarrow \text{Αλίκη:} \quad a^y \bmod p\,, \;\; e_{ks}(s_{k_{dB}}(a^y \,||\, a^x)) \tag{2}$$

$$\text{Αλίκη} \rightarrow \text{Βύρων:} \quad e_{ks}(s_{k_{dA}}(a^x \,||\, a^y)) \tag{3}$$

Αρχικά, εκτελείται το πρώτο βήμα της ανταλλαγής Diffie και Hellman, η Αλίκη στέλνει το δημόσιο τμήμα του κλειδιού στον Βύρωνα (1).

Μόλις ο Βύρων λάβει το τμήμα αυτό, είναι σε θέση να υπολογίσει το κλειδί συνόδου *ks*. Έτσι υπογράφει τα δύο δημόσια τμήματα του κλειδιού και τα κρυπτογραφεί με το μυστικό κλειδί συνόδου. Στη συνέχεια στέλνει το δικό του δημόσιο τμήμα μαζί με την κρυπτογραφημένη υπογραφή στην Αλίκη (2).

Η Αλίκη που παραλαμβάνει τα μηνύματα του Βύρωνα, δεν είναι ακόμη σε θέση να αποκρυπτογραφήσει το κρυπτοκείμενο. Πρέπει πρώτα να υπολογίσει το συμμετρικό κλειδί συνόδου. Αυτό το πραγματοποιεί υψώνοντας το δημόσιο τμήμα του κλειδιού a^y που έστειλε ο Βύρων, στον μυστικό εκθέτη *x*. Εφόσον υπολογίσει το *ks*, αποκρυπτογραφεί το δεύτερο τμήμα του μηνύματος του Βύρωνα και ανακτά την ψηφιακή υπογραφή του Βύρωνα στα δύο δημόσια τμήματα του κλειδιού, a^y και a^x. Με τη βοήθεια του δημόσιου κλειδιού του Βύρωνα k_{eB}, η Αλίκη απομακρύνει το ιδιωτικό κλειδί k_{dB}, και παραλαμβάνει τη σύνοψη $d = h(a^y||a^x)$. Στη συνέχεια υπολογίζει ανεξάρτητα τη σύνοψη $d' = h(a^y||a^x)$ από τις δικές της παραμέτρους a^y και a^x, και ελέγχει εάν αυτές συμπίπτουν, δηλαδή $d = d'$.

Τέλος, η Αλίκη υπογράφει με τη σειρά της τα δημόσια τμήματα των κλειδιών a^x και a^y και τα μεταβιβάζει στον Βύρωνα (3), ο οποίος με τη σειρά του απομακρύνει την ψηφιακή υπογραφή της Αλίκης με το δημόσιό της κλειδί και εξακριβώνει την ακεραιότητα των a^x και a^y.

Το πρωτόκολλο STS είναι ανθεκτικό σε επίθεση ενδιάμεσου ατόμου. Η κρυπτογράφηση της ψηφιακής υπογραφής με το συμμετρικό κλειδί συνόδου *ks*, προσδίδει επικαιρότητα στο μήνυμα, αποτρέποντας έτσι και απειλές επαναχρησιμοποίησης μηνυμάτων του αντιπάλου.

7.5. Διαμοιρασμός μυστικών και τεμαχισμός κλειδιών

Ο διαμοιρασμός μυστικών περιγράφεται παραστατικά με το «πρόβλημα των κληρονόμων». Μια ομάδα συγγενών πρόκειται να κληρονομήσουν έναν ετοιμοθάνατο θείο. Ο θείος έχει μεγάλη περιουσία, αλλά γνωρίζει ότι οι συγγενείς δεν έχουν καλές σχέσεις μεταξύ τους. Έτσι, στη διαθήκη του θέτει τον όρο ότι προκειμένου να αποκτήσουν την περιουσία του, θα πρέπει οι συγγενείς να παραμερίσουν τις διαφορές τους.

Ανάλογη είναι και η αρχή του τεμαχισμού κλειδιών σε επιμέρους μυστικά και ο διαμοιρασμός αυτών. Το κλειδί τεμαχίζεται σε έναν αριθμό κομματιών *n* και μοιράζεται στα μέλη. Το κάθε μέλος δεν μπορεί να ανακαλύψει ολόκληρο το κλειδί, παρά μόνον εάν συνεργασθεί με τουλάχιστον *m* μέλη, όπου $m \leq n$. Το σύστημα που βασίζεται στην παραπάνω αρχή ονομάζεται σχέδιο (*m*, *n*)-κατωφλίου (threshold scheme):

ΟΡΙΣΜΟΣ 7.5 – Το σύστημα το οποίο τεμαχίζει ένα κλειδί *k* σε *n* τεμάχια έτσι ώστε οποιοσδήποτε συνδυασμός πλήθους έως και *m*–1 τεμαχίων να μην καθιστά δυνατή την ανασυγκρότηση του κλειδιού, ενώ οποιοσδήποτε συνδυασμός πλήθους *m* τεμαχίων και άνω να οδηγεί στην ανακατασκευή του κλειδιού, ονομάζεται ***σχέδιο (m, n)-κατωφλίου***. Το κάθε τεμάχιο του κλειδιού ονομάζεται ***σκιά*** ή ***μερίδιο*** του κλειδιού.

Υπάρχει πληθώρα πρακτικών εφαρμογών σχεδίων (*m*, *n*)-κατωφλίου. Για παράδειγμα, σε δημοκρατικά συστήματα στα οποία η λήψη και εκτέλεση αποφάσεων εκτελείται με ψηφοφορία, ο κάθε ψηφοφόρος μπορεί να έχει ένα μερίδιο του κλειδιού. Επίσης, σε συστήματα όπου η ψήφος του προέδρου έχει μεγαλύτερη βαρύτητα, ο πρόεδρος μπορεί να έχει δύο ή και περισσότερα μερίδια.

Στη συνέχεια, θα εξετάσουμε ένα αντιπροσωπευτικό μοντέλο σχεδίου (*m*, *n*)-κατωφλίου.

7.5.1. Σχέδια (*m*, *n*)-κατωφλίου πολυωνύμου παρεμβολής

Έστω το μυστικό κλειδί *k*, το οποίο επιθυμούμε να τεμαχίσουμε σε *n* μερίδια με δυνατότητα ανασυγκρότησης του *k*, επιλέγοντας οποιαδήποτε μερίδια πλήθους *m*. Το σχέδιο χρησιμοποιεί πολυώνυμο βαθμού *m*–1, ως εξής. Επιλέγουμε πρώτο αριθμό *p*, τέτοιον ώστε να είναι μεγαλύτερος από τον αριθμό των μεριδίων, $n < p$. Το πολυώνυμο είναι της μορφής:

$$f(x) = c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + ...c_1x + k \mod p,$$

όπου οι συντελεστές $c_1, c_2, \ldots, c_{m-1}$ είναι μυστικοί, ενώ ο *p* είναι δημόσιος. Τα μερίδια προκύπτουν για $x = 1, 2, \ldots, n$:

$$f(i) = c_{m-1}i^{m-1} + c_{m-2}i^{m-2} + ...c_1i + k \mod p,$$

όπου *f*(*i*) το *i*-στό μερίδιο. Εφόσον οι συντελεστές και το μυστικό κλειδί *k* είναι άγνωστοι, υπάρχουν συνολικά *m* άγνωστοι. Το κάθε μερίδιο αποτελεί μια μερική λύση $(i, f(i))$. Χρειάζονται επομένως *m* το πλήθος λύσεις για να είναι δυνατή η λύση ως προς $c_1, c_2, \ldots, c_{m-1}$ και *k*, φυσικά. Με *m*–1 ή και λιγότερες μερικές λύσεις, δεν είναι δυνατή η επίλυση του *k*. Για περισσότερες από *m* μερικές λύσεις, έχουμε πλεονασμό πληροφορίας και η επίλυση του *k* είναι δυνατή.

ΠΑΡΑΔΕΙΓΜΑ 7.2 – Κατασκευή σχεδίου (3, 5)-κατωφλίου. Για να κατασκευάσουμε ένα σχέδιο (3, 5)-κατωφλίου, ο βαθμός του πολυωνύμου θα είναι 2. Έστω το μυστικό κλειδί $k = 13$. Επιλέγουμε $p = 17$ και το ακόλουθο πολυώνυμο:

$$f(x) = 7x^2 + 9x + 13 \mod 17 .$$

Στη συνέχεια υπολογίζουμε τα 5 μερίδια:

$$f(1) = 7 + 9 + 13 \equiv 12 \pmod{17}$$
$$f(2) = 28 + 18 + 13 \equiv 8 \pmod{17}$$
$$f(3) = 63 + 27 + 13 \equiv 1 \pmod{17}$$
$$f(4) = 112 + 36 + 13 \equiv 8 \pmod{17}$$
$$f(5) = 175 + 45 + 13 \equiv 12 \pmod{17}$$

Συνεπώς τα 5 μερίδια είναι (1, 12), (2, 8), (3, 1), (4, 8) και (5, 12). Οποιαδήποτε τρία από τα μερίδια αυτά μπορούν να συμβάλλουν στη λύση του συστήματος με άγνωστους τους δύο συντελεστές και το μυστικό. Έστω ότι τα μερίδια που συμβάλλουν είναι το δεύτερο, το τρίτο και το πέμπτο. Έτσι, προκύπτει το σύστημα τριών εξισώσεων με τρεις αγνώστους:

$$c_2 2^2 + c_1 2 + k \equiv 8 \pmod{17}$$
$$c_2 3^2 + c_1 3 + k \equiv 1 \pmod{17}$$
$$c_2 5^2 + c_1 5 + k \equiv \pmod{17}$$

του οποίου μοναδική λύση είναι η $(c_2, c_1, k) = (7, 9, 13)$.

7.5.2. Ασφάλεια σχεδίου (*m*, *n*)-κατωφλίου πολυωνύμου παρεμβολής

Ο αντίπαλος σε ένα σχέδιο κατωφλίου θεωρείται ότι είναι το κάθε μέλος. Παρόλο που ο σκοπός του συστήματος είναι να διατεθεί το κλειδί στα μέλη, αυτό δεν μπορεί να γίνει εφόσον δεν υπάρχει η απαραίτητη συναίνεση ενός ελαχίστου επιθυμητού αριθμού μελών. Μέχρι τη στιγμή που θα συμφωνήσουν τα μέλη να ανακτήσουν το μυστικό, αυτό θα πρέπει να φυλαχτεί και να μην γίνει διαθέσιμο σε κανένα από αυτά.

Έτσι προκύπτουν δύο ειδών απειλές. Η πρώτη αφορά τη συνέργια ενός αριθμού μελών μικρότερο του *m* για να ανακτήσουν το μυστικό. Επειδή για οποιονδήποτε συνδυασμό μικρότερο του *m* ο αριθμός των εξισώσεων θα είναι μικρότερος από τον αριθμό των αγνώστων, οι πιθανές τιμές που μπορεί να πάρουν οι άγνωστοι είναι $(p-1)^m$. Ένα ανάλογο σύστημα εξισώσεων στο σύνολο των πραγματικών αριθμών θα έχει άπειρες λύσεις. Έτσι οποιοσδήποτε συνδυασμός των μεριδίων λιγότερος του *m* δεν προσδίδει καμία επιπλέον πληροφορία για το *k*. Το γεγονός αυτό καθιστά την ασφάλεια του σχεδίου ισοδύναμη με αυτή των σημειωματάριων μιας χρήσης. Δηλαδή το σχέδιο κατωφλίου είναι άνευ όρων ασφαλές.

Η δεύτερη απειλή αφορά τη μη έντιμη συμμετοχή ενός ή περισσοτέρων μελών. Σύμφωνα με την απειλή αυτή, κάποιο από τα μέλη μπορεί να απατήσει τα υπόλοιπα μέλη αποκαλύπτοντας ένα τυχαίο μερίδιο κατά την ανασυγκρότηση του μυστικού. Ένα σχέδιο κατωφλίου πολυωνύμου παρεμβολής είναι ευάλωτο σε μια τέτοια επίθεση. Η ανίχνευση απάτης δεν είναι δυνατή, τόσο κατά την κοινοποίηση των μεριδίων, όσο και κατά την ανασυγκρότηση του κλειδιού. Δηλαδή, κανένα από τα μέλη δεν θα είναι σε θέση να διακρίνει ποιο από τα μέλη πραγματοποίησε την απάτη.

Τροποποίηση του σχεδίου (*m*,*n*)-κατωφλίου πολυωνύμου παρεμβολής

Οι Tompa και Wall πρότειναν μια τροποποίηση του σχεδίου, ώστε να είναι δυνατή η ανίχνευση μη έντιμης συμμετοχής. Η τροποποίηση αφορά την επιλογή του p και τη διαδικασία υπολογισμού των μεριδίων. Πιο συγκεκριμένα, αντί τα μερίδια να είναι τα $(i, f(i))$, για $i = 1, 2, 3, \ldots, n$, επιλέγονται για τυχαίο i, όπου $0 < i < p$. Όσον αφορά το p, θα πρέπει να είναι μεγαλύτερο του n αλλά και μεγαλύτερο από:

$$(s-1)(m-1)/e + m,$$

όπου s το μεγαλύτερο δυνατό μυστικό και e η πιθανότητα επιτυχούς απάτης.

Εκτός από την εμπέδωση μηχανισμών στο σχέδιο κατωφλίου για αποτροπή της απάτης, υπάρχουν και τα πρωτόκολλα δέσμευσης των bit (bit commitment protocols), τα οποία μπορούν να συνοδεύσουν ένα σχέδιο κατωφλίου και μπορούν να εγγυηθούν την έντιμη συμμετοχή των μελών. Τα πρωτόκολλα δέσμευσης εξετάζονται στο Κεφάλαιο 9.

7.6. Υποδομές δημόσιου κλειδιού

Οι υποδομές δημόσιου κλειδιού (public key infrastructures, PKIs) είναι μοντέλα τα οποία αναπτύχθηκαν με κύριο σκοπό την πιστοποίηση των οντοτήτων που συμμετέχουν σε ένα σύστημα επικοινωνίας. Έτσι, η ασφάλεια και η αξιοπιστία της διαδικασίας αυθεντικοποίησης των μελών που γίνεται με τη χρήση ενός PKI, συνδέεται με την κρυπτογραφική ισχύ των κρυπταλγόριθμων που υποστηρίζει το PKI. Ωστόσο, η συνολική ασφάλεια της διαδικασίας πιστοποίησης δεν εξαρτάται μόνον από την ισχύ του κρυπταλγόριθμου. Όπως θα δούμε στη συνέχεια, ένα PKI αποτελείται από διάφορες οντότητες, όπου η κάθε οντότητα έχει συγκεκριμένους ρόλους. Έτσι, η συνολική ασφάλεια εξαρτάται από την εκτέλεση των ρόλων από τις οντότητες. Θα διαπιστώσουμε για μια ακόμη φορά ότι η κρυπτογραφία μετασχηματίζει προβλήματα ασφάλειας σε μορφές που επιτρέπουν αποτελεσματικότερη διαχείριση, χωρίς όμως να λύνει τα προβλήματα αυτά.

Η διαδικασία αυθεντικοποίησης ενός μέλους ή γενικότερα μιας οντότητας χαρακτηρίζεται ισχυρή, αν η πιθανότητα απάτης είναι ικανοποιητικά μικρή. Η απάτη αφορά την προσπάθεια του αντιπάλου να προσποιηθεί άλλη ταυτότητα. Μια τέτοια απάτη είναι η επίθεση του ενδιάμεσου ατόμου που συναντήσαμε παραπάνω.

Επειδή η αυθεντικοποίηση ενός μέλους στην ασύμμετρη κρυπτογραφία γίνεται με τη χρήση του δημόσιου κλειδιού του μέλους, έπεται ότι η όλη διαδικασία αυθεντικοποίησης εξαρτάται από την αυθεντικότητα του δημόσιου κλειδιού. Αν κατά την αυθεντικοποίηση ενός μέλους δεν υπάρχει τρόπος να ελεγχθεί η αυθεντικότητα του δημόσιου κλειδιού του μέλους αυτού, τότε ο αντίπαλος θα μπορεί να αντικαταστήσει το δικό του δημόσιο κλειδί χωρίς αυτό να γίνει αντιληπτό.

Χωρίς τη συμμετοχή μιας έμπιστης τρίτης οντότητας, η λύση στο πρόβλημα της αυθεντικότητας των κλειδιών θα ήταν το κάθε μέλος να έχει στην κατοχή του τα δημόσια κλειδιά όλων των μελών, τα οποία τα έχει παραλάβει μέσω ενός καναλιού που προσφέρει υψηλή ακεραιότητα. Ας σημειωθεί ότι το κανάλι δεν απαιτείται να προσφέρει εμπιστευτικότητα, αφού τα κλειδιά είναι δημόσια. Η ακεραιότητα όμως απαιτείται να είναι υψηλή, ώστε ο αντίπαλος να μην έχει τη δυνατότητα να αντικαταστήσει τα δημόσια κλειδιά με τα δικά του. Εναλλακτικά, το κάθε μέλος θα μπορούσε να παραλάβει μόνον εκείνα τα δημόσια κλειδιά τα οποία θα χρειασθεί προκειμένου να επικοινωνήσει με τα αντίστοιχα μέλη. Ένα τέτοιο μοντέλο διανομής δημόσιων κλειδιών δεν είναι πρακτικό, αφού δεν μπορεί να κλιμακωθεί με ευκολία και απαιτεί διαρκώς ασφαλές κανάλι με υψηλή ακεραιότητα.

Η συμμετοχή μιας έμπιστης τρίτης οντότητας μπορεί να απλοποιήσει το παραπάνω πρόβλημα αποτελεσματικά. Αντί να απαιτείται η ασφαλής μεταφορά όλων των δημόσιων κλειδιών, αρκεί να διανεμηθεί με υψηλή ακεραιότητα το δημόσιο κλειδί της έμπιστης τρίτης οντότητας και να χρησιμοποιηθεί αυτό για να πιστοποιήσει τα δημόσια κλειδιά των υπολοίπων. Αυτό σε γενικές γραμμές είναι μια υποδομή δημόσιου κλειδιού, ή ένα PKI για συντομία, που θα εξετάσουμε στη συνέχεια.

7.6.1. Συστατικά ενός PKI

Ένα PKI αποτελείται από τα εξής συστατικά:

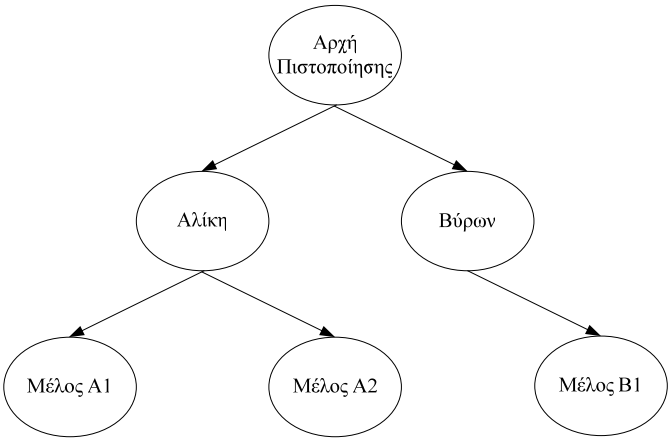
- Αρχή Πιστοποίησης (Certification Authority). Η Αρχή Πιστοποίησης είναι το κεντρικό συστατικό ενός PKI. Αποτελεί την έμπιστη τρίτη οντότητα η οποία είναι υπεύθυνη για την πιστοποίηση των δημόσιων κλειδιών των μελών. Η ακεραιότητα όλης της υποδομής συγκεντρώνεται στην Αρχή Πιστοποίησης.
- Αρχή Εγγραφής (Registration Authority). Η Αρχή Εγγραφής είναι προαιρετική. Εμφανίσθηκε κυρίως για εμπορικούς λόγους και στην περίπτωση απουσίας αυτής, τα καθήκοντά της αναλαμβάνει η Αρχή Πιστοποίησης. Η Αρχή Εγγραφής είναι υπεύθυνη για την αρχική εξακρίβωση των στοιχείων του μέλους, προτού πιστοποιηθεί το δημόσιό του κλειδί.
- Εντολέας (Principal). Είναι η οντότητα η οποία πιστοποιείται από την Αρχή Πιστοποίησης. Οι οντότητες με τις οποίες έχουμε ασχοληθεί είναι τα επικοινωνούντα μέλη, τα οποία είναι φυσικά πρόσωπα, αλλά μπορούν να είναι και υπολογιστές που βρίσκονται σε δίκτυο, μηχανές ATM των τραπεζών, κτλ.

- Πιστοποιητικό δημόσιου κλειδιού (Public key certificate). Το πιστοποιητικό δημόσιου κλειδιού είναι μια δομή δεδομένων η οποία αποτελείται από ένα σύνολο στοιχείων που περιλαμβάνει δύο μέρη. Το πρώτο μέρος αποτελείται από την περιγραφή του εντολέα και το δημόσιο κλειδί του. Το δεύτερο μέρος του πιστοποιητικού αποτελείται από την ψηφιακή υπογραφή της Αρχής Πιστοποίησης επάνω στα στοιχεία του πρώτου μέρους.
- Αποθήκη πιστοποιητικών (certificate repository). Αποτελεί τον χώρο αποθήκευσης των πιστοποιητικών ενός PKI. Στην πράξη αυτό υλοποιείται από υπηρεσία καταλόγου (directory service) στο οποίο μπορούν να απευθυνθούν τα μέλη προκειμένου να παραλάβουν το δημόσιο κλειδί του μέλους με το οποίο επιθυμούν να επικοινωνήσουν.
- Υπηρεσία ανάκλησης πιστοποιητικού (certificate revocation service). Η υπηρεσία ανάκλησης πιστοποιητικού συμμετέχει στη διαδικασία εξακρίβωσης της εγκυρότητας του πιστοποιητικού και παρέχει πληροφορίες σχετικά με την ανάκληση αυτού.
- Δήλωση Χρήσης Πιστοποιητικού (Certificate Practice Statement). Είναι ένα είδος συμφωνητικού το οποίο περιγράφει τους ρόλους, τις διαδικασίες, τα δικαιώματα και τις υποχρεώσεις καθενός από τα μέλη. Για παράδειγμα, περιγράφει τα δικαιολογητικά τα οποία θα πρέπει να κατατεθούν από τον εντολέα προκειμένου να του εκδοθεί το πιστοποιητικό.

Από την παραπάνω περιγραφή των συστατικών μπορεί να γίνει αντιληπτή η καίρια θέση της Αρχής Πιστοποίησης και η εξάρτηση της ασφάλειας του PKI από αυτήν. Η δύναμη που έχει η Αρχή Πιστοποίησης στο να δημιουργεί πιστοποιητικά για τα μέλη είναι και η συνέπεια της απαίτησης εμπιστοσύνης, η οποία καθιστά την Αρχή Πιστοποίησης ως Έμπιστη Τρίτη Οντότητα.

7.6.2. Μοντέλα εμπιστοσύνης

Τα μοντέλα εμπιστοσύνης καθορίζουν τους τρόπους με τους οποίους αλληλεπιδρούν οι οντότητες προκειμένου να διαπιστώσουν την εγκυρότητα ενός πιστοποιητικού. Η Αρχή Πιστοποίησης είναι η Έμπιστη Τρίτη Οντότητα, αλλά αυτό δεν εμποδίζει ορισμένα μέλη να αναλάβουν το ρόλο Αρχής Πιστοποίησης για πιστοποίηση άλλων μελών. Έτσι μια Αρχή Πιστοποίησης μπορεί να δημιουργήσει ένα πιστοποιητικό για κάποιο μέλος, αλλά και το μέλος με τη σειρά του μπορεί να εγγυηθεί για κάποιο άλλο μέλος, δημιουργώντας πιστοποιητικό. Στο δέντρο του Σχήματος 7.5 φαίνεται ένα παράδειγμα όπου η Αλίκη αναλαμβάνει να πιστοποιήσει τα Μέλη Α1 και Α2. Η Αρχή Πιστοποίησης είναι η Έμπιστη Τρίτη Οντότητα, που σημαίνει ότι όλα τα πιστοποιητικά τα οποία έχουν εκδοθεί από αυτήν είναι αποδεκτά από όλα τα μέλη που συμμετέχουν στο PKI. Από το δέντρο φαίνεται ότι ο Βύρων πιστοποιεί το Μέλος Β1. Τα Μέλη Α1 και Α2 εμπιστεύονται την Αλίκη, οπότε μπορεί να εμπιστευθεί το ένα το πιστοποιητικό του άλλου. Εφόσον εμπιστεύονται την Αλίκη, αυτόματα εμπιστεύονται και όλες τις οντότητες που βρίσκονται επάνω από αυτήν, στην περίπτωσή μας την Αρχή Πιστοποίησης.



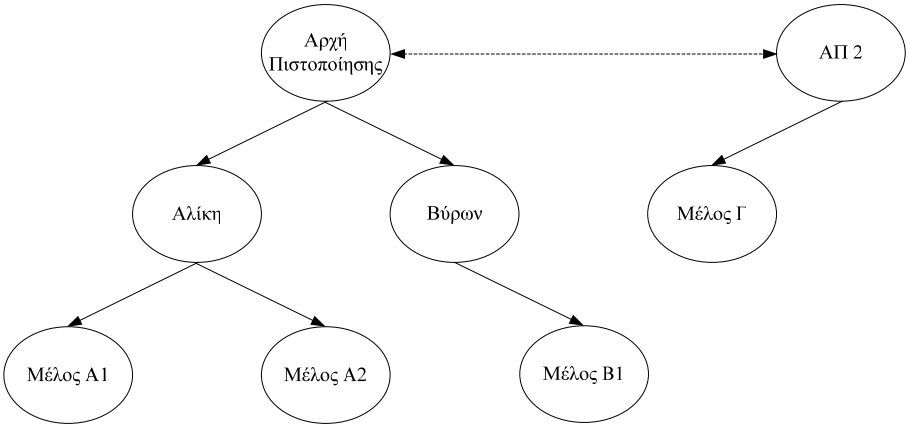
Σχήμα 7.5 Δέντρο πιστοποίησης – Μοντέλο εμπιστοσύνης

Ο Βύρων από την άλλη, για να επικοινωνήσει με την Αλίκη, αρκεί να εμπιστευτεί μόνον την Αρχή Πιστοποίησης, το οποίο είναι αληθές αφού και το δικό του πιστοποιητικό δημιουργήθηκε από την ίδια Αρχή Πιστοποίησης. Το μέλος Β1, δέχεται το πιστοποιητικό της Αλίκης, αφού και αυτό με τη σειρά του εμπιστεύεται την Αρχή Πιστοποίησης μέσω του Βύρωνα.

Στην περίπτωση που το Μέλος Β1 θελήσει να επικοινωνήσει με ένα από τα μέλη Α1 ή Α2, θα πρέπει να εμπιστευτεί τον Βύρωνα, την Αρχή Πιστοποίησης και την Αλίκη. Με άλλα λόγια, η εμπιστοσύνη υπάρχει αν υπάρχει δρόμος στο δέντρο από το Μέλος Β1 στο Μέλος Α1 ή Α2. Στο Σχήμα 7.6 προστίθεται και το Μέλος Γ το οποίο επιθυμεί να επικοινωνήσει με τον Βύρωνα, αλλά έχει πιστοποιητικό από μια άλλη Αρχή Πιστοποίησης, την ΑΠ2. Σε αυτήν την περίπτωση θα πρέπει να ελέγξει ο Βύρων αν η δική του Αρχή Πιστοποίησης εμπιστεύεται την ΑΠ2 και αντίστροφα, ώστε να υπάρχει σύνδεση μεταξύ των δύο δέντρων πιστοποίησης. Η σύνδεση παριστάνεται στο σχήμα με τη διακεκομμένη γραμμή και ονομάζεται ***διαπιστοποίηση*** (cross-certification).

Η δυνατότητα της Αλίκης και του Βύρωνα και γενικότερα των μελών να μπορούν να εκδίδουν πιστοποιητικά δημιουργεί ένα σημαντικότατο πρόβλημα. Το δέντρο αυξάνεται σε βάθος, με αποτέλεσμα να αυξάνεται και το πλήθος των παρεμβαλλόμενων οντοτήτων μεταξύ ενός μέλους και της Αρχής Πιστοποίησης. Αυτό σημαίνει ότι ο δρόμος πιστοποίησης μεταξύ δύο μελών μπορεί να γίνει ανεξέλεγκτα μεγάλος. Όπως είναι αναμενόμενο, η ασφάλεια ενός PKI θα φθίνει με την αύξηση του βάθους του δέντρου. Όσο απομακρυσμένα είναι δύο μέλη, τόσο μικρότερη είναι και η εμπιστοσύνη στην αυθεντικότητα του πιστοποιητικού, αφού αυξάνεται η πιθανότητα να υπάρχει μέσα στο δρόμο αντίπαλος. Ισοδύναμα, η ύπαρξη πολλών μελών στο ενδιάμεσο δίνει περισσότερες ευκαιρίες επίθεσης στον αντίπαλο. Ο αντίπαλος θα επιχειρήσει επίθεση στο μέλος με την ασθενέστερη ασφάλεια. Συνεπώς η υποδομή θα είναι τόσο ασφαλής όσο ο πιο αδύναμος κρίκος.

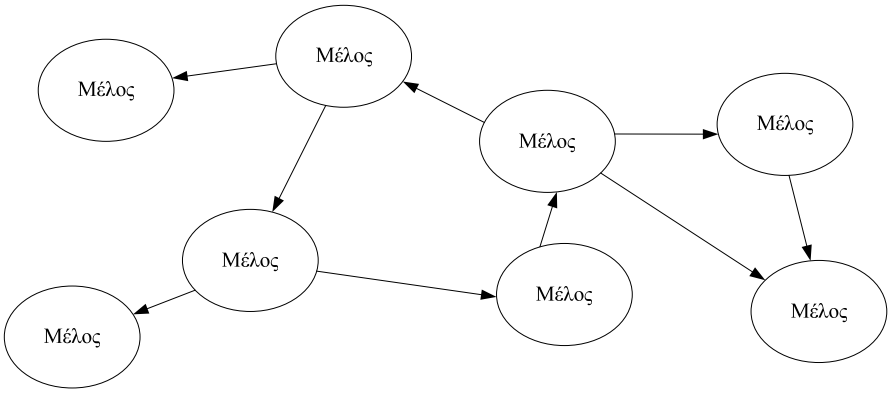
Για το λόγο αυτό ορίζονται και μοντέλα όπου δεν επιτρέπεται τα μέλη να εκδίδουν πιστοποιητικά και να λειτουργούν ως Αρχές Πιστοποίησης. Έτσι τα μοντέλα εμπιστοσύνης διαχωρίζονται σε δύο κατηγορίες, στα επίπεδα και στα ιεραρχικά.



Σχήμα 7.6 Διαπιστοποίηση

Το επίπεδο μοντέλο εμπιστοσύνης

Το επίπεδο μοντέλο εμπιστοσύνης παρουσιάζεται στο Σχήμα 7.7. Είναι παρόμοιο με το μοντέλο που παρουσιάσαμε παραπάνω, με τη διαφορά ότι δεν υπάρχει οντότητα η οποία λειτουργεί αποκλειστικά ως Αρχή Πιστοποίησης. Έτσι, οποιαδήποτε οντότητα έχει το δικαίωμα να εκδώσει πιστοποιητικό για κάποια άλλη. Με αυτόν τον τρόπο δημιουργείται ένα «δίκτυο εμπιστοσύνης» (web of trust), όπου ένα νέο μέλος μπορεί να γίνει μέρος του δικτύου εάν συστηθεί από κάποιο υπάρχον μέλος.



Σχήμα 7.7 Επίπεδο μοντέλο εμπιστοσύνης

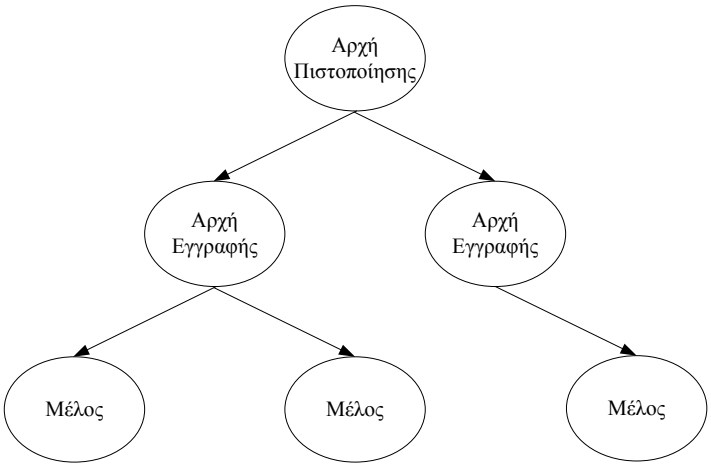
Στο επίπεδο μοντέλο επικρατεί αναρχία. Μάλιστα, ένα μέλος μπορεί να συσταθεί από περισσότερους από ένα μέλη. Αυτό μπορεί να χρησιμοποιηθεί ως μέ-

τρο αξιολόγησης της εγκυρότητας του πιστοποιητικού. Όσο περισσότερα μέλη συστήνουν το νέο μέλος, τόσο θεωρητικά μικρότερη η πιθανότητα να μην είναι έγκυρο το πιστοποιητικό. Επίσης, μια οντότητα που είναι αναγνωρισμένα πιο έμπιστη από τις άλλες, έχει τη δυνατότητα να συμπεριλάβει την υπογραφή της μαζί με άλλα μέλη για τη σύσταση του νέου μέλους, γεγονός το οποίο δυναμώνει την εμπιστοσύνη για το νέο μέλος.

Το δημοφιλές λογισμικό Pretty Good Privacy (PGP) υποστηρίζει το επίπεδο μοντέλο εμπιστοσύνης. Μάλιστα, το επίπεδο μοντέλο ονομάζεται και PGP μοντέλο. Το επίπεδο μοντέλο χρησιμοποιείται σε κλειστούς κύκλους επικοινωνίας μελών, καθώς και σε περιβάλλοντα όπου δεν υπάρχουν ή δεν είναι δυνατό να εφαρμοσθούν αυστηρές προδιαγραφές πιστοποίησης.

Το ιεραρχικό μοντέλο εμπιστοσύνης

Το ιεραρχικό μοντέλο εμπιστοσύνης απαιτεί μια Έμπιστη Τρίτη Οντότητα η οποία λειτουργεί ως Αρχή Πιστοποίησης και προαιρετικά μία ή περισσότερες Αρχές Εγγραφής, όπως φαίνεται στο Σχήμα 7.8.



Σχήμα 7.8 Ιεραρχικό μοντέλο εμπιστοσύνης

Η Αρχή Εγγραφής είναι υπεύθυνη για την αρχική εξακρίβωση των στοιχείων του Μέλους. Η αρχική αυθεντικοποίηση γίνεται εκτός του PKI και ονομάζεται ***αναγνώριση εκτός ζώνης*** (out of band identification), όπου το Μέλος παρουσιάζει κάποιο έγγραφο πιστοποίησης, όπως αστυνομική ταυτότητα, διαβατήριο, κτλ. Στη συνέχεια η Αρχή Εγγραφής συμπληρώνει τα στοιχεία που απαιτούνται για την έκδοση του πιστοποιητικού και τα στέλνει στην Αρχή Πιστοποίησης υπό τη μορφή τυποποιημένης αίτησης. Με τη σειρά της η Αρχή Πιστοποίησης υπογράφει τα στοιχεία που παρέλαβε από την Αρχή Εγγραφής, δημιουργώντας έτσι το πιστοποιητικό.

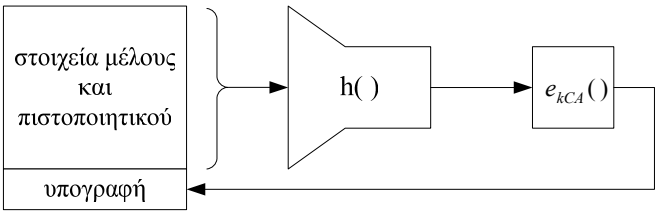
Η χρήση των Αρχών Εγγραφής από τη μια μειώνει την εμπιστοσύνη εφόσον παρεμβάλλεται μεταξύ των Μελών και της Αρχής Πιστοποίησης, αλλά από την άλλη μειώνει και το ρίσκο επίθεσης στην Αρχή Πιστοποίησης. Ο λόγος ύπαρξης περισσοτέρων από μία Αρχές Εγγραφής είναι η καλύτερη εξυπηρέτηση των Μελών. Έτσι τα Μέλη (και κατ' επέκταση οι αντίπαλοι) δεν μπορούν να πλησιάσουν την Αρχή Πιστοποίησης και η προστασία της είναι μεγαλύτερη.

Το πιστοποιητικό που εκδίδει η Αρχή Πιστοποίησης περιλαμβάνει πληροφορίες σχετικά με τον τύπο αυτού. Ο τύπος περιγράφει την επιτρεπτή χρήση αυτού. Έτσι, είναι δυνατόν να γίνει διάκριση εάν ένα πιστοποιητικό μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση μέλους, προγράμματος, server, ή για την έκδοση άλλων πιστοποιητικών. Από κρυπτογραφικής πλευράς, ένα μέλος έχει τη δυνατότητα να εκμεταλλευτεί το πιστοποιητικό για άλλες διαδικασίες. Η κακή χρήση του πιστοποιητικού καλύπτεται μη κρυπτογραφικά, με τη Δήλωση Χρήσης Πιστοποιητικού. Έτσι, αν αποκαλυφθεί η κακή χρήση του πιστοποιητικού, η Αρχή Πιστοποίησης πραγματοποιεί την ανάκληση αυτού.

7.6.3. Το πιστοποιητικό

Το πιστοποιητικό αποτελείται από δύο μέρη, από τα δεδομένα και από την ψηφιακή υπογραφή. Τα δεδομένα περιλαμβάνουν στοιχεία του εντολέα, στοιχεία του πιστοποιητικού, καθώς και πληροφορίες σχετικά με τις κρυπτογραφικές συναρτήσεις που χρησιμοποιήθηκαν στη δημιουργία της ψηφιακής υπογραφής.

Η διαδικασία δημιουργίας ενός ψηφιακού πιστοποιητικού παριστάνεται στο Σχήμα 7.9. Η Αρχή Πιστοποίησης δημιουργεί με τη βοήθεια μιας μονόδρομης hash μια σύνοψη των στοιχείων του πρώτου μέρους το πιστοποιητικού, και στη συνέχεια το κρυπτογραφεί με το ιδιωτικό της κλειδί k_{dCA}.



Σχήμα 7.9 Διαδικασία δημιουργίας ψηφιακού πιστοποιητικού

Το πιστοποιητικό X.509

Το πιστοποιητικό X.509 είναι η τυποποίηση που κυριαρχεί στα PKI που χρησιμοποιούν τεχνολογίες του Διαδικτύου. Τα πεδία του X.509 φαίνονται στον Πίνακα 7.1.

Όνομα πεδίου	Χρήση
version	Η έκδοση του προτύπου X.509. Ορίζονται 3 εκδόσεις του X.509. Η έκδοση 1 δεν περιέχει τα πεδία *issuer unique identifier, subject unique identifier* τα οποία προστέθηκαν στην έκδοση 2, καθώς και το πεδίο *extensions* το οποίο προστέθηκε στην έκδοση 3.
serial number	Ένας μοναδικός ακέραιος που καθορίζεται από την Αρχή Πιστοποίησης για να αναγνωρίσει το πιστοποιητικό.
signature algorithm identifier	Το πεδίο αυτό αποτελείται στην ουσία από 2 πεδία, τα ονόματα των κρυπτογραφικών συναρτήσεων που συμμετέχουν, καθώς και από τις σχετικές παραμέτρους αυτών.
issuer name	Το όνομα της Αρχής Πιστοποίησης
period of validity	Αποτελείται από δύο ημερομηνίες, από την ημερομηνία ενεργοποίησης του πιστοποιητικού και από την ημερομηνία λήξης του πιστοποιητικού
subject name	Το όνομα της οντότητας που πιστοποιείται
algorithms	Το όνομα του κρυπταλγόριθμου που χρησιμοποιεί η οντότητα για να διαθέσει το δημόσιο κλειδί της
parameters	Οι σχετικές παράμετροι που προσδιορίζουν τη λειτουργία του παραπάνω κρυπταλγόριθμου
subject's public key	Το δημόσιο κλειδί της οντότητας που αναγνωρίζεται από το πεδίο subject name. Η οντότητα αυτή κατέχει το ιδιωτικό κλειδί.
issuer unique identifier	Ο αριθμός αυτός χρησιμοποιείται σε συνδυασμό με το όνομα της Αρχής Πιστοποίησης για να ενισχύσει την αναγνώριση αυτής.
subject unique identifier	Ο αριθμός αυτός χρησιμοποιείται σε συνδυασμό με το όνομα της οντότητας για να προσδώσει μοναδικότητα στο πιστοποιητικό, σε περίπτωση που το όνομα της οντότητας χρησιμοποιείται για άλλο πιστοποιητικό.
extensions	Εδώ μπορούν να προστεθούν επιπλέον στοιχεία για να υποστηρίξουν ειδικές απαιτήσεις της εφαρμογής.
signature	Η ψηφιακή υπογραφή με το ιδιωτικό κλειδί της Αρχής Πιστοποίησης επάνω σε όλες τις προαναφερθείσες πληροφορίες.

Πίνακας 7.1 Πεδία του πιστοποιητικού X.509

Η δομή και μορφή του ονόματος της Αρχής Πιστοποίησης καθορίζεται από το πρότυπο ονομασίας X.500, όπου το βασικό πεδίο είναι το ***διακεκριμένο όνομα*** (distinguished name), το οποίο έχει την εξής μορφή:

$dn =$"$\acute{o}\,\nu o\mu\alpha$ _ ΑΠ"

Το διακεκριμένο όνομα μαζί με άλλα πεδία καθορίζουν πλήρως την Αρχή Πιστοποίησης.

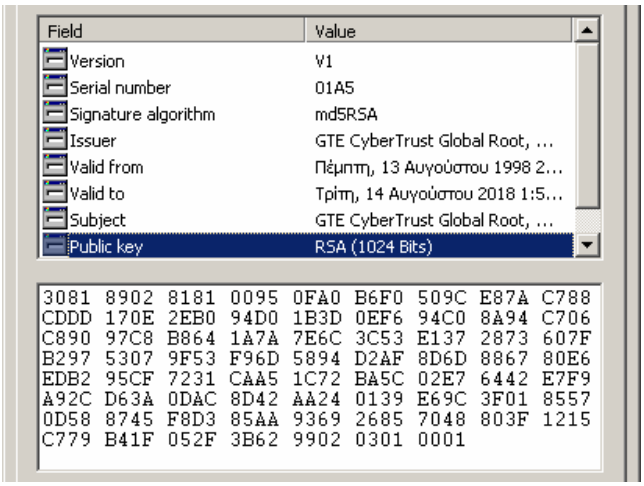
7.6.4. Διαδικασίες δημιουργίας, ελέγχου και ανάκλησης

Σε μια υποδομή δημόσιου κλειδιού η διαχείριση των κλειδιών πραγματοποιείται με πλήρως καθορισμένες διαδικασίες. Από τεχνικής πλευράς, οι διαδικασίες αυτές χρησιμοποιούν πρωτόκολλα προκειμένου να εκτελεσθούν.

Η πρώτη διαδικασία που πραγματοποιείται κατά την εκκίνηση λειτουργίας ενός PKI είναι η ίδρυση της Αρχής Πιστοποίησης και η δημοσίευση του πιστοποιητικού της. Η δημοσίευση γίνεται ανάλογα με το περιβάλλον στο οποίο δρα το PKI.

Για παράδειγμα στο Διαδίκτυο υπάρχουν περισσότερες από 10 Αρχές Πιστοποίησης. Η Αρχή Πιστοποίησης επικοινωνεί με τους παροχείς των λογισμικών πελατών (client software) που χρησιμοποιούνται για πρόσβαση στις υπηρεσίες του Διαδικτύου και τους παρέχει μέσω ασφαλούς καναλιού το πιστοποιητικό που περιέχει το δημόσιο κλειδί της Αρχής Πιστοποίησης.

Στο Σχήμα 7.10 φαίνεται το πιστοποιητικό της GTE CyberTrust που συνοδεύει τον Internet Explorer της Microsoft.



Σχήμα 7.10 Το ψηφιακό πιστοποιητικό της GTE CyberTrust για υπηρεσίες WWW.

Διαδικασία δημιουργίας και δημοσίευσης του πιστοποιητικού του χρήστη

Ο σκοπός του πιστοποιητικού είναι να συνδεθεί ένα όνομα με ένα δημόσιο κλειδί. Έτσι, απαραίτητη προϋπόθεση είναι η δημιουργία ενός ζεύγους δημόσιου και ιδιωτικού κλειδιού. Το δημόσιο κλειδί θα κατατεθεί στην Αρχή Εγγραφής μαζί με τα στοιχεία του χρήστη. Υπάρχουν δύο εναλλακτικές όπου μπορεί να δημιουργηθεί το ζεύγος του κλειδιού:

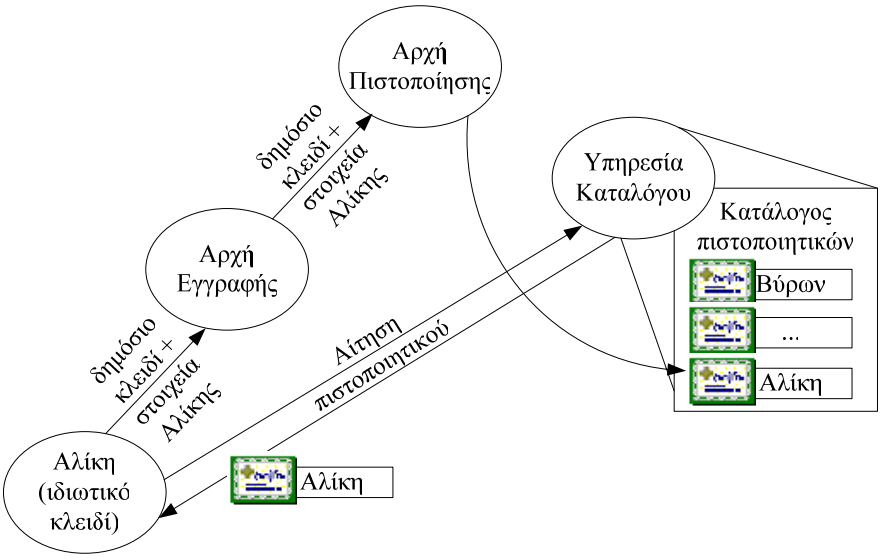
- Στο περιβάλλον του χρήστη. Στην περίπτωση αυτή το ρίσκο να αποκαλυφθεί το ιδιωτικό κλειδί είναι ελάχιστο, αφού ο μόνος γνώστης του κλειδιού είναι ο χρήστης. Ωστόσο, αν το κλειδί χρησιμοποιείται για κρυπτογράφηση μηνυμάτων και όχι για αυθεντικοποίηση, η απώλεια του κλειδιού θα καταστήσει αδύνατη την αποκρυπτογράφηση των μηνυμάτων που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί.
- Στο περιβάλλον της Αρχής Εγγραφής ή Πιστοποίησης. Η δημιουργία του ζεύγους κλειδιών σε τοποθεσία διαφορετική από τον νόμιμο κάτοχο του ιδιωτικού κλειδιού έχει επίπτωση στην αυξημένη πολυπλοκότητα του μοντέλου επικοινωνίας. Αρχικά θα πρέπει να υπάρχει ένα ασφαλές κανάλι από το οποίο θα μεταφερθεί το ιδιωτικό κλειδί στον χρήστη. Επίσης, ο βαθμός εμπιστοσύνης και οι απαιτήσεις ασφάλειας της Αρχής Εγγραφής θα είναι πολύ μεγαλύτερες, γιατί σε περίπτωση επιτυχούς επίθεσης εκτίθενται τα ιδιωτικά κλειδιά των χρηστών. Το πλεονέκτημα της δημιουργίας του ζεύγους κλειδιών στην Αρχή Εγγραφής ή Πιστοποίησης επιτρέπει την ασφαλή αποθήκευση του ιδιωτικού κλειδιού και την ανάκτησή του αν ο χρήστης χάσει το κλειδί.

Σε ένα ανοικτό Διαδικτυακό περιβάλλον τα κλειδιά δημιουργούνται στο περιβάλλον του χρήστη, ενώ σε εταιρικά περιβάλλοντα υπάρχει συνήθως μια υπηρεσία η οποία δημιουργεί και παρέχει τα κλειδιά στους χρήστες.

Όποια εναλλακτική και να ακολουθηθεί, το ιδιωτικό κλειδί καταλήγει στο ***Ασφαλές Προσωπικό Περιβάλλον*** του χρήστη (Personal Security Environment) το οποίο μπορεί να είναι ο σκληρός δίσκος, αποσπώμενος δίσκος ή έξυπνη κάρτα. Από τα τρία, η ασφαλέστερη αποθήκευση είναι η έξυπνη κάρτα, η οποία θεωρείται ανθεκτική σε εξωτερικές επεμβάσεις (tamper proof) και έχει τη δυνατότητα να δημιουργεί τις ψηφιακές υπογραφές χωρίς να απαιτείται το ιδιωτικό κλειδί να μεταφερθεί σε λιγότερο ασφαλές περιβάλλον, όπως ο προσωπικός υπολογιστής του χρήστη.

Όταν η Αρχή Πιστοποίησης υπογράψει τα στοιχεία του χρήστη μαζί με το δημόσιό του κλειδί, το πιστοποιητικό που προκύπτει μεταφέρεται στον χρήστη είτε άμεσα, είτε μέσω της υπηρεσίας καταλόγου. Στη δεύτερη περίπτωση, η Αρχή Πιστοποίησης δημοσιεύει το πιστοποιητικό σε κάποιο κατάλογο ο οποίος διατίθεται δημόσια. Από το δημόσιο κατάλογο όλα τα μέλη έχουν πρόσβαση όπου επιτρέπεται μόνον η ανάγνωση. Αντίθετα, η Αρχή Πιστοποίησης έχει δυνατότητα πρόσβασης ανάγνωσης και εγγραφής. Οι απαιτήσεις ασφάλειας του καταλόγου είναι σχε-

τικά μικρές, αφού η αυθαίρετη τροποποίηση ενός ή περισσοτέρων πιστοποιητικών μπορεί να ανιχνευθεί. Ο αντίπαλος που θα επιχειρήσει να μεταβάλλει το πιστοποιητικό κάποιου χρήστη θα πρέπει να γνωρίζει το ιδιωτικό κλειδί της Αρχής Πιστοποίησης. Η όλη διαδικασία δημιουργίας και δημοσίευσης των πιστοποιητικών των χρηστών παριστάνεται στο Σχήμα 7.11.



Σχήμα 7.11 Διαδικασία δημιουργίας και δημοσίευσης πιστοποιητικού

Διαδικασία ελέγχου του πιστοποιητικού

Θεωρούμε τη διαδικασία όπου η Αλίκη επιθυμεί να επικοινωνήσει με τον Βύρωνα. Επίσης θεωρούμε ότι η ασφαλής επικοινωνία απαιτεί αμοιβαία αυθεντικοποίηση των δύο μελών και καθορισμό κλειδιού συνόδου. Ο καθορισμός του κλειδιού συνόδου εξετάσθηκε στις προηγούμενες παραγράφους. Εδώ θα περιγράψουμε τη διαδικασία αυθεντικοποίησης των μελών από τα ψηφιακά χαρακτηριστικά.

Αρχικά, η Αλίκη επικοινωνεί με τον Βύρωνα ή με τον κατάλογο, προκειμένου να προσκομίσει το δημόσιο κλειδί του Βύρωνα. Στη συνέχεια, εκτελεί τις ακόλουθες δύο ενέργειες ελέγχου:

1. Έλεγχος των στοιχείων του πιστοποιητικού. Κατά τον έλεγχο αυτό, η Αλίκη εξετάζει τα στοιχεία του πιστοποιητικού που περιγράφουν τον Βύρωνα, καθώς και την επικαιρότητα του πιστοποιητικού. Το πιστοποιητικό θεωρείται επίκαιρο, αν η ημερομηνία λήξης είναι μεγαλύτερη από την τρέχουσα ημερομηνία.
2. Έλεγχος ανάκλησης του πιστοποιητικού. Πολλές φορές, λόγω κακής χρήσης του πιστοποιητικού ή λόγω υποψίας διαρροής του ιδιωτικού κλειδιού, το πιστοποιητικό μπορεί να λήξει πριν από την αναγραφόμενη ημερομηνία

λήξης. Η τεχνητή αυτή λήξη ονομάζεται ανάκληση του πιστοποιητικού. Υπάρχουν δύο τεχνολογίες ανάκλησης του πιστοποιητικού: οι ***λίστες ανακληθέντων πιστοποιητικών*** (certificate revocation lists) και το ***πρωτόκολλο κατάστασης πιστοποιητικού*** (online certificate status protocol). Οι λίστες ανακληθέντων πιστοποιητικών είναι πιστοποιητικά ειδικού τύπου τα οποία υπογράφει και εκδίδει η Αρχή Πιστοποίησης, όπου φαίνονται όλα τα πιστοποιητικά τα οποία έχουν ανακληθεί. Το πρωτόκολλο κατάστασης πιστοποιητικού προϋποθέτει σύνδεση με την αντίστοιχη υπηρεσία της Αρχής Πιστοποίησης η οποία παρέχει πληροφορίες σχετικά με την ανάκληση ενός συγκεκριμένου πιστοποιητικού.

Μετά την επιτυχή ολοκλήρωση των δύο παραπάνω ελέγχων και από τις δύο πλευρές, ακολουθεί πρωτόκολλο αυθεντικοποίησης το οποίο βασίζεται σε ασύμμετρη κρυπτογραφία.

Διαδικασία ανάκλησης του πιστοποιητικού

Η ανάκληση του πιστοποιητικού γίνεται σε δύο περιπτώσεις:

- Στην περίπτωση που ο χρήστης υποψιασθεί ότι το ιδιωτικό του κλειδί έχει εκτεθεί και έχει γίνει γνωστό σε τρίτους.
- Στην περίπτωση που γίνει κακή χρήση του πιστοποιητικού από τον χρήστη. Κακή χρήση ορίζεται η οποιαδήποτε χρήση του πιστοποιητικού πέραν της προβλεπόμενης.

Ο προορισμός χρήσης των πιστοποιητικών καθορίζεται από την Αρχή Πιστοποίησης. Ένα πιστοποιητικό μπορεί να χρησιμοποιηθεί για αυθεντικοποίηση, για εμπιστευτικότητα, ή και για τις δύο υπηρεσίες. Λόγω των νομικών περιορισμών, ή για καθαρά πρακτικούς λόγους, η χρήση των πιστοποιητικών είναι συγκεκριμένη. Για την κρυπτογράφηση μηνυμάτων για παράδειγμα, υπάρχουν νομικοί περιορισμοί που διαφέρουν από χώρα σε χώρα. Οι νομικοί περιορισμοί επικεντρώνονται στο μέγεθος του ιδιωτικού κλειδιού. Αντίθετα, στην περίπτωση της αυθεντικοποίησης με τη χρήση της ψηφιακής υπογραφής, δεν υπάρχει ουσιαστικός περιορισμός. Έτσι, η κρυπτογράφηση με ένα κλειδί το οποίο χρησιμοποιείται για αυθεντικοποίηση ενδεχομένως μπορεί να αποτελέσει αδίκημα.

Ο διαχωρισμός της χρήσης των πιστοποιητικών για αυθεντικοποίηση και εμπιστευτικότητα, συμβάλλει στην καλύτερη διαχείριση των κλειδιών. Στην περίπτωση των πιστοποιητικών αυθεντικοποίησης δεν απαιτείται εφεδρική αποθήκευση του ιδιωτικού κλειδιού, διότι εάν ο χρήστης χάσει το κλειδί του, μπορεί να ζητήσει νέο πιστοποιητικό χωρίς να υπάρξουν πρακτικές συνέπειες. Στην περίπτωση όμως που ο χρήστης χάσει το ιδιωτικό κλειδί του πιστοποιητικού που χρησιμοποιεί για εμπιστευτικότητα, τότε αν δεν υπάρχει εφεδρική αποθήκευση του ιδιωτικού κλειδιού, δεν θα είναι σε θέση να αποκρυπτογραφήσει όλα τα κρυπτοκείμενα που κρυπτογραφήθηκαν με το αντίστοιχο δημόσιο κλειδί. Συνεπώς, η εφεδρική αποθή-

κευση του ιδιωτικού κλειδιού ενός πιστοποιητικού εμπιστευτικότητας είναι επιθυμητή, αφού συμβάλει στη μείωση του ρίσκου άρνησης υπηρεσίας.

Όταν η Αρχή Πιστοποίησης κρίνει ότι απαιτείται ανάκληση του πιστοποιητικού ενός χρήστη, ανανεώνει τη λίστα ανακληθέντων πιστοποιητικών και τη δημοσιεύει στον κατάλογο που χρησιμοποιεί για τα πιστοποιητικά. Έτσι κατά τον έλεγχο ανάκλησης, ο χρήστης μπορεί να παραλάβει τη λίστα από τον κατάλογο. Σε κρίσιμες εφαρμογές, η Αρχή Πιστοποίησης (ή η υπηρεσία ανάκλησης, αν αυτή είναι διαφορετική από την Αρχή Πιστοποίησης) αναλαμβάνει τη μετάδοση της λίστας απευθείας στους χρήστες, όποτε γίνεται ανανέωση του περιεχομένου της.

Εναλλακτικά, ο χρήστης μπορεί να επικοινωνήσει με την υπηρεσία ανάκλησης για να πληροφορηθεί σχετικά με την εγκυρότητα ενός πιστοποιητικού, μέσω κάποιου πρωτοκόλλου ανάκλησης, όπως το πρωτόκολλο ανάκλησης πιστοποιητικού, OCSP.

Όροι-κλειδιά του κεφαλαίου

- κρυπτοπερίοδος
- κύκλος ζωής ενός κλειδιού
- κλειδί συνόδου, κλειδί τερματικού και κύριο κλειδί
- τέλεια μυστικότητα προς τα εμπρός και προς τα πίσω
- κέντρο διανομής κλειδιών και κέντρο μετάφρασης κλειδιών
- επίθεση του ενδιάμεσου ατόμου
- τεμαχισμός κλειδιών και σχέδιο (m, n)-κατωφλίου
- υποδομή δημόσιου κλειδιού και ψηφιακά πιστοποιητικά
- μοντέλο εμπιστοσύνης

7.7. Ασκήσεις

1. Το πρόγραμμα κλειδιού του κρυπταλγόριθμου DES, παρουσιάζει τέλεια μυστικότητα προς τα εμπρός ή προς τα πίσω; Θεωρείστε ότι το κλειδί του DES είναι το κύριο κλειδί, και τα κλειδιά των γύρων είναι τα βραχυπρόθεσμα κλειδιά.
2. Η Αλίκη έστειλε το μυστικό κλειδί $k = 12$ στον Βύρωνα μέσω του πρωτοκόλλου εδραίωσης κλειδιών άνευ κέντρου του Shamir. Οι μυστικές ποσότητες που χρησιμοποιήθηκαν ήταν $a = 7$ και $b = 11$. Βρείτε ένα κατάλληλο modulus και δείξτε τα βήματα και τους υπολογισμούς που ακολούθησε το κάθε μέλος.
3. Έχετε υποκλέψει τα ακόλουθα δεδομένα μιας επικοινωνίας ανταλλαγής κλειδιών Diffie-Hellman:
   $a^x = 38, a^y = 28, a = 3 \mod 43$
   Βρείτε το μυστικό κλειδί των επικοινωνούντων μελών.
4. Καθορίστε τις παραμέτρους ενός συστήματος ανταλλαγής κλειδιών Diffie-Hellman, ώστε το κλειδί που προκύπτει να μπορεί να χρησιμοποιηθεί σε συμμετρική κρυπτογράφηση με τον κρυπταλγόριθμο DES.

5. Δίνεται η ελλειπτική καμπύλη:
   $y^2 \equiv x^3 + x + 6 \pmod{17}$
   και το σημείο γεννήτορας της καμπύλης A = (3, 5). Αν οι μυστικές ποσότητες των δύο επικοινωνούντων μελών είναι $x_a = 2$ και $x_b = 3$ αντίστοιχα, δείξτε τα βήματα και τους υπολογισμούς του κάθε μέλους (κατά Diffie-Hellman), προκειμένου να αποκτηθεί το κοινό μυστικό κλειδί.
6. Δίνονται τα ακόλουθα μερίδια κλειδιών, ενός σχεδίου (3, 6)-κατωφλίου:
   (1, 26), (2, 8), (3, 23), (4, 13), (5, 7), (6, 5)
   και το δημόσιο modulus, 29. Βρείτε το αρχικό κλειδί.