ΔΗΜΗΤΡΙΟΥ Γ. ΠΕΠΠΕ

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΚΑΤΑΝΕΜΗΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΠΕΙΡΑΙΑΣ 1999

-

ΔΗΜΗΤΡΙΟΥ Γ. ΠΕΠΠΕ

ΑΣΦΑΛΕΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΚΑΤΑΝΕΜΗΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

ΕΓΚΡΙΘΕΙΣΑ ΑΠΟ ΤΟ ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΤΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

-

-

Αφιερώνεται στους γονείς μου

-

Είναι γεγονός ότι η εκπόνηση διδακτορικής διατριβής στο διαρκώς εξελισσόμενο χώρο της Πληροφορικής, είναι ιδιαζόντως δύσκολη, λόγω των παράλληλων θέσεων, εφαρμογών και αναλύσεων που απαιτούνται, όταν μάλιστα πολλά από τα δεδομένα αυτά αλλάζουν σε σύντομο χρονικό διάστημα.

Θεωρώ υποχρέωση μου να ευχαριστήσω τα μέλη της τριμελούς επιτροπής :

Τον επιβλέποντα Καθηγητή κ Βασίλειο Χρυσικόπουλο που από την αρχή της προσπάθειας πίστεψε στις δυνατότητές μου και με βοήθησε με σωστή και αποτελεσματική καθοδήγηση στο χώρο της κρυπτογραφίας.

Τον Καθηγητή κ Νικόλαο Αλεξανδρή για τη συνεχή επιστημονική υποστήριξη και την ειλικρινή συμπαράστασή του στην προσπάθειά μου.

Τον Καθηγητή κ Γεώργιο Βασιλακόπουλο για την επιστημονική βοήθεια που μου προσέφερε καθώς και την επιμονή και συμπαράσταση που επέδειξε σε κάθε φάση της συνεργασίας μας.

Επίσης ευχαριστώ τον Καθηγητή του Πανεπιστημίου του Λονδίνου, κ Mike Burmester για τη βοήθεια, συμπαράσταση και καθοδήγησή του στο χώρο της κρυπτογραφίας καθώς και για

-

τη θετική του προδιάθεση σε κάθε χρονική στιγμή της συνεργασίας μας, και τον Καθηγητή κ Αντώνιο Παναγιωτόπουλο, δάσκαλό μου που με βοήθησε για την ολοκλήρωση της παρούσας.

Ευχαριστώ τους Καθηγητές κ. Δημήτρη Γκρίτζαλη, κ. Σωκράτη Κάτσικα και κ. Παναγιώτη Γεωργιάδη, μέλη της εξεταστικής μου επιτροπής, για τις παρατήρησεις και την εποικοδομητική κριτική τους.

Ευχαριστώ το Τμήμα Πληροφορικής του Πανεπιστημίου Πειραιώς για τη συμπαράσταση και βοήθεια όλα αυτά τα χρόνια της προσπάθειάς μου. Ειδικότερα, ευχαριστώ την κ Δώρα Καλογεράκη για την ηθική συμπαράσταση.

Ευχαριστώ τη φίλη, φιλόλογο Ευη Μητροπούλου για τα σχόλια και τις παρατηρήσεις που αφορούσαν στη φιλολογική επιμέλεια της παρούσας διατριβής.

Τέλος, ευχαριστώ τις φίλες και τους φίλους μου, Φλώρα, Νένα, Αννα, Μάκη και Ανδρέα για την βοήθεια και την υποστήριξή τους όλα αυτά τα χρόνια καθώς και την Ελένη για την υπομονή, την συμπαράσταση και τη κατανόηση που έδειξε, για όλες τις ώρες που αφιέρωσα στη προετοιμασία και ολοκλήρωση της παρούσας διατριβής.

-

-

ΠΕΡΙΕΧΟΜΕΝΑ

-

ΚΕΦΑΛΑΙΟ 2 : ΜΟΝΤΕΛΑ ΣΥΜΦΩΝΙΑΣ ΚΛΕΙΔΙΟΥ ΑΠΟΔΕΔΕΙΓΜΕΝΗΣ ΑΣΦΑΛΕΙΑΣ

ΚΕΦΑΛΑΙΟ 3 : ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΩΤΟΚΟΛΛΑ ΣΥΝΔΙΑΣΚΕΨΗΣ

-

ΚΕΦΑΛΑΙΟ 4 : ΑΣΦΑΛΗΣ ΕΠΙΚΟΙΝΩΝΙΑ Σ' ΕΝΑ ΣΥΣΤΗΜΑ ΕΠΑΓΡΥΠΝΗΣΗΣ ΓΙΑ ΙΑΤΡΙΚΕΣ ΣΥΣΚΕΥΕΣ

ΚΕΦΑΛΑΙΟ 5 : ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΕΩΝ ΧΡΗΣΤΗ ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΝΟΣΟΚΟΜΕΙΟΥ

-

ΠΑΡΑΡΤΗΜΑ : ΥΛΟΠΟΙΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΠΡΩΤΟΚΟΛΛΩΝ

-

-

ΕΙΣΑΓΩΓΗ

Στην εποχή μας, ***εποχή της πληροφορίας***, η "επικοινωνία" αποτελεί αντικείμενο μελέτης, προβληματισμού και έρευνας. Οι ειδικοί από διάφορους χώρους (πληροφορική, ψυχολόγοι, νομοθέτες κλπ) ασχολούνται με τη διαδικασία μεταφοράς, επεξεργασίας και αποθήκευσης των πληροφοριών και την επικοινωνία, κατ΄ επέκταση. Η ανάγκη αυτή, που συνεχώς γίνεται ολοένα πιο έντονη, συνδέεται άμεσα με την πολυπλοκότητα της σύγχρονης ζωής, την αυξανόμενη χρήση της Πληροφορικής και των μέσων που επιτρέπουν την μετάδοση και την ανταλλαγή άπειρων ταυτόχρονων πληροφοριών και δεδομένων.

Από τα μέσα της δεκαετίας του '80 και μετέπειτα, η ραγδαία ανάπτυξη των επικοινωνιών, των ηλεκτρονικών μέσων μεταφοράς πληροφοριών και δεδομένων και των δικτύων υπολογιστικών συστημάτων έχουν δημιουργήσει νέες προοπτικές. Έχουν συμβάλει δε αποφασιστικά στην ανακάλυψη νέων τρόπων και μεθόδων διανομής και επεξεργασίας πληροφοριών και δεδομένων.

Η εμφάνιση των δικτύων υπολογιστικών συστημάτων, αρχικά των τοπικών δικτύων (LAN) και των εκτεταμένων (WAN) και στη συνέχεια των διαδίκτυων (Internet) παρέχουν τη δυνατότητα σε κάθε οργανισμό να αντιμετωπίσει αποτελεσματικά την επεξεργασία των δεδομένων και πληροφοριών που διαθέτει, καθώς και την ανταλλαγή τους. Ειδικότερα, τα δίκτυα επέτρεψαν στους χρήστες να έχουν τις ακόλουθες - κυρίως - δυνατότητες α) κατανεμημένη αποθήκευση αρχείων (δεδομένων / πληροφοριών), β) απομακρυσμένη (remote) πρόσβαση και επεξεργασία και γ) άμεση και εύκολη επικοινωνία.

Παράλληλα, κατασκευάστηκαν προϊόντα λογισμικού που επέτρεψαν στους χρήστες των δικτύων να αλλάξουν το τρόπο διεκπεραίωσης διαφόρων εργασιών τους. Χαρακτηριστικό

παράδειγμα είναι το ηλεκτρονικό ταχυδρομείο (electronic mail - email) το οποίο έδωσε τη δυνατότητα άμεσης και εύκολης επικοινωνίας μεταξύ των χρηστών. Επιπλέον, μείωσε στο ελάχιστο την απαιτούμενη ποσότητα χαρτιού, ενώ δημιούργησε την ανάγκη παροχής ασφάλειας των δεδομένων και πληροφοριών που ανταλλάσσονταν, στοιχείο που μεταφράζεται σε μυστικότητα, ακεραιότητα και επιβεβαίωση της αποστολής και της παραλαβής τους.

Η κρυπτογραφία αποτελεί ένα αναπόσπαστο κομμάτι των σημερινών πληροφοριακών συστημάτων, λόγω της συνεχούς εξέλιξης και χρήσης τους που απαιτούν όμως, περισσότερη ασφάλεια και προστασία (από το ηλεκτρονικό ταχυδρομείο έως τις ψηφιακές επικοινωνίες, από ασφαλή πρόσβαση Web έως το ψηφιακό χρήμα) παρέχοντας ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα. Ειδικότερα, η κρυπτογραφία -κυρίως- μπορεί να αποτρέψει το δόλο σε διαδικασίες ηλεκτρονικής επικοινωνίας (π.χ. ηλεκτρονικό εμπόριο), να εξασφαλίσει την εγκυρότητα της πληροφορίας, που ανταλλάσσεται (π.χ, οικονομικές συναλλαγές), να προστατεύει την ανωνυμία του χρήστη ή/και να επαληθεύει την ταυτότητα του χρήστη, όταν απαιτείται, να παρεμποδίσει την αθέμιτη μορφοποίηση δεδομένων και πληροφοριών (π.χ. σελίδες Web) και να εμποδίζει "τρίτους" να αποκτήσουν πρόσβαση σε εμπιστευτικά δεδομένα και πληροφορίες

Η κρυπτογραφία υπήρξε αντικείμενο έρευνας από αρχαιοτάτων χρόνων και πολλά δείγματα χρήσης της υπάρχουν σε διάφορα αρχαία κείμενα. Ενα από τα σημαντικά κείμενα που περιγράφουν τις διάφορες μεθόδους προστασίας και εξασφάλισης της μυστικότητας των επικοινωνιών των αρχαίων Ελλήνων είναι το "Αι Μυστικαί Τηλεπικοινωνίαι των Αρχαίων Ελλήνων" του Ε. Σταμάτη [Στα69]. Ενα άλλο χαρακτηριστικό παράδειγμα της κρυπτογραφίας είναι το γράμμα του Ιουλίου Καίσαρα προς τον Κικέρωνα, όπου αντικατάστησε κάθε γράμμα του κειμένου με το τρίτο επόμενο γράμμα του λατινικού αλφαβήτου[Αλε95b, Bra87]. Σύμφωνα με τον D. Kahn, η αρχαία λακωνική σκυτάλη, την οποία περιέγραψε εκτενώς ο Πλούταρχος [Αλκιβ. 38,6' Λυσανρ.19,8-12] αποτελεί το πρώτο σύστημα στρατιωτικής κρυπτογράφησης, καθώς ήταν το επίσημο κρυπτογραφικό σύστημα / μέσο που επέτρεπε την ασφαλή μεταβίβαση μυστικών οδηγιών και αγγελιών μεταξύ των Σπαρτιατών [Kah76].

-

Αρχικά, η κρυπτογραφία ήταν κλάδος των Μαθηματικών. Η αυξανόμενη ανάγκη για περαιτέρω διερεύνηση - σε θεωρητικό επίπεδο- καθώς και η ολοένα μεγαλύτερη εφαρμογή της σε καθημερινά προβλήματα και η εξέλιξη- σε πρακτικό επίπεδο - είχε ως αποτέλεσμα την αυτονόμησή της, και τη δημιουργία ενός νέου επιστημονικού κλάδου, της κρυπτολογίας. Η κρυπτολογία περιλαμβάνει δύο επιμέρους κλάδους, την κρυπτογραφία και την κρυπτοανάλυση. Στην κρυπτογραφία μελετώνται μέθοδοι προστασίας της επικοινωνίας μέσω μη ασφαλών διαύλων, ενώ στην κρυπτοανάλυση μελετώνται μέθοδοι παραβίασης (αποκάλυψης ή πλαστογράφησης) αυτών των επικοινωνιών [Αλε95b, Bra87, Cop87, Sch94, Sim91,Nist800].

Οι λειτουργίες ασφάλειας σχετίζονται με τις πληροφορίες και τα δεδομένα, είτε άμεσα (ακεραιότητα των δεδομένων), είτε έμμεσα (αυθεντικοποίηση των χρηστών). Πιο συγκεκριμένα, η αυθεντικοποίηση των χρηστών παρέχει έμμεση προστασία των πληροφοριών και δεδομένων, αφού αποτρέπει την εμφάνιση ενός χρήστη με την ιδιότητα ενός άλλου, διασφαλίζοντας σε κάποιο βαθμό τις πληροφορίες που αφορούν ή/και ανήκουν στον συγκεκριμένο χρήστη.

Για την υλοποίηση των λειτουργιών ασφάλειας, χρησιμοποιούνται διάφοροι μηχανισμοί, όπως τα κρυπτογραφικά πρωτόκολλα (cryptographic protocols), οι επιδέξιοι χειρισμοί ανίχνευσης (manipulation detection codes), οι ψηφιακές υπογραφές (digital signatures) και τα πλαίσια αυθεντικοποίησης (authentication frameworks) [Jan91, Nist800,Sim91].

Η ανάπτυξη ενός συστήματος ασφάλειας το οποίο αποβλέπει στην παροχή προστασίας ενός πληροφοριακού συστήματος και βάσης δεδομένων προϋποθέτει α) τον προσδιορισμό των απειλών ασφάλειας, β) τον καθορισμό της πολιτικής, στην οποία θα βασίζεται το σύστημα ασφάλειας, καθώς και την ανάπτυξη του κατάλληλου μοντέλου στο οποίο θα βασίζεται η επιλεγμένη πολιτική γ) τον προσδιορισμό των μηχανισμών με τους οποίους θα υλοποιηθεί το μοντέλο και δ) τον έλεγχο και την επιβεβαίωση ότι η παρεχόμενη ασφάλεια και προστασία βασίζεται σε γενικά αποδεκτά πρότυπα και ικανοποιούνται οι υπάρχουσες απαιτήσεις χωρίς επιπτώσεις στην απόδοση και λειτουργικότητα [Fug88] .

-

Η ανάπτυξη στο χώρο της τεχνολογίας της Πληροφορικής έχει οδηγήσει στην ευρεία χρήση των υπολογιστικών συστημάτων σε δημόσιους και σε ιδιωτικούς οργανισμούς, όπως τράπεζες, νοσοκομεία, πανεπιστήμια και επιχειρήσεις.

Η εξέλιξη όσο αφορά την αξιοπιστία του λογισμικού και του υλικού (hardware), η σταδιακή μείωση του απαιτούμενου κόστους, καθώς και η παροχή κατάλληλων εργαλείων υποστήριξης έχουν ως αποτέλεσμα τη βελτίωση των δυνατοτήτων αποθήκευσης και διαχείρισης πληροφοριών από τα υπολογιστικά συστήματα. Συνεπώς, η σωστή και αποτελεσματική παροχή των υπηρεσιών ενός οργανισμού εξαρτάται από την κατάλληλη διαχείριση των δεδομένων μέσω των υπολογιστικών συστημάτων.

Παράλληλα, εμφανίστηκαν τα *Πληροφοριακά Συστήματα Διοίκησης* (Management Information Systems) ή απλά *Πληροφοριακά Συστήματα* (Information Systems). Κάθε πληροφοριακό σύστημα θεωρείται ένα από τα σημαντικά υποσυστήματα ενός οργανισμού. Από τα βασικά συστατικά κάθε πληροφοριακού συστήματος είναι η *Βάση Δεδομένων* (Data Base) που ορίζεται ως η ολοκληρωμένη και δομημένη συλλογή πληροφοριών-δεδομένων που αφορούν έναν ολόκληρο οργανισμό ή τα τμήματά του [Βασ91, Dat90].

Κατά την διαδικασία του σχεδιασμού και της ανάπτυξης ενός πληροφοριακού συστήματος και βάσεων δεδομένων, θα πρέπει να επιλεγεί η μέθοδος διαχείρισης των δεδομένων που αφορούν το συγκεκριμένο οργανισμό. Γενικά, υπάρχουν δύο βασικές μέθοδοι διαχείρισης δεδομένων: η συγκεντρωτική (centralised) και η κατανεμημένη (distributed) [Βασ91, Aue94, Cas95, Sha91].

Η κατανεμημένη διαχείριση δεδομένων είναι ευρέως διαδεδομένη τα τελευταία χρόνια, λόγω της εμφάνισης των δικτύων, τα οποία επιτρέπουν την επικοινωνία και την ανταλλαγή πληροφοριών και δεδομένων μεταξύ των διαφόρων τμημάτων ενός οργανισμού που μπορεί να βρίσκονται σε κοντινή ή σε μακρινή απόσταση.

-

Παράλληλα, εμφανίστηκαν διάφορα προβλήματα ασφάλειας και προστασίας των δεδομένων και των πληροφοριών [Bak92, Cas95, Den79, Dob79, Par84, Tre93]. Η πιθανή καταστροφή, τροποποίηση ή αποκάλυψη των δεδομένων και των πληροφοριών που αποθηκεύονται στη βάση δεδομένων μπορεί να έχει συνέπειες, όχι μόνο σ' έναν συγκεκριμένο χρήστη, ή μια εφαρμογή του συστήματος, αλλά και στη λειτουργία του πληροφοριακού συστήματος. Οι συνέπειες μπορεί να είναι μεγάλες σε έκταση και απρόβλεπτες πολλές φορές. Ορισμένοι από τους λόγους εμφάνισης τέτοιων προβλημάτων μπορεί να είναι α) η εκτέλεση μιας διαδικασίας του οργανισμού σε πολλά διαφορετικά σημεία, β) η ανεπαρκής προστασία που παρέχουν οι δίαυλοι επικοινωνίας και γ) η εύκολη σύνδεση ενός νέου χρήστη[Cou88].

Επομένως, σ' ένα οργανισμό οι διαδικασίες και οι μηχανισμοί, που αφορούν την προστασία των δεδομένων και των πληροφοριών, είναι αναγκαίοι και απαραίτητοι για την διασφάλιση της αξιοπιστίας, την συνέχιση της σωστής λειτουργίας, καθώς και για την προστασία των δεδομένων από αυθαίρετη χρήση (κλοπή, τροποποίηση, μη εξουσιοδοτημένη χρήση).

Η ταυτόχρονη επίτευξη των λειτουργιών ασφάλειας απαιτεί τη χρήση κρυπτογραφικών συστημάτων, είτε μυστικού, είτε δημοσίου κλειδιού, με κύριο στόχο την προστασία της επικοινωνίας δύο ή περισσοτέρων χρηστών του συστήματος. Οι έννοιες κλειδί, κρυπτογραφικά συστήματα μυστικού κλειδιού και δημοσίου κλειδιού, παρουσιάζονται αναλυτικά στο κεφάλαιο 1.

Η μετάδοση ενός μηνύματος μεταξύ δύο ή περισσοτέρων χρηστών πραγματοποιείται μέσω συστημάτων μυστικού κλειδιού. Απαραίτητη προϋπόθεση για τα συστήματα μυστικού κλειδιού είναι η γνωστοποίηση του μυστικού κλειδιού στους χρήστες, που επιθυμούν να επικοινωνήσουν. Η χρήση ασφαλούς διαύλου μεταξύ των χρηστών είναι συνήθως τεχνικά αδύνατη (π.χ. κόστος λειτουργίας). Για το λόγο αυτό, έχει δημιουργηθεί μια ειδική κατηγορία κρυπτογραφικών πρωτοκόλλων, γνωστών ως κρυπτογραφικών πρωτοκόλλων δημιουργίας κλειδιού (key establishment cryptographic protocols), όπου δύο ή περισσότεροι χρήστες

-

αποκτούν ένα κοινό μυστικό κλειδί [Sim91]. Ως *πρωτόκολλο* ορίζεται κάθε αλγόριθμος που πρέπει να ακολουθούν οι χρήστες για να επιτύχουν ένα συγκεκριμένο σκοπό.

Παράλληλα, στο χώρο της κρυπτογραφίας εμφανίστηκε η έννοια της *τρίτης έμπιστης οντότητας* (Trusted Third Party) ή *κέντρου εμπιστοσύνης* (Trusted Centre) [Μαρ95]. Σύμφωνα με το ISO CD 10181-1 "Security Framework for Open Systems" ως τρίτη έμπιστη οντότητα ορίζεται κάθε αρχή-οντότητα, που παρέχει λειτουργίες ασφάλειας στους χρήστες ενός συστήματος κατόπιν αποδεδειγμένης εμπιστοσύνης προς αυτήν.

Σ' ένα κρυπτογραφικό πρωτόκολλο δημιουργίας κλειδιού, η τρίτη έμπιστη οντότητα έχει το ρόλο του συντονιστή και είναι υπεύθυνη για την ασφαλή μεταφορά ενός μυστικού κλειδιού σε δύο ή περισσότερους χρήστες, που επιθυμούν να επικοινωνήσουν μεταξύ τους. Στην περίπτωση που ο ρόλος της τρίτης έμπιστης οντότητας περιορίζεται μόνο στην μεταφορά του κοινού μυστικού κλειδιού στους χρήστες, τότε ονομάζεται και *κέντρο διανομής κλειδιού* (Key Distribution Centre).

Η διανομή του κοινού μυστικού κλειδιού μέσω της τρίτης έμπιστης οντότητας έχει ως μειονεκτήματα το υψηλό κόστος λειτουργίας εφόσον θα πρέπει να είναι σε συνεχή λειτουργία και ότι γνωρίζει όλα τα κοινά μυστικά κλειδιά επικοινωνίας.

Εάν για τεχνικούς λόγους (υψηλό κόστος), η τρίτη έμπιστη οντότητα δεν μπορεί να είναι συνεχώς διαθέσιμη, τότε στην περίπτωση αυτή, κάθε ομάδα χρηστών μπορεί να κατέχει ένα κοινό μυστικό κλειδί, από την αρχή. Έτσι, σ' ένα δίκτυο *n* χρηστών όπου επικοινωνούν μόνο ανά δύο, θα πρέπει να μοιράσουν $\frac{n(n-1)}{2}$ κλειδιά και κάθε χρήστης θα πρέπει να έχει στην κατοχή του *n-1* κλειδιά. Αυτό είναι γνωστό ως n^2 πρόβλημα. Η επίλυση του προβλήματος γίνεται δυσκολότερη όταν το *n* είναι αρκετά μεγάλος αριθμός και δεν μπορεί να προκαθοριστεί, ή/και όταν οι χρήστες που επικοινωνούν ταυτόχρονα μπορεί να είναι περισσότεροι από δύο. Στη δυσκολία του υπολογισμού, αλλά και της λειτουργίας που μπορεί να έχει αυτή η επιλογή, θα πρέπει να συμπεριληφθεί και μία επιπλέον δυσκολία που είναι ποιος και με ποιο τρόπο θα

-

υπολογίζει και θα διανέμει τα κλειδιά αυτά, εάν και εφόσον η τρίτη έμπιστη οντότητα δεν μπορεί να αντεπεξέλθει. Οι Gong και Wheeler [Gon90] έχουν προτείνει μία λύση για το πρόβλημα αυτό, η οποία, για *n* χρήστες μειώνει το συνολικό αριθμό των μυστικών κλειδιών σε *n* και τον αριθμό των κλειδιών που κάθε χρήστης πρέπει να κατέχει σε $2\sqrt{n}-1$. Μία άλλη λύση έχει προταθεί από τους Leighton και Micali [Lei94]. Και στις δύο παραπάνω λύσεις, το κύριο μειονέκτημα είναι ότι η τρίτη έμπιστη οντότητα συνεχίζει να γνωρίζει όλα τα κοινά μυστικά κλειδιά επικοινωνίας.

Τα κρυπτογραφικά πρωτόκολλα δημιουργίας κλειδιού διακρίνονται σε δύο μεγάλες κατηγορίες: στα *πρωτόκολλα μεταφοράς κλειδιού* (key transport cryptographic protocols) και στα *πρωτόκολλα συμφωνίας κλειδιού* (key agreement cryptographic protocols) [ISO95].

⇒ *Κρυπτογραφικό πρωτόκολλο μεταφοράς κλειδιού* είναι κάθε πρωτόκολλο, όπου ένας από τους χρήστες που συμμετέχουν, επιλέγει (με την βοήθεια ενός συγκεκριμένου αλγορίθμου) ποιο θα είναι το κοινό μυστικό κλειδί και στην συνέχεια το μεταφέρει στους υπόλοιπους χρήστες.

⇒ *Κρυπτογραφικό πρωτόκολλο συμφωνίας κλειδιού* είναι κάθε πρωτόκολλο, όπου οι χρήστες συμμετέχουν στην δημιουργία του κοινού μυστικού κλειδιού, αλλά με τέτοιο τρόπο, ώστε κανένας από τους χρήστες να μην μπορεί να υπολογίσει το κοινό μυστικό κλειδί, πριν ολοκληρωθεί η όλη διαδικασία.

Τα κρυπτογραφικά πρωτόκολλα μεταφοράς κλειδιού περιγράφονται αναλυτικά στο Κεφάλαιο 1.

Η *συμφωνία κλειδιού* (Key Agreement) είναι η διαδικασία απόκτησης ενός κοινού μυστικού κλειδιού από δύο ή περισσότερους χρήστες, το οποίο θα χρησιμοποιηθεί στην διαδικασία κωδικοποίησης και αποκωδικοποίησης των μηνυμάτων που θα ανταλλάξουν μεταξύ τους. Με την ολοκλήρωση της διαδικασίας αυτής μόνο οι εξουσιοδοτημένοι χρήστες, δηλαδή οι χρήστες που συμμετείχαν στη διαδικασία συμφωνίας κλειδιού, θα πρέπει να έχουν στην κατοχή τους το σωστό κοινό μυστικό κλειδί ή τις αναγκαίες και απαραίτητες πληροφορίες,

ώστε να μπορούν να υπολογίσουν το κοινό μυστικό κλειδί [Ale92, Ale93, Bel94, Bir92, Chr95, Des93, Dif76, Gol88, ISO95, Kohl, Lei94, Mat86].

Η διαδικασία συμφωνίας κλειδιού μεταξύ των χρηστών ενός συστήματος, όπως και κάθε άλλη διαδικασία, θα πρέπει να υλοποιείται σ' ένα δομημένο περιβάλλον ρυθμίσεων-παραμέτρων του συστήματος. Το περιβάλλον αυτό, θα πρέπει να α) είναι γνωστό στο σύνολο των χρηστών, β) μπορεί να μεταβάλλεται ανάλογα με το κρυπτογραφικό πρωτόκολλο που χρησιμοποιείται για την υλοποίηση της διαδικασίας και γ) είναι ανεξάρτητο και να μην περιορίζεται από τη μορφή / τύπο του δικτύου που χρησιμοποιείται.

Ορισμένα από τα κρυπτογραφικά πρωτόκολλα συμφωνίας κλειδιού παρουσιάζονται αναλυτικά στο Κεφάλαιο 1. Επίσης, τα προτεινόμενα κρυπτογραφικά πρωτόκολλα στα Κεφάλαια 2, 3 και 4 ανήκουν στην ίδια κατηγορία.

Η εμφάνιση πολλών και διαφορετικών κρυπτογραφικών πρωτοκόλλων δημιούργησε την ανάγκη καθορισμού παραμέτρων, οι οποίες χαρακτηρίζουν αν ένα κρυπτογραφικό πρωτόκολλο μπορεί να θεωρηθεί αποδοτικό ή όχι. Οι προσπάθειες αυτές μπορούν να χωριστούν σε δύο κατηγορίες: στις ατομικές και στις ομαδικές, οι οποίες θεωρούνται πιο αποδεκτές και έχουν σκοπό την δημιουργία προτύπων.

Σύμφωνα με τον W. Diffie [Dif93] ένα κρυπτογραφικό πρωτόκολλο για να θεωρηθεί αποδοτικό, πρέπει να είναι ικανοποιητικό, τόσο ως προς τις λειτουργίες ασφάλειας που παρέχει, όσο και προς ορισμένες μετρήσεις, όπως ο απαιτούμενος συνολικός υπολογισμός (Total amount of computation), ο συνολικός αριθμός ανταλλαγής δυαδικών ψηφίων (Total number of bits exchanged), ο συνολικός αριθμός ανταλλαγών (Total number of ping pong exchanges), ο απαιτούμενος συνολικός χρόνος (Total time), οι απαιτήσεις σε εξοπλισμό (Cost of equipment), η αναγκαιότητα και η χρησιμοποίησης ενός κέντρου εμπιστοσύνης (Need for Trusted Centre), η αναγκαιότητα εφαρμογής του κρυπτογραφικού πρωτοκόλλου σε πραγματικό χρόνο (Need for real time involvement of third parties).

Ο L. Gong [Gon94] που εξέτασε διάφορα κρυπτογραφικά πρωτόκολλα, κατέληξε στο συμπέρασμα ότι η αποτελεσματικότητα ενός κρυπτογραφικού πρωτοκόλλου εξαρτάται από τα μηνύματα που ανταλλάσσονται, καθώς και από το συνολικό αριθμό ανταλλαγών που πραγματοποιούνται μεταξύ των χρηστών. Μια άλλη βασική μέτρηση, σύμφωνα με τον L. Gong είναι οι περιορισμοί που υπάρχουν κάθε φορά και προέρχονται από το περιβάλλον στο οποίο θα εφαρμοστεί το κρυπτογραφικό πρωτόκολλο. Καθώς οι δυνατότητες σε λογισμικό και υλικό δεν είναι απεριόριστες και οι απαιτήσεις των χρηστών διαφέρουν, είναι αναγκαία και απαραίτητη μερικές φορές η παράβλεψη ορισμένων μετρήσεων προς όφελος των υπολοίπων. Για παράδειγμα, η αύξηση των απαιτήσεων σε εξοπλισμό ίσως να είναι απαραίτητη στην περίπτωση εκείνη που θα επιτρέψει μεγαλύτερη μείωση στο συνολικό υπολογισμό και στο απαιτούμενο χρόνο. Συνεπώς, τα ιδιαίτερα χαρακτηριστικά του χώρου καθορίζουν ποιες μετρήσεις και σε ποιο βαθμό θα πρέπει να λαμβάνονται υπόψη σε κάθε περίπτωση.

Εκτός όμως από τις παραπάνω ατομικές προσεγγίσεις, υπάρχουν και οι ομαδικές προσπάθειες που έχουν ως στόχο τους τον καθορισμό προτύπων στο χώρο των κρυπτογραφικών πρωτοκόλλων.

Το 1977 παρουσιάστηκε το DES (Data Encryption Standard) από το National Bureau of Standards, που στην συνέχεια μετονομάστηκε σε National Institute of Standards and Technology (NIST). Το 1981, το American National Standards Institute (ANSI) αποδέχτηκε το DES ως πρότυπο με την ονομασία X3-92.

Το 1980, η ISO δημιούργησε μια ειδική ομάδα, την WG1, με σκοπό να ερευνήσει το χώρο της κρυπτογράφησης των δεδομένων. Επίσης το σύστημα RSA έχει γίνει και αυτό πρότυπο. Συγκεκριμένα, το International Organisation of Standards, ISO/IEC 9796 καθόρισε το RSA ως πρότυπο για ψηφιακές υπογραφές.

Σε ότι αφορά το πρωτόκολλο των Diffie - Hellman από τις αρχές της δεκαετίας του 80 αποτελεί επίσημα εργαλείο κρυπτογράφησης στις Ηνωμένες Πολιτείες της Αμερικής και στον Καναδά [Sch94]. Η Ευρωπαϊκή Κοινότητα έχει δείξει ιδιαίτερο ενδιαφέρον για την ασφάλεια

των πληροφοριών, είτε με την διεξαγωγή σχετικών προγραμμάτων, είτε με τον καθορισμό ανάλογων πλαισίων [Παπ95].

Ο σχεδιασμός των κρυπτογραφικών πρωτοκόλλων βασιζόταν αρχικά στη μέθοδο της δοκιμής-λάθους, δηλαδή γινόταν εμπειρικά. Ομως, η εξέλιξη της τεχνολογίας της πληροφορικής και η εμφάνιση νέων τεχνικών κρυπτοανάλυσης έχουν δείξει ότι το ποσοστό επιτυχίας αυτής της μεθόδου δεν είναι ικανοποιητικό, με αποτέλεσμα πολλά κρυπτογραφικά πρωτόκολλα να μην θεωρούνται ασφαλή, αφού ο κρυπτοαναλυτής μπορεί να αποκτήσει γνώση για τα κωδικοποιημένα μηνύματα ή τα κλειδιά που χρησιμοποιούνται [Bur94, Des93,Bur94a].

Στις αρχές της δεκαετίας του 80 οι Blum, Goldwasser, Micali και Yao [Blu84, Gol84, Yao82] έδειξαν ότι η ασφάλεια ενός πρωτοκόλλου μπορεί να αποδεικνύεται με τη βοήθεια προτύπων και αποδεκτών υποθέσεων πολυπλοκότητας, όπως η παραγοντοποίηση (intractability of factoring). Αυτό, που ορίζεται ως μοντέλο αποδεδειγμένης ασφάλειας, συνεπάγεται: α) τον ορισμό ενός στόχου, β) τη διατύπωση ενός κρυπτογραφικού πρωτοκόλλου και γ) μια απόδειξη ότι το πρωτόκολλο επιτυγχάνει τον στόχο, υπό την προϋπόθεση ότι ισχύουν μερικές γενικά αποδεκτές υποθέσεις.

Στα τέλη της δεκαετίας του 80 και στις αρχές της δεκαετίας του 90 οι Bellare, Bird, Gopal, Herberg, Janson, Kutten, Molva, Rogaway και Yung [Bel94, Bir92, Lei94] πρότειναν κρυπτογραφικά πρωτόκολλα για κατανεμημένα συστήματα που παρέχουν διάφορους βαθμούς προστασίας. Το 1993 οι Desmedt και Burmester πρότειναν ένα μοντέλο με τη χρήση πρωτοκόλλων μηδενικής γνώσης, γνωστό ως μοντέλο μηδενικής γνώσης [Des93]. Η έννοια της μηδενικής γνώσης περιγράφεται αναλυτικά στο κεφάλαιο 1.

Η παρούσα διατριβή αναλύεται σε εισαγωγή, πέντε κεφάλαια και ένα παράρτημα. Ειδικότερα:

-

1. Στην εισαγωγή παρουσιάζεται, με εκτενή τρόπο, μια αναδρομή στα όσα έχουν προταθεί και αφορούν τα κρυπτογραφικά μοντέλα, συστήματα και πρωτόκολλα, καθώς και τις μεθόδους που χρησιμοποιούνται για τον έλεγχο πρόσβασης σε πληροφοριακά συστήματα.

2. Στο πρώτο κεφάλαιο περιγράφονται οι βασικές έννοιες που αφορούν το χώρο της κρυπτογραφίας.

3. Στο δεύτερο κεφάλαιο παρουσιάζεται ένα νέο μοντέλο συμφωνίας κλειδιού αποδειγμένης ασφάλειας.

   Ειδικότερα, αναλύονται και παρουσιάζονται συνοπτικά τα διάφορα μοντέλα ασφάλειας και κυρίως αυτά που αφορούν την απόκτηση ενός κοινού κλειδιού από τους χρήστες, που επιθυμούν να επικοινωνήσουν και να προστατέψουν τις πληροφορίες και τα δεδομένα που θα ανταλλάξουν μέσω υπολογιστών. Το σύστημα ασφάλειας που προτείνεται βασίζεται σε υποθέσεις και χρησιμοποιεί παραμέτρους, οι οποίες μπορούν να υλοποιηθούν και να ισχύουν σ' ένα σύστημα υπολογιστών.

4. Το τρίτο κεφάλαιο περιγράφει τα κρυπτογραφικά πρωτόκολλα συνδιάσκεψης.

   Ειδικότερα, αναλύονται και παρουσιάζονται συνοπτικά τα κρυπτογραφικά πρωτόκολλα συνδιάσκεψης και προτείνεται ένα νέο κρυπτογραφικό πρωτόκολλο, το οποίο χαρακτηρίζεται από το μικρό απαιτούμενο υπολογιστικό κόστος, την ελάχιστη πολυπλοκότητα, τη δυνατότητα εφαρμογής του σε συστήματα ηλεκτρονικών υπολογιστών και την αποδεδειγμένη ασφάλειά του.

5. Στο τέταρτο κεφάλαιο παρουσιάζεται η εφαρμογή του προτεινόμενου κρυπτογραφικού πρωτοκόλλου που παρουσιάζεται στο τρίτο κεφάλαιο σ' ένα σύστημα ασφάλειας και

προστασίας της επικοινωνίας των χρηστών του Ευρωπαϊκού Συστήματος Επαγρύπνησης Ιατρικών Συσκευών.

6. Το πέμπτο κεφάλαιο περιγράφει τα συστήματα ελέγχου πρόσβασης χρηστών σε πληροφοριακά συστήματα.

   Ειδικότερα, αναλύονται και περιγράφονται τα συστήματα ελέγχου πρόσβασης χρηστών σε πληροφοριακά συστήματα και παρουσιάζεται ένα νέο σύστημα ελέγχου πρόσβασης που βασίζεται στο μοντέλο ρόλου χρήστη. Τα κύρια χαρακτηριστικά του νέου συστήματος είναι η δυνατότητα ενσωμάτωσης του σ΄ ένα υπάρχον πληροφοριακό σύστημα χωρίς να απαιτείται μεγάλο προγραμματιστικό κόστος, οι κανόνες πρόσβασης να μπορούν να αλλάζουν δυναμικά και η ενεργοποίηση / απενεργοποίησή τους μπορεί να καθορίζεται από παραμέτρους του πληροφοριακού συστήματος, όταν αυτό απαιτείται.

7. Στο παράρτημα περιγράφονται τα αποτελέσματα που προέκυψαν από την -πειραματική- διαδικασία υλοποίησης ορισμένων κρυπτογραφικών πρωτοκόλλων.

Οι βιβλιογραφικές πηγές που αξιοποιήθηκαν για την ανάπτυξη της παρούσας διατριβής παρατίθενται συνολικά, στο τέλος, μετά τα κεφάλαια και το παράρτημα.

-

ΚΕΦΑΛΑΙΟ 1

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

1.1 Το κλειδί

Τόσο στην κρυπτογραφία, όσο και στην κρυπτοανάλυση, βασική έννοια είναι το κλειδί (key). Ως *κλειδί* ορίζεται μια συμβολοσειρά, η οποία μπορεί να είναι μυστική ή δημόσια, και αφορά έναν ή περισσότερους χρήστες [Αλε89, ISO95, Sim91]. Έτσι, κάθε κλειδί μπορεί να χαρακτηρισθεί ως μυστικό κλειδί, δημόσιο κλειδί, κοινό μυστικό κλειδί κ.α. Το κλειδί, σ' ένα υπολογιστικό σύστημα, είναι μια λέξη-συμβολοσειρά χαρακτήρων (αριθμητικών ή μη),της οποίας το μήκος (πλήθος) καθορίζεται κάθε φορά από το σκοπό για το οποίο χρησιμοποιείται.

Ενα βασικό χαρακτηριστικό των κλειδιών, τα οποία είναι γνωστά μόνο σ' έναν χρήστη (π.χ. μυστικό κλειδί του χρήστη) ή σ' ένα υποσύνολο των χρηστών ενός συστήματος (π.χ. κοινό μυστικό κλειδί), είναι η ανάγκη ανανέωσής τους ανά τακτά χρονικά διαστήματα.

Ενας από τους λόγους ανανέωσης των κλειδιών είναι ότι, εάν αποκαλυφθεί το κλειδί που κωδικοποιεί τα μηνύματά του ο χρήστης, τότε θα αποκαλυφθούν και πολλές πληροφορίες που τον αφορούν [Sch94]. Αντίθετα, εάν το κλειδί αυτό ανανεώνεται, τότε τα μηνύματα που ενδέχεται να αποκαλυφθούν θα είναι λιγότερα και οι επιπτώσεις θα είναι αντίστοιχα μικρότερες. Η χρονική διάρκεια ενός κλειδιού χαρακτηρίζεται μικρή ή μεγάλη ανάλογα με τον αριθμό των μηνυμάτων που έχουν κωδικοποιηθεί με αυτό, καθώς και με το περιεχόμενο των μηνυμάτων.

-

Ενας δεύτερος λόγος ανανέωσης των κλειδιών είναι, όταν το χρονικό διάστημα χρήσης ενός κλειδιού είναι μεγάλο, τότε η πιθανότητα ενός κρυπταναλυτή να το αποκαλύψει είναι μεγάλη. Εάν ο κρυπταναλυτής γνωρίζει, ότι ένας χρήστης δεν αλλάζει το κλειδί κωδικοποίησης των μηνυμάτων του συχνά, τότε το χρονικό περιθώριο που έχει για να το αποκαλύψει είναι αντίστοιχα μεγάλο. Επίσης, ο κρυπταναλυτής έχει τη δυνατότητα να αποκαλύπτει τμηματικά το συγκεκριμένο κλειδί, αφού γνωρίζει ότι δεν πρόκειται να αλλάξει σύντομα. Αντίθετα, εάν ο χρήστης ανανεώνει το κλειδί αυτό συχνά (π.χ. κάθε φορά που ολοκληρώνεται μια επικοινωνία), τότε το χρονικό περιθώριο, που έχει ο κρυπταναλυτής για να αποκαλύψει το κλειδί είναι περιορισμένο.

Ο χρόνος ανανέωσης του κλειδιού έχει σχέση με το μήκος του. Στα υπολογιστικά συστήματα, το μήκος του κλειδιού εκφράζεται σε bits. Για να καθοριστεί κάθε φορά το χρονικό όριο, μέσα στο οποίο το κλειδί θα πρέπει να ανανεώνεται, θα πρέπει να ληφθεί υπόψη ο χρόνος που απαιτείται για να ελεγχθούν όλα τα πιθανά κλειδιά που έχουν το ίδιο μήκος. Η μέθοδος αποκάλυψης ενός κλειδιού, όπου εξετάζονται όλα τα πιθανά κλειδιά, είναι γνωστή ως **Brute-Force**. Για παράδειγμα, εάν ένα κλειδί έχει μήκος 56 bits, τότε ο αριθμός των πιθανών κλειδιών είναι 2^{56}. Είναι γνωστό ότι υπάρχουν υπολογιστικά συστήματα, τα οποία μπορούν μέσα σε λιγότερες από 24 ώρες να εξετάσουν όλα τα πιθανά κλειδιά μήκους 56 bits για συγκεκριμένα κρυπτογραφικά πρωτόκολλα. Η δυνατότητα μείωσης των χρόνων αυτών μπορεί να επιτευχθεί με την χρήση υπολογιστικών συστημάτων με παράλληλους επεξεργαστές. Καθώς, η εξέλιξη της τεχνολογίας των υπολογιστικών συστημάτων συνεχώς βελτιώνεται και παράλληλα μειώνεται το κόστος κατασκευή τους, η ανανέωση των κλειδιών είναι ένας σημαντικός παράγοντας διασφάλισης των πληροφοριών και των δεδομένων τα οποία προστατεύουν [Sch94].

Η ύπαρξη πολλών κλειδιών και η κατοχή τους από ένα χρήστη δημιουργεί ενδεχομένως προβλήματα, όπως η δυσκολία διαχείρισής τους και ο απαιτούμενος χώρος αποθήκευσής τους. Για παράδειγμα, εάν το μέσο αποθήκευσης είναι έξυπνη κάρτα (smart cards), τότε, τόσο ο αριθμός των κλειδιών, όσο και το μέγεθός τους είναι χαρακτηριστικά που πρέπει να λαμβάνονται υπόψη λόγω της χωρητικότητας της [Kno88].

1.2 Σύστημα και λειτουργίες ασφάλειας

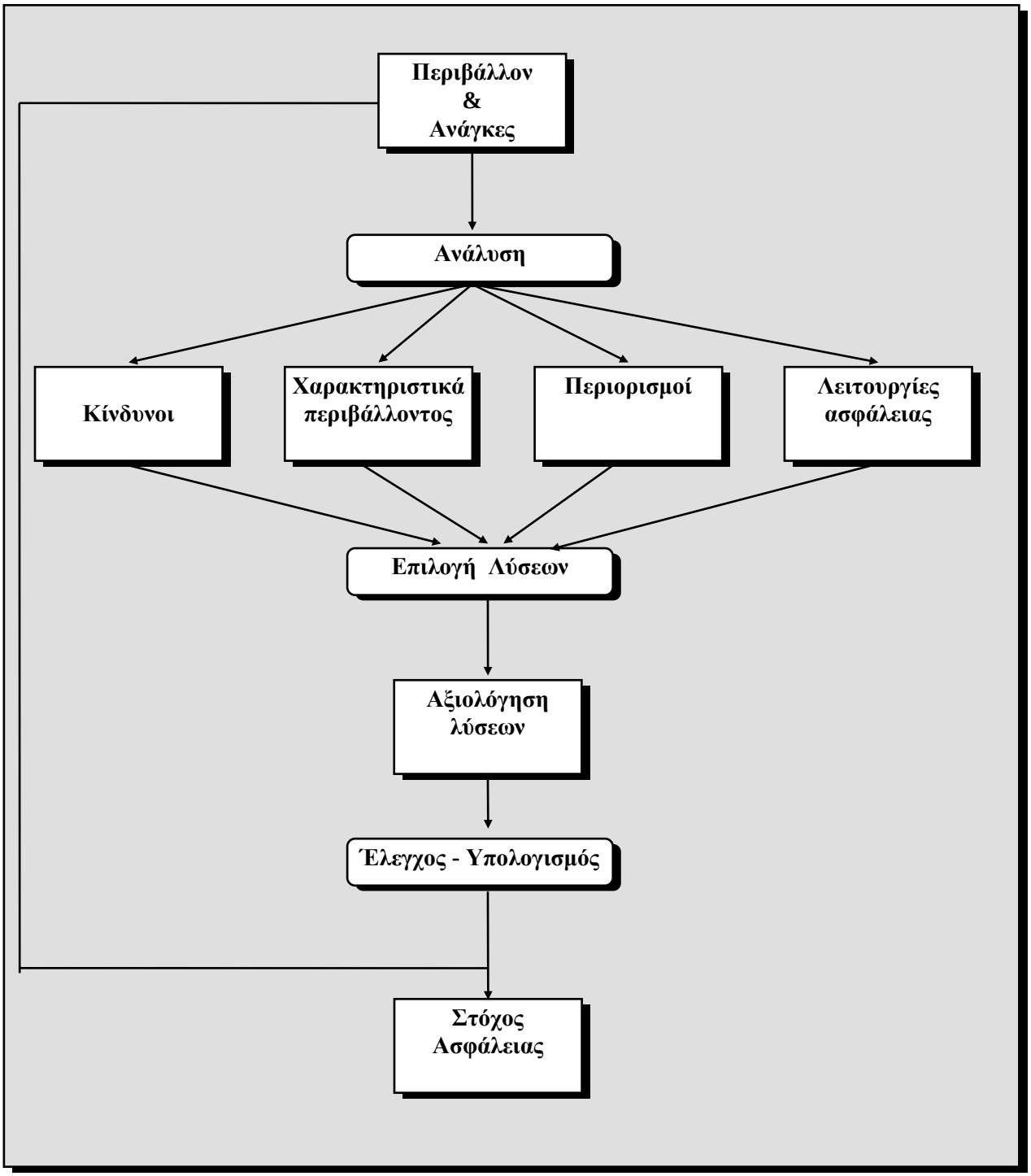
Ο κύριος χώρος εφαρμογής της κρυπτολογίας ήταν οι στρατιωτικές και διπλωματικές επικοινωνίες. Η ραγδαία όμως εξέλιξη της τεχνολογίας των υπολογιστικών συστημάτων και η εμφάνιση των δικτύων που διευκόλυναν τη μετάδοση και την καταχώρηση των πληροφοριών, διεύρυνε ακόμα περισσότερο τους χώρους εφαρμογής της κρυπτολογίας λόγω της αυξημένης ανάγκης για προστασία αυτών των πληροφοριών. Ειδικότερα, η προστασία των πληροφοριών παρέχεται μέσω των λειτουργιών ασφάλειας (security services) ενός συστήματος ασφάλειας (security system), που στόχο (security target) έχει να ικανοποιήσει, σε όσο το δυνατόν μεγαλύτερο βαθμό, τις ανάγκες των χρηστών του συστήματος, λαμβάνοντας υπόψη τα χαρακτηριστικά του συγκεκριμένου περιβάλλοντος. Στο σχήμα 1 παρουσιάζεται η διαδικασία για την επίτευξη ενός στόχου ασφάλειας.

Οι πιο βασικές λειτουργίες ασφάλειας είναι η αυθεντικοποίηση (authentication), η εμπιστευτικότητα και ακεραιότητα των δεδομένων (data confidentiality and integrity), ο έλεγχος πρόσβασης (access control) και ο καταλογισμός ευθύνης (non-repudiation) [Jan91, Sim91,Nist800]. Πιο συγκεκριμένα:

⇒ Η *αυθεντικοποίηση* αποβλέπει στην απόδειξη της ταυτότητας μιας οντότητας (χρήστη, μηχάνημα) του συστήματος.

⇒ Η *εμπιστευτικότητα των δεδομένων* αποβλέπει στην αποτροπή της τυχαίας ή σκόπιμης αποκάλυψή τους.

⇒ Η *ακεραιότητα των δεδομένων* αποβλέπει στην προστασία τους από πιθανή ή ενδεχόμενη τροποποίησή τους από μη εξουσιοδοτημένους χρήστες, είτε βρίσκονται αποθηκευμένα, είτε μεταφέρονται μέσα από τους δίαυλους επικοινωνίας.



Σχήμα 1. Διαδικασία επίτευξης στόχου ασφάλειας

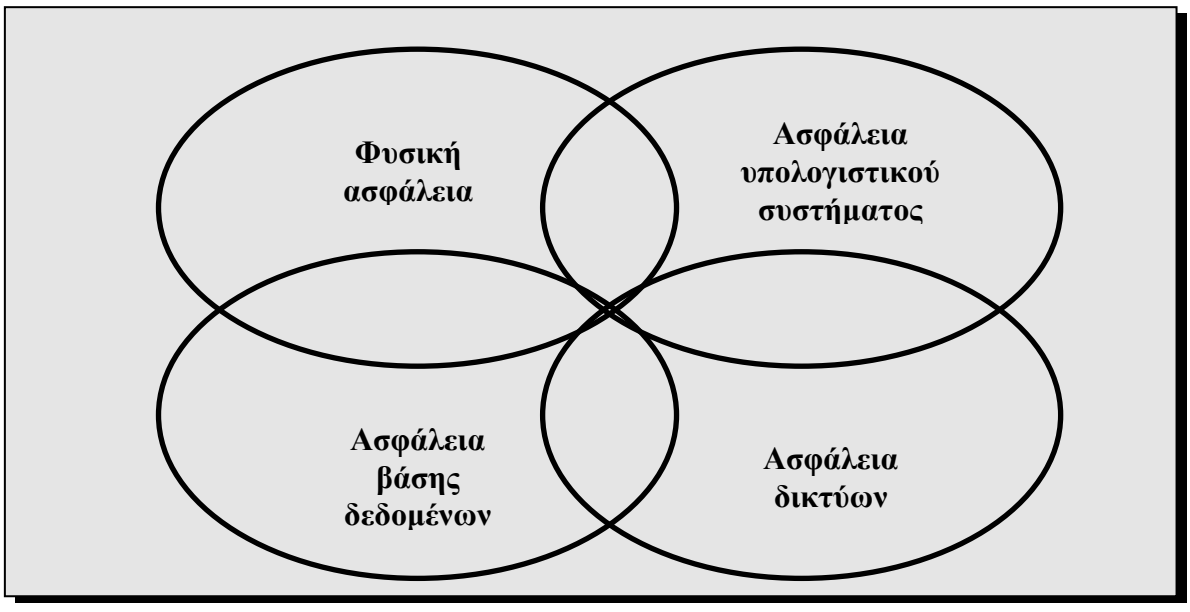
⇒ Ο *έλεγχος πρόσβασης* αποβλέπει στον καθορισμό του είδους πρόσβασης που μπορεί να έχει κάθε χρήστης στα δεδομένα.

⇒ Ο *καταλογισμός ευθύνης* αποβλέπει στον προσδιορισμό της ευθύνης για την αποστολή και την παραλαβή των δεδομένων.

1.3 Συνιστώσες του προβλήματος ασφάλειας

Το πρόβλημα της προστασίας των δεδομένων και των πληροφοριών, που αποθηκεύονται και διαχειρίζονται από το σύστημα, μπορεί να αναλυθεί σε τέσσερις συνιστώσες, σχήμα 2.:

– Τη *φυσική ασφάλεια* (physical security) που συνίσταται στην προστασία του συστήματος από φυσικές καταστροφές όπως φωτιά, πλημμύρες, σεισμός κλπ



Σχήμα 2. Οι τέσσερις βασικές συνιστώσες ενός συστήματος ασφάλειας.

-

- Τη *ασφάλεια του υπολογιστικού συστήματος* (computer security) που συνίσταται στην προστασία των πληροφοριών και των δεδομένων, που έχουν άμεση σχέση με το λειτουργικό σύστημα.

- Την *ασφάλεια της βάσης δεδομένων* (database security) που συνίσταται στην προστασία των δεδομένων και των πληροφοριών, που είναι αποθηκευμένες στη βάση δεδομένων.

- Την *ασφάλεια των δικτύων* (network security) που συνίσταται στην προστασία των δεδομένων του συστήματος, που διακινούνται μέσα στους δίαυλους επικοινωνίας των δικτύων.

Από το σχήμα 2, διαφαίνεται ότι οι συνιστώσες αυτές δεν είναι ανεξάρτητες μεταξύ τους αλλά, η μία επηρεάζει την άλλη. Η ασφάλεια ενός συστήματος μπορεί να παρομοιαστεί με μία αλυσίδα που εξαρτάται από την ανθεκτικότητα του κάθε κρίκου της, ενώ η αποτελεσματικότητά της είναι ίση με την αποτελεσματικότητα του πιο αδύναμου κρίκου της.

Συνεπώς, η ανάλυση, ο σχεδιασμός και η υλοποίηση της μιας συνιστώσας θα πρέπει να λαμβάνει υπόψη την ανάλυση, τον σχεδιασμό και την υλοποίηση των άλλων, έτσι ώστε το σύστημα ασφάλειας να είναι αποτελεσματικό. Για παράδειγμα, εάν δεν δοθεί μεγάλη βαρύτητα στην ασφάλεια των δικτύων, τότε υπάρχει μεγάλη πιθανότητα κλοπής ή οποιασδήποτε άλλη μορφής παρέμβασης στις πληροφορίες, καθώς αυτές θα διακινούνται μέσα στο δίκτυο, με αποτέλεσμα οι διαδικασίες προστασίας να θεωρηθούν αναποτελεσματικές και για τις άλλες συνιστώσες.

Ενας άλλος τρόπος καθορισμού των συνιστωσών ενός συστήματος ασφαλείας είναι ο διαχωρισμός σε λογική και φυσική ασφάλεια. Στην λογική ασφάλεια περιλαμβάνονται η ασφάλεια του υπολογιστικού συστήματος, η ασφάλεια των βάσεων δεδομένων και η ασφάλεια δικτύων.

-

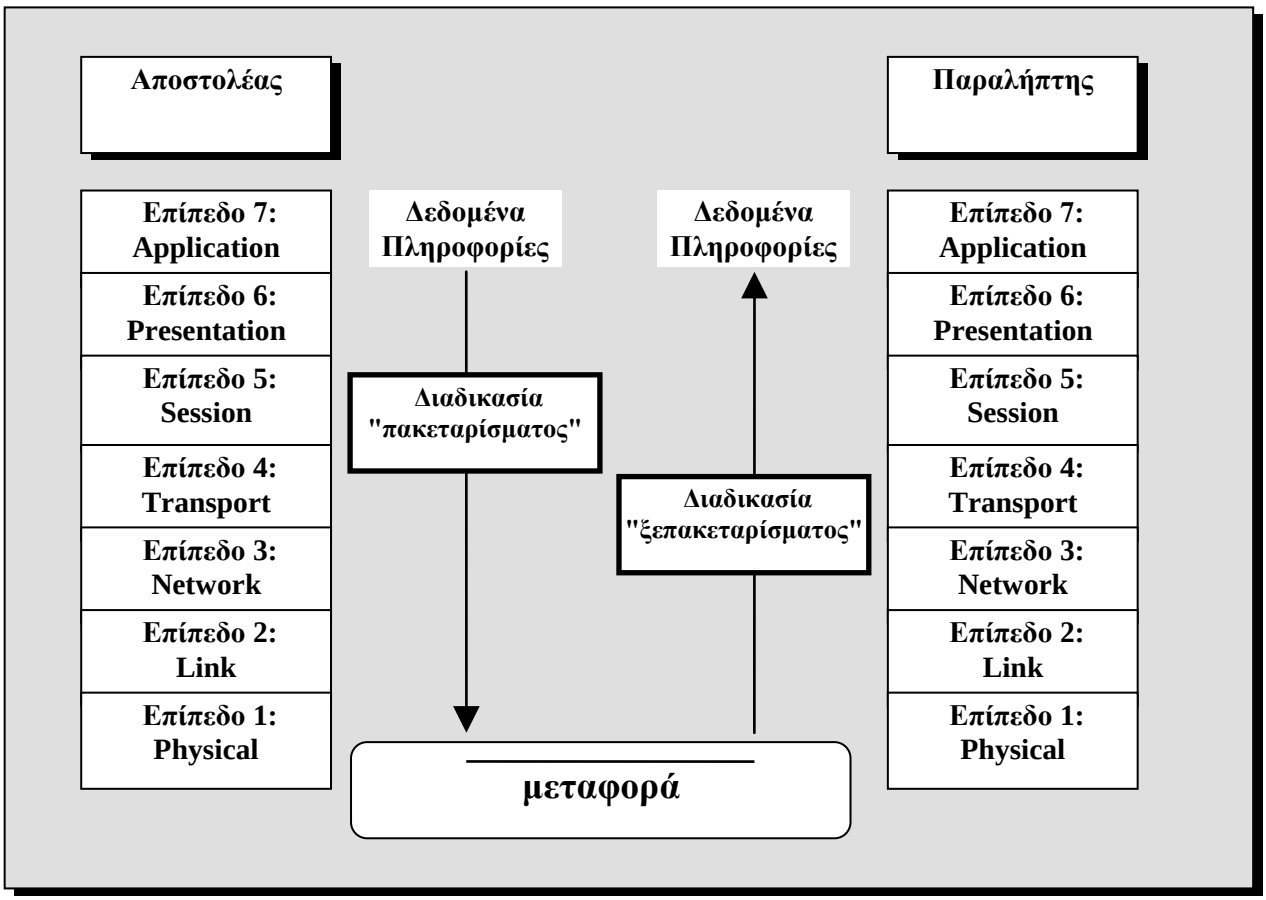
1.4 Ασφάλεια δικτύων

Η ασφάλεια των δικτύων και γενικότερα των επικοινωνιών αφορά, κυρίως την προστασία των δεδομένων και πληροφοριών, τα οποία ανταλλάσσονται από τους χρήστες του. Οταν δύο ή περισσότεροι χρήστες επιθυμούν να επικοινωνήσουν μεταξύ τους μέσω ενός δικτύου με σκοπό την ανταλλαγή δεδομένων και πληροφοριών, τότε ένα πρωτόκολλο επικοινωνίας αναλαμβάνει τη μεταφορά των δεδομένων και πληροφοριών αυτών.

Το πρωτόκολλο επικοινωνίας καθορίζει τη μορφή και τα χαρακτηριστικά που θα πρέπει να έχουν τα δεδομένα και οι πληροφορίες, ώστε να μπορούν να μεταφερθούν μέσα από το δίκτυο. Για το λόγο αυτό, χρησιμοποιούνται οι διαδικασίες "πακεταρίσματος" (packaging) και "ξεπακεταρίσματος" (stripping). Στην πρώτη, το πρωτόκολλο επικοινωνίας προσθέτει εκείνα τα απαιτούμενα στοιχεία, ώστε να είναι δυνατή η μεταφορά των δεδομένων και των πληροφοριών μέσω δικτύου. Αντιστρόφως, στη δεύτερη, το πρωτόκολλο επικοινωνίας αφαιρεί όλα εκείνα τα στοιχεία, ώστε τα δεδομένα και οι πληροφορίες να φτάσουν στον παραλήπτη στην καθορισμένη μορφή τους.

Σύμφωνα με το Διεθνή οργανισμό προτύπων (International Standards Organisation ISO) έχει προταθεί ένα πρωτόκολλο επικοινωνίας γνωστό ως OSI (Open System Interconnect), το οποίο περιλαμβάνει επτά επίπεδα με τα οποία επιτυγχάνεται το "πακετάρισμα" και "ξεπακετάρισμα" των δεδομένων και πληροφοριών που μεταφέρονται μέσω ενός δικτύου. Στο σχήμα 3 παρουσιάζονται το "πακετάρισμα" και "ξεπακετάρισμα" στο πρωτόκολλο επικοινωνίας OSI.

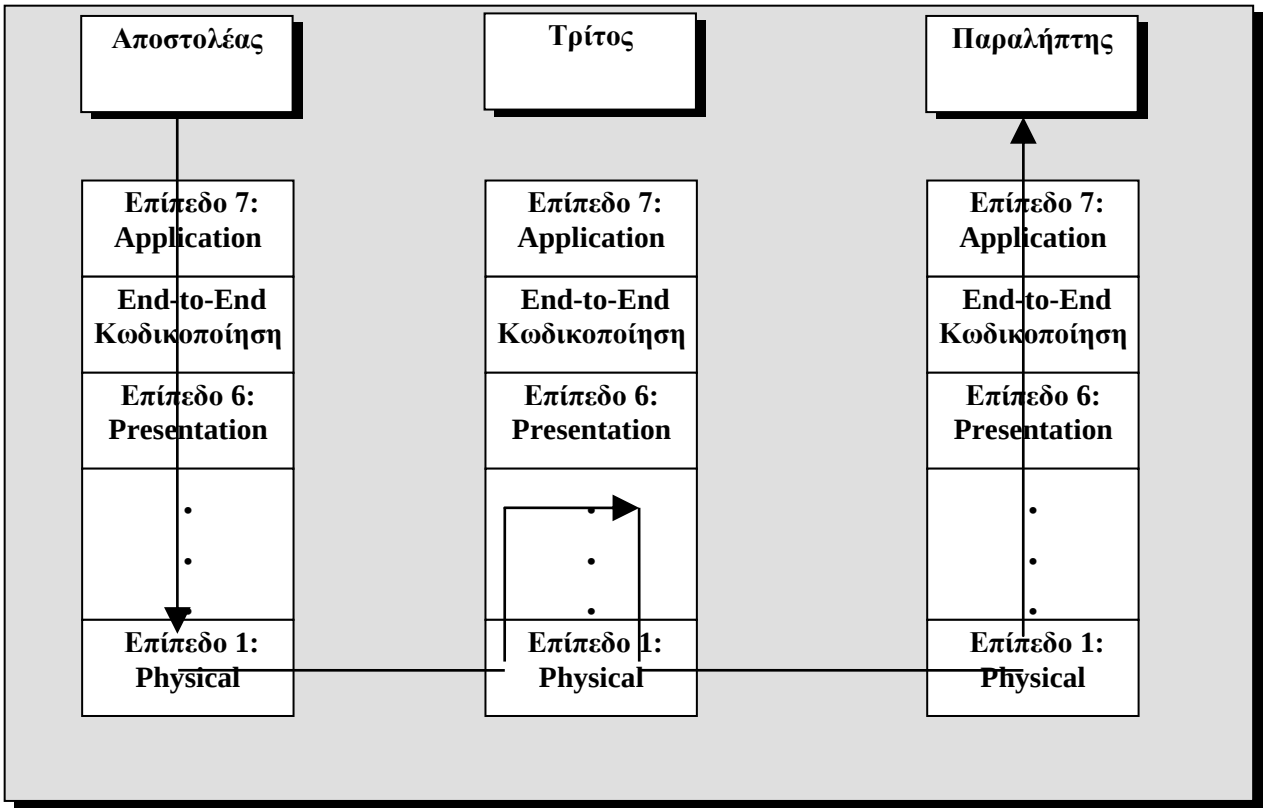
Η προστασία των δεδομένων και πληροφοριών, που μεταφέρονται μέσω δικτύου, καθορίζεται κυρίως από το τρόπο και την τεχνική κωδικοποίησης των δεδομένων και πληροφοριών μέσα στο δίκτυο. Οι τεχνικές κωδικοποίησης ενός δικτύου είναι: end-to-end και link.



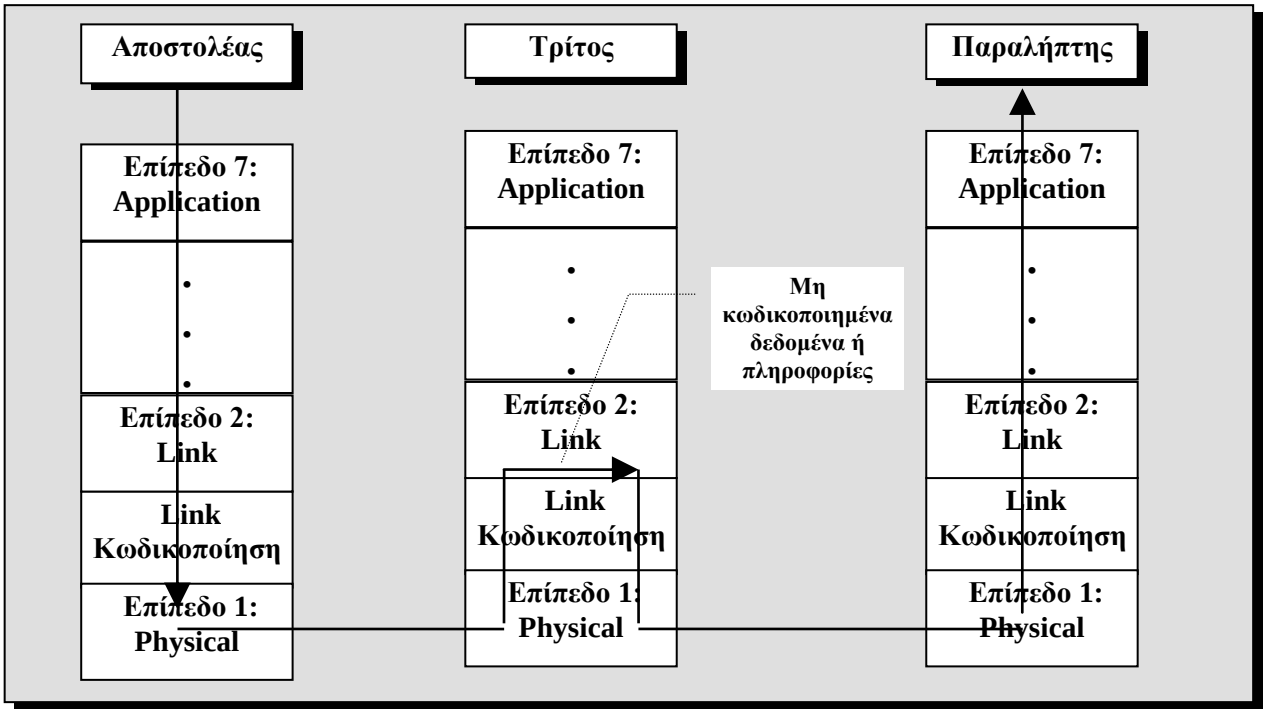
Σχήμα 3 Πρωτόκολλο επικοινωνίας OSI

Κατά την κωδικοποίηση end-to-end, τα δεδομένα και οι πληροφορίες κωδικοποιούνται στο επίπεδο εφαρμογής (application) του OSI. Αντίθετα στη κωδικοποίηση link, τα δεδομένα και οι πληροφορίες κωδικοποιούνται στο επίπεδο σύνδεσης (link).

Τα πιθανά προβλήματα που μπορεί να προκύψουν με την προστασία των δεδομένων και πληροφοριών με τη χρησιμοποίηση των δύο τεχνικών κωδικοποίησης παρουσιάζονται στα σχήματα 4 και 5 όπου θεωρούμε ότι ο αποστολέας και ο παραλήπτης δεν έχουν άμεση σύνδεση, αλλά η επικοινωνία τους πραγματοποιείται μέσω τρίτου.



Σχήμα 4. End-to-end κωδικοποίηση στο OSI



Σχήμα 5. Link κωδικοποίηση στο OSI

-

Οι λειτουργίες ασφάλειας μπορούν να παρέχονται σε περισσότερα από ένα επίπεδα του OSI. Καθώς θα πρέπει, η επίπτωση στη συνολική αποδοτικότητα ενός δικτύου να είναι η ελάχιστη δυνατή, έχει προταθεί ότι οι λειτουργίες ασφάλειας θα πρέπει να παρέχονται κυρίως στο επίπεδο application [Gas88, Kir89] . Στον πίνακα 1 παρουσιάζεται η δυνατότητα παροχής των λειτουργιών ασφάλειας στα επίπεδα του OSI.

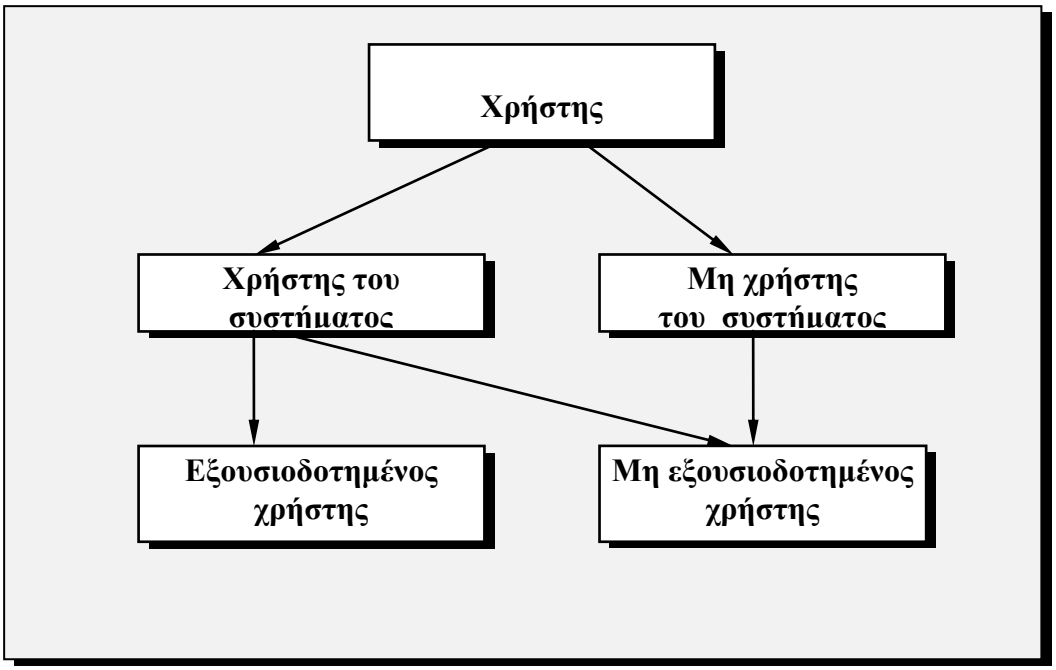
Επίπεδο	**Λειτουργία**
7: Application	αυθεντικοποίηση, ακεραιότητα και εμπιστευτικότητα δεδομένων, καταλογισμός ευθύνης, έλεγχος πρόσβασης
6: Presentation	εμπιστευτικότητα δεδομένων
5: Session	
4: Transport	αυθεντικοποίηση, ακεραιότητα και εμπιστευτικότητα δεδομένων, έλεγχος πρόσβασης
3: Network	αυθεντικοποίηση, ακεραιότητα και εμπιστευτικότητα δεδομένων, έλεγχος πρόσβασης
2: Link	αυθεντικοποίηση, ακεραιότητα και εμπιστευτικότητα δεδομένων, έλεγχος πρόσβασης
1: Physical	εμπιστευτικότητα δεδομένων

Πίνακας 1. Λειτουργίες ασφάλειας και επίπεδα OSI.

Για τη συνέχεια, θεωρούμε ότι η τεχνική κωδικοποίησης end-to-end εφαρμόζεται στο δίκτυο, μέσω του οποίου δύο ή περισσότεροι χρήστες ανταλλάσσουν δεδομένα και πληροφορίες. Για τα προτεινόμενα κρυπτογραφικά πρωτόκολλα που παρουσιάζονται στη συνέχεια, θεωρούμε ότι και αυτά εφαρμόζονται σε δίκτυα με κωδικοποίηση end-to-end.

1.5 Χρήστες του συστήματος

Οι χρήστες που σχετίζονται μ' ένα σύστημα μπορούν να χωρισθούν σύμφωνα με την ιεραρχία που παρουσιάζεται στο σχήμα 6. Στην ιεραρχία αυτή, κάθε χρήστης μπορεί να ανήκει στην ομάδα των χρηστών του συστήματος ή σ' εκείνη των μη χρηστών του συστήματος.



Σχήμα 6 Ιεραρχία χρηστών.

Ένας χρήστης του συστήματος έχει δικαιώματα και υποχρεώσεις που καθορίζονται με βάση την θέση που κατέχει μέσα σ' αυτό. Στην περίπτωση που αυτός ενεργεί σύμφωνα με τις δυνατότητες που του έχουν δοθεί τότε, χαρακτηρίζεται ως *εξουσιοδοτημένος χρήστης* (authorised user) του συστήματος. Στην αντίθετη περίπτωση ορίζεται ως *μη εξουσιοδοτημένος χρήστης* (unauthorised user). Στην ομάδα των μη εξουσιοδοτημένων χρηστών ανήκουν και οι μη χρήστες του συστήματος με τη διαφορά ότι αυτοί δεν έχουν κανένα δικαίωμα ή υποχρέωση μέσα στο σύστημα.

-

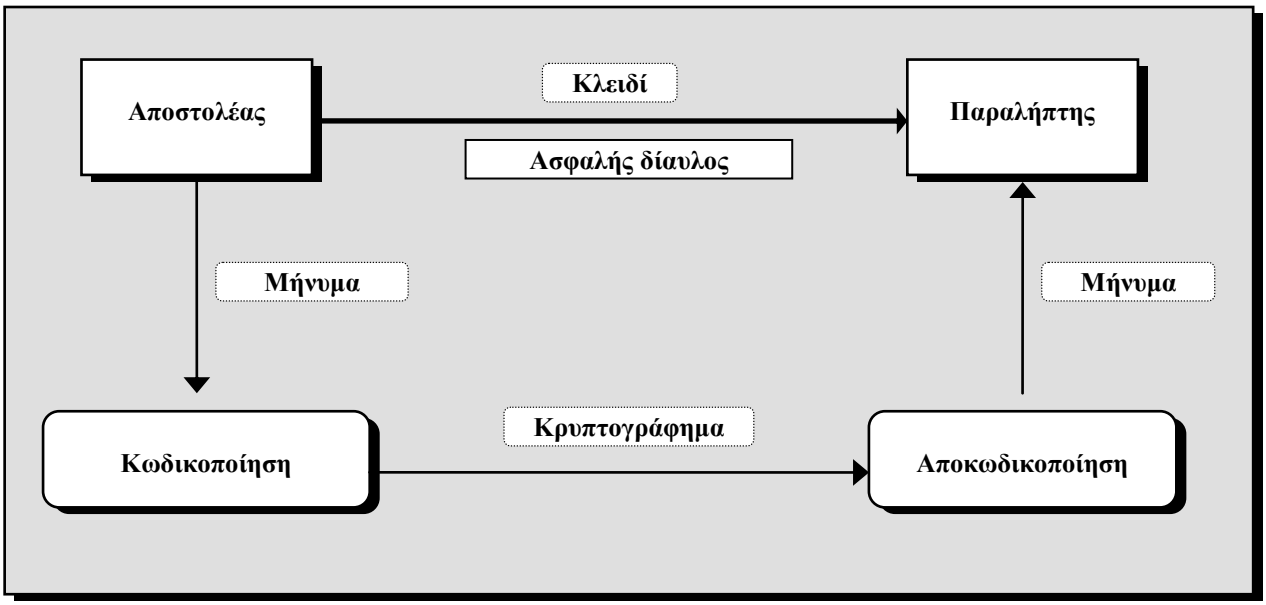
1.6 Κρυπτογραφικά συστήματα

Κρυπτογραφικό σύστημα (cryptographic system) ή *κρυπτοσύστημα* (cryptosystem) ονομάζεται κάθε σύστημα που αποβλέπει στην εφαρμογή των διαδικασιών κρυπτογραφίας [Sch94, Sim91]. Ο χρήστης ενός κρυπτογραφικού συστήματος έχει στην διάθεσή του ένα ή περισσότερα κλειδιά, τα οποία χρησιμοποιεί προκειμένου να μετασχηματίσει ένα απλό κείμενο (plaintext) σε κρυπτογράφημα (ciphertext) και αντιστρόφως. Ο μετασχηματισμός του απλού κειμένου σε κρυπτογράφημα είναι η διαδικασία κωδικοποίησης (encryption), ενώ ο μετασχηματισμός του κρυπτογραφήματος σε απλό κείμενο είναι η διαδικασία αποκωδικοποίησης (decryption)[Bra87, Dif76, Sch94, Sim91].

Γενικά, τα κρυπτογραφικά συστήματα χωρίζονται σε δύο μεγάλες κατηγορίες, ανάλογα με τον αριθμό των κλειδιών που χρησιμοποιούνται σ' αυτά. Στην περίπτωση που το κλειδί είναι μοναδικό, δηλαδή οι χρήστες χρησιμοποιούν ένα κλειδί τόσο για την κωδικοποίηση, όσο και για την αποκωδικοποίηση, το σύστημα ονομάζεται *σύστημα μυστικού κλειδιού* (secret key system). Αντίθετα, όταν οι χρήστες χρησιμοποιούν ένα κλειδί για την κωδικοποίηση και ένα άλλο κλειδί για την αποκωδικοποίηση, τότε το σύστημα ονομάζεται *σύστημα δημοσίου κλειδιού* (public key system) [Bra87, Cop87, Dif76, Jan91, Ned78, Sch94, Sim91].

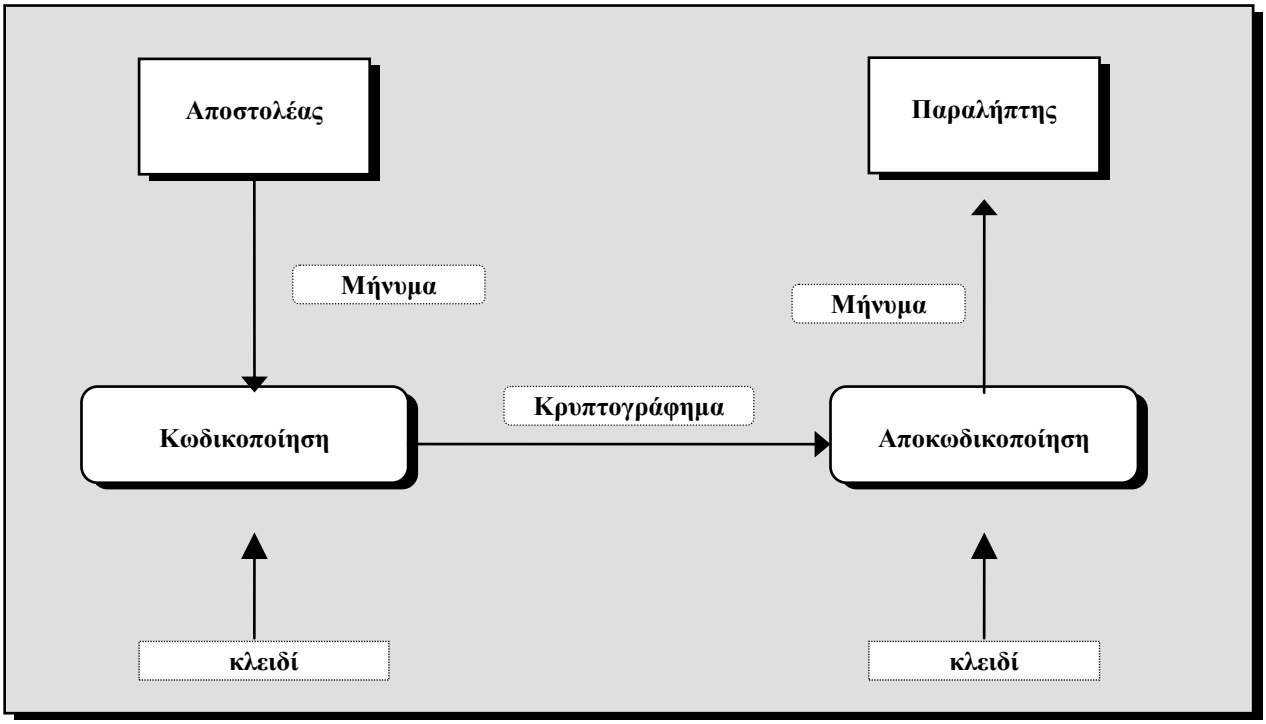
Το κύριο χαρακτηριστικό των συστημάτων μυστικού κλειδιού, είναι η ύπαρξη ενός ασφαλούς δίαυλου επικοινωνίας για την αποστολή του μυστικού κλειδιού από τον αποστολέα στον παραλήπτη. Στο σχήμα 7 παρουσιάζεται η δομή ενός κρυπτογραφικού συστήματος μυστικού κλειδιού. Λόγω της χρήσης ενός μόνο κλειδιού, τα συστήματα μυστικού κλειδιού ονομάζονται και *συστήματα ενός κλειδιού* (one-key cryptosystems) ενώ λόγω της χρήσης του ίδιου κλειδιού από τους χρήστες ονομάζονται και *συμμετρικά* (symmetric) [Sim91]. Το πιο γνωστό σύστημα μυστικού κλειδιού είναι το DES (Data Encryption Standard) [ANS81].

-



Σχήμα 7. Ενα κρυπτογραφικό σύστημα μυστικού κλειδιού.

Η εμφάνιση των κρυπτογραφικών συστημάτων δημοσίου κλειδιού οφείλεται στους Diffie και Hellman που πρότειναν το πρώτο κρυπτογραφικό σύστημα δημοσίου κλειδιού [Dif76]. Στα κρυπτογραφικά συστήματα δημοσίου κλειδιού, κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιά, από τα οποία το ένα κλειδί χρησιμοποιείται στην διαδικασία κωδικοποίησης και το άλλο στην διαδικασία αποκωδικοποίησης. Το ένα από τα δύο κλειδιά, το οποίο γνωρίζει μόνο ο χρήστης ονομάζεται μυστικό κλειδί (secret key), ενώ το άλλο κλειδί, που έχει δημοσιοποιηθεί και στους υπόλοιπους χρήστες του συστήματος, ονομάζεται δημόσιο κλειδί (public key). Τα δύο κλειδιά μπορούν να χρησιμοποιηθούν στις διαδικασίες κωδικοποίησης και αποκωδικοποίησης. Στο σχήμα 8 παρουσιάζεται η δομή ενός κρυπτογραφικού συστήματος δημοσίου κλειδιού.



Σχήμα 8. Ενα κρυπτογραφικό σύστημα δημοσίου κλειδιού.

Στην περίπτωση που το μυστικό κλειδί του αποστολέα χρησιμοποιείται στην κωδικοποίηση, ενώ το δημόσιο κλειδί του αποστολέα στην αποκωδικοποίηση, τότε επιτυγχάνεται αυθεντικοποίηση του αποστολέα, όχι όμως και εμπιστευτικότητα του μηνύματος που ανταλλάσσεται.

Στην περίπτωση που το μυστικό κλειδί του παραλήπτη χρησιμοποιείται στην αποκωδικοποίηση και το δημόσιο κλειδί του παραλήπτη στην κωδικοποίηση, τότε επιτυγχάνεται εμπιστευτικότητα του μηνύματος, όχι όμως και αυθεντικοποίηση του αποστολέα. Εάν το κρυπτογραφικό σύστημα θα πρέπει να παρέχει και τις δύο λειτουργίες ασφάλειας, τότε θα πρέπει να υπάρξει συνδυασμός των δημοσίων και μυστικών κλειδιών, τόσο του αποστολέα, όσο και του παραλήπτη. Για παράδειγμα, η επίτευξη των λειτουργιών αυθεντικοποίησης του αποστολέα και εμπιστευτικότητας του μηνύματος, έχει ως προϋπόθεση ότι ο αποστολέας θα πρέπει να χρησιμοποιήσει το μυστικό κλειδί του και το δημόσιο κλειδί του παραλήπτη στην

κωδικοποίηση του μηνύματος. Αντίστοιχα, ο παραλήπτης θα πρέπει να χρησιμοποιήσει το δικό του μυστικό κλειδί και το δημόσιο κλειδί του αποστολέα στην διαδικασία αποκωδικοποίησης του μηνύματος. Για αυτό, στο σχήμα 2 δεν διευκρινίζεται ποιο είναι το κλειδί που χρησιμοποιείται στην διαδικασία της κωδικοποίησης και της αποκωδικοποίησης. Το κλειδί ή ο συνδυασμός των κλειδιών που χρησιμοποιούνται, τόσο στην διαδικασία κωδικοποίησης, όσο και της αποκωδικοποίησης καθορίζονται από τις απαιτήσεις του συστήματος και των χρηστών που συμμετέχουν στη συγκεκριμένη διαδικασία της επικοινωνίας. Για το δημόσιο και το μυστικό κλειδί κάθε χρήστη υπάρχει μία σχέση, η οποία επιτρέπει τον υπολογισμό του δημοσίου, όταν είναι γνωστό το μυστικό, ενώ το αντίθετο, θεωρείται γενικά υπολογιστικά αδύνατο. Σε αντίθεση με τα συστήματα μυστικού κλειδιού, στα συστήματα δημοσίου κλειδιού δεν είναι απαραίτητη η ύπαρξη ενός ασφαλούς διαύλου επικοινωνίας μεταξύ αποστολέα και παραλήπτη. Το πιο γνωστό σύστημα δημοσίου κλειδιού είναι το RSA σύστημα [Riv78].

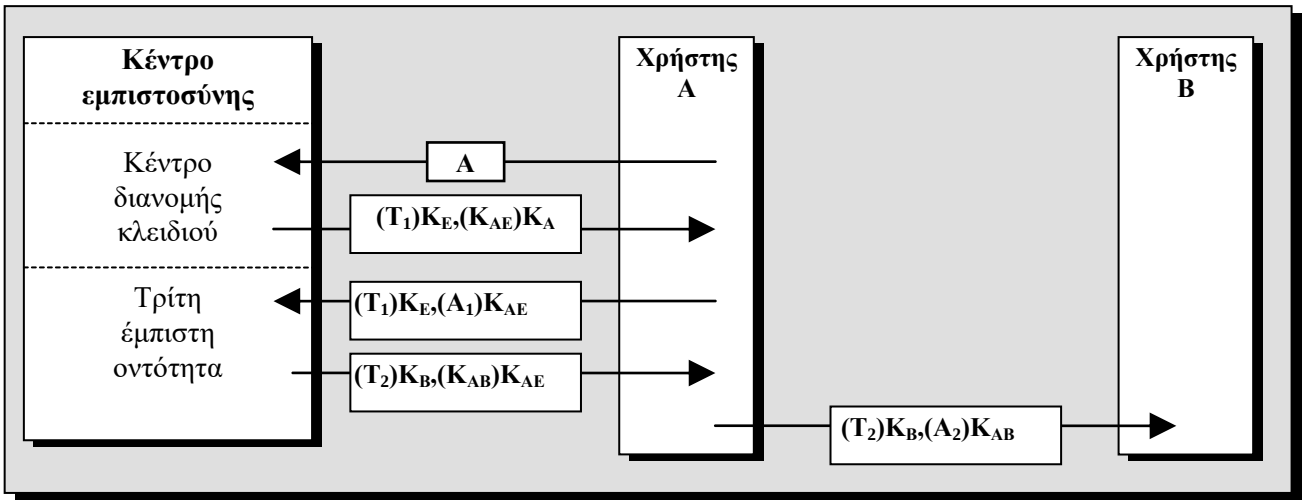
1.7 Κρυπτογραφικά πρωτόκολλα μεταφοράς κλειδιού

Τα *κρυπτογραφικά πρωτόκολλα μεταφοράς κλειδιού* ορίζονται ως τα πρωτόκολλα εκείνα όπου το κοινό μυστικό κλειδί που χρησιμοποιείται από τους χρήστες που επιθυμούν να επικοινωνήσουν, επιλέγεται από έναν χρήστη, ο οποίος το "μεταφέρει" στους υπόλοιπους. Ο χρήστης μπορεί, είτε να συμμετέχει στην επικοινωνία, είτε να είναι μια ανεξάρτητη αρχή. Βασικό χαρακτηριστικό των πρωτοκόλλων αυτών είναι η επιλογή του χρήστη που θα αναλάβει τη "μεταφορά" και η κοινή αποδοχή του από τους άλλους. Ο συγκεκριμένος χρήστης θα πρέπει να είναι αποδεκτός από όλους τους υπόλοιπους, αφού θα γνωρίζει το κλειδί πριν το μάθουν οι υπόλοιποι χρήστες, για να το χρησιμοποιήσουν στην κωδικοποίηση / αποκωδικοποίηση των μηνυμάτων.

Χαρακτηριστικό παράδειγμα κρυπτογραφικού πρωτοκόλλου μεταφοράς κλειδιού είναι εκείνο των Needham και Schroeder [Ned78] το οποίο χρησιμοποιείται στο σύστημα αυθεντικοποίησης Kerberos [Lec90, Ker90, Kohl, Koh91,Kokl93]. Στο σχήμα 9 παρουσιάζεται το σύστημα Kerberos, όπου:

T : ticket, που περιλαμβάνει τον χρήστη, τη χρονική διάρκεια που ισχύει και ένα μυστικό κλειδί

$(X)K_i$: η πληροφορία X έχει κωδικοποιηθεί με το κλειδί K του χρήστη i. Το κλειδί αυτό μπορεί να χρησιμοποιηθεί από τον χρήστη i για να αποκωδικοποιήσει την πληροφορία, ενώ από τους άλλους χρήστες μπορεί να χρησιμοποιηθεί μόνο όταν θέλουν να κωδικοποιήσουν τις πληροφορίες που θέλουν να στείλουν μυστικά στον χρήστη i



Σχήμα 9. Το σύστημα Kerberos.

Τα κύρια μειονεκτήματα του πρωτοκόλλου αυτού είναι ότι το κέντρο εμπιστοσύνης α) πρέπει να είναι συνεχώς διαθέσιμο (on-line), β) μπορεί να αποκαλύψει το κοινό κλειδί σε χρήστες που δεν συμμετέχουν στην επικοινωνία, οποιαδήποτε χρονική στιγμή, γ) μπορεί να παρεμβάλλεται στην επικοινωνία των δύο χρηστών τροποποιώντας τα μηνύματα και δ) μπορεί να υποκλέπτει πληροφορίες

Μια παραλλαγή του συστήματος αυτού έχει προταθεί από τους Leighton και Micali [Lei94], στην οποία όμως παραμένει η απαίτηση ότι το κέντρο εμπιστοσύνης πρέπει να είναι συνεχώς διαθέσιμο.

-

Στα πρωτόκολλα εκείνα που το κέντρο εμπιστοσύνης έχει τον απόλυτο έλεγχο, ανήκουν και εκείνα στα οποία το κέντρο αντιπροσωπεύεται από πολλούς χρήστες. Χαρακτηριστικό παράδειγμα είναι το πρωτόκολλο που έχει προταθεί από τους Yahalom, Klein και Beth [Yah93]. Στην ίδια κατηγορία πρωτοκόλλων περιλαμβάνονται και εκείνα που χρησιμοποιούν πολλά κέντρα εμπιστοσύνης, ώστε στη διανομή κοινού μυστικού κλειδιού να είναι δυνατή η συμμετοχή όλων, χωρίς όμως να υπάρχει η δυνατότητα αποκάλυψης. Ο Gong έχει προτείνει ένα αντίστοιχο πρωτόκολλο [Gon93].

Η δυνατότητα ενός κέντρου εμπιστοσύνης να γνωρίζει τα κοινά μυστικά κλειδιά αποτελεί πρόβλημα, εφόσον τα αποκάλυπτε σε τρίτους. Για το λόγο αυτό προτάθηκαν πρωτόκολλα, τα οποία περιορίζουν τον ρόλο του κέντρου εμπιστοσύνης στην επιλογή των βασικών παραμέτρων του συστήματος. Σε πολλά από αυτά τα πρωτόκολλα, την δημιουργία του κοινού μυστικού κλειδιού αναλαμβάνει ένας από τους χρήστες που επιθυμεί να επικοινωνήσει με τους άλλους.

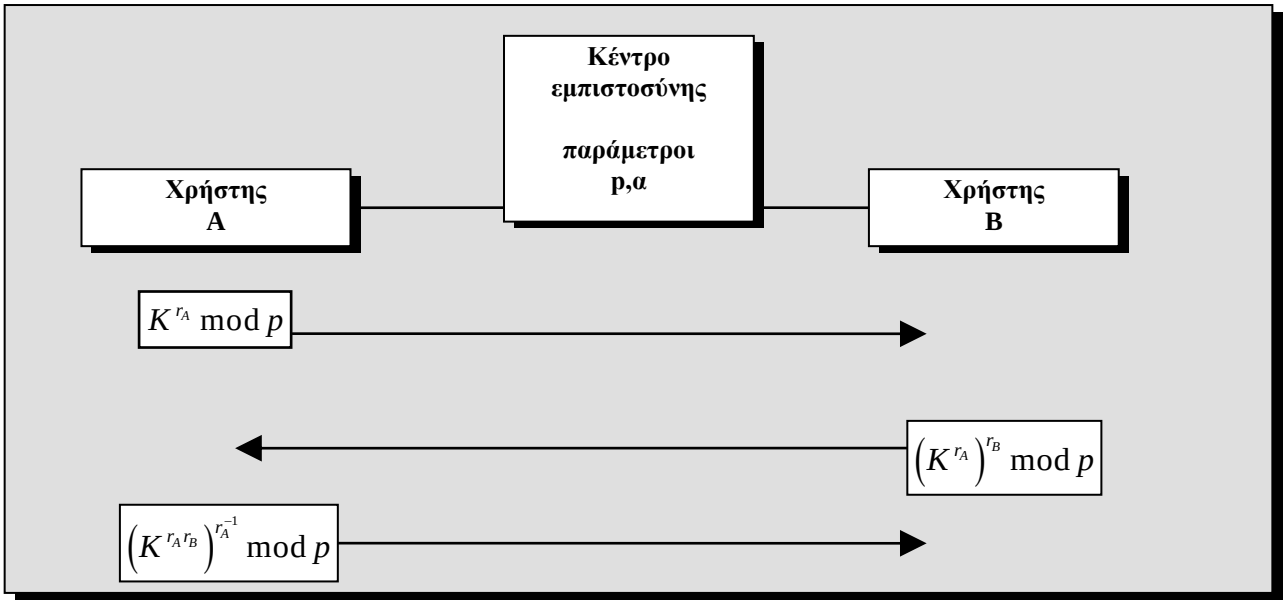
Στην περίπτωση αυτή, το μειονέκτημα είναι ότι ο χρήστης γνωρίζει από την αρχή, το κοινό μυστικό κλειδί. Αυτό όμως θεωρείται περισσότερο αποδεκτό, καθώς οι επιπτώσεις της αποκάλυψης του κοινού κλειδιού θα επιβαρύνουν και τον ίδιο. Δεν ισχύει όμως το ίδιο, όταν το κέντρο εμπιστοσύνης είναι μια ανεξάρτητη αρχή που δεν συμμετέχει σε επικοινωνίες και κατά συνέπεια οι επιπτώσεις επιβαρύνουν μόνο τους χρήστες που επικοινωνούν. Αντιπροσωπευτικό παράδειγμα τέτοιου πρωτοκόλλου είναι εκείνο που προτάθηκε από τον Shamir [Sha85] και παρουσιάζεται στο σχήμα 10, στο οποίο οι χρήστες που επιθυμούν να επικοινωνήσουν δεν χρειάζεται να έχουν αρχικά στην κατοχή τους κάποιο δημόσιο ή κοινά μυστικό κλειδί.

Στο πρωτόκολλο αυτό, το κέντρο εμπιστοσύνης έχει ως μοναδικό ρόλο την επιλογή των παραμέτρων *p, α* του συστήματος, όπου *p* είναι ένας πρώτος αριθμός και *α* είναι ένας γεννήτορας του Z_p^*. Στην περίπτωση που δύο χρήστες *A* και *B* επιθυμούν να επικοινωνήσουν μεταξύ τους, επιλέγουν από έναν τυχαίο αριθμό r_A και r_B αντίστοιχα, με $r_A, r_B \in [1,p-2]$ είναι

πρώτοι αριθμοί ως προς το *p-1*. Ο υπολογισμός του κοινού μυστικού κλειδιού μεταξύ των χρηστών πραγματοποιείται με τον ακόλουθο τρόπο:

α) ο χρήστης *A* επιλέγει έναν αριθμό $K \in [1,p-1]$ και στέλνει στο χρήστη *B* το $K^{r_A} \bmod p$.

β) Ο χρήστης *B* στέλνει στον *A* το $\left(K^{r_A}\right)^{r_B} \bmod p$.



Σχήμα 10. Το κρυπτογραφικό πρωτόκολλο μεταφοράς κλειδιού του Shamir

γ) Ο χρήστης Α υψώνει το μήνυμα που έλαβε στην δύναμη $r_A^{-1} \bmod p-1$ και στέλνει το αποτέλεσμα $K^{r_B} \bmod p$ στον χρήστη *B*, ο οποίος με την σειρά του το υψώνει στην δύναμη $r_B^{-1} \bmod p-1$. Ως αποτέλεσμα των παραπάνω υπολογισμών είναι ο χρήστης *B* να αποκτήσει το κοινό μυστικό κλειδί *K* που είχε επιλέξει αρχικά ο χρήστης Α.

Το πρωτόκολλο αυτό, παρέχει μυστικότητα στον υπολογισμό του κοινού μυστικού κλειδιού στην περίπτωση, που κάποιος τρίτος προσπαθεί μέσα από τα μηνύματα που οι δύο

χρήστες ανταλλάσσουν να ανακαλύψει το κοινό μυστικό κλειδί. Ως μειονέκτημα του θεωρείται το ότι δεν παρέχει αυθεντικοποίηση των χρηστών που συμμετέχουν στην επικοινωνία.

1.8 Κρυπτογραφικά πρωτόκολλα συμφωνίας κλειδιού

Τα κρυπτογραφικά πρωτόκολλα συμφωνίας κλειδιού χωρίζονται σε δύο κατηγορίες ανάλογα την συμμετοχή του κέντρου εμπιστοσύνης στην δημιουργία του κλειδιού. Ειδικότερα, το κέντρο εμπιστοσύνης μπορεί να συμμετέχει ενεργά στην δημιουργία του κοινού μυστικού κλειδιού ή να έχει περιορισμένο ρόλο, ο οποίος να αφορά μόνο τη διαχείριση του συστήματος και την επιλογή των βασικών παραμέτρων. Οπως αναφέρθηκε, και στα κρυπτογραφικά πρωτόκολλα μεταφοράς κλειδιού, η ενεργή συμμετοχή του κέντρου εμπιστοσύνης στη δημιουργία του κοινού κλειδιού έχει βασικά μειονεκτήματα. Γι' αυτό, και τα προτεινόμενα κρυπτογραφικά πρωτόκολλα που περιγράφονται στα κεφάλαια 2 και 3, δεν απαιτούν ενεργή συμμετοχή από το κέντρο εμπιστοσύνης, αλλά μόνο την επιλογή και διανομή των παραμέτρων που χρησιμοποιούνται.

1.9 Το πρόβλημα των Diffie - Hellman

Η ασφάλεια του πρωτοκόλλου των Diffie-Hellman που παρέχει αυθεντικοποίηση των χρηστών ή ανανέωση του κοινού μυστικού κλειδιού, βασίζεται στην δυσκολία υπολογισμού του αριθμού $g^{ab} \bmod p$ όταν τα p, g, $g^a \bmod p$ και $g^b \bmod p$ είναι γνωστά. Το πρόβλημα αυτό είναι γνωστό ως *πρόβλημα των Diffie-Hellman* [Dif76] και είναι παρόμοιο με το πρόβλημα του διακριτού λογάριθμου, το οποίο αφορά την εύρεση της τιμής c της ισοδυναμίας $g^c \equiv x \bmod p$, όταν είναι γνωστά τα p, x και g [Μελ95, Sch94].

Το πρόβλημα των Diffie-Hellman μπορεί να εκφραστεί και ως ακολούθως:

-

Εάν οι ακέραιοι p, a, X, Y *είναι γνωστοί, τότε να υπολογιστεί η τιμή* $X^{\log_a Y}$ *, εφόσον υπάρχει.*

Το πρόβλημα αυτό θεωρείται δύσκολο, ακόμα και εάν η ανάλυση σε γινόμενο πρώτων παραγόντων του *α* είναι γνωστή [Blu84, Bra88]. Εχει αποδειχθεί ότι, το πρόβλημα των Diffie-Hellman είναι εύκολο στην επίλυσή του, εάν και το πρόβλημα του διακριτού λογάριθμου είναι εύκολο στην επίλυσή του. Το αντίστροφο όμως δεν ισχύει, το πρόβλημα του διακριτού λογάριθμου δεν επιλύεται εύκολα, εφόσον το πρόβλημα των Diffie-Hellman επιλύεται εύκολα [Cop86, Men91, Odl84].

Στην περίπτωση που το *p* δεν είναι πρώτος αριθμός, τότε υπάρχει γενίκευση του προβλήματος, το οποίο είναι γνωστό ως *γενικευμένο πρόβλημα των Diffie-Hellman*.

1.10 Το πρωτόκολλο των Diffie - Hellman

Το πιο γνωστό κρυπτογραφικό πρωτόκολλο συμφωνίας κλειδιού δύο χρηστών, όπου το κέντρο εμπιστοσύνης έχει περιοριστεί στην επιλογή και δημοσιοποίηση των βασικών παραμέτρων, είναι το πρωτόκολλο των Diffie - Hellman [Dif76]. Στο πρωτόκολλο αυτό, κάθε χρήστης έχει στην κατοχή του ένα μυστικό κλειδί, με την βοήθεια του οποίου, υπολογίζει ένα δεύτερο κλειδί, το δημόσιο κλειδί του. Κάθε χρήστης U_i, που έχει για μυστικό κλειδί το s_i, υπολογίζει το δημόσιο κλειδί του P_i με την βοήθεια της ακόλουθης ισοδυναμίας:

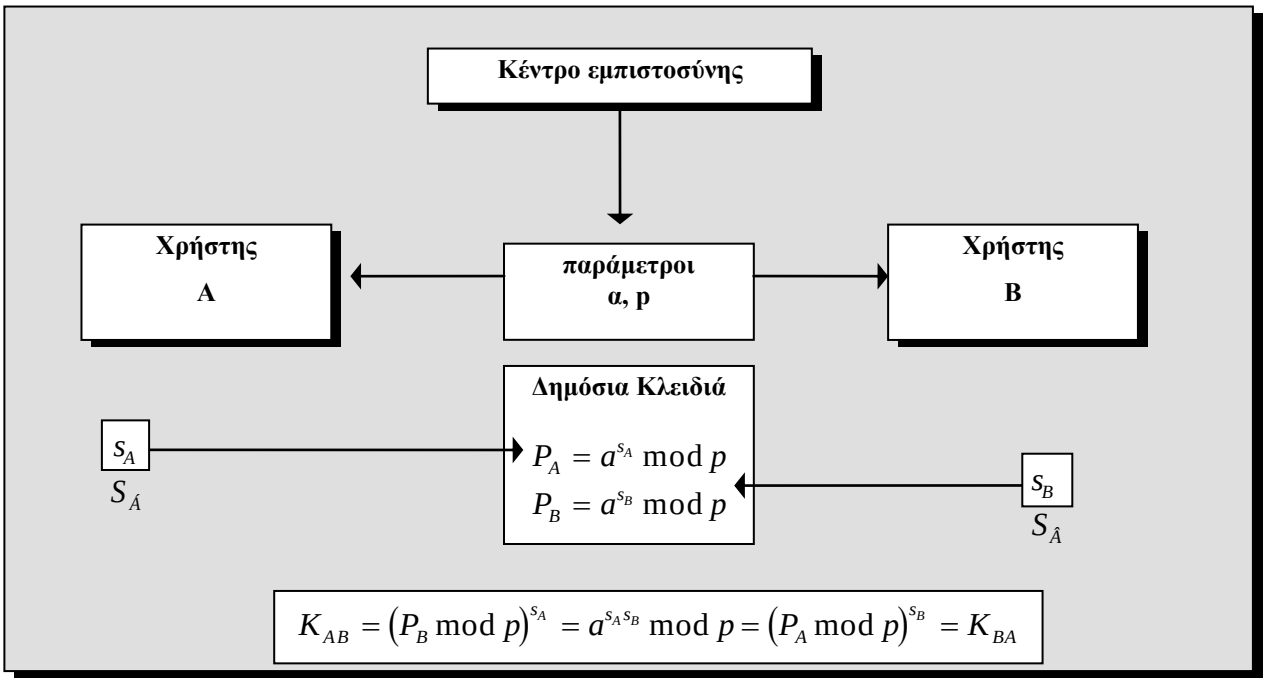
$$P_i = a^{s_i} \bmod p$$

όπου

α: ένα στοιχείο-γεννήτορας του Z_p

p: ένας μεγάλος πρώτος αριθμός

Το έργο του κέντρου εμπιστοσύνης είναι η επιλογή και δημοσιοποίηση των παραμέτρων α και *p*.



Σχήμα 11. Το πρωτόκολλο των Diffie-Hellman με αυθεντικοποίηση χρηστών.

Η διαδικασία υπολογισμού και δημοσιοποίησης του δημόσιου κλειδιού πραγματοποιείται μία φορά, συνήθως κατά τη διαδικασία ένταξης του χρήστη στο σύστημα, και δεν επαναλαμβάνεται κάθε φορά που επιθυμεί να επικοινωνήσει με άλλους χρήστες του συστήματος.

Στην περίπτωση που δύο χρήστες U_i και U_j επιθυμούν να δημιουργήσουν ένα κοινό μυστικό κλειδί K_{ij}, κάθε χρήστης χρησιμοποιεί το μυστικό κλειδί του, το δημόσιο κλειδί του άλλου και την ακόλουθη ισοδυναμία:

$$K_{ij} = (P_j \bmod p)^{s_i} = a^{s_i s_j} \bmod p = (P_i \bmod p)^{s_j} = K_{ji}$$

-

Ειδικότερα:

$$K_{ij} = \left(P_j \bmod p\right)^{s_i} = P_j^{s_i} \bmod p = a^{s_i s_j} \bmod p = P_i^{s_j} \bmod p = \left(P_i \bmod p\right)^{s_j} = K_{ji}$$

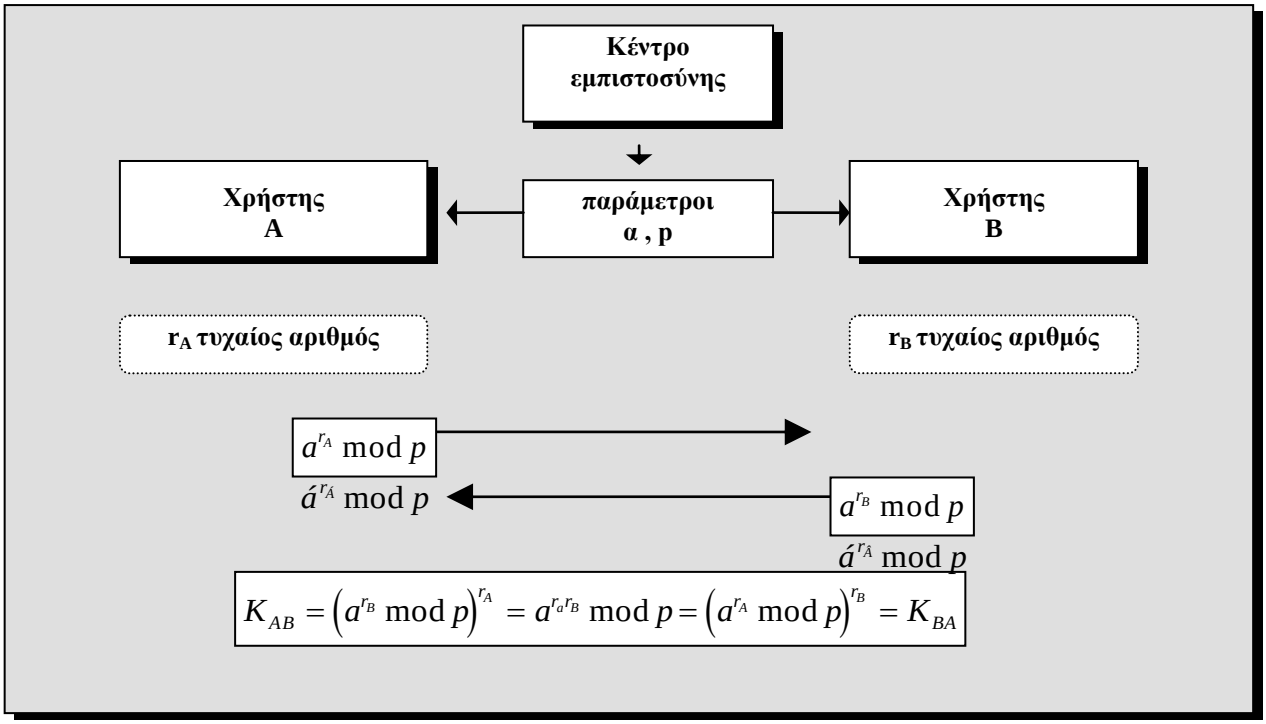
Το σύστημα αυτό, που παρουσιάζεται στο σχήμα 11, παρέχει αυθεντικοποίηση των δύο χρηστών, καθώς είναι οι μόνοι που μπορούν να γνωρίζουν τα μυστικά κλειδιά. Στην περίπτωση που οι χρήστες είναι σε θέση να επαληθεύουν το αμετάβλητο του κοινού κλειδιού, δεν χρειάζεται να υπολογίζουν ή να ανταλλάσσουν μεταξύ τους κάποιο μήνυμα, με αποτέλεσμα το πρωτόκολλο να χαρακτηρίζεται ως *πρωτόκολλο χωρίς ανταλλαγή μηνυμάτων* (zero pass protocol). Αυτό έχει ως αποτέλεσμα, το απαιτούμενο υπολογιστικό κόστος να είναι μηδενικό, καθώς οι δύο χρήστες δεν χρειάζονται κανένα υπολογισμό, παρά μόνο να προστατεύουν το κοινό μυστικό κλειδί.

Το κύριο μειονέκτημα του πρωτοκόλλου των Diffie-Hellman με αυθεντικοποίηση χρηστών είναι ότι οι δύο χρήστες χρησιμοποιούν το ίδιο κοινό μυστικό κλειδί, το οποίο δεν ανανεώνεται κάθε φορά που επιθυμούν να επικοινωνήσουν.

Μια άλλη έκδοση του πρωτοκόλλου αυτού παρουσιάζεται στο σχήμα 12. Στην περίπτωση αυτή, κάθε φορά που οι χρήστες θέλουν να επικοινωνήσουν, χρησιμοποιούν τυχαίους αριθμούς, ενώ το κοινό μυστικό κλειδί που υπολογίζουν είναι κάθε φορά διαφορετικό σε σχέση με τα προηγούμενα. Πιο συγκεκριμένα στην έκδοση αυτή για δύο χρήστες U_i και U_j, έχουν για κοινό μυστικό κλειδί :

$$K_{ij} = \left(a^{r_j} \bmod p\right)^{r_i} = a^{r_i r_j} \bmod p = \left(a^{r_i} \bmod p\right)^{r_j} = K_{ji}$$

Το κύριο πλεονέκτημα, σε σχέση με την αρχική έκδοση, είναι ότι κάθε φορά υπάρχει ανανέωση του κοινού μυστικού κλειδιού. Τα κύρια μειονεκτήματά του είναι α) δεν υπάρχει αυθεντικοποίηση των χρηστών που συμμετέχουν και β) απαιτείται ανταλλαγή μηνυμάτων κάθε φορά, άρα αυξάνεται το υπολογιστικό κόστος.



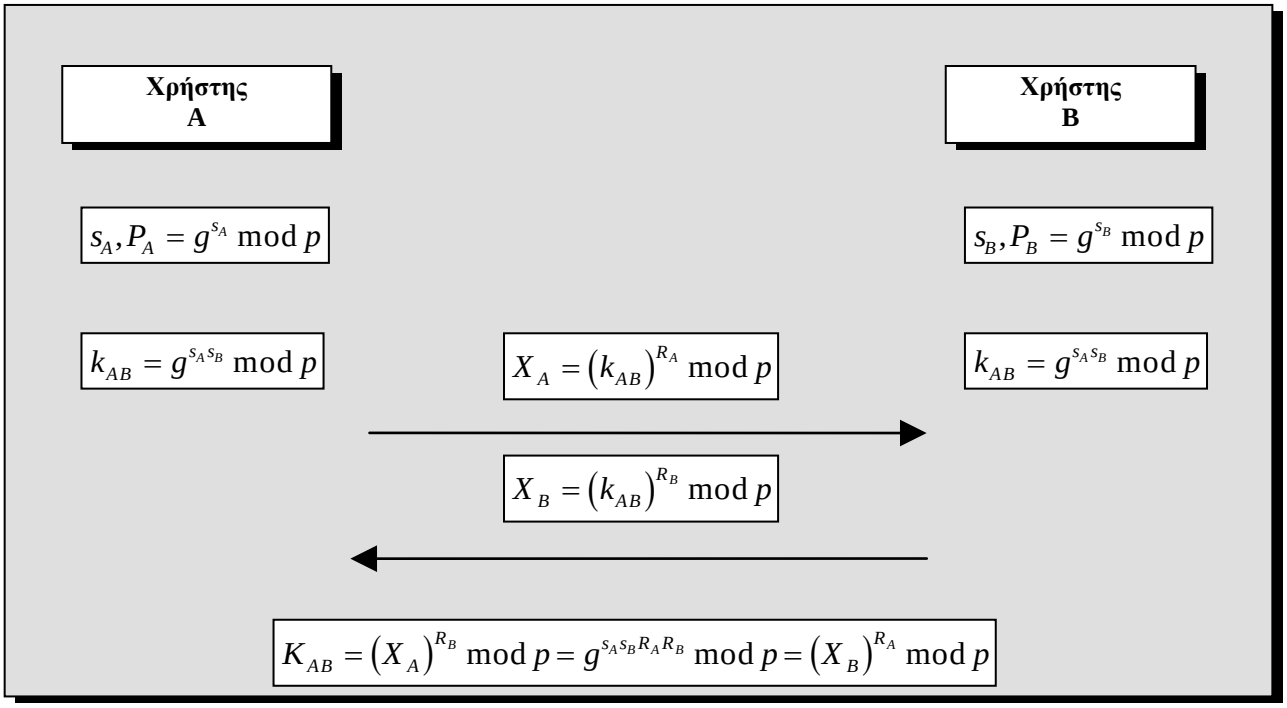
Σχήμα 12. Το πρωτόκολλο των Diffie-Hellman με ανανέωση του κοινού μυστικού κλειδιού.

Από το 1976 και μετά έχουν προταθεί πολλά κρυπτογραφικά πρωτόκολλα δημοσίου κλειδιού, που αποτελούν παραλλαγές του πρωτοκόλλου των Diffie - Hellman, παρέχοντας περισσότερες λειτουργίες ασφάλειας [Bau90, Bel94, Bet91, Bir92, Bra89a, Gun90, Koy88, Mat86, Oko88, Oko89, Tsu89, Yac90, Yac91]. Στο Παράρτημα 1 παρουσιάζεται η υλοποίηση ορισμένων κρυπτογραφικών πρωτοκόλλων που αφορούν στην επικοινωνία μεταξύ δύο χρηστών και είναι παραλλαγές του πρωτοκόλλου των Diffie - Hellman.

1.11 Το κρυπτογραφικό πρωτόκολλο των Matsumoto, Takashima, Imai (MTI)

Το κρυπτογραφικό πρωτόκολλο που έχει προταθεί από τους Matsumoto, Takashima και Imai [Mat86,ISO95] και είναι γνωστό ως πρωτόκολλο MTI, αποτελεί παραλλαγή του πρωτοκόλλου των Diffie - Hellman [Dif76].

Στο πρωτόκολλο MTI, το κέντρο εμπιστοσύνης είναι υπεύθυνο μόνο για την επιλογή των βασικών παραμέτρων του πρωτοκόλλου, οι οποίες είναι ένας πρώτος αριθμός p και ένα g γεννήτορας του Z_p^*.



Σχήμα 13. Το κρυπτογραφικό πρωτόκολλο των Matsumoto, Takashima - Imai.

Στο σχήμα 13 παρουσιάζεται το κρυπτογραφικό πρωτόκολλο MTI. Κύριο χαρακτηριστικό του πρωτοκόλλου αυτού είναι ότι οι χρήστες, κάθε φορά που επικοινωνούν, μπορούν να υπολογίζουν διαφορετικό κοινό μυστικό κλειδί.

Κατά τη διαδικασία ένταξής του στο σύστημα ένας νέος χρήστης i, επιλέγει ένα τυχαίο αριθμό $s_i \in Z_p^*$ και με τη βοήθεια του κέντρου εμπιστοσύνης καταχωρεί ως δημόσιο κλειδί του το $P_i = g^{S_i} \bmod p$. Η διαδικασία αυτή πραγματοποιείται μία φορά και δεν χρειάζεται να επαναλαμβάνεται, εκτός εάν η αλλαγή του μυστικού κλειδιού του χρήστη, θεωρηθεί απαραίτητη.

-

Στη περίπτωση που δύο χρήστες *A* και *B* επιθυμούν να επικοινωνήσουν με ασφάλεια, υπολογίσουν αρχικά το:

$$k_{AB} \equiv \left(g^{s_A}\right)^{s_B} \equiv \left(g^{s_B}\right)^{s_A} \equiv g^{s_A s_B} \bmod p \qquad (1)$$

που είναι γνωστό ως κλειδί Diffie και Hellman. Στην συνέχεια επιλέγουν ο καθένας από ένα μυστικό τυχαίο εκθέτη $R_{\acute{A}}, R_{\hat{A}}$ που ανήκει στο Z_{p-1} και ανταλλάσσουν τα

$$X_A = k_{AB}^{R_A} \bmod p \text{ και } X_B = k_{AB}^{R_B} \bmod p, \qquad (2)$$

αντίστοιχα. Σύμφωνα με τις παραπάνω ισότητες (1) και (2), το κοινό μυστικό κλειδί μεταξύ των χρηστών *A* και *B* είναι το ακόλουθο :

$$K_{AB} = k_{AB}^{R_A R_B} \bmod p = \left(X_A\right)^{R_B} \bmod p = \left(X_B\right)^{R_A} \bmod p,$$

το οποίο και οι δύο χρήστες μπορούν να υπολογίσουν.

1.12 Επιθέσεις στα κρυπτογραφικά πρωτόκολλα

Η προστασία των δεδομένων και των πληροφοριών που παρέχεται από ένα κρυπτογραφικό πρωτόκολλο, εξαρτάται κυρίως από το πόσο "ισχυρό" είναι το κλειδί ή τα κλειδιά που χρησιμοποιούνται στη διαδικασία. Ενα κλειδί θεωρείται ισχυρό σε οποιαδήποτε μορφή παρέμβασης, εάν ο χρήστης που πραγματοποιεί την παρέμβαση δεν μπορέσει να κατορθώσει να αποκτήσει μια επιπλέον γνώση σχετικά μ' αυτό. Οι χρήστες που πραγματοποιούν τις παρεμβάσεις μπορεί να ονομάζονται ωτακουστές (eavesdroppers), αντίπαλοι (adversaries), επιτιθέμενοι (attackers), αναχαιτιστές (interceptors), παρείσακτοι (interlopers), απρόσκλητοι (intruders), ανταγωνιστές (opponents), ή εχθρός (enemy) . Στην συνέχεια, θα χρησιμοποιείται ο όρος **αντίπαλος**.

-

Αρχικά, ο αντίπαλος προσπαθεί να αποκαλύψει το μήνυμα που έχει κρυπτογραφηθεί, χωρίς να έχει γνώση σχετικά με το ποιο είναι το κλειδί (ή τα κλειδιά). Ως *επιτυχής κρυπτοανάλυση* ορίζεται η αποκάλυψη του κρυπτογραφημένου κειμένου ή του κλειδιού, καθώς επίσης και η εύρεση αδυναμιών στο συγκεκριμένο κρυπτογραφικό πρωτόκολλο, οι οποίες θα επιτρέψουν την αποκάλυψη του περιεχομένου του μηνύματος ή/και των κλειδιών.

Κάθε απόπειρα κρυπτοανάλυσης ορίζεται ως *επίθεση* (attack). Κάθε επιτυχής επίθεση μπορεί να αποτελέσει μια μέθοδο κρυπτοανάλυσης. Σε κάθε επίθεση θεωρείται ότι ο αντίπαλος έχει όλες τις πληροφορίες σχετικά με τα βήματα και τους απαιτούμενους υπολογισμούς του κρυπτογραφικού πρωτοκόλλου. Πιο συγκεκριμένα, ένα κρυπτογραφικό πρωτόκολλο δεν θεωρείται ότι παρέχει ασφάλεια και προστασία των μηνυμάτων, εάν η ασφάλειά του βασίζεται στην μη δημοσιοποίηση του κρυπτογραφικού πρωτοκόλλου.

Οι επιθέσεις χωρίζονται σε διάφορες κατηγορίες, από τις οποίες οι πιο βασικές είναι οι ακόλουθες [Ben91, Des88, Sch94]:

- **Κρυπτογραφημένου κειμένου μόνο (ciphertext only),** όταν ο αντίπαλος έχει στην διάθεσή του ορισμένα ή όλα τα κρυπτογραφημένα κείμενα τα οποία έχουν κρυπτογραφηθεί με το ίδιο κλειδί.

- **Γνωστού κειμένου (known-plaintext),** όταν ο αντίπαλος έχει στην διάθεσή του ορισμένα κρυπτογραφημένα κείμενα, καθώς επίσης και τα ίδια τα κείμενα.

- **Επιλεγμένου κειμένου (chosen-plaintext),** όταν ο αντίπαλος έχει στην διάθεσή του ορισμένα κρυπτογραφημένα κείμενα και σε ό,τι αφορά τα μη κρυπτογραφημένα κείμενα μπορεί αυτός να επιλέξει συγκεκριμένα από αυτά.

-

- **Διασκευασμένου επιλεγμένου κειμένου (adaptive chosen plaintext),** που αποτελεί μια ειδική περίπτωση της προηγουμένης μορφής (επιλεγμένου κειμένου), όπου ο αντίπαλος δεν επιλέγει μόνο απλά δικά του κείμενα, αλλά μπορεί να τα προσαρμόζει κάθε φορά ανάλογα με τα αποτελέσματα που έχει από προηγούμενα κείμενα.

- **Επιλεγμένου κρυπτογραφημένου κειμένου (chosen ciphertext),** όταν ο αντίπαλος επιλέγει ορισμένα κρυπτογραφημένα κείμενα, τα οποία στην συνέχεια αποκρυπτογραφούνται. Ο αντίπαλος έχει στην διάθεσή του τόσο τα κρυπτογραφημένα κείμενα, όσο και τα ίδια τα κείμενα.

Εκτός από τις παραπάνω κατηγορίες, οι επιθέσεις μπορούν να χωριστούν σε παθητικές (passive attacks) και σε ενεργητικές (active attacks) [Sch94]. Μια επίθεση χαρακτηρίζεται ως παθητική, όταν ο αντίπαλος δεν συμμετέχει ενεργά στη διαδικασία του πρωτοκόλλου, αλλά υποκλέπτει μόνο τα μηνύματα που ανταλλάσσονται. Οι παθητικές επιθέσεις αντιστοιχούν στις επιθέσεις "κρυπτογραφημένου κειμένου μόνο" που περιγράφτηκε παραπάνω.

Αντίθετα, στην περίπτωση που ο αντίπαλος συμμετέχει ενεργά στην διαδικασία ενός κρυπτογραφικού πρωτοκόλλου τότε μπορεί να εισάγει νέα δικά του μηνύματα (τα οποία να γίνονται αποδεκτά από τους παραλήπτες), να τροποποιεί μηνύματα, να διαγράφει μηνύματα, να καταστρέφει τους διαύλους επικοινωνίας ή να τροποποιεί πληροφορίες που είναι καταχωρημένες.

Ενα κρυπτογραφικό πρωτόκολλο, θεωρείται ότι παρέχει αποτελεσματική ασφάλεια και προστασία των μηνυμάτων, εάν μπορεί να αντεπεξέλθει τόσο σε παθητικές, όσο και σε ενεργητικές επιθέσεις. Στο κεφάλαιο 3, τα προτεινόμενα κρυπτογραφικά πρωτόκολλα ελέγχονται σε ότι αφορά την ασφάλεια τους, τόσο σε παθητικές επιθέσεις, όσο και σε ενεργητικές επιθέσεις.

-

1.13 Απόδειξη μηδενικής γνώσης

Εστω, ότι σε ένα κρυπτογραφικό πρωτόκολλο με δύο χρήστες, ο ένας πρέπει να αποδείξει στον άλλον, ότι γνωρίζει μια μυστική πληροφορία (π.χ. ένα μυστικό κλειδί). Στην απόδειξη αυτή θα βασιστεί ο δεύτερος χρήστης για να επαληθεύσει ότι ο πρώτος χρήστης είναι αυθεντικός ή δεν προσποιείται. Ορίζεται ο χρήστης, που θέλει να αποδείξει ότι γνωρίζει τη μυστική πληροφορία, ως χρήστης Α και ο χρήστης, που θα επαληθεύσει ότι ο χρήστης Α δεν προσποιείται, ως χρήστης Β. Για να είναι μια απόδειξη μηδενικής γνώσης θα πρέπει να ισχύουν οι ακόλουθοι κανόνες:

1. Ο χρήστης Α δεν μπορεί να προσποιηθεί με επιτυχία στον χρήστη Β. Πιο συγκεκριμένα, εάν ο χρήστης Α δεν γνωρίζει τη μυστική πληροφορία, τότε η πιθανότητα επιτυχίας του να πείσει τον χρήστη Β είναι αμελητέα.

2. Ο χρήστης Β δεν μπορεί να προσποιηθεί με επιτυχία στον χρήστη Α. Πιο συγκεκριμένα, ο χρήστης Β δεν μπορεί να αποδείξει σε τρίτο χρήστη ότι γνωρίζει την όλη διαδικασία μόνο έαν αποκαλύψει τη διαδικασία ή τη μυστική πληροφορία.

3. Ο χρήστης Β δεν αποκτά καμιά επιπλέον γνώση από την επικοινωνία του με τον χρήστη Α, την οποία, είτε δεν την γνώριζε πριν την επικοινωνία, είτε δε θα μπορούσε να υπολογίσει από μόνος του.

Οι τρεις παραπάνω κανόνες προτάθηκαν τόσο από τους Goldreich, Micali και Wigderson [Gol87], όσο και από τους Goldwasser, Micali και Rackoff [Gol85]. Παρόμοιες προσπάθειες, βασισμένες όμως σε διαφορετικές υποθέσεις, έχουν επίσης προταθεί [Bra86,Bra88,Cha87a].

Στην περίπτωση που ισχύουν μόνο οι δύο πρώτοι κανόνες, τότε η διαδικασία απόδειξης δεν χαρακτηρίζεται ως μηδενικής γνώσης, αλλά ως απόδειξη *ελάχιστης αποκάλυψης* (minimum disclosure proof).

Ενα κρυπτογραφικό πρωτόκολλο χαρακτηρίζεται ως κρυπτογραφικό πρωτόκολλο μηδενικής γνώσης, όταν οι χρήστες που συμμετέχουν δεν αποκαλύπτουν καμιά επιπλέον γνώση στον κρυπταναλυτή, ο οποίος προσπαθεί να παραβιάσει το συγκεκριμένο πρωτόκολλο.

1.14 Απειλές σε περιβάλλον βάσεων δεδομένων

Ως *απειλή* (threat), σ' ένα περιβάλλον βάσεων δεδομένων, ορίζεται η επιτυχημένη προσπάθεια ενός μη εξουσιοδοτημένου χρήστη να αποκαλύψει ή να τροποποιήσει τις πληροφορίες που αποθηκεύονται ή διακινούνται μέσα σ' ένα σύστημα [Cas95, Hin88]. Οι απειλές μπορεί να χωρισθούν σε διάφορες κατηγορίες ανάλογα με το κριτήριο διαχωρισμού. Εάν το κριτήριο διαχωρισμού είναι το είδος πρόσβασης που μπορεί ένας μη-εξουσιοδοτημένος χρήστης να έχει, τότε υπάρχουν οι ακόλουθες κατηγορίες απειλών:

- *Μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες* (improper release of information), που οφείλεται στην τυχαία ή μη ανάκτηση πληροφοριών από μη εξουσιοδοτημένους χρήστες.

- *Μη εξουσιοδοτημένη τροποποίηση των δεδομένων* (improper modification of data), που οφείλεται στην ενημέρωση, καταχώρηση, διαγραφή και αλλαγή δεδομένων από μη εξουσιοδοτημένους χρήστες.

- *Άρνηση εξυπηρέτησης* (denial of service), που οφείλεται στην παρεμπόδιση πρόσβασης στις πληροφορίες ή χρησιμοποίησης των μέσων από τους εξουσιοδοτημένους χρήστες.

Ένα άλλο κριτήριο διαχωρισμού μπορεί να είναι η αιτία, που προκάλεσε την απειλή. Στην περίπτωση αυτή, οι κατηγορίες απειλών είναι οι ακόλουθες:

-

– Φυσική αιτία (natural or accidental disaster) όπως σεισμός, φωτιά κλπ

– Λάθος στην υλοποίηση του υλικού ή του λογισμικού.

– Ανθρώπινο λάθος.

Η ασφάλεια και η προστασία των δεδομένων και των πληροφοριών μπορούν να αναλυθούν σύμφωνα με τις απαιτήσεις για την αντιμετώπιση των απειλών, όπως [Αλε95, Παγ95, Cas95] :

– *Προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση*, που αφορά την δυνατότητα πρόσβασης σε οποιοδήποτε μέσο αποθήκευσης δεδομένων μόνο από τους εξουσιοδοτημένους χρήστες.

– *Προστασία δεδομένων από συμπερασματολογία* (inference), η οποία αφορά την απόκτηση δεδομένων από χρήστες που δεν έχουν πρόσβαση σ' αυτά, με την βοήθεια άλλων δεδομένων στα οποία έχουν πρόσβαση.

– *Ακεραιότητα των δεδομένων*, που αφορά την προστασία των δεδομένων από οποιαδήποτε μορφή τροποποίησης, είτε αυτά βρίσκονται αποθηκευμένα στη βάση δεδομένων, είτε μεταφέρονται μέσα από τους δίαυλους επικοινωνίας των δικτύων από χρήστες που δεν έχουν τέτοιο δικαίωμα.

– *Λειτουργική ακεραιότητα των δεδομένων*, που αφορά τον τρόπο οργάνωσης μέσω του οποίου θα γίνεται η πρόσβαση, ώστε οι εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση στα σωστά δεδομένα.

– *Αυθεντικοποίηση των χρηστών*, που αφορά την απόδειξη της γνησιότητας μιας οντότητας (χρήστη ή μη) του συστήματος, ώστε να παρεμποδίζεται η εμφάνιση της οντότητας αυτής ως μία άλλη (impersonation).

-

– *Έλεγχο πρόσβασης*, που αφορά τον έλεγχο της χρήσης ενός υπολογιστικού πόρου ή μιας ομάδας δεδομένων από κάποιο συγκεκριμένο χρήστη, ώστε να επιτρέπεται η χρήση τους από χρήστες, που έχουν αυτό το δικαίωμα ενώ ταυτόχρονα να παρεμποδίζεται για τους υπόλοιπους χρήστες.

– *Εμπιστευτικότητα των δεδομένων*, που αφορά την εγγύηση ότι οι πληροφορίες δεν είναι διαθέσιμες ούτε αποκαλύπτονται σε μη εξουσιοδοτημένους χρήστες.

– Διαθεσιμότητα των δεδομένων, που αφορά την δυνατότητα άμεσης πρόσβασης των δεδομένων από εξουσιοδοτούμενους χρήστες.

1.15 Διαδικασία επαλήθευσης και αξιολόγησης του συστήματος ασφάλειας σε περιβάλλον βάσεων δεδομένων

Η ανάγκη για κοινή αποδοχή ενός συστήματος ασφαλείας τόσο από τους κατασκευαστές, όσο και από τους τελικούς χρήστες, οδήγησε στην ανάπτυξη προτύπων ασφάλειας (security standards). Η χρήση ενός προτύπου ασφάλειας εξαρτάται από το συγκεκριμένο περιβάλλον στο οποίο θα λειτουργήσει το σύστημα ασφάλειας [Str94].

Από τα τέλη της δεκαετίας του 70 άρχισαν να εμφανίζονται τα πρώτα πρότυπα ασφάλειας. Πιο συγκεκριμένα, το 1977 το Υπουργείο Άμυνας των Η.Π.Α ανέπτυξε μια σειρά προτύπων που αφορούσαν την αξιολόγηση συστημάτων ασφάλειας καθώς και τις προδιαγραφές που θα πρέπει να έχουν τα νέα συστήματα ασφάλειας [DoD85].

Στην συνέχεια εμφανίστηκε το National Bureau of Standards (NBS), το οποίο μετονομάστηκε σε National Institute of Standards and Technology (NIST). Από τότε εμφανίστηκαν και άλλα παρόμοια κέντρα τόσο στην Αμερική, όσο και στην Ευρώπη (ITSEC, ITSEM) που σκοπό είχαν την αξιολόγηση συστημάτων ασφάλειας [ITS91, ITS92].

Παράλληλα εμφανίστηκαν ομάδες ειδικών που ασχολήθηκαν με συγκεκριμένα περιβάλλοντα (π.χ. νοσοκομεία) λαμβάνοντας υπόψη τις ιδιαιτερότητές τους [Bar91, Bar92, Rog91].

Η ανάπτυξη ενός συστήματος ασφάλειας σε περιβάλλον βάσεων δεδομένων, καθορίζεται κυρίως από τα χαρακτηριστικά του περιβάλλοντος και το βαθμό ασφάλειας που απαιτείται. Τρεις είναι οι βασικές μέθοδοι ανάπτυξης ενός συστήματος ασφάλειας:

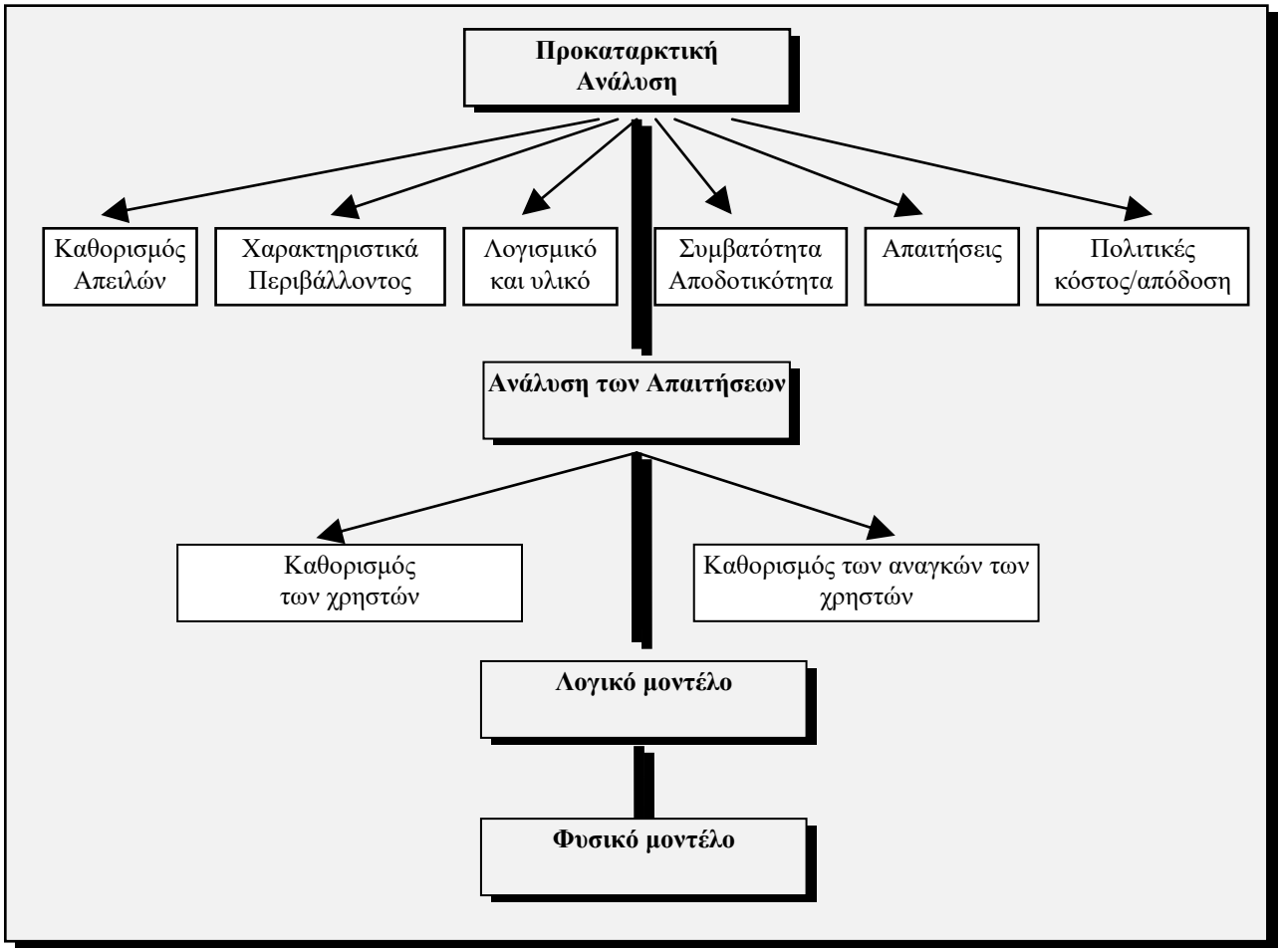
– Η χρησιμοποίηση ενός κλασσικού συστήματος διαχείρισης βάσεων δεδομένων, το οποίο παρέχει ορισμένες από τις λειτουργίες όπως, αυθεντικοποίηση χρήστη και έλεγχο προσπέλασης.

– Η χρησιμοποίηση ενός κλασσικού συστήματος διαχείρισης βάσεων δεδομένων, σε συνεργασία με άλλους εξωτερικούς μηχανισμούς ασφάλειας που παρέχουν επιπρόσθετες λειτουργίες ασφάλειας.

– Η χρησιμοποίηση ασφαλών συστημάτων διαχείρισης βάσεων δεδομένων. Ένα σύστημα διαχείρισης βάσεων δεδομένων είναι ασφαλές, όταν οι μηχανισμοί ασφάλειας ενεργοποιούνται αυτόματα και πραγματοποιούν ελέγχους ανάλογα με την απειλή που μπορεί να εμφανιστεί ή που ήδη έχει εμφανιστεί. Η σωστή λειτουργία των μηχανισμών αυτών έχει επαληθευτεί μέσω μιας καλά καθορισμένης διαδικασίας, η οποία προϋποθέτει την ύπαρξη μιας πολιτικής ασφάλειας που περιγράφεται μέσω ενός μοντέλου. Τέτοια συστήματα χρησιμοποιούνται, όταν η προστασία των δεδομένων είναι καθοριστική παράμετρος για την σωστή λειτουργία του οργανισμού [Man88].

Ο σχεδιασμός και η υλοποίηση ενός συστήματος ασφάλειας σ’ ένα οργανισμό, για να είναι αποτελεσματικός θα πρέπει να θεωρηθεί ως μέρος του σχεδιασμού και της υλοποίησης της βάσης δεδομένων. Είναι γενικά αποδεκτό ότι όλοι οι παραπάνω σχεδιασμοί πρέπει να

πραγματοποιούνται ταυτόχρονα και παράλληλα. Τα επιμέρους βήματα του σχεδιασμού και της υλοποίησης ενός συστήματος ασφάλειας παρουσιάζονται στο σχήμα 14 [Παγ95, Fug88].



Σχήμα 14. Σχεδιασμός και υλοποίηση ενός συστήματος ασφάλειας.

Στην περίπτωση που το σύστημα ασφάλειας και το πληροφοριακό σύστημα αφορούν ένα συγκεκριμένο περιβάλλον (π.χ. νοσοκομείο), θα πρέπει να λαμβάνονται υπόψη τόσο οι ιδιαιτερότητες του συγκεκριμένου χώρου, όσο και οι πιθανές ιδιαίτερες απαιτήσεις των χρηστών του [Mil93].

1.16 Μοντέλα ασφάλειας

Μοντέλο ασφάλειας (Security Model) είναι κάθε μοντέλο, ανεξάρτητο λογισμικού, που ικανοποιεί τον βαθμό προστασίας και καθορίζεται σύμφωνα με τις απαιτήσεις, τις ανάγκες και τις απειλές που υπάρχουν [Cas95, Den83].

Πολιτική ασφάλειας (security policy) είναι το σύνολο των κανόνων που καθορίζουν τις διαδικασίες, που επιτρέπονται ή απαγορεύονται μέσα σ' ένα σύστημα, σύμφωνα με τις απαιτήσεις, τις ανάγκες αλλά και τις απειλές που υπάρχουν σ' αυτό [Cas95, Den83].

Ο σωστός καθορισμός των πολιτικών ασφάλειας οδηγεί στον ολοκληρωμένο και χωρίς αδυναμίες καθορισμό των στρατηγικών, που επιτρέπουν την ανάλυση σημαντικών σημείων και πιθανών αντιθέσεων, με σκοπό την όσο δυνατόν αποτελεσματικότερη λειτουργία του προτεινόμενου μοντέλου.

Μια πολιτική ασφάλειας χαρακτηρίζεται ως:

- Ελαχίστου δικαιώματος (minimum privilege policy) ή μεγίστου δικαιώματος (maximum privilege policy), ανάλογα με το μέγεθος των πληροφοριών που είναι προσπελάσιμες.

- Κλειστή (closed) ή ανοικτή (open) ανάλογα με τον τρόπο που καθορίζεται κάθε πρόσβαση.

- Ιεραρχικά κατανεμημένης εξουσιοδότησης (hierarchical decentralised authorisation), ιδιοκτήτη (ownership) ή εξουσιοδότηση συνεργασίας (co-operative authorisation) ανάλογα το ποιος καθορίζει την προσπέλαση.

Σ' ένα περιβάλλον βάσεων δεδομένων, μια πολιτική ασφάλειας περιγράφεται ως ένα σύνολο κανόνων εξουσιοδότησης (authorisation rules) που καθορίζουν "ποιος" από τους εξουσιοδοτημένους χρήστες έχει "τι είδους" πρόσβαση σε "ποιες" πληροφορίες ή δεδομένα.

-

Διάφορα μοντέλα ασφάλειας έχουν προταθεί. Τα πιο βασικά είναι τα ακόλουθα:

- Μοντέλα ασφάλειας διακριτικής ικανότητας (Discretionary security models).
- Μοντέλα ασφάλειας πολλαπλών επιπέδων (Multilevel or Mandatory security models).
- Μοντέλα ασφάλειας προσωπικής γνώσης (Personal Knowledge security models).
- Μοντέλα ασφάλειας βασισμένα σε ρόλους-χρήστη (User role based security models).

1.17 Μοντέλα ασφάλειας διακριτικής ικανότητας

Τα μοντέλα ασφάλειας διακριτικής ικανότητας βασίζονται στην αρχή ότι η πρόσβαση στην πληροφορία καθορίζεται από την ταυτότητα του χρήστη (user's identify) και των κανόνων πρόσβασης [Παγ95, Bis91, Cas95, Eic92, Pan93b, Per95].

Στα μοντέλα αυτά, κάθε χρήστης που προσπαθεί να επιτύχει πρόσβαση σε πληροφορίες ή δεδομένα πρέπει να ελεγχθεί, εάν αυτός ικανοποιεί τον αντίστοιχο κανόνα πρόσβασης. Εάν επαληθεύεται ο κανόνας, τότε η πρόσβαση θεωρείται επιτυχής, ενώ στην αντίθετη περίπτωση θεωρείται αδύνατη.

Γενικά, τα μοντέλα αυτά επιτρέπουν στους χρήστες να μεταφέρουν τα δικαιώματά τους σ' άλλους χρήστες. Η διαδικασία αυτή βασίζεται στην πολιτική ιδιοκτησίας (ownership), όπου ο ιδιοκτήτης των πληροφοριών ή δεδομένων έχει την δυνατότητα χορήγησης ή ανάκλησης των δικαιωμάτων σε ή από άλλους χρήστες, αντίστοιχα. Ένα από τα βασικά πλεονεκτήματα των μοντέλων ασφάλειας διακριτικής ικανότητας, είναι ο εύκαμπτος τρόπος που αυτά διαχειρίζονται την υλοποίηση διαφορετικών απαιτήσεων.

-

1.18 Μοντέλα ασφάλειας πολλαπλών επιπέδων

Τα μοντέλα ασφάλειας πολλαπλών επιπέδων καθορίζουν την πρόσβαση σε πληροφορίες ή δεδομένα με βάση τον διαχωρισμό σε υποκείμενα (subject) και αντικείμενα (objects), ενώ εξετάζει παράλληλα και την ροή της πληροφορίας μέσα στο σύστημα [Παγ95, Bis91, Cas95, Eic92, Pan93b, Per95].

Ως υποκείμενο ορίζεται κάθε ενεργή οντότητα του συστήματος, που επιθυμεί να εξασφαλίσει πρόσβαση σ' ένα αντικείμενο. Συνήθως, το ρόλο του υποκειμένου έχει κάθε εξουσιοδοτημένος χρήστης του συστήματος.

Ως αντικείμενο ορίζεται κάθε παθητική οντότητα του συστήματος στην οποία αποθηκεύεται οποιαδήποτε μορφή πληροφορίας ή δεδομένου, όπως αρχείο, πεδίο κ.α.

Οι κλάσεις πρόσβασης (access classes) σχετίζονται με κάθε υποκείμενο και αντικείμενο του συστήματος. Κάθε υποκείμενο αποκτά οποιαδήποτε μορφή πρόσβασης σ' ένα αντικείμενο, εάν ικανοποιείται η σχέση μεταξύ της κλάσης του συγκεκριμένου υποκειμένου και της κλάσης του συγκεκριμένου αντικειμένου.

Συχνά, οι απαιτήσεις των μοντέλων ασφάλειας πολλαπλών επιπέδων βασίζονται στο παράδειγμα ασφάλειας των Bell-LaPadula και περιγράφονται μέσα από δύο βασικούς κανόνες [Bel76]:

- Ένα υποκείμενο μπορεί να "διαβάσει" ένα αντικείμενο, εάν η κλάση του υποκειμένου είναι μεγαλύτερη ή ίση με την κλάση του αντικειμένου.

-

– Ένα υποκείμενο μπορεί να "γράψει" σ’ ένα αντικείμενο, εάν η κλάση του υποκειμένου είναι ίση με την κλάση του αντικειμένου.

1.19 Μοντέλα ασφάλειας προσωπικής γνώσης

Τα μοντέλα ασφάλειας προσωπικής γνώσης επικεντρώνουν τον έλεγχό τους στην προστασία της μυστικότητας των χρηστών που σχετίζονται με μία βάση δεδομένων ή μ' ένα πληροφοριακό σύστημα. Τα μοντέλα αυτά βασίζονται στο παράδειγμα ασφάλειας των Biskup-Bruggemannn που είναι το πρωτότυπο σύστημα διαχείρισης δεδομένων Doris [Παγ95, Bis88, Bis89, Bis91, Pan93b].

Ο βασικός στόχος ενός μοντέλου ασφάλειας προσωπικής γνώσης, είναι ο καθορισμός των δικαιωμάτων ενός χρήστη από την υπάρχουσα νομοθεσία. Η μυστικότητα του χρήστη, η οποία θεωρείται βασικό δικαίωμά του, ορίζεται ως η δυνατότητα που έχει να επιτρέπει την αποκάλυψη μέρος των πληροφοριών του. Συνεπώς, κάθε χρήστης μπορεί εφόσον αυτός επιθυμεί, να ενημερωθεί για τις πληροφορίες που τον αφορούν.

Η υλοποίηση μοντέλων ασφάλειας προσωπικής γνώσης επιτυγχάνεται με την βοήθεια και το συνδυασμό τεχνικών, που αφορούν σχεσιακές βάσεις δεδομένων και αντικειμενοστραφή προγραμματισμό, καθώς και τις δυνατότητες που μπορεί να παρέχει ένα λειτουργικό σύστημα.

1.20 Μοντέλα ασφάλειας βασισμένα σε ρόλους-χρήστη

Τα μοντέλα ασφάλειας ρόλου-χρήστη εμφανίστηκαν την τελευταία δεκαετία και η ασφάλειά τους βασίζεται στους ρόλους, που κάθε χρήστης μπορεί να έχει μέσα στο σύστημα [Loc88, Moh94, Tin88, Tin92].

Οι βασικοί παράμετροι ενός τέτοιου μοντέλου είναι: οι ρόλοι ενός χρήστη, τα αντικείμενα και ένα σύνολο καλά δομημένων προσπελάσεων (well form transactions). Κάθε

χρήστης σύμφωνα με τους ρόλους που έχει μέσα στο σύστημα, περιορίζεται στο να έχει πρόσβαση μόνο σ' ένα συγκεκριμένο αριθμό καλά δομημένων προσπελάσεων που καθορίζονται από τους ρόλους του, ενώ κάθε καλά δομημένη προσπέλαση σχετίζεται μόνο μ' ένα συγκεκριμένο σύνολο αντικειμένων.

Τα μοντέλα ασφάλειας ρόλου-χρήστη, σε αντίθεση με τα άλλα μοντέλα, είναι πιο ικανοποιητικά όσον αφορά στην επίλυση προβλημάτων, που προκαλούνται από την απειλή είτε της συμπερασματολογίας είτε της συνάθροισης.

Ο καθορισμός των ρόλων, των αντικειμένων και των καλά δομημένων προσπελάσεων είναι ο πιο σημαντικός παράγοντας για την αποτελεσματική εφαρμογή και υλοποίηση του μοντέλου ασφάλειας μέσα σ' ένα σύστημα.

Ενα νέο προτεινόμενο μοντέλο ελέγχου πρόσβασης σε περιβάλλον νοσοκομείου, καθώς και ο σχεδιασμός, η ανάπτυξη και η υλοποίηση του, προτείνεται στο κεφάλαιο 4 και έχει βασιστεί στο μοντέλο ασφάλειας ρόλου-χρήστη.

1.21 Μηχανισμοί ασφάλειας

Ως *μηχανισμοί ασφάλειας* (security mechanisms) ορίζονται οι λειτουργίες στις οποίες βασίζεται ένα σύστημα ασφάλειας για την υλοποίηση των πολιτικών και των στρατηγικών που έχουν επιλεγεί [Cas95, Den83, San93].

Οι μηχανισμοί ασφάλειας αποβλέπουν είτε στην παρεμπόδιση της μη-εξουσιοδοτημένης πρόσβασης και ονομάζονται μηχανισμοί ελέγχου πρόσβασης (access control mechanisms) είτε στην πρόβλεψη, στον εντοπισμό και στην αντιμετώπιση μη-εξουσιοδοτημένων προσβάσεων και ονομάζονται μηχανισμοί ελέγχου και ανίχνευσης (auditing and intrusion detection mechanisms). Για την σωστή λειτουργία τέτοιων μηχανισμών απαιτούνται αποτελεσματικοί μηχανισμοί αυθεντικοποίησης (authentication mechanisms).

-

Κατά την ανάπτυξη ενός συστήματος ασφάλειας είναι αναγκαίος ο διαχωρισμός μεταξύ των εννοιών "πολιτικής" και "μηχανισμός", καθώς ο καθορισμός της πολιτικής πρέπει να γίνεται ανεξάρτητα από την διαδικασία υλοποίησής του και ο σχεδιασμός και η ανάπτυξη των μηχανισμών θα πρέπει να παρέχει την δυνατότητα λειτουργίας τους σε διαφορετικές πολιτικές [Cas95, Den83].

Οι μηχανισμοί ασφάλειας χωρίζονται σε δύο κατηγορίες, στους εξωτερικούς (external) και στους εσωτερικούς (internal) μηχανισμούς. Στην πρώτη κατηγορία ανήκουν οι μηχανισμοί που έχουν ως στόχο τους την παρεμπόδιση της μη-εξουσιοδοτημένης πρόσβασης στους φυσικούς πόρους του συστήματος και την αντιμετώπιση τυχαίων απειλών που οφείλονται σε φυσικές καταστροφές (σεισμός, φωτιά κλπ). Καθώς η ολοκληρωμένη και απόλυτη προστασία από τέτοιου είδους απειλές είναι αδύνατη, οι εξωτερικοί μηχανισμοί αποβλέπουν στη μείωση της πιθανότητας εμφάνισής τους και στην σωστή πρόβλεψή τους.

Στην δεύτερη κατηγορία ανήκουν οι μηχανισμοί, οι οποίοι παρέχουν τη σωστή λειτουργία του συστήματος, όταν οι εξωτερικοί μηχανισμοί επιτρέπουν την πρόσβαση. Οι μηχανισμοί αυτοί χωρίζονται σε τρεις κατηγορίες: της αυθεντικοποίησης, του ελέγχου πρόσβασης και του ελέγχου (audit).

Ένας άλλος τρόπος διαχωρισμού των μηχανισμών ασφάλειας δημιουργεί τρεις κατηγορίες: τους εξωτερικούς, τους εσωτερικούς και τους επικοινωνίας χρήστη (user interface) [San93].

Επιπλέον, οι μηχανισμοί ασφάλειας μπορούν να διαχωριστούν σύμφωνα με τον έλεγχο που πραγματοποιούν μέσα σ’ ένα σύστημα. Στην περίπτωση αυτή, οι κύριες κατηγορίες είναι [Cas95]:

- Μηχανισμοί ελέγχου ροής (control flow), που εξετάζουν εάν η ροή των πληροφοριών γίνεται με τέτοιο τρόπο, ώστε να μην υπάρχει θέμα προστασίας.

-

- Μηχανισμοί ελέγχου συμπερασματολογίας (inference control), που εξετάζουν την περίπτωση της εσφαλμένης απόκτησης πληροφοριών από μη εξουσιοδοτημένους χρήστες με έμμεσο τρόπο.

- Μηχανισμοί ελέγχου πρόσβασης (access control), που εξετάζουν την περίπτωση της εσφαλμένης απόκτησης πληροφοριών από μη εξουσιοδοτημένους χρήστες με άμεσο τρόπο.

- Μηχανισμοί που βασίζονται σε κρυπτογραφικές τεχνικές (cryptographic techniques) και ασχολούνται με την κωδικοποίηση και αποκωδικοποίηση των πληροφοριών και των δεδομένων, ώστε η προσπέλασή τους να επιτρέπεται μόνο στους εξουσιοδοτημένους χρήστες.

-

ΚΕΦΑΛΑΙΟ 2

ΜΟΝΤΕΛΑ ΣΥΜΦΩΝΙΑΣ ΚΛΕΙΔΙΟΥ ΑΠΟΔΕΔΕΙΓΜΕΝΗΣ ΑΣΦΑΛΕΙΑΣ

2.1 Αποδεδειγμένη ασφάλεια βασισμένη σε ψευδοτυχαίες συναρτήσεις

2.2 Το μοντέλο των Bellare - Rogaway

Οι Bellare και Rogaway έχουν προτείνει ένα γενικό μοντέλο ασφάλειας, στο οποίο βασίζονται κρυπτογραφικά πρωτόκολλα αποδεδειγμένης ασφάλειας [Bel94]. Ο βασικός στόχος του μοντέλου είναι η ελαχιστοποίηση της πιθανότητας ενός κρυπτοαναλυτή να αποκαλύψει το κοινό μυστικό κλειδί επικοινωνίας μεταξύ δύο ή περισσοτέρων χρηστών.

Απαραίτητη προϋπόθεση αποτελεί το γεγονός ότι οι χρήστες, που επιθυμούν να επικοινωνούν με ασφάλεια, θα πρέπει να ανανεώνουν το κοινό μυστικό κλειδί, έτσι ώστε στην περίπτωση που ο κρυπταναλυτής το αποκαλύψει, να αποκτήσει γνώση μόνο για το περιεχόμενο της συγκεκριμένης επικοινωνίας. Τα κύρια χαρακτηριστικά του μοντέλου αυτού είναι τα ακόλουθα:

1. Οι διαδικασίες επικοινωνίας ανάμεσα στους χρήστες μπορούν να ελέγχονται απόλυτα από τον κρυπτοαναλυτή. Πιο συγκεκριμένα, ο κρυπταναλυτής έχει την δυνατότητα α) να διαβάζει τα κωδικοποιημένα μηνύματα, που οι χρήστες ανταλλάσσουν μεταξύ τους, β) να στέλνει δικά του μηνύματα στους χρήστες, γ) να τροποποιεί μηνύματα πριν καταλήξουν στο προορισμό τους, δ) να καθυστερεί τη μετάδοση μηνυμάτων, ε) να αντικαθιστά μηνύματα με

μηνύματα προηγούμενων επικοινωνιών και στ) να επικοινωνεί με πολλούς χρήστες ταυτόχρονα

2. Σε κάθε χρήστη *A* αντιστοιχούν ένα σύνολο "χρησμών" (oracles) $\prod_{A,B}^{X}$, *x=1,...t* όπου *t* ο αριθμός των επικοινωνιών ανάμεσα στους δύο χρήστες, τους οποίους "χρησμούς", ο κρυπταναλυτής μπορεί να "καλέσει". Στο μοντέλο Bellare-Rogaway υπάρχει μόνο ένας κρυπτοαναλυτής και δεν είναι χρήστης του συστήματος

3. Ο "χρησμός" $\prod_{A,B}^{s}$ συμβολίζει το ότι ο χρήστης *A* προσπαθεί να δημιουργήσει ένα κοινό μυστικό κλειδί με το χρήστη *B* κατά την επικοινωνία *s*.

4. Κάθε "χρησμός" επικοινωνεί μέσω του κρυπταναλυτή με τους υπόλοιπους "χρησμούς".

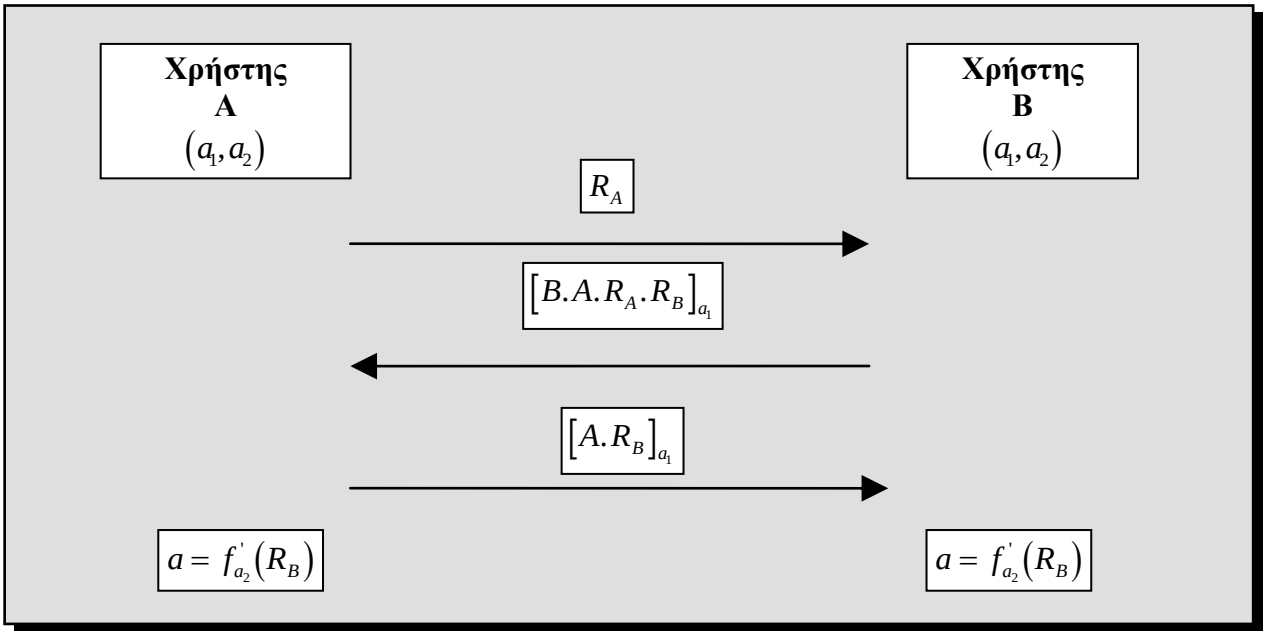
5. Κάθε επικοινωνία των "χρησμών", την οποία ο κρυπταναλυτής επιτρέπει να πραγματοποιηθεί χωρίς καμία παρέμβασή του, χαρακτηρίζεται ως "επικοινωνία που ταιριάζει" (matching conversations).

6. Ο κρυπταναλυτής μπορεί να αποκτήσει προηγούμενα κλειδιά επικοινωνίας "ανοίγοντας" τους κατάλληλους χρησμούς. "Μη ανοιγμένοι" χρησμοί είναι ενεργοί (fresh), εάν η επικοινωνία τους έχει γίνει αποδεκτή.

7. Ο σκοπός του κρυπταναλυτή είναι να αποκαλύψει το κοινό κλειδί επικοινωνίας μεταξύ δύο "χρησμών" $\prod_{A,B}^{s}$ $\prod_{B,A}^{t}$. Η επιτυχία του κρυπταναλυτή βασίζεται στη ικανότητά του να μπορεί να διακρίνει με πιθανότητα μεγαλύτερη του *1/2* ένα πραγματικό κλειδί επικοινωνίας από μια τυχαία συμβολοσειρά.

Οι Bellare και Rogaway έχουν προτείνει πρωτόκολλα κλειδιών επικοινωνίας αποδεδειγμένης ασφάλειας βασισμένα σε ψευδοτυχαίες συναρτήσεις. Η χρήση των

συναρτήσεων αυτών δεν επιτρέπει στον κρυπταναλυτή να διαχωρίσει το αποτέλεσμα μιας ψευδοτυχαίας συνάρτησης από μια οποιαδήποτε τυχαία συμβολοσειρά. Επιπλέον, ο κρυπταναλυτής δεν μπορεί να συνδυάσει τέτοιες συμβολοσειρές για τον υπολογισμό νέων, γεγονός που συντελεί στην αντιμετώπιση των επιθέσεων επιλεγμένων κρυπτογραφικών μηνυμάτων. Στη συνέχεια περιγράφεται ένα από τα πρωτόκολλα, που έχουν προταθεί από τους Bellare και Rogaway, στο οποίο οι χρήστες αποκτούν ένα κοινό μυστικό κλειδί επικοινωνίας [Bel94].



Σχήμα 1. Πρωτόκολλο Κλειδιού Συμφωνίας των Bellare και Rogaway.

Στο πρωτόκολλο αυτό, που περιγράφεται στο σχήμα 1, όπου $[x]_{a_1} = (x, f'_{a_1}(x))$, οι χρήστες *A* και *B* έχουν στην κατοχή τους κοινά μυστικά κλειδιά $(\acute{a}_1, \acute{a}_2)$ μεγάλης διάρκειας, μήκους *2k-bits* ,τα οποία επιλέγει ένα κέντρο εμπιστοσύνης. Το πρώτο μέρος α_1 χρησιμοποιείται ως κλειδί μιας ψευδοτυχαίας συνάρτησης $f_{\acute{a}_1}$ για τη διαδικασία της αυθεντικοποίησης και το δεύτερο μέρος α_2 χρησιμοποιείται ως κλειδί μιας ψευδοτυχαίας συνάρτησης $f'_{\acute{a}_2}$ για τον προσδιορισμό του κοινού κλειδιού επικοινωνίας $\alpha = f'_{\acute{a}_2}(R_{\hat{A}})$, όπου R_B είναι ένας τυχαίος αριθμός που έχει επιλέξει ο χρήστης *B*.

-

Το κύριο χαρακτηριστικό του συστήματος αυτού είναι η χρησιμοποίηση των ψευδοτυχαίων συναρτήσεων, που εξασφαλίζουν την μυστικότητα του κλειδιού επικοινωνίας, ενώ το κύριο μειονέκτημα είναι η αυθαίρετη έκδοση ζευγαριών κειμένου/ κρυπτογραφήματος, τα οποία έχουν κρυπτογραφηθεί με το ίδιο κλειδί.

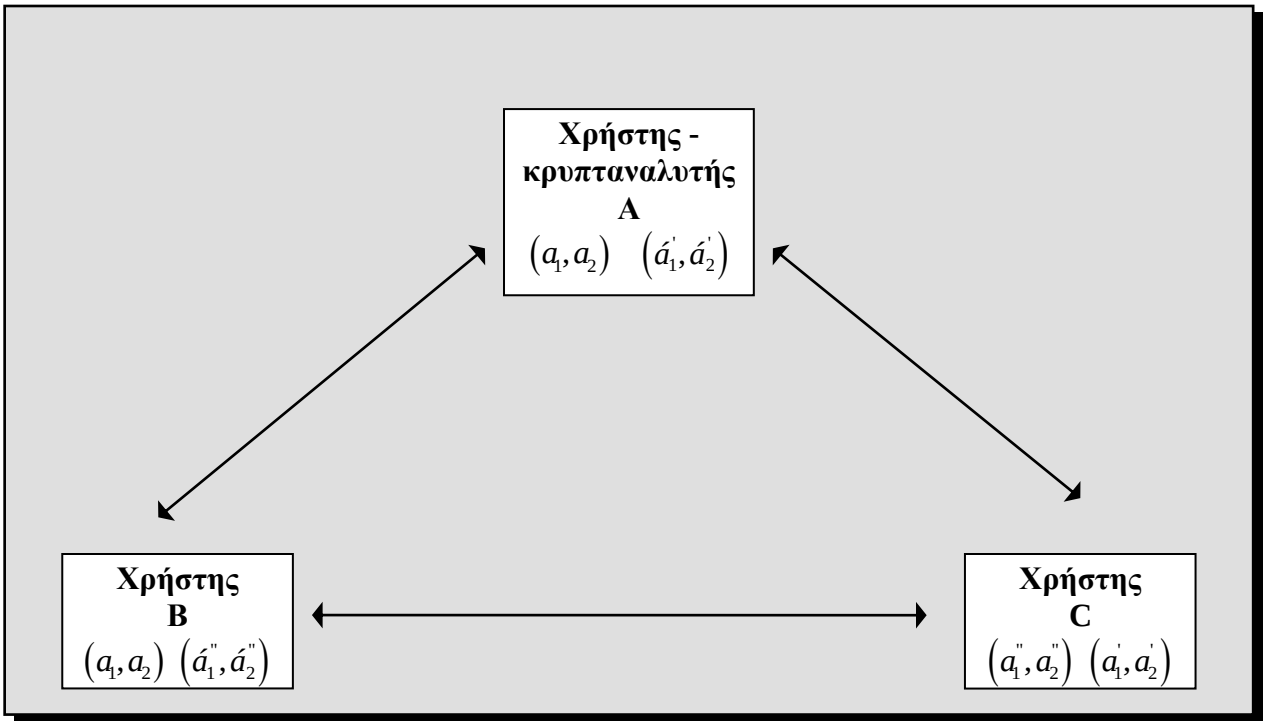
2.3 Ασφάλεια του μοντέλου Bellare - Rogaway

Οι Bellare και Rogaway χρησιμοποιούν "χρησμούς" για να αποδείξουν την ασφάλεια των πρωτοκόλλων που προτείνουν. Σύμφωνα με τα κύρια χαρακτηριστικά που αναφέρθηκαν στην προηγούμενη παράγραφο, ο σκοπός του κρυπταναλυτή είναι να αποκαλύψει το κοινό κλειδί επικοινωνίας *α* των χρησμών $\prod_{A,B}^{s}$ $\prod_{B,A}^{t}$. Η επιτυχία της προσπάθειας αυτής βασίζεται στη ικανότητα του κρυπτοαναλυτή να μπορεί να διακρίνει με πιθανότητα μεγαλύτερη του *1/2* ένα πραγματικό κλειδί επικοινωνίας από μια τυχαία συμβολοσειρά. Εάν οι συναρτήσεις, $f_{\acute{a}_1}$ και $f'_{\acute{a}_2}$ είναι ψευδοτυχαίες, τότε η δυνατότητα του κρυπταναλυτή να προβλέψει το κοινό κλειδί επικοινωνίας με πιθανότητα μεγαλύτερη από *1/2* είναι αμελητέα [Bel94].

Ο κρυπταναλυτής, στο πρωτόκολλο των Bellare και Rogaway, δε μπορεί να αποκτήσει καμιά επιπλέον γνώση, τόσο από τα μηνύματα $R_{\acute{A}}$, $A.R_{\hat{A}}$ $f_{\acute{a}_1}(\acute{A}.R_{\hat{A}})$ του χρησμού $\prod_{A,B}^{s}$, όσο και από τα μηνύματα $B,A,R_{\acute{A}},R_{\hat{A}}$, $f_{\acute{a}_1}(\hat{A}.\acute{A}.R_{\acute{A}}.R_{\hat{A}})$ του χρησμού $\prod_{B,A}^{t}$. Η μη δυνατότητα αυτή, οφείλεται στο ότι, ενώ μπορεί εύκολα να τα προσομοιώσει επιλέγοντας τυχαία $R_{\acute{A}}$ και $R_{\hat{A}}$ και αντικαθιστώντας τα $f_{\acute{a}_1}(\acute{A}.R_{\hat{A}})$, $f_{\acute{a}_1}(\hat{A}.\acute{A}.R_{\acute{A}}.R_{\hat{A}})$ με τυχαίες συμβολοσειρές, δε γνωρίζει το μυστικό κλειδί α_1. Συνεπώς δε μπορεί να διαχωρίσει τα κωδικοποιημένα μηνύματα από τυχαίες συμβολοσειρές, αφού η $f_{\acute{a}_1}$ είναι ψευδοτυχαία συνάρτηση. Με τον ίδιο τρόπο, μπορεί εύκολα να προσομοιώσει το κοινό κλειδί επικοινωνίας $\alpha=f'_{\acute{a}_2}(R_{\hat{A}})$ επιλέγοντας μία τυχαία συμβολοσειρά,

αλλά δεν μπορεί να διαχωρίσει το πραγματικό κοινό μυστικό κλειδί από το τυχαίο, αφού και η συνάρτηση f_{a_2} είναι ψευδοτυχαία συνάρτηση.

Σημαντικό είναι, ότι οι "χρησμοί" είναι αντίγραφα "έντιμων" χρηστών και οι τιμές $R_{\acute{A}}, R_{\hat{A}}$ ακολουθούν την ομοιόμορφη κατανομή. Παρατηρούμε ότι το σύστημα αυτό δεν επιτρέπει "επιθέσεις" από χρήστες του συστήματος, καθώς οι χρησμοί δεν μπορούν να "συνεργαστούν" με τον κρυπταναλυτή και συνεπώς ένας κρυπταναλυτής να αποκτήσει επιπλέον γνώση.



Σχήμα 2. Μια "επίθεση" του κρυπταναλυτή *A* σε επικοινωνία δύο χρηστών *B* και *C*.

Εστω ότι ο κρυπτοαναλυτής *A* προσπαθεί να επέμβει στα μηνύματα που οι χρήστες *B* και *C* ανταλλάσσουν, με σκοπό την απόκτηση του κοινού μυστικού κλειδιού επικοινωνίας των δύο χρηστών. Για να το πετύχει αυτό, ξεκινά μια διαδικασία επικοινωνίας με τους δύο χρήστες και στη συνέχεια προσπαθεί με τη βοήθειά της, να αποκτήσει γνώση τέτοια, ώστε να του επιτραπεί ο υπολογισμός ενός νέου κλειδιού επικοινωνίας. Στο σχήμα 2 παρουσιάζεται η προσπάθεια αυτή του χρήστη *A*.

-

Τα κοινά κλειδιά των χρηστών *A* και *B* είναι τα $\left(\acute{a}_1, \acute{a}_2\right)$,των *B* και *C* είναι $\left(\acute{a}_1^{''}, \acute{a}_2^{''}\right)$ και των *A* και *C* είναι $\left(\acute{a}_1^{'}, \acute{a}_2^{'}\right)$, αντίστοιχα. Στην "επίθεση" αυτή ο χρήστης *A* μπορεί να χρησιμοποιήσει μη-ομοιόμορφη κατανομή για τις τυχαίες μεταβλητές, με σκοπό τα μηνύματα να εξαρτώνται από τα μηνύματα των άλλων χρηστών και κατά συνέπεια να αυξάνεται η πιθανότητα επίτευξης του στόχου του.

Ομως, και στην περίπτωση αυτή, δεν μπορεί να υπάρχει δυνατότητα απόκτησης επιπλέον γνώσης από τον χρήστη *A*, καθώς οι χρήστες *B* και *C* χρησιμοποιούν ψευδοτυχαίες συναρτήσεις. Εάν και μία τυχαία μεταβλητή *X* μπορεί να μην ακολουθεί κανονική κατανομή και να εξαρτάται από τις άλλες μεταβλητές, το $f_a(X)$ που είναι ψευδοτυχαία συνάρτηση, έχει ως αποτέλεσμα να ακολουθεί πάντα την ομοιόμορφη κατανομή, αφού δεν μπορεί να διακριθεί από μια ομοιόμορφη συμβολοσειρά. Συνεπώς, η μόνη χρήσιμη πληροφορία, που ο χρήστης *A* μπορεί να αποκτήσει από μια τέτοια επίθεση, είναι το είδος της κατανομής των R_A και R_B, την οποία όμως δεν μπορεί να προσομοιώσει, καθώς οι συμβολοσειρές που προέρχονται από ψευδοτυχαίες συναρτήσεις είναι ανεξάρτητες των πραγματικών κοινών μυστικών κλειδιών επικοινωνίας.

2.4. Αποδεδειγμένη ασφάλεια βασισμένη σε μηδενική γνώση

Στην παράγραφο αυτή, περιγράφεται το μοντέλο που προτάθηκε από τους Desmedt και Burmester και βασίζεται σε *μηδενική γνώση* (zero-knowledge) [Des93]. Ειδικότερα, εξετάζονται κρυπτογραφικά πρωτόκολλα, τα οποία δεν παρέχουν αποδεδειγμένη ασφάλεια, και πως αυτά, με τη βοήθεια του μοντέλου των Desmedt και Burmester, μπορούν να παρέχουν αποδεδειγμένη ασφάλεια. Στην παράγραφο 2.5 προτείνεται ένα νέο κρυπτογραφικό πρωτόκολλο αποδεδειγμένης ασφάλειας καθώς και μια αποτελεσματική διαδικασία υλοποίησής του.

-

Ο σκοπός του προτεινόμενου κρυπτογραφικού πρωτοκόλλου δεν είναι μόνο η ύπαρξη ενός επιπλέον κρυπτογραφικού πρωτοκόλλου, το όποιο θα έχει περισσότερα πλεονεκτήματα, αλλά και η αποτελεσματική διαδικασία υλοποίησής του, καθώς η καθιέρωση των συστημάτων ασφάλειας στο ευρύ χώρο εξαρτάται σε μεγάλο βαθμό από τη δυνατότητα υλοποίησης όσων το "θεωρητικό" μέρος της κρυπτογραφίας έχει θεμελιώσει. Είναι γενικά αποδεκτό, ότι η αδυναμία εφαρμογής της κρυπτογραφίας, δεν οφείλεται στην έλλειψη αποτελεσματικών και θεωρητικά αποδεδειγμένων κρυπτογραφικών πρωτοκόλλων, αλλά στην δυσκολία αποτελεσματικής υλοποίησής τους.

Οι Desmedt και Burmester εξέτασαν το κρυπτογραφικό πρωτόκολλο MTI (παρουσιάστηκε αναλυτικά στο κεφάλαιο 1) που δεν είναι ούτε αποδεδειγμένης ασφάλειας, ούτε μη μηδενικής γνώσης.

Η ασφάλεια του κρυπτογραφικού πρωτοκόλλου εξαρτάται από τις δυνατότητες που έχει ένας κρυπτοαναλυτής. Στην περίπτωση που ο κρυπτοαναλυτής υποκλέπτει μόνο τις πληροφορίες και τα μηνύματα που ανταλλάσσουν μεταξύ τους οι χρήστες, το πρωτόκολλο είναι ασφαλές, καθώς η ασφάλεια του βασίζεται στην δυσκολία υπολογισμού του $g^{ab} \bmod p$ εφόσον είναι γνωστά τα p, g, $g^a \bmod p$ και $g^b \bmod p$, το οποίο είναι γνωστό ως πρόβλημα των Diffie και Hellman. Επομένως, εάν υποθέσουμε ότι το πρόβλημα των Diffie και Hellman είναι εύκολο στον υπολογισμό του, τότε για το συγκεκριμένο πρωτόκολλο είναι εύκολος ο υπολογισμός του κοινού μυστικού κλειδιού K_{AB} γνωρίζοντας τις παραμέτρους p, g, P_A, P_B, X_A και X_B. Επιπλέον, εάν θεωρήσουμε ότι τα $g^a \bmod p$ και $g^b \bmod p$ είναι αντίστοιχα περίπτωση του προβλήματος των Diffie και Hellman, τότε επιλέγοντας τυχαίους εκθέτες s_A, s_B για τα δημόσια κλειδιά P_A, P_B, αντίστοιχα, και υπολογίζοντας τα $X_A = \left(g^a\right)^{s_A s_B} \bmod p$ και $X_B = \left(g^b\right)^{s_A s_B} \bmod p$ είναι εύκολο να υπολογίσουμε το $K_{AB} = \left(g^{ab}\right)^{s_A s_B} \bmod p$ και επομένως και το $g^{ab} \bmod p$ για μη αμελητέες περιπτώσεις [Adl77].

-

Αντίθετα, στην περίπτωση που ο κρυπταναλυτής δεν υποκλέπτει μόνο τα μηνύματα, αλλά παρεμβαίνει ενεργά στην επικοινωνία των χρηστών, η ασφάλεια του πρωτοκόλλου MTI δεν είναι αποδεδειγμένη. Αυτό οφείλεται στο ότι το συγκεκριμένο πρωτόκολλο δεν είναι μηδενικής γνώσης. Η απόδειξη ότι δεν είναι μηδενικής γνώσης βασίζεται, και πάλι, στην δυσκολία επίλυσης του προβλήματος των Diffie και Hellman. Πιο συγκεκριμένα, εάν το πρωτόκολλο MTI είναι μηδενικής γνώσης, τότε το πρόβλημα των Diffie και Hellman είναι εύκολο στην επίλυσή του. Οι Desmedt και Burmester [Des93] έχουν προτείνει μια απόδειξη, την οποία έχουν εφαρμόσει για το πρωτόκολλο του Yacobi [Yac90,Yac91]. Σύμφωνα με αυτή, το πρωτόκολλο MTI παρέχει επιπλέον γνώση στον κρυπτοαναλυτή, εάν το κοινό μυστικό κλειδί αποκαλυφθεί. Επομένως, ο κρυπτοαναλυτής μπορεί να χρησιμοποιήσει τα μηνύματα που ανταλλάσσουν μεταξύ τους οι χρήστες και το συγκεκριμένο κοινό μυστικό κλειδί για να υπολογίσει ένα μελλοντικό κοινό μυστικό κλειδί [Des93,Bur94a]. Την δυνατότητα αυτή δεν μπορεί να την έχει ο κρυπτοαναλυτής στην περίπτωση που το πρωτόκολλο είναι των Bellare και Rogaway [Bel94], καθώς το κοινό μυστικό κλειδί δεν μπορεί να διαχωριστεί από ψευδοτυχαίες συμβολοσειρές.

2.5. Ενα κρυπτογραφικό πρωτόκολλο αποδεδειγμένης ασφάλειας

Οπως περιγράφηκε στην προηγούμενη παράγραφο, το πρωτόκολλο MTI δεν είναι αποδεδειγμένης ασφάλειας, καθώς ο κρυπταναλυτής αποκτά επιπλέον γνώση, την οποία μπορεί να χρησιμοποιήσει για να υπολογίσει μελλοντικά κοινά μυστικά κλειδιά, όταν δεν χρησιμοποιείται μη-ομοιόμορφη κατανομή.

Ενας τρόπος αντιμετώπισης της αδυναμίας αυτής, ο οποίος έχει προταθεί από τους Desmedt και Burmester [Des93], είναι, όταν κάθε χρήστης αποδεικνύει στον άλλο χρήστη ότι γνωρίζει τόσο το μυστικό κλειδί του, όσο και τον τυχαίο αριθμό που επιλέγει, κάθε φορά που θέλουν να υπολογίσουν ένα νέο κοινό μυστικό κλειδί.

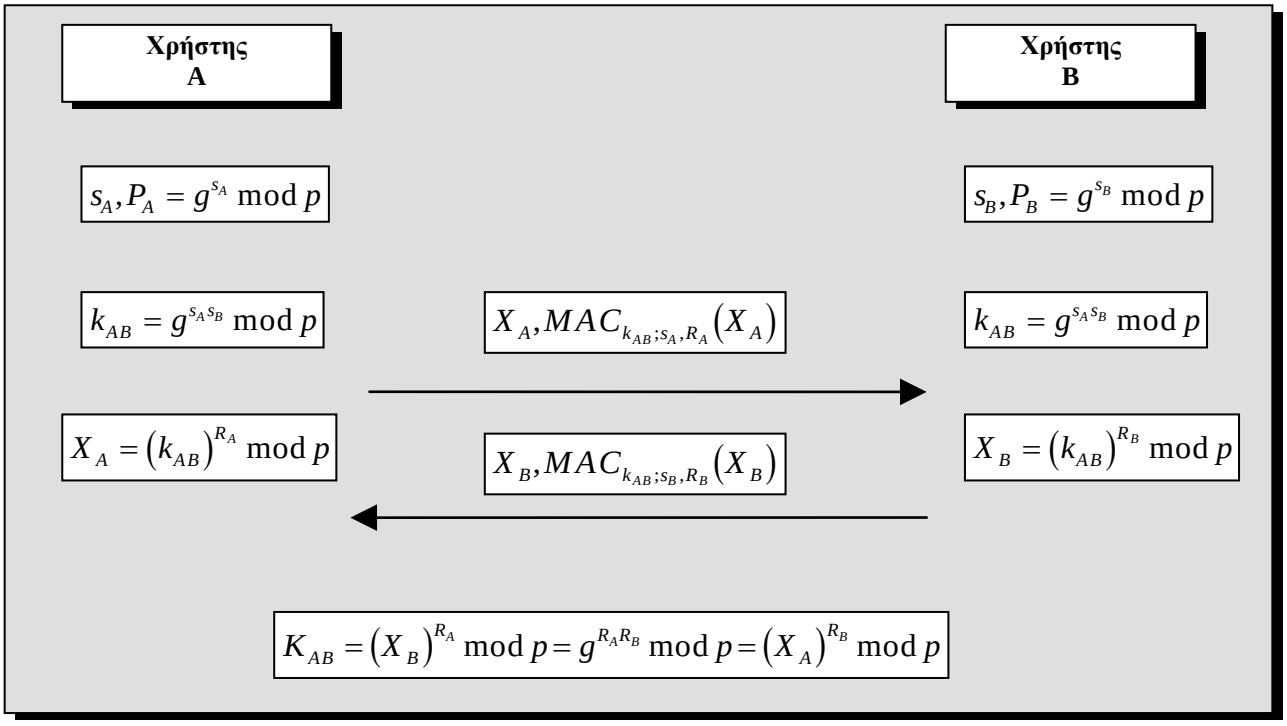
Στην συνέχεια προτείνεται ένα νέο κρυπτογραφικό πρωτόκολλο, το οποίο βασίζεται στο πρωτόκολλο MTI και χρησιμοποιεί κώδικες αυθεντικοποίησης μηνυμάτων Message

-

Authentication Codes (MAC) , βασισμένο σε αποδείξεις μηδενικής γνώσης και το αντίστοιχο κλειδί (του MAC) να εξαρτάται από τις συναρτήσεις κατάτμησης [Bur95a,Bur96].

Οπως είναι γνωστό, οι ψηφιακές υπογραφές και οι εξαρτημένου κλειδιού MAC έχουν πολλά κοινά μεταξύ τους [Sch94]. Η βασική διαφορά βασίζεται στο γεγονός ότι η επαλήθευση των ψηφιακών υπογραφών μπορεί να πραγματοποιηθεί από οποιοδήποτε χρήστη, ενώ των MAC μόνο από αυτούς που γνωρίζουν το συγκεκριμένο κλειδί.

Εστω, ότι ισχύει ό,τι και στο πρωτόκολλο MTI, με μόνη διαφορά ότι κατά την διαδικασία που οι δύο χρήστες *A* και *B* υπολογίζουν τα μηνύματα X_A και X_B αντίστοιχα, δεν ανταλλάσσουν μόνο τα μηνύματα αυτά, αλλά και το αποτέλεσμα ενός MAC στα μηνύματα αυτά. Στο σχήμα 3 παρουσιάζεται το νέο προτεινόμενο κρυπτογραφικό πρωτόκολλο.



Σχήμα 3. Μια παραλλαγή αποδεδειγμένης ασφάλειας του πρωτοκόλλου MTI.

-

Πιο συγκεκριμένα, κάθε χρήστης προσπαθεί να αυθεντικοποιήσει το μήνυμα που ανταλλάσσει, χρησιμοποιώντας ένα MAC με δύο μυστικά κλειδιά. Το ένα κλειδί είναι το γνωστό κλειδί των Diffie και Hellman για τους δύο συγκεκριμένους χρήστες και το δεύτερο κλειδί είναι το μυστικό κλειδί του κάθε χρήστη μαζί με τον τυχαίο εκθέτη που έχει επιλέξει για τον υπολογισμό του μηνύματος που ανταλλάσσει. Οπως και στο πρωτόκολλο MTI, το κοινό μυστικό κλειδί μεταξύ των δύο χρηστών είναι ανεξάρτητο των δημοσίων κλειδιών των χρηστών που συμμετέχουν στην επικοινωνία.

2.6. Αποτελεσματική διαδικασία υλοποίησης

Στο νέο προτεινόμενο κρυπτογραφικό πρωτόκολλο, κάθε χρήστης, που επιθυμεί να έχει ασφαλή επικοινωνία με έναν άλλο χρήστη του συστήματος, θα πρέπει να αποσκοπεί στο ότι ο κρυπτοαναλυτής δεν θα αποκτήσει καμιά γνώση σχετικά με το μυστικό κλειδί του ή/και τον τυχαίο εκθέτη που επιλέγει κάθε φορά. Για την επίτευξη αυτού του στόχου θα χρησιμοποιηθεί η παραλλαγή που έχει προταθεί από τον Schnorr [Sch91] και αφορά την απόδειξη *μηδενικής γνώσης του διακριτού λογάριθμου* που έχει προταθεί από τους Chaum, Evertse και Van de Graaf [Cha87].

Στην παραλλαγή αυτή, ένα κέντρο εμπιστοσύνης επιλέγει ένα μεγάλο πρώτο αριθμό *p*, ένα γεννήτορα *g* και ένα μεγάλο πρώτο διαιρέτη *q* του *p-1* και υπολογίζει το $a = g^{p-1/q} (\mathrm{mod}\, q)$. Στην συνέχεια, δημοσιοποιεί τα *p,q,a*, μια παράμετρο ασφάλειας *t*, όπου $t < \log_2 q$ και τις παραμέτρους μιας ψευδοτυχαίας συνάρτησης $f_{\cdot}(\cdot): Z_q \times \left(Z_q \times Z_q\right) \to \{0,1\}^*$.

Σύμφωνα με την παραλλαγή του Schnorr θα πρέπει οι δύο χρήστες να ακολουθήσουν τα επόμενα βήματα:

1ï. Ο χρήστης Α με μυστικό κλειδί *s* και δημόσιο κλειδί $P = a^s (\mathrm{mod}\, p)$, επιλέγει ένα τυχαίο αριθμό $r \in Z_q$ και στέλνει στον επαληθευτή το μήνυμα $x = a^r (\mathrm{mod}\, p)$.

-

2ï. Ο χρήστης Β απαντά στο μήνυμα που έλαβε με μία τυχαία συμβολοσειρά e με στοιχεία στο $\{0,...,2^{t-1}\}$

3ï. Ο χρήστης Α στέλνει στον χρήστη Β το μήνυμα $y = r - es(\mathrm{mod}\, q)$.

4ï. Ο χρήστης Β, μόλις παραλάβει το μήνυμα, ελέγχει εάν ισχύει το $x = a^y P^e (\mathrm{mod}\, p)$.

Στην περίπτωση που η ισότητα ισχύει, τότε ο χρήστης Β αποδέχεται ότι ο χρήστης Α γνωρίζει το διακριτό λογάριθμο του $P = a^s (\mathrm{mod}\, p)$.

Η πιθανότητα ο χρήστης Α να μη γνωρίζει το μυστικό κλειδί s και συνεπώς να προσποιείται στον χρήστη Α, μπορεί να υπάρχει, εφόσον ο χρήστης Α έχει προβλέψει σωστά την συμβολοσειρά e και έχει υπολογίσει σωστά το αντίστοιχο μήνυμα στο τρίτο βήμα. Η πιθανότητα στην περίπτωση αυτή ονομάζεται *πιθανότητα λάθους* ή *πιθανότητα επιτυχούς προσποίησης* (cheating probability). Σύμφωνα με τον Schnorr, η πιθανότητα λάθους για την παραπάνω απόδειξη είναι ίση με 2^{-t}.

Για μια αποτελεσματική διαδικασία υλοποίησης του προτεινόμενου πρωτοκόλλου συνιστώνται τα ακόλουθα:

1. Στην θέση του γεννήτορα g, το $a = g^{p-1/q} (\mathrm{mod}\, q)$

2. Όλοι οι εκθέτες θα υπολογίζονται στο Z_q (ακόμα και για τα μυστικά κλειδιά)

Για την ταυτόχρονη απόδειξη γνώσης του διακριτού λογάριθμου των $P_A = a^{s_A} (\mathrm{mod}\, p)$ και $X_A = a^{R_A} (\mathrm{mod}\, p)$, ο χρήστης A επιλέγει ένα τυχαίο εκθέτη $r \in Z_q$ και

στέλνει στο χρήστη B το μήνυμα $x = a^r \pmod p$. Στην συνέχεια, ο χρήστης B απαντά με δύο συμβολοσειρές e,e', όπου e,e' έχουν στοιχεία στο $\{0,...,2^{t-1}\}$. Ο χρήστης A στέλνει το μήνυμα $y = r - es_A - e'R_A \pmod q$ στο χρήστη B. Ο χρήστης B υπολογίζει το $x = a^y P_A^e X_A^{e'} \pmod p$. Εάν η ισότητα ισχύει, τότε ο χρήστης A γνωρίζει και το μυστικό του κλειδί αλλά και τον τυχαίο εκθέτη.

Για την ενσωμάτωση του MAC στο προτεινόμενο πρωτόκολλο χρησιμοποιήθηκε μια τεχνική που έχει προταθεί από τους Fiat και Shamir [Fia87] και αφορά *ψηφιακές υπογραφές* βασισμένες σε αποδείξεις μηδενικής γνώσης. Η τεχνική αυτή χρησιμοποιεί μια τυχαία συνάρτηση f. Η υπογραφή ενός μηνύματος m βασισμένη στην απόδειξη του διακριτού λογάριθμου, που περιγράφτηκε παραπάνω, αποτελείται από ένα ζευγάρι (y, e), όπου το e είναι πρόθεμα του $f(m,x)$ όπου $x = a^y P^e \pmod p$. Συνεπώς, στο προτεινόμενο πρωτόκολλο χρησιμοποιείται μια ψευδοτυχαία συνάρτηση $f_{k_{AB}}$ με κλειδί το κλειδί των Diffie και Hellman για τους χρήστες A και B. Ο MAC, που χρησιμοποιείται από τον χρήστη A για να αυθεντικοποιήσει το μήνυμα X_A στον χρήστη B, είναι το $MAC_{k_{AB};s_A,R_A}(X_A) = (y,e,e')$,για το οποίο ee' είναι πρόθεμα της $f_{k_{AB}}(X_A,x)$.

Το βασικό χαρακτηριστικό μιας τέτοιας διαδικασίας αυθεντικοποίησης είναι ότι είναι μηδενικής γνώσης. Η γνώση, η οποία ένας κρυπταναλυτής μπορεί να αποκτήσει, είναι περιορισμένη στο βαθμό ασφάλειας του MAC [Sak93].

2.7 Η ασφάλεια του προτεινόμενου κρυπτογραφικού πρωτοκόλλου

Η ασφάλεια του νέου προτεινόμενου κρυπτογραφικού πρωτοκόλλου βασίζεται στις δύο ακόλουθες προτάσεις:

- Εάν δύο χρήστες χρησιμοποιούν απόδειξη μηδενικής γνώσης των μυστικών κλειδιών και των τυχαίων αριθμών που επιλέγουν και ένας κρυπταναλυτής μπορεί να υπολογίσει το κοινό

μυστικό κλειδί μεταξύ των δύο χρηστών με πιθανότητα μη αμελητέα, τότε το πρόβλημα των Diffie και Hellman είναι εύκολο στον υπολογισμό του [Des93].

- Εάν η τυχαία συνάρτηση και ο MAC που χρησιμοποιούνται μπορούν να αντιγραφούν από έναν κρυπταναλυτή, τότε το πρόβλημα των Diffie και Hellman είναι εύκολο στον υπολογισμό του [Fia87].

Στο προτεινόμενο κρυπτογραφικό πρωτόκολλο η συνάρτηση *f* που χρησιμοποιείται είναι ψευδοτυχαία συνάρτηση. Η απόδειξη, ότι και στην περίπτωση αυτή ισχύει η δεύτερη παρατήρηση, βασίζεται στην ακόλουθη πρόταση:

- Εάν ένας κρυπταναλυτής μπορεί να αντιγράψει τον MAC, όταν χρησιμοποιείται ως ψευδοτυχαία συνάρτηση ενώ, όταν η συνάρτηση είναι τυχαία, αυτό δεν μπορεί να συμβεί, τότε ο συγκεκριμένος κρυπταναλυτής είναι σε θέση να διαχωρίσει μια ψευδοτυχαία συνάρτηση από μία τυχαία. Αυτό όμως δεν ισχύει σύμφωνα με τα όσα έχουν αναφερθεί στις προηγούμενες παραγράφους σχετικά με τις ψευδοτυχαίες συναρτήσεις και τις δυνατότητες που έχει ο κρυπταναλυτής σε σχέση μ' αυτές.

Στην διαδικασία υλοποίησης του προτεινόμενου μοντέλου κατάλληλες ψευδοτυχαίες συναρτήσεις είναι αυτές που προτείνονται από τους Bellare και Rogaway [Bel94] όπου χρησιμοποιείται το DES σε κατάσταση Cipher-Block-Chaining, ενώ κατάλληλη συνάρτηση κατάτμησης μπορεί να είναι η MD5 [Riv92, Sch94].

2.8 Συμπεράσματα

Στο κεφάλαιο αυτό εξετάσθηκε ένα από τα βασικά προβλήματα στο χώρο της κρυπτογραφίας, της δημιουργίας ενός κοινού μυστικού κλειδιού μεταξύ δύο χρηστών, που επιθυμούν να επικοινωνήσουν μεταξύ τους.

-

Για την επίλυση του συγκεκριμένου προβλήματος έχουν προταθεί διάφορα μοντέλα, από τα οποία εξετάσθηκαν αυτά που είναι αποτελεσματικά και αποδεδειγμένης ασφάλειας.

Συγκεκριμένα, εξετάστηκε το μοντέλο που προτάθηκε από τους Bellare και Rogaway το οποίο βασίζεται σε ψευδοτυχαίες συναρτήσεις. Απαραίτητη προϋπόθεση είναι οι χρήστες, που θέλουν να επικοινωνήσουν, να έχουν στην κατοχή τους μυστικά κλειδιά, τα οποία έχουν αποκτήσει με ασφαλή τρόπο. Στο μοντέλο των Bellare - Rogaway βασίζεται και η προσπάθεια των Wilson-Johnson-Menezes να παρουσιάσουν κρυπτογραφικά πρωτόκολλα συμφωνίας κλειδιού, αλλά και διαδικασίες υλοποίησής τους [Wil97].

Το δεύτερο μοντέλο βασίζεται σε συστήματα μηδενικής γνώσης. Στο μοντέλο αυτό, για τους χρήστες που επιθυμούν να επικοινωνήσουν μεταξύ τους δεν απαιτείται να αποκτήσουν με τρόπο ασφαλή τα μυστικά κλειδιά, καθώς κάθε χρήστης μπορεί να διαλέξει το δικό του μυστικό κλειδί. Επίσης, το κέντρο εμπιστοσύνης περιορίζεται στην διαχείριση των δημόσιων κλειδιών χωρίς να έχει καμιά άλλη συμμετοχή στη δημιουργία του κοινού μυστικού κλειδιού.

Τέλος, παρουσιάστηκε ένα νέο κρυπτογραφικό πρωτόκολλο που είναι μια παραλλαγή του πρωτοκόλλου Diffie-Hellman. Τα κύρια χαρακτηριστικά του είναι η αποδεδειγμένη ασφάλειά του και η δυνατότητα αποτελεσματικής υλοποίησης. Η ανάγκη, να προτείνονται κρυπτογραφικά πρωτόκολλα, τα οποία όχι μόνο ικανοποιούν την θεωρητική πλευρά της κρυπτογραφίας, αλλά και μπορούν να υλοποιηθούν, εμφανίζεται όλο και περισσότερο έντονη, καθώς αποτελεί το μοναδικό τρόπο καθιέρωσης και χρησιμοποίησης συστημάτων ασφάλειας σε πραγματικά περιβάλλοντα.

-

ΚΕΦΑΛΑΙΟ 3

ΚΡΥΠΤΟΓΡΑΦΙΚΑ ΠΡΩΤΟΚΟΛΛΑ ΣΥΝΔΙΑΣΚΕΨΗΣ

3.1 Τα κρυπτογραφικά πρωτόκολλα συνδιάσκεψης

Καθώς τα περισσότερα κρυπτογραφικά πρωτόκολλα αφορούσαν την ασφαλή επικοινωνία δύο μόνο χρηστών, εμφανίστηκε η ανάγκη για κρυπτογραφικά πρωτόκολλα τα οποία θα επέτρεπαν την ασφαλή επικοινωνία ανάμεσα σε περισσότερους από δύο χρήστες [Jan91, Ing82, Koy88, Oko89, Fis92, Blu93]. Τα πρωτόκολλα αυτά ονομάζονται *κρυπτογραφικά πρωτόκολλα συνδιάσκεψης* (conference cryptographic protocols). Πιο συγκεκριμένα, κρυπτογραφικό πρωτόκολλο συνδιάσκεψης θεωρείται κάθε γενίκευση ενός πρωτοκόλλου συμφωνίας κλειδιού για δύο χρήστες, το οποίο επιτρέπει και σε περισσότερους από δύο χρήστες να έχουν στην κατοχή τους ένα κοινό μυστικό κλειδί. Τα πρωτόκολλα αυτά ονομάζονται και *κρυπτογραφικά πρωτόκολλα κλειδιού συνδιάσκεψης* (conference key cryptographic protocols).

Ενα χαρακτηριστικό παράδειγμα κρυπτογραφικού πρωτοκόλλου συνδιάσκεψης είναι η ταυτόχρονη τηλεφωνική επικοινωνία πολλών χρηστών (telephone conference calls). Το τηλεφωνικό κέντρο θα επιτρέψει σ' ένα σύνολο χρηστών να έχουν ταυτόχρονη τηλεφωνική επικοινωνία, συνδιάλεξη, αφού πρώτα έχουν στην κατοχή τους ένα κοινό μυστικό κλειδί. Ενας εύκολος τρόπος δημιουργίας ενός κοινού μυστικού κλειδιού ή κλειδιού συνδιάσκεψης για ένα σύνολο χρηστών n, με $n>3$, είναι ο ακόλουθος:

-

Επιλέγεται ένα κέντρο εμπιστοσύνης, το οποίο είναι κοινά αποδεκτό από όλους τους χρήστες που θα συμμετέχουν στη συνδιάσκεψη. Το ρόλο του κέντρου εμπιστοσύνης, στο συγκεκριμένο παράδειγμα, έχει το τηλεφωνικό κέντρο. Κάθε χρήστης μοιράζεται ένα μοναδικό κοινό κλειδί με το κέντρο εμπιστοσύνης. Το κέντρο εμπιστοσύνης επιλέγει ένα τυχαίο κλειδί. Το επιλεγμένο τυχαίο κλειδί διανέμεται στους χρήστες μέσω ενός κρυπτογραφικού πρωτοκόλλου μεταφοράς κλειδιού.

Τα βασικά μειονεκτήματά του είναι η ενεργός συμμετοχή του κέντρου εμπιστοσύνης στην δημιουργία του κοινού κλειδιού, που έχει ως αποτέλεσμα, το κέντρο εμπιστοσύνης να γνωρίζει το κοινό μυστικό κλειδί, καθώς και το υπολογιστικό κόστος που απαιτείται για το μεγάλο αριθμό των μηνυμάτων που ανταλλάσσονται μέχρι όλοι οι χρήστες να αποκτήσουν το κοινό κλειδί.

Τα κυρία χαρακτηριστικά των πρωτοκόλλων συνδιάσκεψης είναι τα ακόλουθα:

- Κάθε σύνολο χρηστών πρέπει να έχει διαφορετικό κοινό κλειδί συνδιάσκεψης. Τα σύνολα χρηστών μπορούν να διαφέρουν τόσο στο πλήθος των χρηστών, όσο και στο ποιοι είναι οι συγκεκριμένοι χρήστες

- Κάθε κλειδί συνδιάσκεψης, που είναι μεταβλητό και όχι σταθερό, θα πρέπει να ανανεώνεται κάθε φορά που οι χρήστες ξεκινούν μια νέα επικοινωνία ή που οι ίδιοι το επιθυμούν.

- Οι πληροφορίες και τα δεδομένα που ανταλλάσσουν οι χρήστες για να δημιουργήσουν το κλειδί συνδιάσκεψης, μπορεί να είναι γνωστές σε όλους τους χρήστες και η μεταφορά τους δεν πρέπει να απαιτεί ασφαλή δίαυλο επικοινωνίας.

- Κάθε χρήστης, που συμμετέχει στην επικοινωνία, δεν έχει τη δυνατότητα πριν την ολοκλήρωσή της, να υπολογίσει το κοινό μυστικό κλειδί από τις πληροφορίες και τα δεδομένα που θα έχει στην κατοχή του.

-

Σε ορισμένα προτεινόμενα κρυπτογραφικά πρωτόκολλα γίνεται προσπάθεια επίλυσης του προβλήματος, που δημιουργείται από την απαίτηση της συνεχούς διαθεσιμότητας του κέντρου εμπιστοσύνης [Koy88, Oka89, Tsu89]. Ο πιο γνωστός τρόπος αντιμετώπισης του συγκεκριμένου προβλήματος, είναι το κέντρο εμπιστοσύνης να παρέχει σε κάθε χρήστη του συστήματος μία έξυπνη κάρτα, στην οποία έχουν καταχωρηθεί οι αναγκαίοι παράμετροι. Ομως και στην περίπτωση αυτή, το κέντρο εμπιστοσύνης, που γνωρίζει τις παραμέτρους αυτές, μπορεί να αποκαλύψει τα μηνύματα που ανταλλάσσουν οι χρήστες μεταξύ τους και συνεπώς να υπολογίσει το κοινό μυστικό κλειδί.

Οι Ingemarsson, Tang και Wong έχουν προτείνει ένα πρωτόκολλο συνδιάσκεψης, όπου το κοινό κλειδί μεταξύ των χρηστών είναι μία *συμμετρική συνάρτηση* [Ing82]. Το βασικό μειονέκτημα αυτού του πρωτοκόλλου είναι η ασφάλειά του, καθώς οι πληροφορίες που οι χρήστες ανταλλάσσουν για τη δημιουργία του κοινού κλειδιού μπορούν να χρησιμοποιηθούν από έναν κρυπτοαναλυτή και έτσι να αποκαλυφθεί το κοινό κλειδί. Οι Fischer και Wright έχουν προτείνει μια ομάδα πρωτοκόλλων συνδιάσκεψης τα οποία βασίζονται στην τυχαία επιλογή και μπορούν να χρησιμοποιηθούν σε ορισμένες περιπτώσεις [Fis92].

Οι Burmester και Desmedt [Bur95], έχουν προτείνει ένα πρωτόκολλο συνδιάσκεψης, το οποίο είναι παρόμοιο με το πρωτόκολλο των Ingemarsson, Tang και Wong, αλλά χρησιμοποιούν *κυκλική συνάρτηση*. Τα βασικά του πλεονεκτήματα είναι:

- Ο αριθμός των ανταλλαγών, που απαιτούνται για τον υπολογισμό του κοινού κλειδιού συνδιάσκεψης, είναι ανεξάρτητος από τον αριθμό των χρηστών που συμμετέχουν στην επικοινωνία.

- Παρέχει αυθεντικοποίηση των χρηστών, χρησιμοποιώντας ένα σχήμα αυθεντικοποίησης δημοσίου κλειδιού, το οποίο είναι αποδεδειγμένης ασφάλειας.

-

– Εχει αποδεδειγμένη ασφάλεια.

Πρωτόκολλα / **Χαρακτηριστικά**	Koyama Ohta 1	Koyama Ohta 2	Koyama Ohta 3	Tsujii Itoh	Okamato Tanaka	Burmester Desmedt
Το κέντρο εμπιστοσύνης γνωρίζει τα κοινά κλειδιά	Ναι	Ναι	Ναι	Ναι	Ναι	Οχι
Απαιτούμενοι υπολογισμοί χρήστη (για m χρήστες)	11exp	8m+1 exp	8m+1 exp	2 exp	2 exp	m+2 exp
Υπολογιστικά βήματα	m-1	3	3	1	1	3
Αυθεντικοποίηση χρηστών	Ναι	Ναι	Ναι	Ναι	Ναι	Ναι
Συνολικός αριθμός μηνυμάτων που ανταλλάσσουν μεταξύ τους οι χρήστες	m (m-1)	3m (m-1)	3 (m-1)	---	1	2(m-1)
Ανανέωση κλειδιών (Freshness)	Ναι	Ναι	Ναι	Οχι	Ναι	Ναι
Η Ασφάλεια βασίζεται σε	παραγοντοποίηση μεγάλων αριθμών και υπολογισμό του διακριτού λογαρίθμου			υπολογι-σμό του διακριτού λογαρίθμου	πρόβλημα D-H και RSA	πρόβλημα D-H

Πίνακας 1. Συγκριτικός πίνακας πρωτοκόλλων συνδιάσκεψης

Στον πίνακα 1, παρουσιάζονται τα αποτελέσματα ορισμένων "μετρήσεων"[1] και αφορούν τα πρωτόκολλα των Koyama και Ohta, των Tsujii και Itoh, των Okamato και Tanaka, και των

[1] Οι "μετρήσεις" παρουσιάζονται αναλυτικά στην Εισαγωγή, παράγραφος 5 - Κριτήρια αποδοτικότητας ενός κρυπτογραφικού πρωτοκόλλου

-

Burmester και Desmedt. Η επιλογή των πρωτοκόλλων έχει πραγματοποιηθεί, ώστε να περιγράφονται όλες οι προσεγγίσεις που αναφέρθηκαν προηγούμενα.

Ειδικότερα, το πρωτόκολλο των Koyama και Ohta έχει ως πλεονεκτήματα το μικρό αριθμό υπολογιστικών βημάτων, καθώς και την ανανέωση κλειδιών, ενώ ως κύριο μειονέκτημα έχει ότι το κέντρο εμπιστοσύνης γνωρίζει τα κοινά μυστικά κλειδιά.

Το πρωτόκολλο των Tsujii και Itoh έχει ως πλεονεκτήματα το μικρό υπολογιστικό κόστος και το μηδενικό αριθμό ανταλλαγής μηνυμάτων, ενώ ως βασικό μειονέκτημα έχει τη μη ανανέωση των κλειδιών.

Το πρωτόκολλο των Okamoto και Tanaka έχει ως πλεονεκτήματα το μικρό υπολογιστικό κόστος και αριθμό μηνυμάτων που ανταλλάσσονται μεταξύ των χρηστών και την ανανέωση των κλειδιών, ενώ ως κύριο μειονέκτημα έχει, ότι το κέντρο εμπιστοσύνης γνωρίζει τα κοινά μυστικά κλειδιά.

Το πρωτόκολλο των Burmester και Desmedt έχει ως πλεονεκτήματα ότι το κέντρο εμπιστοσύνης δεν πρέπει να γνωρίζει τα κοινά κλειδιά συνδιάσκεψης και το μικρό απαιτούμενο υπολογιστικό κόστος.

Το πρωτόκολλο των Burmester και Desmedt αποτελεί τη βάση για το νέο προτεινόμενο κρυπτογραφικό πρωτόκολλο, που περιγράφεται στις επόμενες παραγράφους, το οποίο προσπαθεί να περιλάβει όλα τα πλεονεκτήματα των παραπάνω κρυπτογραφικών πρωτοκόλλων (στο βαθμό που αυτό είναι δυνατό). Παράλληλα, γίνεται μια προσπάθεια να ληφθούν υπόψη και άλλες παράμετροι, που θεωρούνται αναγκαίες και απαραίτητες, ώστε το προτεινόμενο κρυπτογραφικό πρωτόκολλο να μπορεί να χρησιμοποιηθεί σε πραγματικά περιβάλλοντα.

-

3.2 Ενα κρυπτογραφικό πρωτόκολλο συνδιάσκεψης

Ενα κρυπτογραφικό πρωτόκολλο χαρακτηρίζεται ως ασφαλές, όταν η ασφάλεια που παρέχει, βασίζεται σε ένα μοντέλο αποδεδειγμένης ασφάλειας και μπορεί να αντιμετωπίσει διάφορες *επιθέσεις* (όπως κρυπτογραφημένου κειμένου μόνο, γνωστών κειμένων κλπ [Bra87, Sch94, Sim91]).

Αρχικά, η επαλήθευση της ασφάλειας των κρυπτογραφικών πρωτοκόλλων, ήταν βασισμένη στην αποτυχία των προσπαθειών εύρεσης κάποιας αδυναμίας του πρωτοκόλλου. Από τις αρχές της δεκαετίας του '80 πολλοί ειδικοί στο χώρο της κρυπτογραφίας, όπως οι Bellare, Blum, Burmester, Desmedt, Goldwasser, Micali, Rivest, Rogaway και Yao, προσπάθησαν να ορίσουν ένα γενικό πλαίσιο, μέσα στο οποίο θα επαληθευόταν κατά πόσο ένα κρυπτογραφικό πρωτόκολλο παρέχει αποδειγμένη ασφάλεια. [Bel94, Bir92, Blu84, Des93, Gol84, Gol88, Lei94, Yao82].

Η ασφάλεια ενός κρυπτογραφικού πρωτοκόλλου μπορεί να βασίζεται σε πρότυπα και γενικά αποδεκτές υποθέσεις πολυπλοκότητας. Σύμφωνα με τους Burmester και Desmedt [Bur95] ένα κρυπτογραφικό πρωτόκολλο συνδιάσκεψης θεωρείται ασφαλές, εάν ισχύει η πρόταση:

> *Εστω* $U_1,U_2,..,U_n$ *οι χρήστες του συστήματος και ότι από αυτούς οι* $n' > 0$ *είναι έντιμοι , ενώ οι υπόλοιποι* $n''=n-n' \geq 0$ *δεν είναι έντιμοι και έστω ότι υπάρχει η δυνατότητα επικοινωνίας μεταξύ των μη-έντιμων χρηστών και ενός κρυπταναλυτή, τότε ασφαλές κρυπτογραφικό πρωτόκολλο συνδιάσκεψης είναι το πρωτόκολλο εκείνο, όπου είναι υπολογιστικά αδύνατον για κάθε υποσύνολο των μη-έντιμων χρηστών σε συνεργασία με τον κρυπταναλυτή να υπολογίσουν το ίδιο κοινό μυστικό κλειδί, το οποίο υπολογίζουν οι έντιμοι χρήστες του συστήματος.*

Με τον όρο "έντιμος" χρήστης χαρακτηρίζεται, κάθε χρήστης που δεν αποσκοπεί στη παραβίαση του κρυπτογραφικού πρωτοκόλλου.

-

Στη συνέχεια, προτείνεται ένα νέο κρυπτογραφικό πρωτόκολλο συνδιάσκεψης, το CP. Η ασφάλεια του κρυπτογραφικού πρωτοκόλλου συνδιάσκεψης CP βασίζεται στην δυσκολία επίλυσης του προβλήματος των Diffie-Hellman [Dif76]. Ο ρόλος του κέντρου εμπιστοσύνης περιορίζεται στην επιλογή των βασικών παραμέτρων του κρυπτογραφικού πρωτοκόλλου, *p*, *α* και *q*. Η παράμετρος *α* είναι η βάση της δύναμης της ισοδυναμίας του ισουπολοίπου, της οποίας η τάξη *q* είναι μεγάλη.

Κάθε χρήστης του συστήματος U_i επιλέγει ένα μυστικό κλειδί $s_i \in Z_q$, υπολογίζει το δημόσιο κλειδί του $P_i = a^{s_i} \bmod p$ και το δημοσιοποιεί στους υπόλοιπους χρήστες του συστήματος με τη βοήθεια του κέντρου εμπιστοσύνης. Ο υπολογισμός του δημοσίου κλειδιού και η δημοσιοποίησή του στους υπόλοιπους χρήστες πραγματοποιείται κατά την διαδικασία ένταξης του χρήστη στο σύστημα.

Εστω ότι $U_1,U_2,...,U_n$ είναι οι χρήστες του συστήματος που επιθυμούν να αποκτήσουν ένα κοινό μυστικό κλειδί επικοινωνίας ώστε να μπορούν να ανταλλάξουν τα μηνύματα που θέλουν μεταξύ τους με ασφάλεια.

1ï Κάθε χρήστης U_i , *i=1,2,..., n* επιλέγει τυχαία $r_i \in Z_q$ και υπολογίζει

$$X_i = a^{r_i} \bmod p . \qquad (1)$$

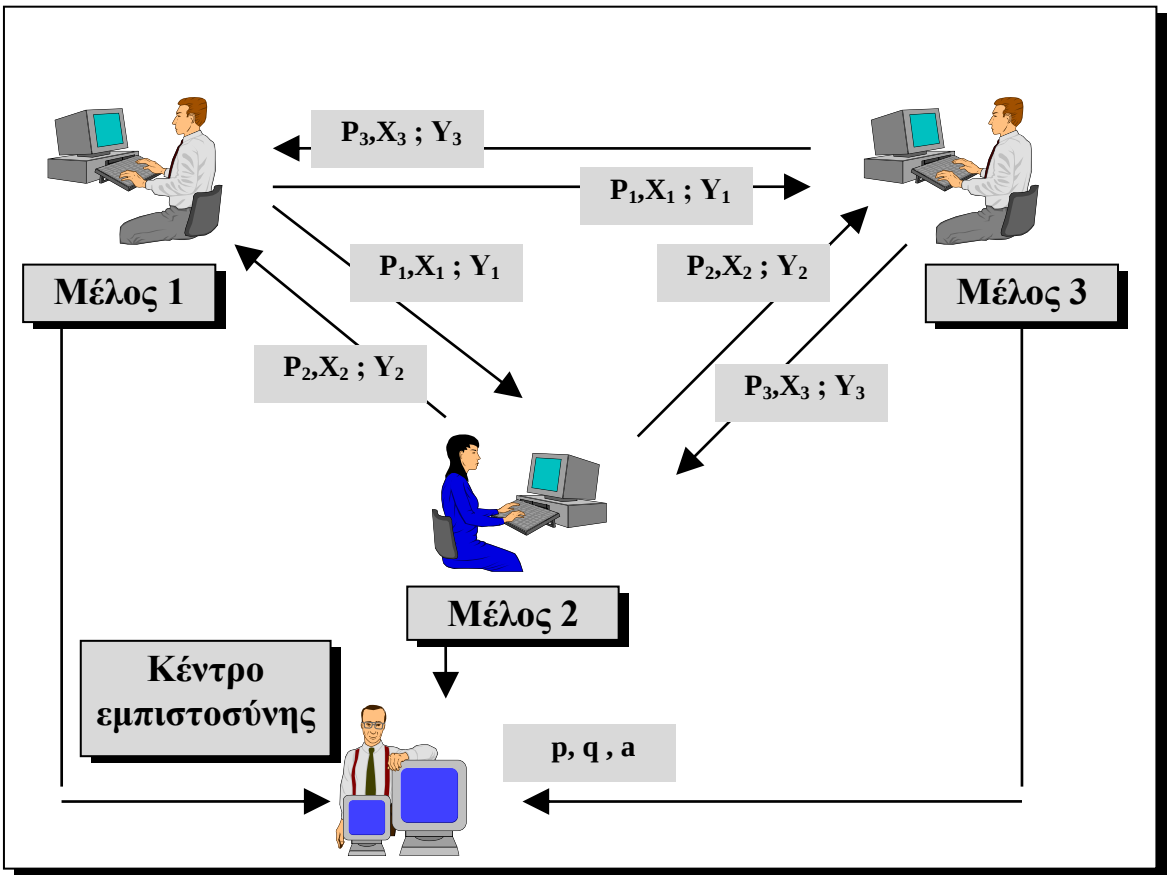
το οποίο γνωστοποιεί σ' όλους τους υπόλοιπους χρήστες που συμμετέχουν στην επικοινωνία. Στη περίπτωση που τα μηνύματα X_i, γίνουν γνωστά σ' άλλους χρήστες - χρήστες που δεν θα συμμετέχουν στην επικοινωνία - τότε η ασφάλεια του κρυπτογραφικού πρωτοκόλλου παραμένει αμετάβλητη.

2ï Κάθε χρήστης U_i , *i=1,2,..., n* υπολογίζει

-

$$Y_i \equiv \left(P_{i+1}\right)^{r_i} \Big/ \left(X_{i-1}\right)^{s_i} \equiv \left(X_i\right)^{s_{i+1}} \Big/ \left(P_i\right)^{r_{i-1}} (\mathrm{mod}\ p) \qquad (2)$$

με την προϋπόθεση, ότι οι χρήστες βρίσκονται σε κύκλο. Στη συνέχεια, κάθε χρήστης U_i δημοσιοποιεί το Y_i στους υπόλοιπους χρήστες. Στην περίπτωση που τα μηνύματα Y_i γίνουν γνωστά σ' άλλους χρήστες - χρήστες, που δε θα συμμετέχουν στην επικοινωνία, τότε η ασφάλεια του κρυπτογραφικού πρωτοκόλλου παραμένει αμετάβλητη.



Σχήμα 1. Κρυπτογραφικό πρωτόκολλο CP για τρεις χρήστες.

Το κοινό μυστικό κλειδί για τους χρήστες $U_1,U_2,...,U_n$ είναι το

-

$$K \equiv a^{r_1 s_2 + r_2 s_3 + \ldots + r_n s_1} (\mathrm{mod}\, p),$$

το οποίο κάθε χρήστης U_i μπορεί να υπολογίσει με τη βοήθεια των (1) και (2) και αφού:

$$K \equiv K_i \equiv \left(X_{i-1}\right)^{n s_1} . Y_i^{n-1} . Y_{i+1}^{n-2} \ldots Y_{i-2} (\mathrm{mod}\, p)$$

Επομένως, εάν ένας τρίτος χρήστης - χρήστης που δεν συμμετέχει στην επικοινωνία - έχει στην κατοχή του όλα τα Y_i και X_i, δεν μπορεί να υπολογίσει το κοινό μυστικό κλειδί *K*, αφού δεν γνωρίζει το μυστικό κλειδί s_i

Στην δημιουργία του κοινού μυστικού κλειδιού οι δείκτες *i-1*, *i+1*, ... καθορίζονται σύμφωνα με την θέση που κατέχουν οι χρήστες στον κύκλο. Στο σχήμα 1 παρουσιάζεται το προτεινόμενο κρυπτογραφικό πρωτόκολλο για τρεις χρήστες.

Στην περίπτωση που ο αριθμός των χρηστών είναι δύο ($n = 2$), τότε για το 2ϊ βήμα του κρυπτογραφικού πρωτοκόλλου ισχύει:

$$Y_1 \equiv Y_2^{-1} \equiv P_2^{r_1} \Big/ P_1^{r_2} (\mathrm{mod}\, p).$$

Συνεπώς, οι δύο χρήστες δεν χρειάζεται να ανταλλάξουν τα Y_i ,καθώς μπορούν να τα υπολογίσουν μόνοι τους, αφού γνωρίζουν τα δημόσια κλειδιά. Το κοινό μυστικό κλειδί για δύο χρήστες είναι:

$$K = a^{r_1 s_2 + r_2 s_1} \bmod p$$

το οποίο είναι το ίδιο με το 'non-paradoxical' πρωτόκολλο διανομής κλειδιού που έχει προταθεί από τον Yacobi [Yac91].

-

Το προτεινόμενο πρωτόκολλο αποτελεί τροποποίηση του πρωτοκόλλου των Burmester και Desmedt [Bur95]. Η βασική διαφορά των δύο κρυπτογραφικών πρωτοκόλλων είναι ότι, στο πρωτόκολλο των Burmester και Desmedt, το κοινό κλειδί περιέχει μόνο τους τυχαίους αριθμούς, που οι χρήστες επιλέγουν κατά τη διαδικασία της επικοινωνίας, ενώ στο προτεινόμενο κρυπτογραφικό πρωτόκολλο περιέχονται και τα μυστικά κλειδιά των χρηστών.

Στο Κεφάλαιο 4 περιγράφεται η εφαρμογή του προτεινόμενου κρυπτογραφικού πρωτοκόλλου CP σ' ένα ευρωπαϊκό σύστημα ανταλλαγής πληροφοριών που αφορά τη διαδικασία που θα πρέπει να ακολουθηθεί σε περίπτωση ατυχήματος, που πιθανώς να οφείλεται σε ιατρική συσκευή.

Σε αντίθεση με το κρυπτογραφικό πρωτόκολλο των Burmester και Desmedt, το κρυπτογραφικό πρωτόκολλο CP, επιτρέπει σε κρυπτοαναλυτές να αποκτήσουν γνώση, στην περίπτωση, όπου για *m* χρήστες, οι *m-1* μπορούν να είναι μη-έντιμοι χρήστες (δηλ. χρήστες που προσπαθούν να αποκτήσουν γνώση για το κοινό μυστικό κλειδί ή να το υπολογίσουν βασιζόμενοι σε προηγούμενες πληροφορίες ή κλειδιά).

Στις επόμενες παραγράφους, 3.2 και 3.3., θα αναλυθούν όλες οι πιθανές επιθέσεις που μπορεί να υπάρχουν στο συγκεκριμένο κρυπτογραφικό πρωτόκολλο, καθώς και οι τρόποι με τους οποίους μπορούν αυτές να αντιμετωπισθούν. Ενώ στη συνέχεια, παράγραφο 3.5, θα περιγραφεί μια παραλλαγή του πρωτοκόλλου CP, το CP2, με τα πλεονεκτήματα /μειονεκτήματά του.

3.3 Ανθεκτικότητα σε παθητικές επιθέσεις

Η απόδειξη ότι το προτεινόμενο κρυπτογραφικό πρωτόκολλο CP είναι ανθεκτικό σε παθητικές επιθέσεις, δηλαδή παρέχει ασφάλεια σε περίπτωση παθητικού αντιπάλου, βασίζεται στο ακόλουθο θεώρημα [Bur95]:

-

Θεώρημα

Εάν το μέγεθος του μυστικού κοινού κλειδιού είναι πολυωνυμικά περιορισμένο σε σχέση με το p και εάν το πρόβλημα των Diffie-Hellman είναι υπολογιστικά αδύνατο να λυθεί, τότε το κρυπτογραφικό πρωτόκολλο είναι ανθεκτικό σε παθητικούς αντιπάλους.

Απόδειξη :

Η απόδειξη του θεωρήματος είναι παρόμοια με την απόδειξη του θεωρήματος 1 στο [Bur95].

3.4 Ανθεκτικότητα σε ενεργητικές επιθέσεις

Ενεργητικές επιθέσεις αφορούν την περίπτωση, κατά την οποία ο αντίπαλος Ε έχει πολλές δυνατότητες [Ben91, Des88]. Πιο συγκεκριμένα, θεωρούμε ότι ο αντίπαλος Ε μπορεί να διαβάζει τα μηνύματα που οι χρήστες ανταλλάσσουν, τροποποιεί τα μηνύματα που ανταλλάσσονται, αντικαθιστά νέα μηνύματα με προηγούμενα (δηλαδή μηνύματα που αφορούν προηγούμενες χρονικά επικοινωνίες), επικοινωνεί παράλληλα με τους πιθανούς χρήστες και μπορεί να γνωρίζει κοινά μυστικά κλειδιά προηγουμένων συνδιασκέψεων. Ο μόνος περιορισμός είναι ότι ο αντίπαλος Ε είναι πολυωνυμικά περιορισμένος.

Σύμφωνα με τους Burmester και Desmedt [Des93], στην περίπτωση που οι χρήστες που συμμετέχουν είναι μόνο δύο και ο αντίπαλος γνωρίζει ορισμένα από τα προηγούμενα κοινά μυστικά κλειδιά, τότε το σύστημα παρέχει επιπλέον γνώση (leaks knowledge) σε γενικής μορφής επίθεση [Bur94].

Στην συνέχεια, περιγράφεται ο τρόπος που μπορεί να ακολουθήσει ο αντίπαλος, στην περίπτωση των τριών χρηστών που συμμετέχουν στην συνδιάσκεψη, ώστε να αποκτήσει γνώση σχετικά με το κοινό μυστικό κλειδί συνδιάσκεψης.

-

Υποθέτουμε ότι οι χρήστες U_1,U_2,U_3 του συστήματος έχουν υπολογίσει το κοινό μυστικό κλειδί

$$K \equiv a^{r_1 s_2 + r_2 s_3 + r_3 s_1} (\mathrm{mod}\ p) \qquad (8)$$

και X_1, X_2, X_3 είναι αντίστοιχα τα μηνύματα που οι τρεις χρήστες έχουν υπολογίσει και δημοσιοποιήσει στους άλλους χρήστες. Εστω ότι ο αντίπαλος $\tilde{U}_4$ είναι χρήστης του συστήματος με μυστικό κλειδί s_4, και δημόσιο κλειδί P_4,και επιθυμεί να αποκαλύψει το κοινό μυστικό κλειδί *K*. Ο αντίπαλος $\tilde{U}_4$ γνωρίζει τα μηνύματα X_1, X_2, X_3 σύμφωνα με τις δυνατότητες του αντιπάλου που περιγράψαμε στην αρχή της παραγράφου. Για τον υπολογισμό του κοινού μυστικού κλειδιού *K*, ο αντίπαλος $\tilde{U}_4$ ακολουθεί τα εξής βήματα:

1ï: Ο αντίπαλος $\tilde{U}_4$ ενημερώνει το χρήστη U_1 ότι επιθυμεί να επικοινωνήσει μαζί του και χρησιμοποιείται το πρωτόκολλο για δύο χρήστες $\left(U_1,\tilde{U}_4\right)$. Ο αντίπαλος χρησιμοποιεί το μήνυμα X_3 το οποίο και στέλνει στο χρήστη U_1 ενώ ο χρήστης U_1 στέλνει το ακόλουθο μήνυμα στον αντίπαλο:

$$X_1' = a^{r_1'} \bmod p. \qquad (9)$$

Οι δύο χρήστες υπολογίζουν το κοινό μυστικό κλειδί:

$$K_1 = a^{r_1' s_4 + r_3 s_1} \bmod p. \qquad (10)$$

Ο αντίπαλος $\tilde{U}_4$ (που γνωρίζει το s_4) μπορεί με τη βοήθεια της (10) να υπολογίσει το:

$$k_1 = a^{r_3 s_1} \bmod p \qquad (11)$$

-

2ï: (Επανάληψη του βήματος 1 αλλά η επικοινωνία του αντίπαλου είναι τώρα με το χρήστη U_2). Ειδικότερα, ο αντίπαλος χρησιμοποιεί το μήνυμα X_1 το οποίο και στέλνει στο χρήστη U_2, ενώ ο χρήστης U_2 στέλνει στον αντίπαλο το μήνυμα :

$$X_2' = a^{r_2'} \bmod p \qquad (12)$$

Οι δύο χρήστες υπολογίζουν το κοινό μυστικό κλειδί:

$$K_2 = a^{r_2' s_4 + r_1 s_2} \bmod p \qquad (13)$$

Ο αντίπαλος που γνωρίζει το s_4, με την βοήθεια της (13) μπορεί να υπολογίσει το:

$$k_2 = a^{r_1 s_2} \bmod p. \qquad (14)$$

3ï: (Επανάληψη του βήματος 1 αλλά η επικοινωνία του αντίπαλου είναι τώρα με τον χρήστη U_3). Ειδικότερα, ο αντίπαλος χρησιμοποιεί το μήνυμα X_2, το οποίο και στέλνει στο χρήστη U_3 ενώ ο χρήστης U_3 στέλνει στον αντίπαλο το μήνυμα:

$$X_3' = a^{r_3'} \bmod p. \qquad (15)$$

Οι δύο χρήστες υπολογίζουν το κοινό μυστικό κλειδί:

$$K_3 = a^{r_3' s_4 + r_2 s_3} \bmod p. \qquad (16)$$

Ο αντίπαλος, που γνωρίζει το s_4, με την βοήθεια της ισότητας (16) μπορεί να υπολογίσει το:

-

$$k_3 = a^{r_2 s_3} \bmod p. \qquad (17)$$

4ï: Από τις (11) , (14) και (17) ο αντίπαλος $\tilde{U}_4$ μπορεί να υπολογίσει το κοινό μυστικό κλειδί *K*.

Οι τρόποι αντιμετώπισης τέτοιων επιθέσεων έχουν αναλυθεί και παρουσιαστεί από τον Burmester [Bur94]. Ενας από τους τρόπους αντιμετώπισης, είναι η χρήση *συναρτήσεων κατάτμησης* (hash functions). Ειδικότερα, οι χρήστες που συμμετέχουν σε μια συνδιάσκεψη μπορούν να χρησιμοποιούν αντί για το κοινό μυστικό κλειδί, το αποτέλεσμα μιας συνάρτησης κατάτμησης με μεταβλητή το κοινό μυστικό κλειδί. Με το τρόπο αυτό εμποδίζονται τέτοιες επιθέσεις.

Αντίθετα, στα μηνύματα Y_i, τα οποία οι χρήστες υπολογίζουν και ανταλλάσσουν στο 2ï βήμα του κρυπτογραφικού πρωτοκόλλου, δεν μπορούν να χρησιμοποιηθούν συναρτήσεις κατάτμησης, με αποτέλεσμα να παρέχεται γνώση, την οποία ο αντίπαλος μπορεί να χρησιμοποιήσει για να υπολογίσει προηγούμενα κοινά μυστικά κλειδιά.

Εστω, ότι οι χρήστες που συμμετέχουν στην επικοινωνία είναι δύο (U_i, U_{i+1}),και σύμφωνα με το κρυπτογραφικό πρωτόκολλο, X_i, X_{i-1}^{-1} είναι τα μηνύματα που ανταλλάσσουν στο 1ï βήμα και $Y_i = a^{r_i s_{i+1} - r_{i-1} s_i} \bmod p$ στο 2ï βήμα. Τα μηνύματα Y_i δεν μπορούν να προστατευθούν με τη χρήση συναρτήσεων κατάτμησης, καθώς πρέπει να χρησιμοποιηθούν στον υπολογισμό του κοινού μυστικού κλειδιού K.

Εφόσον ο αντίπαλος $\tilde{U}_{i+1} = U_{i+1}$ μπορεί να χρησιμοποιήσει το αντίστροφο ενός προηγούμενου μηνύματος X_{i-1}, τότε ο $\tilde{U}_{i+1}$ μπορεί να υπολογίσει το $k_i = a^{r_{i-1} s_i} \bmod p$. Συνεπώς, εάν ο αντίπαλος επικοινωνεί με τους χρήστες που συμμετέχουν στη συνδιάσκεψη, τότε μπορεί να υπολογίζει κάθε φορά ένα διαφορετικό τμήμα του κοινού μυστικού κλειδιού.

-

Ο αντιμετώπιση τέτοιας επίθεσης μπορεί να υλοποιηθεί, εάν τα μηνύματα X_i αυθεντικοποιούνται. Η αυθεντικοποίηση ενός μηνύματος θα εμποδίσει κάθε αντίπαλο να χρησιμοποιήσει προηγούμενα χρονικά μηνύματα σε μελλοντικές συνδιασκέψεις. Διάφοροι τρόποι υλοποίησης της μεθόδου αυτής παρουσιάζονται από τους Burmester και Desmedt [Bur95].

Στην περίπτωση του κρυπτογραφικού πρωτοκόλλου CP, η αυθεντικοποίηση θα πρέπει να εφαρμοστεί στο 1ϊ βήμα, όπου κάθε χρήστης U_i πρέπει να αποδεικνύει ότι γνωρίζει το διακριτό λογάριθμο του r_i, που χρησιμοποιείται στον υπολογισμό του X_i. Αυτό μπορεί να πραγματοποιηθεί με τη χρήση αποδείξεων μηδενικής γνώσης (zero-knowledge proof) του διακριτού λογάριθμου (e.g. [Cha87]).

Ειδικότερα, ένα σύστημα υπογραφών βασισμένο σε απόδειξη μηδενικής γνώσης (signature scheme based on zero-knowledge proofs) μπορεί να χρησιμοποιηθεί, όπως περιγράφεται στο [Fia87]. Αυτό θα έχει ως αποτέλεσμα, κάθε χρήστης U_i στο 1ϊ βήμα του κρυπτογραφικού πρωτοκόλλου να στέλνει ένα επιπλέον μήνυμα, που να περιέχει την υπογραφή των $P_1,\ldots,P_n$ με κλειδί το X_i.

3.5 Μια νέα παραλλαγή του κρυπτογραφικού πρωτοκόλλου CP

Σύμφωνα με τα όσα αναφέρθηκαν στις παραγράφους 3.2 και 3.4, η δυνατότητα του αντίπαλου να μπορέσει να υπολογίσει το κοινό μυστικό κλειδί συνδιάσκεψης βασίζεται στην ακόλουθη παρατήρηση:

> *Τα μηνύματα $\tilde{O}_{\acute{e}}$, που ανταλλάσσονται στο δεύτερο βήμα, δεν είναι απόλυτα τυχαία και ανεξάρτητα, από μηνύματα που έχουν ανταλλάξει οι ίδιοι χρήστες σε προηγούμενες επικοινωνίες, αλλά περιέχουν συγκεκριμένη και σταθερή πληροφορία. Στο πρωτόκολλο CP, το μήνυμα*

-

$Y_i \equiv \left(P_{i+1}\right)^{r_i} \Big/ \left(X_{i-1}\right)^{s_i} \equiv \left(X_i\right)^{s_{i+1}} \Big/ \left(P_i\right)^{r_{i-1}} (\mathrm{mod}\, p)$ *έχει ως σταθερή πληροφορία το* $\left(X_{i-1}\right)^{s_i} \left(X_i\right)^{s_{i+2}}$.

Πιο συγκεκριμένα, στο κρυπτογραφικό πρωτόκολλο CP, ανεξαρτήτου αριθμού χρηστών που συμμετέχουν στην επικοινωνία, καθώς και εάν είναι συγκεκριμένοι αυτοί οι χρήστες, το μήνυμα $Y_i \equiv \left(P_{i+1}\right)^{r_i} \Big/ \left(X_{i-1}\right)^{s_i} \equiv \left(X_i\right)^{s_{i+1}} \Big/ \left(P_i\right)^{r_{i-1}} (\mathrm{mod}\, p)$ θα περιέχει πάντοτε το $\left(X_{i-1}\right)^{s_i} \left(X_i\right)^{s_{i+2}}$.

Από την παρατήρηση αυτή προκύπτει ότι, εάν δεν υπάρχει καμιά σταθερή πληροφορία, τότε ο αντίπαλος δεν μπορεί να προβλέψει και να υπολογίσει τμηματικά το κοινό μυστικό κλειδί *K*, αφού κάθε φορά θα είναι αποτέλεσμα πράξεων τυχαίων πληροφοριών. Η παρατήρηση αυτή, που ισχύει και στο πρωτόκολλο των Burmester και Desmedt [Bur95], αποτελεί τη βάση για το νέο προτεινόμενο κρυπτογραφικό πρωτόκολλο, το CP2, που είναι μια παραλλαγή του CP και όπου κανένα τμήμα των μηνυμάτων $\tilde{O}_{\acute{e}}$ δεν είναι σταθερό.

Εστω $U_1, U_2, \ldots, U_n$, οι χρήστες που επιθυμούν να επικοινωνήσουν μεταξύ τους και πρέπει να αποκτήσουν ένα κοινό μυστικό κλειδί επικοινωνίας . Η διαδικασία ένταξης ενός νέου χρήστη στο σύστημα, ο υπολογισμός του δημοσίου κλειδιού του και η επιλογή των παραμέτρων παραμένουν τα ίδια, όπως και στο πρωτόκολλο CP:

1ϊ Κάθε χρήστης U_i , i=1,2,..., n επιλέγει τυχαία $r_i \in Z_q$ και υπολογίζει

$$X_i = a^{r_i s_i} \bmod p. \qquad (1)$$

και το δημοσιοποιεί σ' όλους τους υπόλοιπους χρήστες.

-

2ï Κάθε χρήστης U_i , i=1,2,..., n υπολογίζει

$$Y_i \equiv \left(X_{i+1}\right)^{s_i} \left(X_{i+1}\right)^{s_i r_i} \Big/ \left(X_{i-1}\right)^{s_i r_i} \left(P_{i-1}\right)^{s_i r_i} (\text{mod } p) \qquad (2)$$

με την προϋπόθεση, ότι οι χρήστες είναι σε κύκλο. Στη συνέχεια κάθε χρήστης U_i δημοσιοποιεί το Y_i στους υπόλοιπους χρήστες.

Το κοινό μυστικό κλειδί επικοινωνίας είναι το:

$$,K \equiv a^{s_1 s_2 (r_1 r_2 + r_2) + s_2 s_3 (r_2 r_3 + r_3) + \ldots + s_n s_1 (r_n r_1 + r_1)} (\text{mod } p)$$

το οποίο κάθε χρήστης U_i μπορεί να υπολογίσει με τη βοήθεια των (1) και (2) και αφού:

$$K \equiv K_i \equiv \left(\left(X_{i-1}\right).\left(P_{i-1}\right)\right)^{n r_i s_i} . Y_i^{\,n-1} . Y_{i+1}^{\,n-2} \ldots Y_{i-2} (\text{mod } p)$$

Στην περίπτωση που ο αριθμός των χρηστών που επιθυμούν να επικοινωνήσουν είναι δύο (n = 2), τότε ισχύει ό,τι και στο αρχικό πρωτόκολλο CP, δηλαδή $Y_1 \equiv Y_2^{-1}$, όπου και οι δύο χρήστες μπορούν να υπολογίσουν το κοινό μυστικό κλειδί χωρίς να χρειάζεται να ανταλλάξουν τα μηνύματα Y_1, Y_2 . Το κοινό μυστικό κλειδί για δύο χρήστες είναι:

$$K = a^{s_1 s_2 (2 r_1 r_2 + r_1 + r_2)} \bmod p$$

-

Σχετικά με το νέο προτεινόμενο κρυπτογραφικό πρωτόκολλο, CP2, ισχύουν τα ακόλουθα:

1. Κάθε χρήστης για τον υπολογισμό του X_i χρησιμοποιεί και το μυστικό του κλειδί s_i. Αυτό δεν επιφέρει καμιά επιπλέον διαρροή πληροφορίας ή μείωση της ασφάλειας, καθώς το X_i παραμένει τυχαίο μήνυμα. Είτε στην περίπτωση του CP, όπου έχουμε $X_i = a^{r_i} \bmod p$, είτε στη περίπτωση του CP2, όπου το $X_i = a^{r_i s_i} \bmod p$, το αποτέλεσμα μπορεί να θεωρηθεί τυχαίο, αφού r_i είναι τυχαίος αριθμός. Συνεπώς, ένας αντίπαλος δε μπορεί να επιτύχει καμιά πρόβλεψη και επομένως δεν μπορεί να αποκτήσει γνώση.

2. Ο τύπος υπολογισμού των μηνυμάτων Y_i έχει τροποποιηθεί στο CP2, ώστε οι δυνάμεις που χρησιμοποιούνται να περιέχουν τυχαίο αριθμό και συνεπώς το αποτέλεσμα να είναι τυχαίο. Ειδικότερα, ισχύει:

$$Y_i \equiv \left(X_{i+1}\right)^{s_i}\left(X_{i+1}\right)^{s_i r_i} \Big/ \left(X_{i-1}\right)^{s_i r_i}\left(P_{i-1}\right)^{s_i r_i} \equiv \left(\left(X_{i+1}\right)^{s_i}\right)^{r_i+1} \Big/ \left(\left(X_{i-1}\right).\left(P_{i-1}\right)\right)^{s_i r_i} (\text{mod } p)$$

Στον πίνακα 2 παρουσιάζονται τα βασικά σημεία των δύο προτεινόμενων κρυπτογραφικών πρωτοκόλλων CP και CP2.

-

Πρωτόκολλα **Χαρακτηριστικά**	**CP**	**CP2**
Απαιτούμενοι υπολογισμοί κάθε χρήστη	4 exp	4 exp
Αυθεντικοποίηση των μηνυμάτων Y_i	Ναι	Οχι
Αριθμός μηνυμάτων που κάθε χρήστης υπολογίζει	2	2
Αποδεδειγμένη ασφάλεια	Ναι	Ναι
Υπολογιστικά βήματα	3	3
Διαρροή πληροφορίας	Ναι σε ορισμένες περιπτώσεις	Οχι

Πίνακας 2. Συγκριτικός πίνακας πρωτοκόλλων CP και CP2

-

3.6 Συμπεράσματα

Τα κρυπτογραφικά πρωτόκολλα αποβλέπουν στον καθορισμό μιας διαδικασίας, η οποία παρέχει ασφαλή επικοινωνία σε δύο ή περισσοτέρους χρήστες σ' ένα σύστημα. Ανάλογα με τις απαιτήσεις των χρηστών που συμμετέχουν σε μια επικοινωνία, ένα κρυπτογραφικό πρωτόκολλο πρέπει να παρέχει αυθεντικοποίηση του αποστολέα ή/και του παραλήπτη, αλλά και ακεραιότητα και μυστικότητα των δεδομένων που ανταλλάσσονται μεταξύ τους.

Κατά τη διαδικασία της ανάλυσης, του σχεδιασμού και της υλοποίησης μιας ασφαλούς επικοινωνίας μέσα σ' ένα δίκτυο, θα πρέπει να λαμβάνονται υπόψη και άλλοι παράγοντες (όπως το απαιτούμενο υπολογιστικό κόστος, το είδος των δικτύων), καθώς αυτοί δεν θα πρέπει να επιδρούν αρνητικά στην αποδοτικότητα του συγκεκριμένου δικτύου ή να αλλάζουν την λειτουργία μιας διαδικασίας σε τέτοιο βαθμό, ώστε να μην είναι εύχρηστη ή αποδεκτή από τους χρήστες. Για παράδειγμα, η χρήση κρυπτογραφικών πρωτοκόλλων σε οργανισμούς, όπως οι τράπεζες και τα νοσοκομεία, δεν θα πρέπει ούτε να δυσχεραίνει την όλη λειτουργία, ούτε να απαιτεί μεγάλο υπολογιστικό χρόνο, καθώς ο βασικός σκοπός είναι η γρήγορη και αποτελεσματική εξυπηρέτηση των πελατών και η υγεία των ασθενών, αντίστοιχα. Επίσης, τα κρυπτογραφικά πρωτόκολλα που εφαρμόζονται σε δίκτυα, όπου ο αριθμός των χρηστών είναι μεγάλος και οι απαιτήσεις τους διαφοροποιούνται, θα πρέπει να χαρακτηρίζονται από ευελιξία και προσαρμοστικότητα ανάλογα με τις απαιτήσεις που εμφανίζονται κάθε φορά.

Μία από τις βασικές παραμέτρους ενός κρυπτογραφικού πρωτοκόλλου είναι το κλειδί. Κάθε χρήστης μπορεί να έχει στην κατοχή του, να γνωρίζει ή να μπορεί να υπολογίσει ένα ή περισσότερα κλειδιά, τα οποία χρησιμοποιεί με διάφορες διαδικασίες. Συνήθως ένα κρυπτογραφικό πρωτόκολλο χρησιμοποιείται για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων, που ανταλλάσσονται μεταξύ των χρηστών, εφόσον αυτοί γνωρίζουν ένα κοινό μυστικό κλειδί, το οποίο και έχουν υπολογίσει με τη βοήθεια ενός κρυπτογραφικού πρωτοκόλλου συμφωνίας κλειδιού.

-

Στο κεφάλαιο αυτό αναλύθηκε ένα από τα πιο βασικά προβλήματα εφαρμογής και υλοποίησης κρυπτογραφικών πρωτοκόλλων, γνωστό ως πρόβλημα διανομής / δημιουργίας κλειδιού. Το πρόβλημα αυτό γίνεται δύσκολο και πολύπλοκο στην επίλυσή του, όταν οι χρήστες που επιθυμούν να επικοινωνήσουν μεταξύ τους μπορεί να είναι περισσότεροι από δύο, το κέντρο εμπιστοσύνης δεν πρέπει να έχει ενεργή συμμετοχή και το αντίστοιχο κρυπτογραφικό πρωτόκολλο να παρέχει αποδεδειγμένη ασφάλεια.

Επίσης, μια άλλη βασική παράμετρος που πρέπει να λαμβάνεται υπόψη στη διαδικασία εφαρμογής και υλοποίησης ενός κρυπτογραφικού πρωτοκόλλου, είναι η τοπολογία του δικτύου.

Για παράδειγμα, όταν η τοπολογία του δικτύου είναι άστρο (star), οι πληροφορίες και η επικοινωνία μεταξύ των χρηστών πραγματοποιείται με διαφορετικό τρόπο απ' όταν η τοπολογία είναι δακτύλιος (ring) ή διάδρομος (bus).

Είναι γνωστό ότι σε τοπολογία άστρο, όλες οι πληροφορίες και τα μηνύματα διέρχονται μέσω του κεντρικού κόμβου, συνεπώς ένα κρυπτογραφικό πρωτόκολλο που απαιτεί μεγάλο αριθμό ανταλλαγής μηνυμάτων μεταξύ των χρηστών θα μπορούσε να είναι μη αποδοτικό, λαμβάνοντας υπόψη ότι και ο αριθμός των χρηστών μπορεί να είναι πολύ μεγάλος.

Επιπλέον, θα πρέπει να ληφθεί υπόψη η περίπτωση που ένας ή περισσότεροι από τους χρήστες που συμμετέχουν σε μία επικοινωνία δεν έχουν τους ίδιους διαθέσιμους πόρους (μνήμη, χωρητικότητα). Για παράδειγμα, όταν ο χρήστης επιθυμεί να χρησιμοποιήσει το σύστημα σύνδεσης της οικίας του με την τράπεζα (home banking), όπου απλές τηλεφωνικές γραμμές πρέπει να συνδεθούν με το σύστημα της τράπεζας, οι δυνατότητες του χρήστη είναι περιορισμένες, ενώ ο απαιτούμενος χρόνος δε μπορεί να είναι μεγάλος.

Στην περίπτωση που ένας απλός χρήστης χρησιμοποιεί έξυπνη κάρτα, για να επικοινωνήσει με άλλους χρήστες, τότε οι δυνατότητές του περιορίζονται σ΄ αυτές της κάρτας. Συνεπώς, εάν ένα πρωτόκολλο απαιτεί μεγαλύτερη χωρητικότητα ή πολλούς υπολογισμούς, από ότι η έξυπνη κάρτα μπορεί να παρέχει, τότε δημιουργείται πρόβλημα στην όλη λειτουργία του

συστήματος. Το πρόβλημα μπορεί να είναι πιο σοβαρό, όταν ο χρόνος που απαιτείται λόγω της κάρτας είναι μεγάλος και το σύστημα απαιτεί σε πολλές περιπτώσεις μεγάλη ταχύτητα (π.χ. τράπεζες, νοσοκομεία).

Το κρυπτογραφικό πρωτόκολλο CP, είναι ένα κρυπτογραφικό πρωτόκολλο συνδιάσκεψης, το οποίο έχει ως χαρακτηριστικά α) το μικρό υπολογιστικό κόστος, β) τη μικρή πολυπλοκότητα, γ) είναι πρακτικό και δ) έχει αποδεδειγμένη ασφάλεια

Επίσης παρουσιάστηκε μια παραλλαγή του πρωτοκόλλου αυτού, το CP2, η οποία έχει τα ίδια χαρακτηριστικά με το αρχικό προτεινόμενο κρυπτογραφικό πρωτόκολλο, το CP, αλλά αντιμετωπίζει τις πιθανές επιθέσεις ενός αντιπάλου με διαφορετικό τρόπο.

Πιθανές επεκτάσεις των προτεινόμενων κρυπτογραφικών πρωτοκόλλων CP και CP2, θα οδηγούσαν στη δημιουργία ενός νέου κρυπτογραφικού πρωτοκόλλου, όπου το κοινό μυστικό κλειδί θα είχε τα ίδια χαρακτηριστικά, αλλά η διαδικασία υλοποίησης θα απαιτούσε μικρότερο υπολογιστικό κόστος από αυτό του προτεινόμενου κρυπτογραφικού πρωτοκόλλου, καθώς και μικρότερο αριθμό μηνυμάτων που ανταλλάσσονται μεταξύ των χρηστών για τη δημιουργία του κλειδιού αυτού. Επίσης, ένα άλλο πρόβλημα που υπάρχει στα κρυπτογραφικά πρωτόκολλα σύσκεψης είναι η αποτελεσματική αντιμετώπιση της περίπτωσης, όπου ένας νέος χρήστης θέλει να συμμετέχει στην επικοινωνία, ενώ οι υπόλοιποι χρήστες έχουν ήδη υπολογίσει το κοινό μυστικό κλειδί.

Τέλος, μια πιθανή βελτίωση της διαδικασίας υλοποίησης, η οποία περιγράφεται αναλυτικά στο Παράρτημα 1, σε συνεργασία με το ανάλογο υλικό μπορεί να έχει καλύτερα αποτελέσματα στον απαιτούμενο χρόνο και θα επέτρεπε τη χρήση του προτεινόμενου κρυπτογραφικού πρωτοκόλλου σε διάφορους χώρους όπου εφαρμόζονται νέες εξελίξεις της τεχνολογίας της πληροφορικής (π.χ. πολυμέσα).

-

ΚΕΦΑΛΑΙΟ 4

ΑΣΦΑΛΗ ΕΠΙΚΟΙΝΩΝΙΑ Σ' ΕΝΑ ΣΥΣΤΗΜΑ ΕΠΑΓΡΥΠΝΗΣΗΣ ΓΙΑ ΙΑΤΡΙΚΕΣ ΣΥΣΚΕΥΕΣ

4.1. Το σύστημα MDVS

Το Ευρωπαϊκό *Σύστημα Επαγρύπνησης για τις Ιατρικές Συσκευές* MDVS (Medical Device Vigilance System) είναι ένα από τα συστήματα που ασχολείται με την ανταλλαγή πληροφοριών και δεδομένων κατά την διαδικασία έρευνας ενός ατυχήματος, το οποίο πιθανώς να οφείλεται σε ιατρική συσκευή. Οι κατευθυντήριες οδηγίες (directives) του AIMD και του MD της Ευρωπαϊκής Ενωσης ΕΕ για τις ιατρικές συσκευές καθορίζουν τις απαιτήσεις και ανάγκες του συστήματος αυτού [Com93, Cou90, Cou93]. Πιο συγκεκριμένα, το σύστημα MDVS έχει τρεις βασικούς στόχους:

1. Την προστασία από πιθανή επανάληψη του ίδιου ατυχήματος, πιθανώς σε άλλο γεωγραφικό τόπο και χρονική περίοδο.

2. Την ενθάρρυνση των κατασκευαστών ιατρικών συσκευών να ερευνούν κάθε περίπτωση ατυχήματος και να λαμβάνουν όλα τα απαραίτητα μέτρα που θα μειώσουν την πιθανότητα επανάληψης του ατυχήματος.

3. Τη δυνατότητα ελέγχου των διαδικασιών έρευνας και παρέμβασης, εάν θεωρείται αναγκαίο, από τις αρμόδιες αρχές.

-

Η επιτυχία των στόχων αυτών απαιτεί τη συλλογή, αποθήκευση και διαχείριση ενός μεγάλου αριθμού δεδομένων, ώστε τα μέλη που θα συμμετέχουν στην έρευνα να έχουν στην κατοχή τους όλες τις αναγκαίες και απαραίτητες πληροφορίες. Η ανάγκη ύπαρξης των δεδομένων αυτών οδήγησε στην ανάπτυξη ενός Ευρωπαϊκού Συστήματος Ανταλλαγής Πληροφοριών Ιατρικών Συσκευών EUROMEDIES (European Medical Device Information Exchange System) [EUR95]. Ο βασικός στόχος του συστήματος EUROMEDIES είναι ο καθορισμός των απαιτήσεων για ένα σύστημα τηλεματικής αποβλέποντας στη διαχείριση όλων των δεδομένων και πληροφοριών, καθώς και στην παροχή των απαραίτητων λειτουργιών για την ανταλλαγή των πληροφοριών μεταξύ των μελών που συμμετέχουν στην έρευνα και στη διαδικασία έκδοσης της τελικής αναφοράς.

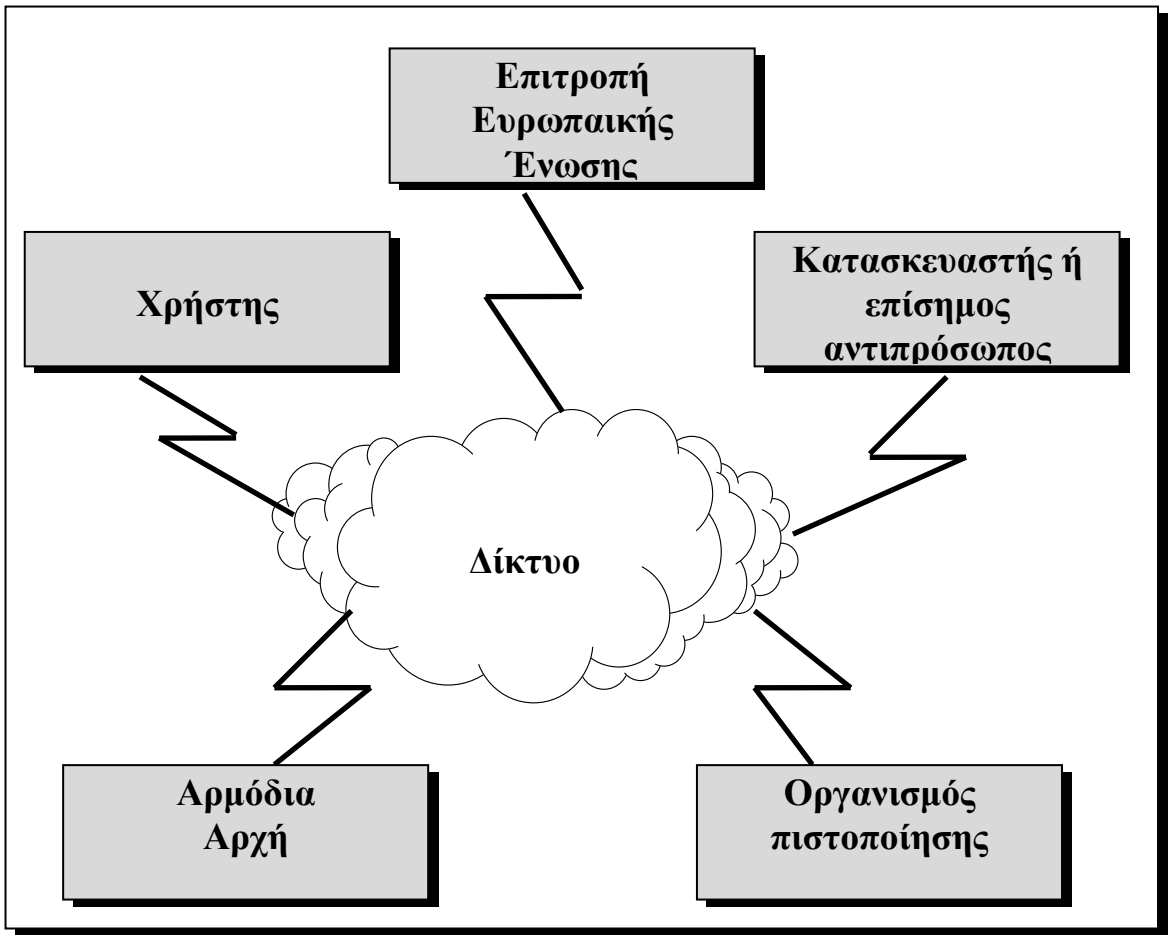
Οι πληροφορίες που αποθηκεύονται ή ανταλλάσσονται μεταξύ των ενδιαφερομένων μελών είναι σημαντικές, ειδικότερα τη χρονική περίοδο πριν την έκδοση της τελικής αναφοράς, η οποία θα καθορίσει το ποσοστό ευθύνης της συγκεκριμένης ιατρικής συσκευής.

Για το λόγο αυτό, η ασφάλεια των δεδομένων αποτέλεσε ένα από τα βασικά θέματα έρευνας στο EUROMEDIES. Κατάλληλοι μηχανισμοί ασφάλειας θα έπρεπε να οριστούν, με σκοπό τη διατήρηση της μυστικότητας και ακεραιότητας των πληροφοριών λαμβάνοντας υπόψη και άλλους παράγοντες όπως χρησιμότητα, αποτελεσματικότητα και κόστος. Οι μηχανισμοί αυτοί αφορούν την ασφάλεια σε επίπεδο τόσο βάσεων δεδομένων όσο και δικτύων. Η συνέχεια του κεφαλαίου θα επικεντρωθεί στην προστασία της επικοινωνίας των μελών που συμμετέχουν σε μια διαδικασία έρευνας σχετικά με ένα ατύχημα σε ιατρική συσκευή. Ειδικότερα, παρουσιάζεται και προτείνεται ένας τρόπος εφαρμογής και λειτουργίας του κρυπτογραφικού πρωτοκόλλου CP μέσα στο σύστημα MDVS. Το κρυπτογραφικό πρωτόκολλο CP παρουσιάστηκε αναλυτικά στο κεφάλαιο 3.

-

4.2. Οι απαιτήσεις μιας επικοινωνίας στο MDVS

Τα μέλη που συμμετέχουν σε μια διαδικασία έρευνας και έκδοσης της τελικής αναφοράς στο MDVS ,σχήμα 1, μπορεί να είναι:



Σχήμα 1. Γενική θεώρηση της επικοινωνίας στο MDVS

- Αρμόδια Αρχή (Competent Authority), (π.χ. ένα Υπουργείο Υγείας).

- Οργανισμός Πιστοποίησης (Notified Body), (π.χ. ένας οργανισμός τυποποίησης).

-

- Κατασκευαστής (Manufacturer) ιατρικών συσκευών ή επίσημος αντιπρόσωπος (Authorised Representative).

- Χρήστης ιατρικής συσκευής (User), (π.χ. ένα νοσοκομείο).

- Η Επιτροπή της Ευρωπαϊκής Ενωσης σε θέματα Υγείας.

Σύμφωνα με τις κατευθυντήριες οδηγίες, για τη δημιουργία της αναφοράς ενός ατυχήματος πρέπει να γίνουν οι ακόλουθες ενέργειες :

- Μία αρχική εκτίμηση των συνθηκών που επικρατούσαν την χρονική στιγμή του ατυχήματος και αφορούν την ιατρική συσκευή.

- Την έκδοση της αρχικής αναφοράς από τον κατασκευαστή και την ενημέρωση της αρμόδιας αρχής, προτείνοντας τον τερματισμό της έρευνας ή τη συνέχισή της. Η χρονική διάρκεια της έκδοσης της αρχικής αναφοράς είναι από 10 έως 30 ημέρες.

- Επαφές μεταξύ των ενδιαφερομένων μελών.

- Μια λεπτομερή έρευνα για το ατύχημα, από τον κατασκευαστή της ιατρικής συσκευής υπό την επίβλεψη της αρμόδιας αρχής.

- Την έκδοση της τελικής αναφοράς, η οποία θα καθορίζει τις ενέργειες που θα πρέπει να ακολουθήσουν τα ενδιαφερόμενα μέλη εφόσον είναι απαραίτητο.

- Την ενημέρωση των υπολοίπων αρμόδιων αρχών, των ενδιαφερομένων μελών καθώς και της αντίστοιχης επιτροπής της Ευρωπαϊκής Ενωσης σχετικά με τα τελικά αποτελέσματα της έρευνας και των πιθανών μέτρων αντιμετώπισης, για τη αποφυγή πιθανής επανάληψης του ίδιου ατυχήματος.

-

Από τις παραπάνω ενέργειες προκύπτει ότι το κύριο χαρακτηριστικό είναι η συχνή ροή δεδομένων και πληροφοριών μεταξύ των ενδιαφερομένων μελών κατά την χρονική περίοδο της έρευνας. Ειδικότερα, η ανταλλαγή των δεδομένων και των πληροφοριών είναι απαραίτητη, όταν διάφορες μετρήσεις θα πρέπει να πραγματοποιηθούν ως αποτέλεσμα της αρχικής αναφοράς. Παράλληλα, πολλές από τις πληροφορίες αυτές θα πρέπει να παραμείνουν μυστικές μέχρι την έκδοση της τελικής αναφοράς. Για παράδειγμα, σε όλες τις αρμόδιες αρχές θα πρέπει να γνωστοποιηθούν δεδομένα σχετικά με την τελική αναφορά της έρευνας, αντίθετα, δεδομένα που αφορούν τις ενδιάμεσες ενέργειες θα μπορούν να γνωστοποιηθούν μόνο ύστερα από απαίτηση των ενδιαφερομένων.

Επίσης, κατά την χρονική διάρκεια της έρευνας είναι αναγκαία η προστασία των δεδομένων που ανταλλάσσονται, ώστε να μην είναι προσπελάσιμα από άλλα μέλη του συστήματος. Για παράδειγμα, τέτοια μέλη μπορεί να είναι οι κατασκευαστές ανταγωνιστικών ιατρικών συσκευών της ιατρικής συσκευής που σχετίζεται με το ατύχημα.

Από την αποτελεσματικότητα της προστασίας των δεδομένων αυτών εξαρτάται η αξιοπιστία της συγκεκριμένης ιατρικής συσκευής, καθώς πριν την έκδοση της τελικής αναφοράς δεν επιτρέπεται κανένας καταλογισμός των ευθυνών. Συνεπώς, στην ανάλυση, σχεδιασμό και υλοποίηση του δικτύου για την ανταλλαγή αυτών των δεδομένων, θα πρέπει να ληφθεί υπόψη η προστασία τους. Ομως, οι λειτουργίες ασφάλειας που θα παρέχονται από το σύστημα θα πρέπει να καθορίζονται σε σχέση με τις πιθανές απειλές που μπορεί να υπάρχουν, καθώς και με τις αντίστοιχες επιπτώσεις [EEC91]. Για το λόγο αυτό διάφορες διαδικασίες ανάλυσης κινδύνου ερευνήθηκαν στο πλαίσιο του EUROMEDIES.

-

4.3. Σύστημα ασφαλούς επικοινωνίας στο MDVS

Γενικά, η ασφάλεια των δεδομένων σε επίπεδο δικτύου προϋποθέτει την κωδικοποίηση και αποκωδικοποίηση των δεδομένων που ανταλλάσσονται μέσω αυτού. Η ανάγκη παροχής ασφάλειας στο MDVS οφείλεται στην προστασία, από διάφορες απειλές και κινδύνους, της μεταφοράς των δεδομένων που αφορούν ένα ατύχημα, καθώς και της προσπέλασης των δεδομένων αυτών μόνο από ορισμένα μέλη.

Μαζί με τις λειτουργίες ασφάλειας θα πρέπει να ληφθούν υπόψη και οι απαιτήσεις που προκύπτουν από το περιβάλλον του συγκεκριμένου συστήματος. Μια τέτοιου είδους απαίτηση, για το σύστημα MDVS, είναι ότι τα μέλη που συμμετέχουν στις διάφορες επικοινωνίες με τελικό σκοπό την ολοκλήρωση της έρευνας και την έκδοση της τελικής αναφοράς μπορεί να περισσότερα από δύο. Για παράδειγμα, όταν συμβεί ένα ατύχημα, ο χρήστης, η αρμόδια αρχή της συγκεκριμένης χώρας και ο κατασκευαστής (ή ο επίσημος αντιπρόσωπος) της ιατρικής συσκευής θα πρέπει να ξεκινήσουν μία επικοινωνία αναφορικά με το ατύχημα.

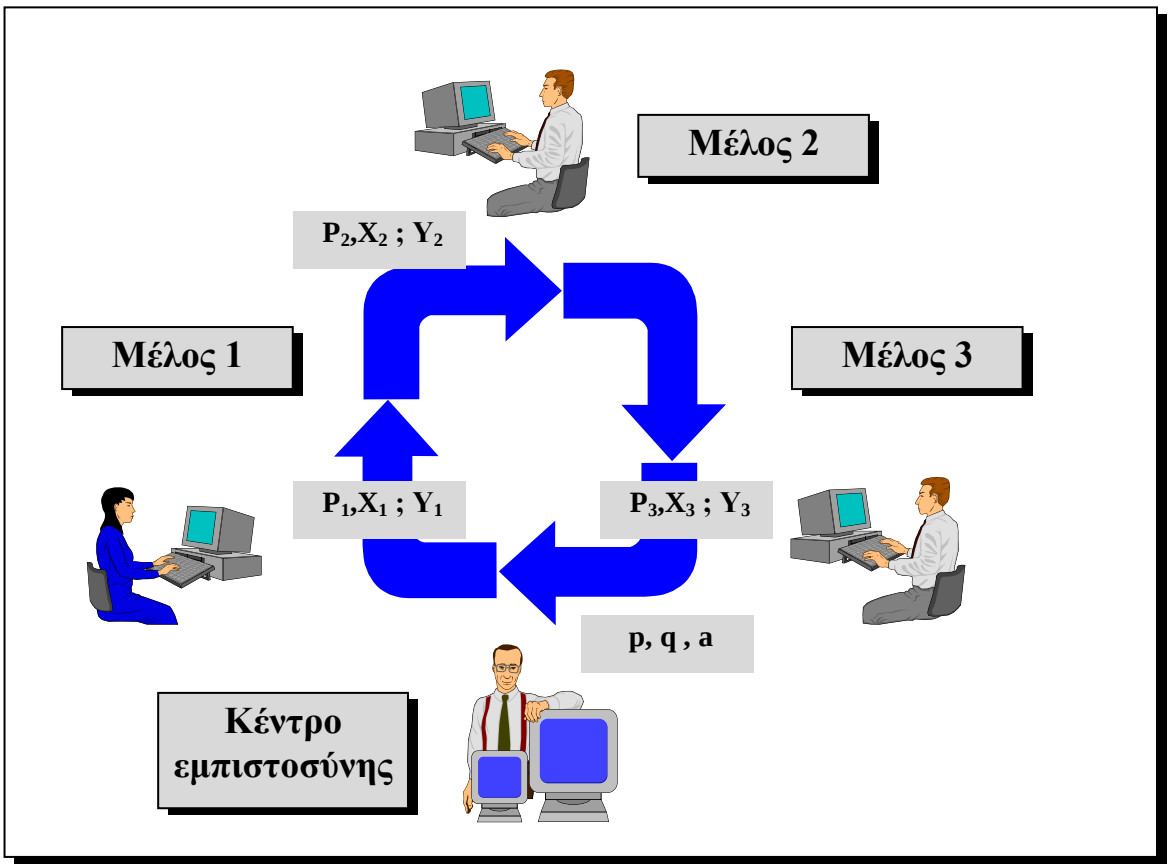
Επιπλέον, ο οργανισμός πιστοποίησης που έχει εκδώσει πιστοποιητικό για την συγκεκριμένη ιατρική συσκευή μπορεί να συμμετέχει στην επικοινωνία. Σύμφωνα με τα παραπάνω, προκύπτει η ανάγκη ενός κρυπτογραφικού πρωτοκόλλου το οποίο να παρέχει ασφαλή επικοινωνία μεταξύ δύο ή περισσοτέρων μελών και παράλληλα να είναι πρακτικό στην υλοποίηση του.

Το κρυπτογραφικό πρωτόκολλο CP, που παρουσιάζεται στο σχήμα 2 για τρεις χρήστες, ικανοποιεί τις λειτουργίες ασφάλειας και απαιτήσεις ενώ παρέχει χαμηλή υπολογιστική πολυπλοκότητα, μικρό αριθμό μηνυμάτων που πρέπει να ανταλλάσσουν τα μέλη μεταξύ τους καθώς και η ασφάλεια του είναι μαθηματικά αποδεδειγμένη. Επίσης, δεν περιορίζεται από την τοπολογία του δικτύου στο οποίο εφαρμόζεται.

Κάθε φορά που δύο ή περισσότερα μέλη επιθυμούν να ξεκινήσουν μία επικοινωνία το κρυπτογραφικό πρωτόκολλο, παρέχει την δυνατότητα υπολογισμού ενός κοινού μυστικού

-

κλειδιού, το οποίο θα χρησιμοποιηθεί για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων που ανταλλάσσουν.



Σχήμα 2. Το κρυπτογραφικό πρωτόκολλο για "τρία μέλη".

Πιο συγκεκριμένα, όταν τα μέλη έχουν στην κατοχή τους το κοινό μυστικό κλειδί, μπορούν να χρησιμοποιήσουν ένα συμμετρικό αλγόριθμο για να κωδικοποιούν και αποκωδικοποιούν τις πληροφορίες που θα ανταλλάσσουν μεταξύ τους χωρίς να απαιτείται η χρήση ασφαλούς διαύλου επικοινωνίας. Ο πιο γνωστός συμμετρικός αλγόριθμος, όπως έχει αναφερθεί στη εισαγωγή, είναι ο DES [ANS81, Dep77].

-

4.4. Σενάριο λειτουργίας και υλοποίησης

Η χρησιμοποίηση ενός κρυπτογραφικού πρωτοκόλλου για την παροχή ασφάλειας οδηγεί στην ανάγκη καθιέρωσης ενός συστήματος ασφάλειας μέσω του οποίου θα υλοποιείται το πρωτόκολλο.

Για το προτεινόμενο κρυπτογραφικό πρωτόκολλο υπάρχει η ανάγκη επιλογής ενός οργανισμού που θα έχει τον ρόλο του κέντρου εμπιστοσύνης. Στην περίπτωση του MDVS το ρόλο του κέντρου εμπιστοσύνης θα έχει η αντίστοιχη επιτροπή της Ευρωπαϊκής Κοινότητας κυρίως για δύο λόγους:

– Πρέπει να είναι κοινά αποδεκτός και απόλυτης εμπιστοσύνης από όλα τα μέλη, ενώ,

– Δε δημιουργείται κανένα πρόβλημα στην αποδοτικότητα και αποτελεσματικότητα του κρυπτογραφικού πρωτοκόλλου, εάν το κέντρο εμπιστοσύνης θα πρέπει να συμμετέχει στην επικοινωνία.

Στις ενέργειες της επιτροπής της Ευρωπαϊκής Κοινότητας, ως κέντρο εμπιστοσύνης, είναι η επιλογή των βασικών παραμέτρων του κρυπτογραφικού πρωτοκόλλου καθώς και η ανάπτυξη των εφαρμογών που απαιτούνται για την υλοποίηση και λειτουργία του κρυπτογραφικού πρωτοκόλλου μέσα στο δίκτυο.

Το προτεινόμενο σενάριο λειτουργίας του όλου συστήματος είναι το ακόλουθο:

Επιλογή Παραμέτρων.

Το κέντρο εμπιστοσύνης επιλέγει τις βασικές παραμέτρους του συστήματος.

-

Εγγραφή των Μελών.

Κάθε ενδιαφερόμενος (χρήστης, αρμόδια αρχή, κατασκευαστής ή οργανισμός πιστοποίησης) που επιθυμεί να γίνει μέλος του δικτύου θα πρέπει να επικοινωνήσει με το κέντρο Εμπιστοσύνης για τη διαδικασία εξουσιοδότησης.

Μετά την αποδοχή από το Κέντρο εμπιστοσύνης, κάθε εξουσιοδοτημένο μέλος επιλέγει (μόνο του) το μυστικό κλειδί του και υπολογίζει το δημόσιο κλειδί του, το οποίο και δημοσιοποιεί με τη βοήθεια του κέντρου εμπιστοσύνης.

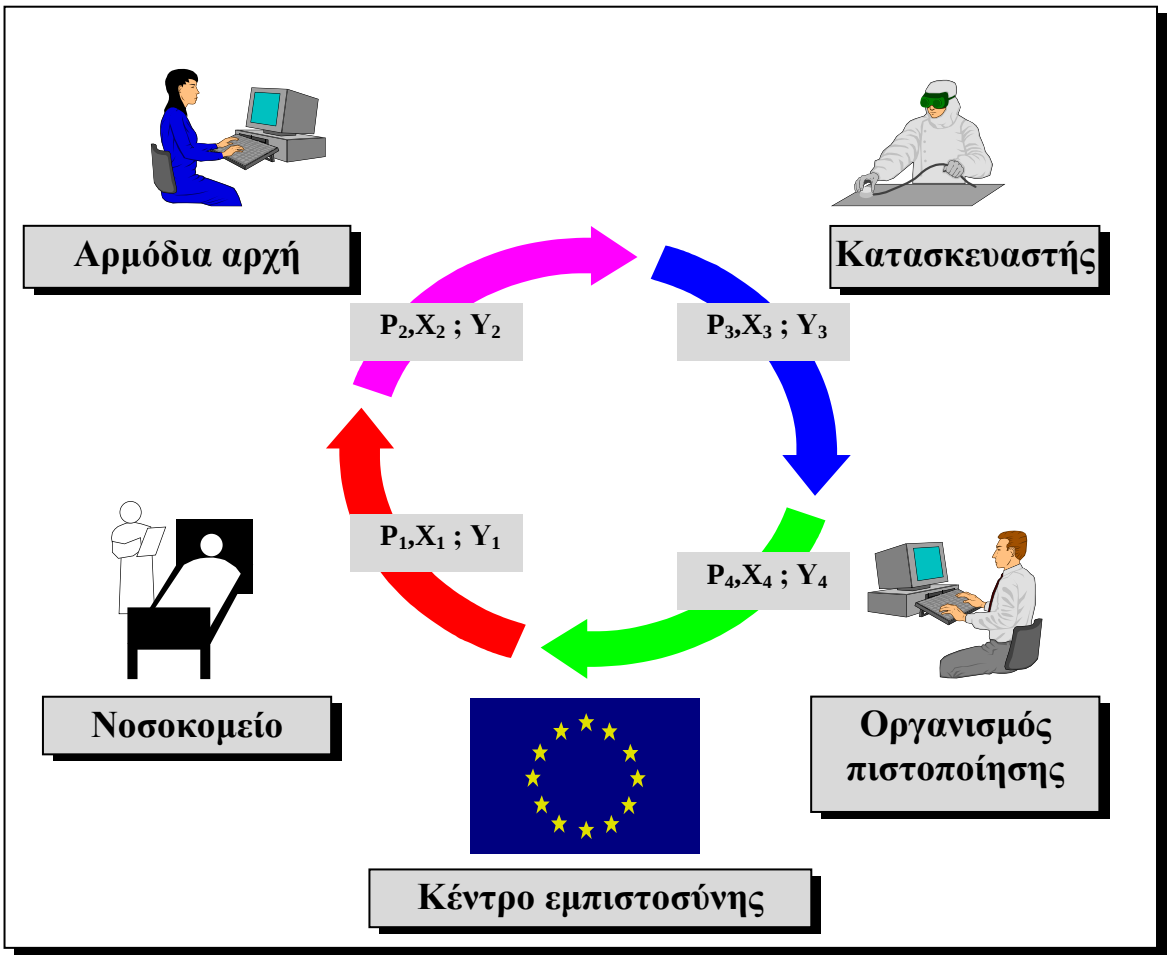
Το δημόσιο κλειδί κάθε μέλους διανέμεται σ' όλα τα εξουσιοδοτημένα μέλη ή καταχωρείται σε μια κεντρική βάση δεδομένων (η οποία ελέγχεται από το κέντρο εμπιστοσύνης) προσπελάσιμη από κάθε εξουσιοδοτημένο μέλος.

Κάθε εξουσιοδοτημένο μέλος έχει μόνο πρόσβαση ανάγνωσης για τα δημόσια κλειδιά των άλλων χρηστών στη βάση δεδομένων των δημόσιων κλειδιών. Ενώ, στην περίπτωση που επιθυμεί να τροποποιήσει το δικό του δημόσιο κλειδί, θα πρέπει να συνεργαστεί με το κέντρο εμπιστοσύνης.

Ασφαλή Επικοινωνία.

Οταν προκύψει ένα ατύχημα, ο υπεύθυνος χρήστης ενημερώνει την αρμόδια αρχή μέσω του εθνικού συστήματος αναφοράς. Ο κατασκευαστής της ιατρικής συσκευής ενημερώνεται από την αρμόδια αρχή, ενώ καλείται και ο αντίστοιχος οργανισμός πιστοποίησης για την έναρξη της επικοινωνίας. Το πρώτο βήμα της επικοινωνίας είναι η δημιουργία ενός κοινού μυστικού κλειδιού μεταξύ των μελών, με σκοπό να χρησιμοποιούν το κλειδί αυτό για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων που επιθυμούν να ανταλλάσσουν στη διαδικασία της έρευνας. Στο σχήμα 3 παρουσιάζεται μία θεώρηση της ασφαλούς επικοινωνίας μεταξύ τεσσάρων μελών στο δίκτυο του MDVS (θεωρούμε ότι, μετά τον υπολογισμό του κοινού μυστικού κλειδιού, οι συμμετέχοντες επικοινωνούν μέσω του δικτύου του MDVS).

-



Σχήμα 3. Μια ασφαλή επικοινωνία μέσα στο δίκτυο του MDVS

4.5. Δυνατότητα συνεργασίας με σύστημα EDI

Στις συναντήσεις που αφορούσαν το EUROMEDIES, προτάθηκε η χρησιμοποίηση της Ηλεκτρονικής Μεταφοράς Δεδομένων EDI (Electronic Data Interchange) μέσα στο δίκτυο του MDVS [EUR95, Pra95]. Η διαδικασία ηλεκτρονικής μεταφοράς δεδομένων επιτρέπει τη χρησιμοποίηση προκαθορισμένων φορμών- πληροφοριών που ανταλλάσσονται μεταξύ των μελών, ακόμα και στην περίπτωση που τα μέλη αυτά δε χρησιμοποιούν τις ίδιες εφαρμογές [Δου93].

-

Ενα από τα βασικά πλεονεκτήματα του προτεινόμενου κρυπτογραφικού πρωτοκόλλου CP είναι ότι το συγκεκριμένο πρωτόκολλο είναι ανεξάρτητο της δομής της πληροφορίας που ανταλλάσσεται. Συνεπώς, θα μπορούσε να χρησιμοποιηθεί σε συνεργασία με ένα σύστημα EDI. Η ανάγκη προστασίας των δεδομένων που μεταδίδονται μέσω ενός δικτύου ηλεκτρονικής μεταβίβασης δεδομένων έχει αναλυθεί και παρουσιαστεί στη βιβλιογραφία [Δου93, Oln93, Wil91].

4.6. Συμπεράσματα

Στο κεφάλαιο αυτό παρουσιάστηκε μια υλοποίηση του κρυπτογραφικού πρωτοκόλλου CP, που προτάθηκε στο κεφάλαιο 3, σε περιβάλλον δικτύου. Ειδικότερα, το κρυπτογραφικό πρωτόκολλο χρησιμοποιήθηκε για την προστασία των δεδομένων που ανταλλάσσουν τα μέλη που συμμετέχουν στην έρευνα που πραγματοποιείται όταν υπάρξει ένα ατύχημα σε μια ιατρική συσκευή, στα πλαίσια του ευρωπαϊκού προγράμματος EUROMEDIES.

Το κρυπτογραφικό πρωτόκολλο επιτρέπει σε περισσότερους από δύο χρήστες να επικοινωνούν με ασφάλεια, παρέχοντας ακεραιότητα και μυστικότητα των δεδομένων που ανταλλάσσονται, καθώς κάθε μη εξουσιοδοτημένος χρήστης δεν μπορεί να έχει ή να αποκτήσει στην κατοχή του το κοινό μυστικό κλειδί. Επομένως, δεν μπορεί να κωδικοποιήσει και αποκωδικοποιήσει αποτελεσματικά τα δεδομένα και τις πληροφορίες που ανταλλάσσονται.

Μετά την ολοκλήρωση της εκτέλεσης του κρυπτογραφικού πρωτοκόλλου τα εξουσιοδοτημένα μέλη (και μόνο) έχουν στην κατοχή τους το κοινό μυστικό κλειδί, το οποίο μπορούν να χρησιμοποιούν για να κωδικοποιούν και να αποκωδικοποιούν τα δεδομένα που ανταλλάσσουν με τη βοήθεια ενός συμμετρικού αλγορίθμου.

-

ΚΕΦΑΛΑΙΟ 5

ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΕΩΝ ΧΡΗΣΤΗ ΣΕ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΝΟΣΟΚΟΜΕΙΟΥ

5.1 Έλεγχος πρόσβασης

Στις αρχές της δεκαετίας του 80 παρουσιάστηκε η ανάγκη για ανάπτυξη ολοκληρωμένων Πληροφοριακών Συστημάτων Νοσοκομείου ΠΣΝ (Hospital Information System) [Ehl89, Mil92, Rog91, Tak92, Tan94]. Παράλληλα, εμφανίστηκε το πρόβλημα της προστασίας των πληροφοριών που διακινούνται και διαχειρίζονται μέσα σ' ένα ΠΣΝ [Bak92, Bis91, Tre93, Eic92, Fok83, Gri93, Not91, Pan93b, Rog91, San93, Sto89].

Συγκεκριμένα, στα περισσότερα σύγχρονα ΠΣΝ θεωρείται αποδεκτό ότι η πρόσβαση στις πληροφορίες, που αποθηκεύονται στη βάση δεδομένων του νοσοκομείου, επιτρέπεται αποκλειστικά στους εξουσιοδοτημένους χρήστες [Bak92, Eic92, Not91, Pan93b]. Γι’ αυτό, υπάρχει ανάγκη ενός μοντέλου ελέγχου πρόσβασης το οποίο να συγχρονίζεται με τις απαιτήσεις και τις πολιτικές του εκάστοτε νοσοκομείου.

Επίσης, στο χώρο του νοσοκομείου, όπως και σε κάθε άλλο οργανισμό, είναι αναγκαία και απαραίτητη η εναρμόνιση των κανόνων που αφορούν τις απαιτήσεις ενός συστήματος ελέγχου με την ισχύουσα νομοθεσία. Στην Ελλάδα, η σχετική νομοθεσία δεν είναι τόσο ανεπτυγμένη όσο σε άλλες προηγμένες χώρες [Gri91, Gri91b, Gri91c, Gri92, Lee83, Rob92].

-

Στις περισσότερες περιπτώσεις, οι απαιτήσεις και οι πολιτικές ελέγχου πρόσβασης εκφράζονται μέσα από κανόνες (rules) της μορφής: "ποιος" έχει, "τι είδους πρόσβαση", "που", σύμφωνα με "ποιες" συνθήκες. Ένα σύστημα ελέγχου έχει ως στόχο τη μεσολάβηση μεταξύ του "ποιος" και "που", για τον καθορισμό της μη επιτρεπόμενης πρόσβασης [Cas95, Eic92, Fag78, Fug87, Gri76, Per95, Rab91, Ste91, Woo80].

Στα ΠΣΝ, τόσο τα μοντέλα όσο και οι μηχανισμοί ελέγχου πρόσβασης, θα πρέπει να είναι μέρος της διαδικασίας σχεδιασμού των εφαρμογών και της βάσης δεδομένων, ώστε να επιτευχθεί με αποτελεσματικότητα η διευθέτηση πολύπλοκων απαιτήσεων [Eic92, Not91, Pan95, Fug88, Tin88]. Στην περίπτωση που το ΠΣΝ υπάρχει, οι πιθανές αλλαγές που απαιτούνται μπορεί να είναι σημαντικές και με υψηλό κόστος υλοποίησης, τόσο στο επίπεδο λογισμικού όσο και στο επίπεδο υλικού [Pan95, Cas95, Fug88]. Δηλαδή, η υλοποίησή τους μπορεί να είναι πρακτικά αδύνατη για οικονομικούς, τεχνικούς ή λειτουργικούς λόγους.

Οπως συχνά συμβαίνει σε πολλά πληροφοριακά συστήματα, έτσι και στα πληροφοριακά συστήματα νοσοκομείου, ο σχεδιασμός και η υλοποίησή τους βασίζονται σε συστήματα διαχείρισης σχεσιακών βάσεων δεδομένων (relational database management systems). Ομως τα πιο πολλά από τα συστήματα αυτά παρέχουν λειτουργίες ασφάλειας περιορισμένου αριθμού και δεν μπορούν να αντεπεξέλθουν στις σύνθετες και πολύπλοκες απαιτήσεις ενός περιβάλλοντος νοσοκομείου [Eic92, ING91, SYB]. Έτσι, η προστασία των πληροφοριών πραγματοποιείται είτε μέσω ενός προτεινόμενου λογισμικού κώδικα (source code), ο οποίος ενσωματώνεται στο λογισμικό κώδικα του πληροφοριακού συστήματος, είτε από ειδικά πακέτα λογισμικού ασφάλειας, είτε τέλος από το υλικό ασφάλειας [Fug88, Woo80].

Οι παραπάνω τρόποι υλοποίησης έχουν ως μειονέκτημα την απόλυτη εξάρτηση του συστήματος ελέγχου πρόσβασης από το ίδιο το πληροφοριακό σύστημα με αποτέλεσμα, να μειώνεται η ευελιξία που πρέπει να έχει το σύστημα ελέγχου πρόσβασης σε πιθανές αλλαγές των απαιτήσεων χωρίς μεγάλη επιβάρυνση στο υπάρχον πληροφοριακό σύστημα.

-

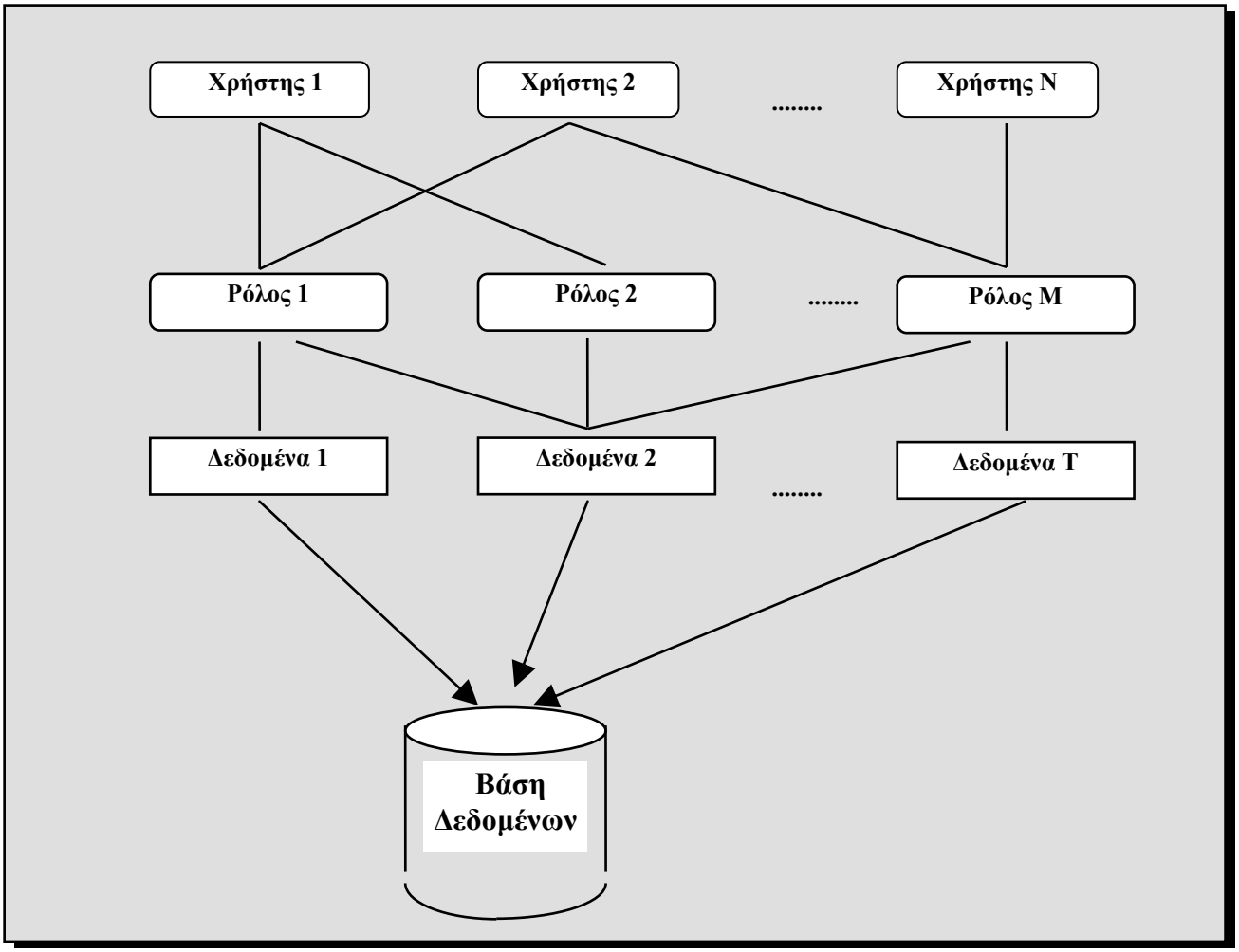
Επιπλέον, η αδυναμία χρήσης κλασσικών συστημάτων διαχείρισης βάσεων δεδομένων σ' ένα περιβάλλον νοσοκομείου προκύπτει από το μεγάλο αριθμό των κατηγοριών των χρηστών που υπάρχουν μέσα σ' αυτό (ιατροί, διοικητικοί, τεχνικοί, νοσηλευτικό προσωπικό κ.α.) καθώς και από το μεγάλο βαθμό σημαντικότητας των πληροφοριών που διακινούνται μέσα στο πληροφοριακό σύστημα [Eic92].

Επομένως, υπάρχει συχνά η ανάγκη ανάπτυξης λογισμικού, το οποίο να ενσωματώνεται στο λογισμικό του πληροφοριακού συστήματος νοσοκομείου ή/και χρήσης επιπρόσθετων πακέτων και υλικού ασφάλειας [Fug88, Pan93]. Τα μειονεκτήματα των τρόπων αντιμετώπισης του προβλήματος ελέγχου πρόσβασης σ' ένα περιβάλλον νοσοκομείου είναι: α) ότι η υλοποίηση του συστήματος ελέγχου πρόσβασης εξαρτάται από το λογισμικό του πληροφοριακού συστήματος και β) η αδυναμία ευελιξίας και εύκολης προσαρμογής του συστήματος ελέγχου πρόσβασης, κάθε φορά που οι απαιτήσεις αλλάζουν, με την λιγότερη προγραμματιστική επιβάρυνση στο υπάρχον σύστημα.

Ένας άλλος παράγοντας που πρέπει να ληφθεί υπόψη για την ανάπτυξη και υλοποίηση ενός συστήματος ελέγχου πρόσβασης σ' ένα ΠΣΝ, είναι η επιλογή μεταξύ ενός ολοκληρωμένου συστήματος βάσης δεδομένων (integrated system) και ενός συστήματος πολλαπλών βάσεων δεδομένων (π.χ. κάθε τμήμα του νοσοκομείου να έχει τη δική του βάση δεδομένων), οι οποίες επικοινωνούν μεταξύ τους (interfaced system). Αν και οι δύο περιπτώσεις παρουσιάζουν μειονεκτήματα και πλεονεκτήματα, τα τελευταία χρόνια υπάρχει μία τάση μεγαλύτερης αποδοχής των συστημάτων μιας μοναδικής βάσης δεδομένων, η οποία μπορεί να είναι κατανεμημένη [Ble92, Ger89]. Η αρχιτεκτονική του συστήματος θα πρέπει να αποτελεί έναν άλλο σημαντικό παράγοντα, όπου θα βασιστεί η ανάπτυξη και υλοποίηση ενός συστήματος ελέγχου πρόσβασης και γενικότερα ενός συστήματος ασφάλειας και προστασίας σε ένα ΠΣΝ [Med90].

Στη συνέχεια παρουσιάζεται ένας νέος μηχανισμός ελέγχου πρόσβασης χρηστών, που βασίζεται στα συστήματα κανόνων (rule systems) και σχεσιακές βάσεις δεδομένων (relational database) [Hoe91, Sto88, Sto92].

-



Σχήμα 1 Μοντέλο ασφάλειας ρόλου-χρήστη

Ο νέος μηχανισμός ανήκει στη κατηγορία των μοντέλων ασφάλειας ρόλου-χρήστη (αναλύθηκε στο κεφάλαιο 1) και θεωρεί ότι, κάθε χρήστης ενός ΠΣΝ μπορεί να έχει πολλούς ρόλους, ενώ κάθε φορά χρησιμοποιεί έναν από αυτούς για να αποκτήσει πρόσβαση σε συγκεκριμένα δεδομένα ή πληροφορίες [Loc88, SYB, Tin88]. Επομένως, κάθε πρόσβαση σε δεδομένα και πληροφορίες εξαρτάται από την δυνατότητα που έχουν οι χρήστες να την αποκτήσουν και σχετίζεται με τους ρόλους του κάθε χρήστη. Έτσι, ένας συγκεκριμένος χρήστης μπορεί να έχει πρόσβαση σε δεδομένα ή πληροφορίες, εάν ο χρήστης αυτός σχετίζεται μ' ένα ρόλο, για τον οποίο το σύστημα ελέγχου πρόσβασης επιτραπεί τη συγκεκριμένη πρόσβαση στα συγκεκριμένα δεδομένα. Στο σχήμα 1 παρουσιάζεται το γενικό μοντέλο ρόλου-χρήστη.

-

Ο έλεγχος πρόσβασης σ' ένα ΠΣΝ βασίζεται στη γενική παραδοχή ότι κάθε πρόσβαση σε δεδομένα ή πληροφορίες επιτρέπεται μόνο μέσω των εφαρμογών του συστήματος και ειδικότερα μέσω των φορμών (form) ή των οθόνων (screen) του συστήματος. Η προστασία και η ασφάλεια των δεδομένων και των πληροφοριών υλοποιείται μέσα από τις δυνατότητες που έχει το σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων. Ομως, σ' ένα περιβάλλον νοσοκομείου και κατά συνέπεια σ' ένα ΠΣΝ, η ασφάλεια και η προστασία των δεδομένων και των πληροφοριών σε τελικό επίπεδο (front-end) πρέπει να παρέχεται επαρκώς. Στην βιβλιογραφία έχουν προταθεί λεπτομερείς αρχιτεκτονικές ασφάλειας δεδομένων σε περιβάλλον νοσοκομείου, οι οποίες είναι βασισμένες σε διακριτά και σε πολλαπλών επιπέδων μοντέλα ασφάλειας [Eic92, Gri93, Not91, Per95]. Η αποτελεσματική εφαρμογή τους στην καθημερινή λειτουργία ενός νοσοκομείου δεν έχει όμως αποδειχτεί. Η βασική αιτία για αυτό είναι, ότι οι αρχιτεκτονικές αυτές δίνουν ελάχιστη βαρύτητα στο απαιτούμενο κόστος και την ευκολία των χρηστών. Επίσης, δεν λαμβάνουν υπόψη τους την περίπτωση επαύξησης της ασφάλειας και της προστασίας των δεδομένων και των πληροφοριών, σε ήδη υπάρχοντα συστήματα καθώς και την ανάγκη δυναμικής αλλαγής των απαιτήσεων ελέγχου πρόσβασης.

Οι περιορισμοί που αφορούν τον έλεγχο πρόσβασης, χρησιμοποιούνται σε δύο επίπεδα: στο επίπεδο της φόρμας (form level) ή της οθόνης (screen level) και στο επίπεδο των δεδομένων (data level). Οι περιορισμοί του πρώτου επίπεδου χρησιμοποιούνται για τον έλεγχο στις φόρμες του συστήματος και του δεύτερου επιπέδου για τον έλεγχο σε τιμές των δεδομένων της φόρμας (form-based data set occurrence level) με την προϋπόθεση ότι η πρόσβαση στο επίπεδο φόρμας ήταν επιτυχής.

Ενας άλλος παράγοντας που πρέπει να ληφθεί υπόψη είναι ότι η πολιτική ασφάλειας και ειδικότερα η πολιτική ελέγχου πρόσβασης, που προτείνεται κατά την φάση της ανάπτυξης και του σχεδιασμού, ικανοποιεί ένα υποσύνολο από τις ιδιαιτερότητες του χώρου και τις απαιτήσεις των χρηστών. Αυτό οφείλεται κυρίως στη μη απαιτούμενη βαρύτητα που πρέπει να δίνεται κατά την συλλογή και ανάλυση των απαιτήσεων ελέγχου πρόσβασης του νοσοκομείου. Οι συνέπειες της κατάστασης αυτής είναι α) η λανθασμένη κατηγοριοποίηση των χρηστών, β) ο λανθασμένος καθορισμός των δικαιωμάτων πρόσβασης και γ) το γεγονός ότι δεν λαμβάνονται

καθόλου υπόψη ορισμένες ειδικές απαιτήσεις (π.χ. δυναμική εξουσιοδότηση που οφείλεται στην ύπαρξη συγκεκριμένου γεγονότος) .

Η ανάγκη ύπαρξης ενός συστήματος ελέγχου πρόσβασης, το οποίο να ικανοποιεί τις παραπάνω συνθήκες, είναι εμφανής. Το σύστημα αυτό, θα πρέπει να υλοποιηθεί έτσι, ώστε να μην επιφέρει σοβαρές επιπτώσεις σ' άλλες λειτουργίες του ΠΣΝ (π.χ. κόστος αναβάθμισης, αποτελεσματικότητα, ευκολία συντήρησης, ικανοποίηση των χρηστών) καθώς επίσης και να μπορεί να λειτουργήσει μέσα στις καθορισμένες δυνατότητες του υπάρχοντος λογισμικού, εξοπλισμού, αρχιτεκτονικής και βάσεων δεδομένων.

Η ενσωμάτωση του ελέγχου πρόσβασης σ' ένα ΠΣΝ μπορεί να πραγματοποιηθεί με δύο μεθόδους:

α) οι διαδικασίες του ελέγχου πρόσβασης να τοποθετούν σε ανώτερο επίπεδο και
β) οι διαδικασίες ελέγχου πρόσβασης να χρησιμοποιούνται σε επίπεδο βάσης δεδομένων.

Με τη δεύτερη μέθοδο λειτουργούν τα διάφορα μοντέλα ασφάλειας διακριτικής ικανότητας, πολλών επιπέδων ή συνδυασμός αυτών [Eic92, Pan95, Tin88]. Η χρησιμοποίηση της δεύτερης μεθόδου προϋποθέτει αλλαγές στην δομή του συστήματος τόσο σε επίπεδο βάσης δεδομένων όσο και σε επίπεδο επικοινωνίας [Cas95, Fug88]. Η αποφυγή τέτοιων αλλαγών μπορεί να πραγματοποιηθεί, εάν η ασφάλεια των δεδομένων παρέχεται "εξωτερικά" χωρίς όμως να μειώνεται η απόδοσή της [Fug88,Tin88].

Σύμφωνα με τα όσα αναφέρθηκαν, ο νέος προτεινόμενος μηχανισμός ελέγχου πρόσβασης θα πρέπει: α) να λειτουργεί σε ανώτερο επίπεδο από το υπάρχον σύστημα, β) η ενσωμάτωση του με το ΠΣΝ να πραγματοποιηθεί με όσο το δυνατόν λιγότερες προγραμματιστικές παρεμβάσεις και γ) να είναι σύμφωνο με τους περιορισμούς που καθορίζονται, τόσο από το λογισμικό όσο και από το υλικό.

-

Επίσης, για να είναι ο μηχανισμός ευέλικτος και αποτελεσματικός, και ταυτόχρονα να ικανοποιεί τις απαιτήσεις ελέγχου πρόσβασης, θα πρέπει να είναι α) διακριτικής ικανότητας έλεγχος πρόσβασης βασισμένος σε ρόλους χρηστών, β) έλεγχος πρόσβασης εξαρτημένου περιεχομένου, γ) δυναμικής παροχής και ανάκλησης εξουσιοδότησης και δ) εύκολης διαχείρισης των κανόνων ελέγχου πρόσβασης από τον υπεύθυνο.

5.2 Οι απαιτήσεις ελέγχου πρόσβασης

Το πρώτο βήμα για την υλοποίηση του συστήματος ελέγχου πρόσβασης ενός ΠΣΝ θα πρέπει να είναι η συλλογή πληροφοριών από συνεντεύξεις με τα μέλη του νοσοκομείου και της διοίκησής του καθώς και η συνεχής επανεξέταση των σχετικών κανόνων λειτουργίας του νοσοκομείου, με σκοπό τον όσο το δυνατόν πιο ολοκληρωμένο καθορισμό ενός πλαισίου, που θα περιλαμβάνει τις απαιτήσεις και τις πολιτικές που θα προκύψουν.

Οι απαιτήσεις που αφορούν τη διαδικασία ελέγχου πρόσβασης καθορίζονται από: α) τις λειτουργίες του νοσοκομείου που υποστηρίζονται από το πληροφοριακό σύστημα, β) τις κατηγορίες των δεδομένων ή των πληροφοριών που σχετίζονται με τις λειτουργίες αυτές, γ) τον καθορισμό των ρόλων των χρηστών που μπορούν να εκτελούν τις λειτουργίες, δ) τον καθορισμό των συνθηκών που πρέπει να υπάρχουν για να επιτραπεί οποιαδήποτε πρόσβαση και ε) τον καθορισμό των υπεύθυνων για την όλη διαδικασία.

Συνεπώς, μια απαίτηση ορίζεται σε πρώτο στάδιο, σε σχέση με τις λειτουργίες του νοσοκομείου και στη συνέχεια, θα πρέπει να μετατραπεί σε κανόνα έλεγχο πρόσβασης σε σχέση με τις κατηγορίες των δεδομένων και των πληροφοριών. Για παράδειγμα, η απαίτηση "ένας ιατρός μπορεί να πραγματοποιεί διάγνωση για τους ασθενείς του " μετατρέπεται σ' ένα αριθμό απαιτήσεων αναφορικά με εκείνες τις κατηγορίες δεδομένων που χρησιμοποιούνται ή δημιουργούνται μέσα από την λειτουργία "διάγνωση"

-

1. Θεράπων ιατρός είναι μόνο κάθε ιατρός με ειδικότητα ή διευθυντής ιατρός.
2. Σύμβουλος ιατρός είναι μόνο κάθε ιατρός με ειδικότητα ή διευθυντής ιατρός.
3. Εφημερεύων ιατρός και ερευνητής ιατρός είναι μόνο κάθε μέλος του ιατρικού προσωπικού.
4. Ένας διευθυντής ιατρός μπορεί να εξουσιοδοτήσει έναν ιατρό με ειδικότητα, που ανήκει στο τμήμα του, με τον ρόλο "διευθυντή ιατρού", για την χρονική διάρκεια που θα απουσιάζει.
5. Ενας διευθυντής ιατρός μπορεί να διαβάζει τα ιατρικά δεδομένα των ασθενών του τμήματός του.
6. Ένας θεράπων ιατρός μπορεί να διαβάζει και να γράψει ιατρικά δεδομένα για όλους τους ασθενείς του.
7. Ένας θεράπων ιατρός μπορεί να διαβάζει μόνο τα ιατρικά ιστορικά όλων των ασθενών του.
8. Ένας θεράπων ιατρός μπορεί να εκδίδει εντολή εξέτασης και φαρμάκου για όλους τους ασθενείς του.
9. Ενας θεράπων ιατρός μπορεί να διαβάζει τις αναφορές ενός ακτινολόγου ή ενός συμβούλου ιατρού ,που αφορούν τους ασθενείς του.
10. Ένας εκπαιδευόμενος ιατρός ή ιατρός με ειδικότητα μπορεί να διαβάσει μόνο ιατρικά δεδομένα των ασθενών του τμήματός του, όταν εξουσιοδοτηθεί από τους αντίστοιχους θεράποντες ιατρούς.
11. Ένας ακτινολόγος μπορεί να διαβάσει ιατρικά δεδομένα ασθενών, για τους οποίους έχει εκδοθεί ακτινολογική εξέταση.
12. Σύμβουλος ιατρός και εφημερεύων ιατρός δεν μπορούν να μεταφέρουν τα δικαιώματα τους σ' άλλους ιατρούς με ειδικότητα.
13. Ένας σύμβουλος ιατρός μπορεί να διαβάσει ιατρικά δεδομένα για ασθενείς, που του έχει ζητηθεί να τους εξετάσει.
14. Ένας εφημερεύων ιατρός μπορεί να διαβάζει και να γράφει ιατρικά δεδομένα για όλους τους ασθενείς του τμήματός του κατά την διάρκεια της εφημερίας του.
15. Ένας ερευνητής ιατρός μπορεί να διαβάσει μόνο ανώνυμα ιατρικά ιστορικά για κάθε ασθενή του νοσοκομείου.

Πίνακας 1 Περιορισμοί και απαιτήσεις ελέγχου πρόσβασης του νοσοκομείου

-

Στον πίνακα 1, παρουσιάζονται ορισμένοι περιορισμοί και απαιτήσεις που προέκυψαν από την έρευνα που πραγματοποιήθηκε σε πραγματικό περιβάλλον νοσοκομείου.

Από τον πίνακα αυτό προκύπτει ότι ένας χρήστης μπορεί να αποκτήσει πρόσβαση σε συγκεκριμένα δεδομένα και πληροφορίες, εάν και μόνο εάν έχει κάποιο ρόλο, για τον οποίο επιτρέπεται η πρόσβαση σ' αυτά. Η έννοια του ρόλου, που εμφανίζεται συχνά στα συστήματα ελέγχου πρόσβασης, επιτρέπει τη συσχέτιση μίας πρόσβασης μ' ένα σύνολο χρηστών, χωρίς να απαιτείται η επανάληψη της συσχέτισης της πρόσβασης με κάθε μέλος του συνόλου χωριστά [Fug87, Loc88, Not91, Pan95, SYB, Tin88].

Οι ρόλοι χωρίζονται σε *μόνιμους*, όπου μπορούν να απεικονισθούν στην οργανωτική δομή του νοσοκομείου (π.χ. διευθυντής ιατρός) και σε προσωρινούς, όπου ένας χρήστης μπορεί να έχει ένα ρόλο εφόσον έχει τη δυνατότητα να συμμετέχει σε συγκεκριμένες διαδικασίες (π.χ. σύμβουλος ιατρός). Οι προσωρινοί ρόλοι χρησιμοποιούνται κυρίως για την καλύτερη εναρμόνιση των προσβάσεων σε δεδομένα και πληροφορίες με τις απαιτήσεις των χρηστών [Ber94, Loc88, Moh94, Tin88].

Από την ανάλυση των απαιτήσεων θα πρέπει να ληφθούν υπόψη διάφορα σημεία που απεικονίζονται μέσα στο πλαίσιο της καθημερινής λειτουργίας του νοσοκομείου. Ένα από τα σημεία αυτά είναι η δυνατότητα των χρηστών να έχουν πολλούς ρόλους ταυτόχρονα. Για παράδειγμα, ένας χρήστης που είναι ιατρός μπορεί να είναι ερευνητής ιατρός ή/και εφημερεύων ιατρός, εάν ανήκει στη λίστα εφημεριών ή/και σύμβουλος ιατρός εφόσον του έχει δοθεί αντίστοιχη εντολή από έναν άλλο ιατρό διαφορετικού τμήματος.

Ενα άλλο σημείο, είναι ότι κάθε δικαίωμα πρόσβασης μπορεί να αφορά ένα συγκεκριμένο χρήστη ή έναν ρόλο, να παρέχεται άμεσα ή έμμεσα, να συνοδεύεται ή να μη συνοδεύεται από το δικαίωμα εξουσιοδότησης.

-

Για παράδειγμα, ένας εκπαιδευόμενος ιατρός μπορεί να εξουσιοδοτηθεί από έναν θεράποντα ιατρό ενός ασθενή για να "διαβάσει" το ιατρικό ιστορικό του. Στην περίπτωση αυτή, η εξουσιοδότηση αφορά ένα συγκεκριμένο χρήστη, πραγματοποιείται άμεσα και ο εκπαιδευόμενος ιατρός δεν έχει το δικαίωμα να μεταφέρει τη συγκεκριμένη εξουσιοδότηση σ' άλλο χρήστη.

Ενας ακτινολόγος όμως, μπορεί να έχει πρόσβαση σε συγκεκριμένα δεδομένα ενός ασθενή, όταν εκκρεμεί εντολή για ακτινολογική εξέταση του ασθενή και του έχει ανατεθεί η εκτέλεση της εξέτασης αυτής. Στην περίπτωση αυτή, η εξουσιοδότηση είναι έμμεση, αφού γίνεται στο ρόλο ακτινολόγο, ενεργοποιείται τη χρονική στιγμή ανάθεσης της εξέτασης στο συγκεκριμένο ακτινολόγο, απενεργοποιείται τη χρονική στιγμή που εκδίδεται η ακτινολογική αναφορά, ενώ παρέχεται το δικαίωμα μεταφοράς της συγκεκριμένης εξουσιοδότησης σε άλλο ακτινολόγο. Συνεπώς, η πρόσβαση παρέχεται για κάποια χρονική περίοδο η οποία καθορίζεται από δύο γεγονότα. Στις περιπτώσεις αυτές, το γεγονός "εκκίνηση" είναι ικανή και αναγκαία συνθήκη για να αποκτήσει ο χρήστης την πρόσβαση. Στο παραπάνω παράδειγμα, ο ακτινολόγος μπορεί να έχει πρόσβαση στα δεδομένα του ασθενή μόνο όταν υπάρχει εντολή για ακτινολογική εξέτασή του.

Από τις απαιτήσεις ελέγχου που αναφέρθηκαν παραπάνω προκύπτει η ανάγκη ύπαρξης εξαρτημένου περιεχομένου (content-dependent) διακριτού ελέγχου πρόσβασης που βασίζεται στην αρχή της "ανάγκης να γνωρίζω" (need-to-know). Ο πιο συνήθης τρόπος υλοποίησης του ελέγχου πρόσβασης σε περιβάλλοντα βάσεων δεδομένων είναι η χρήση των θεωρήσεων (views) και με τη βοήθεια των φορμών [Cas95, Pan95, Tin88].

Η δυνατότητα πρόσβασης κάθε χρήστη στη βάση δεδομένων μέσω των φορμών (form-based application) συνεπάγεται ότι, το που έχει πρόσβαση ο χρήστης κάθε φορά ταυτίζεται με τα δεδομένα που υπάρχουν στη συγκεκριμένη φόρμα (form based data sets). Επίσης, κάθε θεώρηση καθορίζει τις συνθήκες που θα πρέπει να ικανοποιούνται, ώστε να επιτραπεί η πρόσβαση σ' ένα συγκεκριμένο χρήστη ή ρόλο. Συνεπώς, τα σύνολα των δεδομένων των φορμών

χρησιμοποιούνται ως αντικείμενα ελέγχου πρόσβασης στη μετατροπή των απαιτήσεων σε κανόνες πρόσβασης ελέγχου εξαρτημένου περιεχομένου.

5.3 Κανόνες ελέγχου πρόσβασης

Ο καθορισμός των κανόνων ελέγχου πρόσβασης ενός συστήματος εξαρτημένου περιεχομένου, που βασίζεται σε ρόλους, απαιτεί τον ορισμό των ρόλων αυτών, των ειδών πρόσβασης, των αντικειμένων και τις συνθήκες που θα επιτρέψουν να πραγματοποιηθεί η πρόσβαση. Έτσι, το σύνολο των απαιτήσεων ελέγχου πρόσβασης μπορεί να μετατραπεί σ' ένα σύνολο κανόνων πρόσβασης με την ακόλουθη μορφή:

(R, r, o, p)

όπου:

R ο ρόλος
r το είδος πρόσβασης
o το αντικείμενο πρόσβασης
p οι περιορισμοί-συνθήκες

Κατά την διαδικασία ανάπτυξης και σχεδιασμού του μηχανισμού ελέγχου πρόσβασης, θεωρήθηκε απαραίτητη η επέκταση της παραπάνω μορφής, ώστε να καλύπτει και δυνατότητα για ανάθεση / ανάκληση δικαιωμάτων (right).

Ως *δικαίωμα* ορίζεται κάθε τριάδα που αποτελείται από το είδος πρόσβασης, το αντικείμενο πρόσβασης και τις συνθήκες (κατηγορήματα περιορισμών) που πρέπει να ισχύουν για να επιτραπεί η συγκεκριμένη πρόσβαση στο συγκεκριμένο αντικείμενο. Δηλαδή, κάθε δικαίωμα έχει την ακόλουθη μορφή:

(r, o, p)

-

όπου:

r το είδος πρόσβασης

o το αντικείμενο πρόσβασης

p οι περιορισμοί-συνθήκες

Η νέα μορφή των κανόνων πρόσβασης είναι η ακόλουθη:

$$(u_1, \quad u_2, \quad r, \quad o, \quad p, \quad f)$$

όπου

u_1 ο ρόλος-χρήστης που έχει το δικαίωμα (r, o, p)

u_2 ο ρόλος-χρήστης στον οποίο μπορεί να μεταφερθεί το δικαίωμα (r, o, p) από το ρόλο-χρήστη u_1

r τα επιτρεπόμενα είδη πρόσβασης για τα δεδομένα του αντικειμένου πρόσβασης o (π.χ. φόρμα)

o τα δεδομένα του αντικειμένου πρόσβασης στο οποίο ορίζεται η πρόσβαση

p οι συνθήκες - περιορισμοί που καθορίζουν το δικαίωμα πρόσβασης στα δεδομένα του αντικειμένου πρόσβασης για το χρήστη u_1

f η δυνατότητα μεταφοράς του δικαιώματος (r, o, p) από το ρόλο-χρήστη u_2 σ' άλλο ρόλο-χρήστη

Η παραπάνω μορφή των κανόνων ελέγχου πρόσβασης βασίζεται στις ακόλουθες υποθέσεις:

-

– Ενας χρήστης του συστήματος έχει το ρόλο του *χρήστη με αυξημένες αρμοδιότητες* (super user). Ο χρήστης αυτός έχει την υποχρέωση και το δικαίωμα να καθορίσει τους κανόνες πρόσβασης, σύμφωνα με τους οποίους, κάθε ρόλος-χρήστης θα έχει αρχικά ορισμένα δικαιώματα πρόσβασης

– Η απουσία ενός κανόνα ελέγχου πρόσβασης συνεπάγεται την απαγόρευσή της. Δηλαδή, το προτεινόμενο σύστημα είναι "κλειστό σύστημα", αφού η πρόσβαση στα δεδομένα μιας φόρμας δεν επιτρέπεται, εκτός εάν υπάρχει ή μπορεί να προκύψει δικαίωμα πρόσβασης.

Οπως αναφέρθηκε και προηγούμενα, οι προσωρινοί ρόλοι μπορούν να παρέχονται ή να ανακαλούνται, σε ή από χρήστες, άμεσα ή έμμεσα, σύμφωνα με την πραγματοποίηση συγκεκριμένων ενεργειών. Για παράδειγμα, εάν σ' ένα συγκεκριμένο ιατρό με ειδικότητα, του έχει ζητηθεί να δώσει απάντηση σε μια εντολή, και αυτός μπορεί να αποκτήσει το ρόλο του συμβούλου ιατρού, τότε η ενέργεια είναι "*του έχει ζητηθεί να δώσει απάντηση σε κάποια εντολή*". Η ενέργεια που θα πρέπει να πραγματοποιηθεί, ώστε να ανακληθεί το δικαίωμα πρόσβασης, είναι η έκδοση της αντίστοιχης αναφοράς-απάντησης από τον χρήστη. Με τον τρόπο αυτό το δικαίωμα μεταφοράς της εξουσιοδότησης μεταξύ των ρόλων μπορεί να ελέγχεται.

Οι ενέργειες στις οποίες οφείλονται η μεταφορά ή ανάκληση ενός δικαιώματος πρέπει να καθορίζονται με σκοπό την παροχή δυναμικής αλλαγής των ρόλων που κάθε χρήστης μπορεί να έχει [Moh94,Woo80]. Οταν πραγματοποιείται μια συγκεκριμένη ενέργεια τότε η αντίστοιχη διαδικασία ενεργοποιείται, ώστε να πραγματοποιηθεί η απόκτηση ή ανάκληση του ρόλου από το συγκεκριμένο χρήστη.

Η μείωση του αριθμού των κανόνων ελέγχου πρόσβασης, που απαιτούνται για την πλήρη περιγραφή των απαιτήσεων ελέγχου πρόσβασης στο περιβάλλον του νοσοκομείου, επιτυγχάνεται:

-

- με την αντιστοίχηση των δικαιωμάτων (r, o, p) που αντιστοιχούν σ' ένα ρόλο χρήστη με τον ίδιο το ρόλο,

- με τη χρήση των επαγωγικών κανόνων (implication rules).

Καθώς τα δικαιώματα σχετίζονται με τους ρόλους των χρηστών και το σύνολο των δικαιωμάτων, που αφορά ένα ρόλο-χρήστη, μπορεί να αντικατασταθεί από το ρόλο, [Moh94, Tin88] τότε κάθε κανόνας ελέγχου πρόσβασης μπορεί να ερμηνευτεί ως ακολούθως:

> Κάθε χρήστης, που έχει το ρόλο u_1, μπορεί να εξουσιοδοτήσει έναν άλλο χρήστη, που έχει τον ρόλο u_2, με το ρόλο u_3.

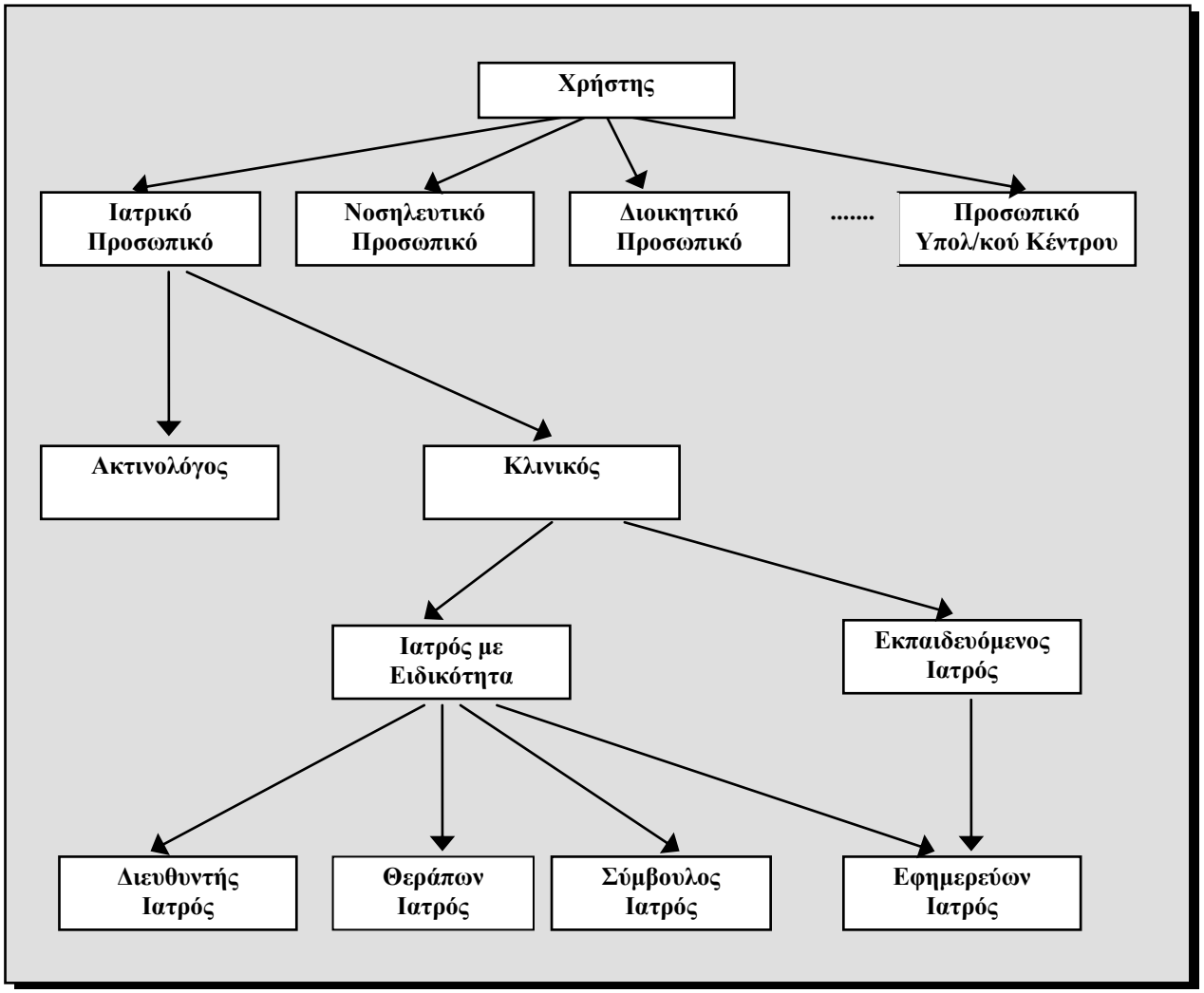
Κάθε επαγωγικός κανόνας αντικαθιστά παραμετρικά ένα σύνολο κανόνων ελέγχου πρόσβασης. Οι επαγωγικοί κανόνες καθορίζονται σύμφωνα με τους ρόλους των χρηστών, τα σύνολα των δεδομένων των φορμών και τα είδη της πρόσβασης. Οι επαγωγικοί κανόνες μπορούν να χρησιμοποιηθούν για να καθορίζουν ένα βασικό σύνολο κανόνων ελέγχου πρόσβασης για κάθε ρόλο χρήστη. Τα κύρια πλεονεκτήματα της χρήσης των επαγωγικών κανόνων είναι η μη αναγκαία απεικόνιση και καταχώρηση όλων των κανόνων ελέγχου πρόσβασης και μια τυποποίηση των κανόνων αυτών, ώστε να μπορούν αναγνωριστούν εύκολα πιθανές αντιθέσεις-συγκρούσεις μεταξύ τους. Ομως, κατά τη διαδικασία υλοποίησης, θα πρέπει τα πλεονεκτήματα αυτά να εξετάζονται σε σχέση με τις δυνατότητες που παρέχονται σε λογισμικό και σε εξοπλισμό[Ber94].

5.4 Ρόλοι

Το σύνολο των ρόλων που υπάρχουν μέσα σ' ένα νοσοκομείο μπορεί να περιγραφεί από ένα δίκτυο, που ονομάζεται *δίκτυο των ρόλων* (role network) [Ber94, Loc88, Tin88]. Ένα δίκτυο ρόλων που αφορά τις απαιτήσεις ελέγχου πρόσβασης του πίνακα 1 παρουσιάζεται στο σχήμα 2.

-

Το δίκτυο των ρόλων για το προτεινόμενο σύστημα ελέγχου πρόσβασης έχει τα ακόλουθα χαρακτηριστικά:



Σχήμα 2. Δίκτυο ρόλων χρηστών

– Ένας ρόλος μπορεί να περιέχει άλλους ρόλους. Για παράδειγμα, ο ρόλος "Ακτινολόγος" έχει τα δικαιώματα πρόσβασης που απευθύνονται για τον συγκεκριμένο ρόλο καθώς και τα δικαιώματα πρόσβασης του ρόλου "Ιατρικό Προσωπικό"

-

- Ένας χρήστης μπορεί να έχει πολλούς ρόλους και ένας ρόλος μπορεί να αναφέρεται σε πολλούς χρήστες.

- Ένας χρήστης μπορεί να χρησιμοποιεί ένα μόνο ρόλο κάθε φορά, ενώ μπορεί να αλλάζει ρόλο ανάλογα τις συνθήκες που επικρατούν.

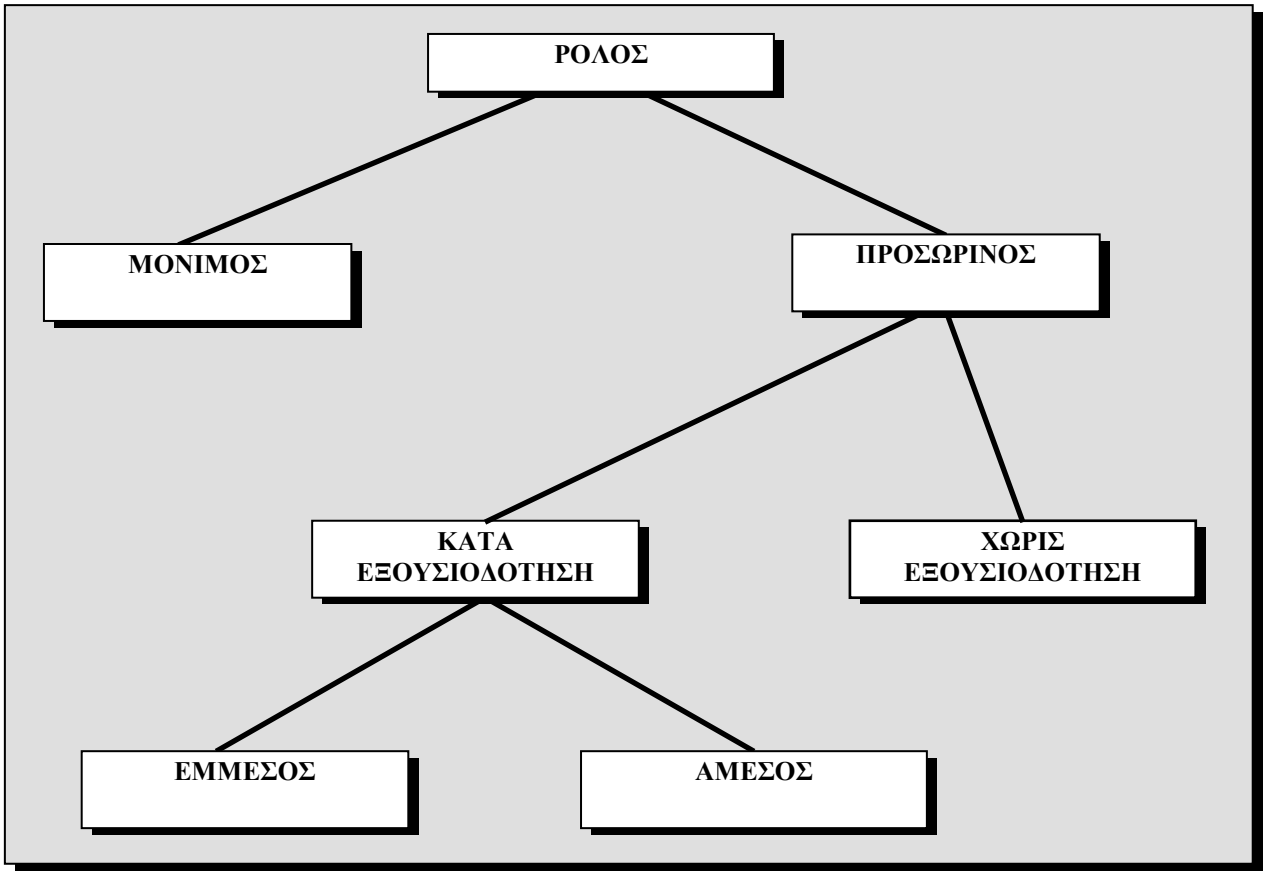
- Μόνιμος είναι κάθε ρόλος που απεικονίζεται στην οργανωτική δομή του νοσοκομείου (π.χ. διευθυντής ιατρός, ιατρός, εκπαιδευόμενος ιατρός).

- Προσωρινός είναι κάθε ρόλος που μπορεί ένας χρήστης να έχει για ένα χρονικό διάστημα και όταν αυτός εκτελεί συγκεκριμένες ενέργειες (π.χ. ερευνητής ιατρός).

- Μια ειδική κατηγορία των προσωρινών ρόλων είναι οι *εξουσιοδοτούμενοι ρόλοι* (authorised role). Ως εξουσιοδοτούμενος ρόλος ορίζεται, κάθε ρόλος τον οποίο ένας χρήστης έχει λόγω της παροχής του από άλλον ρόλο-χρήστη για καθορισμένη χρονική διάρκεια. Η καθορισμένη χρονική διάρκεια ξεκινά από τη χρονική στιγμή της παροχής του δικαιώματος και ολοκληρώνεται τη χρονική στιγμή ανάκλησής του. Ένας εξουσιοδοτούμενος ρόλος μπορεί να παρέχεται έμμεσα ή άμεσα ανάλογα με το γεγονός που τον προκαλεί. Για παράδειγμα, ένας ιατρός μπορεί έμμεσα να αποκτήσει το ρόλο του διευθυντή ιατρού κατά την διάρκεια της απουσίας του διευθυντή ιατρού και εφόσον υπάρχει εντολή, ενώ ένας ιατρός είναι και εφημερεύων ιατρός εφόσον το όνομα του υπάρχει στην λίστα των εφημεριών. Στο σχήμα 3, παρουσιάζονται οι κατηγορίες των ρόλων.

- Οι ρόλοι στο δίκτυο των ρόλων έχουν ιεραρχική δομή. Εάν ένας ρόλος σχετίζεται με ένα χρήστη, τότε όλοι οι υπέρ-ρόλοι (ρόλοι ανωτέρου επιπέδου) του συγκεκριμένου ρόλου σχετίζονται με τον ίδιο χρήστη. Επομένως, οι προσβάσεις που έχει ένας ρόλος μεταφέρονται και σ' όλους του υπό-ρόλους (ρόλους κατωτέρου επιπέδου). Για παράδειγμα στο σχήμα 3, ένας χρήστης που έχει ως μόνιμο ρόλο εκείνο του ιατρού με ειδικότητα,

μπορεί να χρησιμοποιήσει και το ρόλο του σύμβουλου ιατρού (ύστερα από εξουσιοδότηση ενός άλλου ιατρού με ειδικότητα). Στην περίπτωση αυτή, ο συγκεκριμένος χρήστης έχει τις προσβάσεις ενός συμβούλου ιατρού καθώς επίσης και τις προσβάσεις ενός ιατρού με ειδικότητα.



Σχήμα 3. Κατηγορίες ρόλων.

5.5 Είδη πρόσβασης

Τα είδη πρόσβασης (modes of access) για τα δεδομένα μιας φόρμας είναι "εισαγωγή" (insert), "επιλογή" (select) και "ανάκληση" (cancel). Κάθε διαδικασία "ανάκλησης" μπορεί να πραγματοποιηθεί μόνο και εφόσον ισχύουν συγκεκριμένες συνθήκες και έχει ως αποτέλεσμα την

απενεργοποίηση ενός ή περισσοτέρων κανόνων ελέγχου πρόσβασης. Τόσο οι διαγραφές όσο και οι ενημερώσεις δομής SQL δεν επιτρέπονται για λόγους ελέγχου και αποδοχής χρηστών.

Η εισαγωγή συνεπάγεται και επιλογή και ανάκληση, ενώ η ανάκληση επίσης συνεπάγεται επιλογή. Για παράδειγμα, ένας χρήστης που έχει πρόσβαση εισαγωγής στα δεδομένα μιας φόρμας έχει ταυτόχρονα και πρόσβαση επιλογής και ανάκλησης σ' αυτά.

Οι λειτουργίες των δεδομένων φορμών πραγματοποιούνται μόνο μέσω φορμών και δεν επιτρέπεται κανένας άλλος τρόπος πραγματοποίησης μιας τέτοιας λειτουργίας (εσωτερικά ή εξωτερικά). Παρόλο που κάτι τέτοιο φαίνεται ως περιορισμός για τους χρήστες του συστήματος, η δυνατότητα χρήσης άλλων μέσων επικοινωνίας με τα δεδομένα θα οδηγούσε στην παράκαμψη των περιορισμών πρόσβασης.

5.6 Αντικείμενα πρόσβασης

Στον προτεινόμενο μηχανισμό ελέγχου πρόσβασης τα αντικείμενα πρόσβασης έχουν οριστεί ως τα δεδομένα των φορμών του ΠΣΝ μαζί με τους περιορισμούς που προέρχονται κάθε φορά από το ρόλο του χρήστη. Καθώς οι φόρμες σχετίζονται με τις λειτουργίες του νοσοκομείου, είναι δυνατόν να καθορισθεί ένα σύνολο φορμών για κάθε συγκεκριμένη λειτουργία. Τότε μόνο ο ρόλος που σχετίζεται με τη συγκεκριμένη λειτουργία να μπορεί να έχει πρόσβαση στο συγκεκριμένο σύνολο φορμών. Συνεπώς, οι φόρμες που αφορούν ένα ΠΣΝ μπορούν να εκφραστούν από ένα κατευθυνόμενο δίκτυο, όπου κάθε φόρμα συνδέεται με εκείνες τις φόρμες που μπορούν να ενεργοποιηθούν μέσα από αυτή.

Επομένως, κάθε επιτρεπόμενη πρόσβαση σ' ένα σύνολο δεδομένων φόρμας συνεπάγεται την πρόσβαση σ' όλα τα δεδομένα φορμών που έχουν σχέση μ' αυτό. Για παράδειγμα, ένας θεράπων ιατρός που έχει πρόσβαση στη φόρμα "πορεία νόσου", πρέπει και έχει πρόσβαση σ' όλες τις φόρμες που "καλούνται" από τη φόρμα "πορεία νόσου" (π.χ. φόρμα "στοιχείων του ασθενή").

-

5.7 Κατηγορήματα περιορισμών

Τα κατηγορήματα περιορισμών (predicate constraints) καθορίζουν τα επιτρεπόμενα περιεχόμενα των δεδομένων φόρμας για κάθε ρόλο χρήστη. Για παράδειγμα, τα επιτρεπόμενα περιεχόμενα για τα δεδομένα της φόρμας "ιστορικό ασθενή" για ένα θεράποντα ιατρό είναι μόνο τα ιστορικά των ασθενών του. Περιορισμοί που αφορούν τόπο και χρόνο (π.χ. είδος τερματικού και ημερομηνία-ώρα) δεν έχουν ληφθεί υπόψη για λόγους ευκολίας του χρήστη. Τα κατηγορήματα περιορισμών εκφράζονται ως παραμετρικοί προσδιορισμοί, οι οποίοι ενσωματώνονται δυναμικά στις αντίστοιχες διαδικασίες με σκοπό την παροχή ελέγχου πρόσβασης εξαρτημένου περιεχομένου.

5.8 Υλοποίηση του μοντέλου ελέγχου πρόσβασης

Το προτεινόμενο μοντέλο ελέγχου πρόσβασης μπορεί να υλοποιηθεί με δύο τρόπους:

– οι λειτουργίες ασφάλειας να παρέχονται από μηχανισμούς ασφάλειας που είναι ανεξάρτητοι από το σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων και

– οι λειτουργίες ασφάλειας να παρέχονται από μηχανισμούς ασφάλειας μέσα από το σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων.

Με σκοπό την αποφυγή σημαντικών τροποποιήσεων στο σχήμα της βάσης δεδομένων, αποφασίστηκε η παροχή λειτουργιών ασφάλειας να υλοποιηθεί με μηχανισμούς ανεξάρτητους από το σύστημα διαχείρισης σχεσιακών βάσεων δεδομένων (1ϊὸ τρόπος). Παράλληλα, ο μηχανισμός ασφάλειας θα επιτρέπει την ενσωμάτωση των κανόνων πρόσβασης στο λογισμικό των εφαρμογών μέσω ενός συστήματος κανόνων.

-

Το γεγονός ότι, η υλοποίηση του προτεινόμενου μοντέλου ελέγχου πρέπει να εξετασθεί μέσα από το γενικό πλαίσιο ανάπτυξης και αναβάθμισης ενός ΠΣΝ, οδηγεί στη συνεχή επανεξέταση της υλοποίησης των μέτρων ασφάλειάς του, ώστε να διατηρείται μια ισορροπία μεταξύ διαφόρων παραμέτρων, όπως κόστος αναβάθμισης, αποτελεσματικότητα του συστήματος, εύκολη χρήση κλπ. Επιπλέον, το μοντέλο ελέγχου πρόσβασης, για να είναι αποτελεσματικό, θα πρέπει εύκολα και χωρίς μεγάλο προγραμματιστικό κόστος να συνεργάζεται και να συνλειτουργεί με ένα ήδη υπάρχον πληροφοριακό σύστημα, παρέχοντας συγχρόνως τη δυνατότητα πιθανών μελλοντικών αλλαγών στην πολιτική ασφάλειας του νοσοκομείου. Για την αποφυγή του επανασχεδιασμού του όλου συστήματος, το προτεινόμενο μοντέλο ελέγχου ασφάλειας θα υλοποιηθεί σε επίπεδο εφαρμογής, ενώ η διαδικασία ελέγχου πρόσβασης θα πρέπει να είναι σ' ένα βαθμό ανεξάρτητη από το σύστημα διαχείρισης των βάσεων δεδομένων. Με στόχο την επίτευξη των παραπάνω, το προτεινόμενο μοντέλο ελέγχου πρόσβασης θα υλοποιηθεί ως ένα σύστημα κανόνων.

Τέσσερις είναι οι δυνατές περιπτώσεις συνλειτουργίας των σχεσιακών βάσεων δεδομένων με τα συστήματα κανόνων [Cer87, Hoe91, Sto89] :

– Οι κανόνες να αποτελούν τμήμα του λογισμικού και τα δεδομένα να βρίσκονται σε σχεσιακή βάση.

– Οι κανόνες και τα δεδομένα να διαχειρίζονται από ένα πυρήνα έμπειρου συστήματος (expert system shell).

– Οι κανόνες να βρίσκονται σ’ ένα έμπειρο σύστημα και τα δεδομένα σε σχεσιακή βάση δεδομένων.

– Οι κανόνες και τα δεδομένα να διαχειρίζονται από μια βάση κανόνων / δεδομένων σύνθετη τύπου (rule/data base).

-

Παρόλο που και οι τέσσερις παραπάνω περιπτώσεις μπορούν να χρησιμοποιηθούν στην υλοποίηση του μοντέλου ελέγχου πρόσβασης, η τρίτη θεωρήθηκε η πιο κατάλληλη αποβλέποντας στο διαχωρισμό του συστήματος ελέγχου πρόσβασης από τις βάσεις δεδομένων. Το προτεινόμενο σύστημα ελέγχου πρόσβασης εάν και δεν αποτελεί ένα κλασικό έμπειρο σύστημα, συμπεριφέρεται με παρόμοιο τρόπο και ακολουθεί την ίδια λειτουργικότητα. Είναι γνωστό ότι η χρήση έμπειρων συστημάτων στο χώρο των νοσοκομείων και γενικότερα στην επιστήμη της ιατρικής έχει εξετασθεί με σημαντικά οφέλη, αλλά και επιφυλάξεις όσον αφορά τις επιπτώσεις που μπορεί να προκύψουν στον ασθενή σε περίπτωση λάθους [Dus92].

Στο σχήμα 4 παρουσιάζεται το μοντέλο οντοτήτων-σχέσεων του συστήματος ελέγχου πρόσβασης, όπου ανήκουν οι ακόλουθες βασικές οντότητες και σχέσεις:

Οντότητες

1. Χρήστης
2. Ρόλος
3. Φόρμα
4. Σύνολο δεδομένων φόρμας
5. Κατηγορήματα περιορισμών
6. Είδη πρόσβασης
7. Δικαίωμα (είδος πρόσβασης, σύνολο δεδομένων φόρμας, κατηγόρημα περιορισμού)

Σχέσεις

1. Ένας χρήστης μπορεί να έχει πολλούς ρόλους και ένας ρόλος μπορεί να αναφέρεται σε πολλούς χρήστες.
   Είναι μία σχέση "πολλά προς πολλά" και ορίζεται με τρεις διαφορετικές οντότητες: Χρήστης, Ρόλος, Χρήστης-Ρόλος (σχέσεις 1 και 2).

2. Ένας ρόλος μπορεί να περιέχει άλλους ρόλους.

-

Είναι μία "επαναληπτική" σχέση και ορίζεται με δύο διαφορετικές οντότητες: Ρόλος και Ιεραρχία-Ρόλων (σχέση 3).

3. Μία φόρμα μπορεί να σχετίζεται με άλλες φόρμες.
   Είναι μία "επαναληπτική" σχέση και ορίζεται με δύο διαφορετικές οντότητες: Φόρμα και Ιεραρχία-Φορμών (σχέση 10).

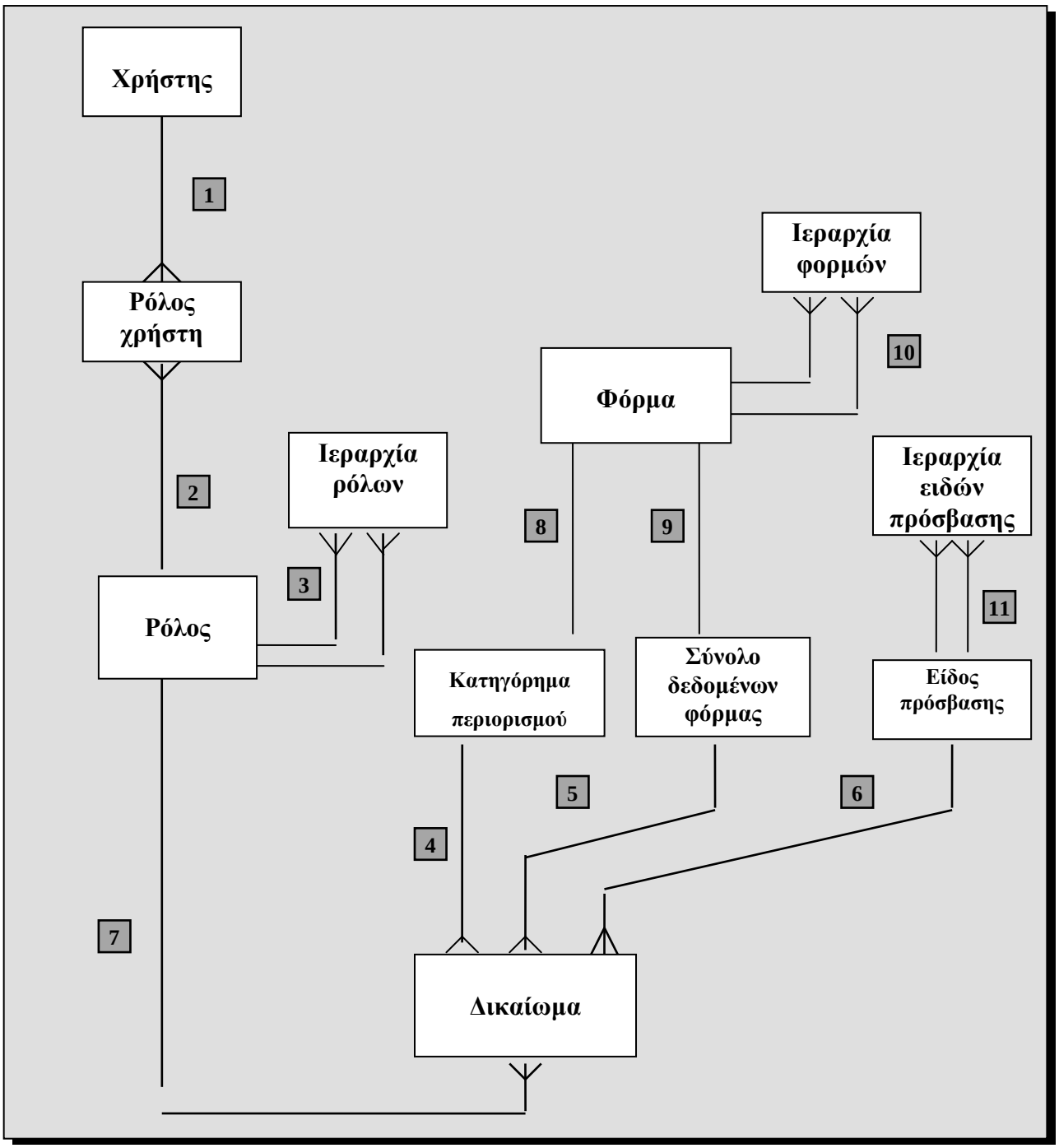
4. Μια φόρμα συνδέεται με ένα κατηγόρημα περιορισμών και ένα κατηγόρημα περιορισμών ανήκει μόνο σε μία φόρμα.
   Είναι μία σχέση "1-1" και ορίζεται με δύο διαφορετικές οντότητες: Φόρμα και Κατηγόρημα περιορισμών (σχέση 8).

5. Μια φόρμα συνδέεται μ' ένα σύνολο δεδομένων φορμών και ένα σύνολο δεδομένων φόρμας ανήκει μόνο σε μία φόρμα.
   Είναι μία σχέση "1-1" και ορίζεται με δύο διαφορετικές οντότητες: Φόρμα και Σύνολο δεδομένων φόρμας (σχέση 9).

6. Ενα είδος πρόσβασης μπορεί να σχετίζεται με άλλα είδη πρόσβασης.
   Είναι μία "επαναληπτική" σχέση και ορίζεται με δύο διαφορετικές οντότητες: Είδος πρόσβασης και Ιεραρχία-ειδών πρόσβασης (σχέση 11).

7. Ενας Ρόλος μπορεί να συνδέεται με πολλά Κατηγορήματα περιορισμών, Σύνολα δεδομένων φόρμας και Είδη πρόσβασης ενώ ένα Κατηγόρημα περιορισμών, ένα Σύνολο δεδομένων φόρμας και ένα Είδος πρόσβασης με πολλούς Ρόλους.
   Είναι μία σχέση "πολλά προς πολλά" και ορίζεται με πέντε διαφορετικές οντότητες: Δικαίωμα, Ρόλος, Κατηγόρημα περιορισμών, Σύνολο δεδομένων φόρμας και Είδος πρόσβασης (σχέσεις 4, 5, 6 και 7).

-



Σχήμα 4. Μοντέλο οντοτήτων-σχέσεων του συστήματος ελέγχου πρόσβασης.

-

5.9 Σύστημα ελέγχου πρόσβασης

Το σύστημα ελέγχου πρόσβασης χωρίζεται σε τρία μέρη: μια βάση δεδομένων, έναν επεξεργαστή και έναν επόπτη.

Η *βάση δεδομένων* περιλαμβάνει τις δομές δεδομένων που απαιτούνται για την απεικόνιση των δικτύων ρόλων, φορμών, ειδών πρόσβασης, των σχέσεων ρόλου - χρήστη, φόρμας - είδους πρόσβασης, τους επαγωγικούς κανόνες καθώς και ένα σύνολο κανόνων ελέγχου πρόσβασης για κάθε ρόλο χρήστη (άμεσοι κανόνες πρόσβασης) το οποίο περιέχει εκείνους τους κανόνες που δεν μπορούν να προέλθουν μέσω των επαγωγικών κανόνων. Με τη χρήση των επαγωγικών κανόνων επιτυγχάνεται η παραμετρική παρουσίαση των κανόνων ελέγχου πρόσβασης.

Οι άμεσοι κανόνες πρόσβασης έχουν την ακόλουθη γενική μορφή:

< ρόλος-1, ρόλος-2, δικαίωμα, f >

όπου

ρόλος-1: ο ρόλος χρήστη που έχει το "δικαίωμα"

ρόλος-2: ο ρόλος χρήστη που μπορεί να αποκτήσει το "δικαίωμα"

f: η δυνατότητα του ρόλου-2 να μεταβιβάσει το "δικαίωμα" σε τρίτον.

Ο *επεξεργαστής* χωρίζεται σε δύο υπό-τμήματα. Το πρώτο χρησιμοποιείται για τη διαχείριση των δικτύων και των σχέσεων που αναφέρθηκαν παραπάνω και το δεύτερο για τη διαχείριση των άμεσων κανόνων πρόσβασης (π.χ. ενημέρωση, διαγραφή, εμφάνιση, καταχώρηση).

-

Επιπρόσθετα, ο επεξεργαστής περιέχει διαδικασίες ελέγχου σύγκρουσης και διπλοεγγραφής μεταξύ ενός νέου και των ήδη καταχωρημένων κανόνων. Στην περίπτωση της διπλοεγγραφής, το σύστημα απαγορεύει την καταχώρηση του νέου κανόνα. Στην περίπτωση σύγκρουσης κανόνων, το σύστημα θα πρέπει να απαντά με ένα προειδοποιητικό μήνυμα. Ο χρήστης έχει υποχρέωση να καταχωρήσει τον νέο κανόνα αφού πρώτα διαγράψει τον παλαιό ή να σταματήσει την καταχώρηση του νέου κανόνα. Η διαγραφή ενός καταχωρημένου κανόνα θα πρέπει να γίνεται με μεγάλη προσοχή καθώς επιφέρει μια σειρά επιπλέον διαγραφών που αφορούν τους κανόνες εκείνους που σχετίζονται αποκλειστικά με τον αρχικά διαγραφέντα κανόνα, με σκοπό την αποφυγή ασυνέπειας τους.

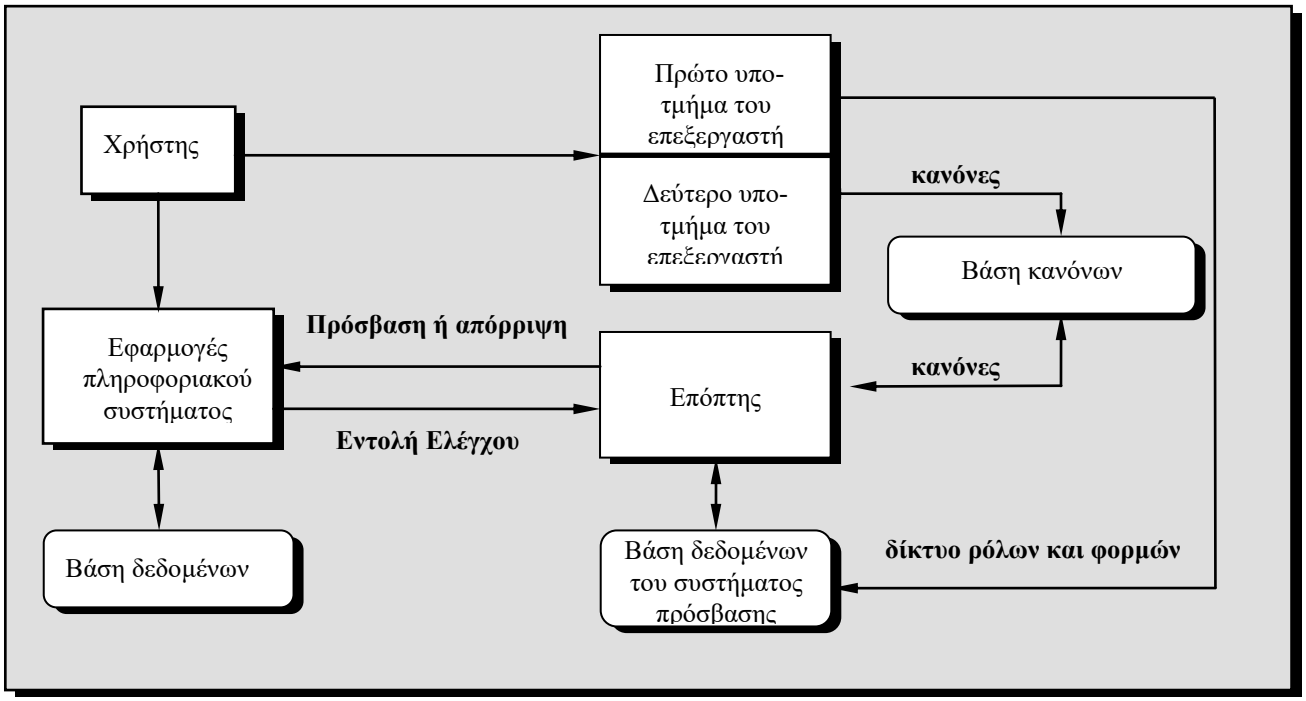
Το τρίτο τμήμα του συστήματος ελέγχου πρόσβασης, *ο επόπτης*, είναι υπεύθυνο για την συλλογή και αποθήκευση των κανόνων ελέγχου πρόσβασης που αφορούν:

- τον αρχικό ρόλο κάθε χρήστη, σ' ένα προσωρινό αρχείο, κατά την είσοδο του στο σύστημα
- την δημιουργία νέων κανόνων πρόσβασης με την βοήθεια των αντίστοιχων δικτύων (ρόλων, φορμών κ.α.) και των επαγωγικών κανόνων και την αποθήκευση τους στο προσωρινό αρχείο,
- τον έλεγχο κάθε επιθυμητής πρόσβασης,
- την παροχή ή/και ανάκληση δικαιωμάτων από ή/και προς άλλους χρήστες, και
- την διαγραφή του προσωρινού αρχείου κατά την έξοδο του χρήστη από το σύστημα.

5.10 Η σύνδεση του συστήματος ελέγχου πρόσβασης με το ΠΣΝ

Η σύνδεση του συστήματος ελέγχου πρόσβασης με το πληροφοριακό σύστημα του νοσοκομείου, παρουσιάζεται στο σχήμα 5

-



Σχήμα 5. Σύνδεση του συστήματος ελέγχου πρόσβασης με το πληροφοριακό σύστημα του νοσοκομείου**.**

Κατά τη διάρκεια της εκτέλεσης του λογισμικού του πληροφοριακού συστήματος νοσοκομείου, ο έλεγχος πρόσβασης πραγματοποιείται με τη χρήση διαδικασιών Prolog οι οποίες αποβλέπουν στη συλλογή και στην αποθήκευση στην κύρια μνήμη των κανόνων πρόσβασης που σχετίζονται με τον χρήστη, στον έλεγχο της επιθυμητής πρόσβασης του χρήστη σε συνάρτηση με τους κανόνες αυτούς και στη διαγραφή των κανόνων από την κύρια μνήμη, εφόσον ο χρήστης αποχωρήσει από το σύστημα

Έτσι, έχουν χρησιμοποιηθεί ειδικές εντολές "καλέσματος" (call) στο λογισμικό ΠΣΝ για την εκτέλεση των διαδικασιών Prolog. Κάθε φορά που μια τέτοια διαδικασία εκτελείται και ολοκληρώνεται, η ροή της λειτουργίας επιστρέφει και πάλι στην εντολή του λογισμικού του συστήματος που ακολουθεί την εντολή "καλέσματος". Οι διαδικασίες Prolog περιλαμβάνουν ορίσματα εισόδου (input) και εξόδου (output).

-

Κατά την είσοδο του χρήστη στο σύστημα, ελέγχεται ο κωδικός του και εφόσον γίνει αποδεκτός, τότε πραγματοποιείται η συλλογή και η καταχώρηση σ' ένα προσωρινό αρχείο των κανόνων πρόσβασης που σχετίζονται με το μόνιμο ρόλο του χρήστη. Επίσης, συλλέγονται και καταγράφονται όλοι οι κανόνες πρόσβασης που αφορούν το χρήστη και είναι ρόλοι κατά εξουσιοδότηση.

Η διαδικασία Prolog που χρησιμοποιείται για το σκοπό αυτό είναι η ακόλουθη:

load-rules (user-id)

όπου:

user-id: ο κωδικός του χρήστη

Οταν το προσωρινό αρχείο που δημιουργείται δεν περιέχει τουλάχιστον έναν κανόνα τότε η λειτουργία του συστήματος διακόπτεται.

Στην περίπτωση μεταβίβασης δικαιώματος, το σύστημα ελέγχει εάν η μεταβίβαση επιτρέπεται, δηλαδή, εάν ο εξουσιοδότης μπορεί να παρέχει στον εξουσιοδοτούμενο το ρόλο, ελέγχοντας εάν υπάρχει αντίστοιχος κανόνας στο προσωρινό αρχείο του εξουσιοδότη. Εφόσον υπάρχει, το σύστημα χρησιμοποιεί τους επαγωγικούς κανόνες για να καταχωρήσει τους νέους κανόνες πρόσβασης στον εξουσιοδοτούμενο.

Η διαδικασία εξουσιοδότησης υλοποιείται μέσω της ακόλουθης διαδικασίας Prolog:

grant-role (user-id-1, user-id-2, role)

όπου:

user-id-1: ο κωδικός του εξουσιοδότη

user-id-2: ο κωδικός του εξουσιοδοτούμενου

role: ο ρόλος που ο εξουσιοδότης θέλει να παρέχει στον εξουσιοδοτούμενο

-

Οταν ο χρήστης επιθυμεί πρόσβαση σε κάποιο σύνολο δεδομένων μιας φόρμας, το σύστημα ελέγχει εάν ο αντίστοιχος κανόνας πρόσβασης υπάρχει στο προσωρινό αρχείο, ώστε να επιτρέψει ή να απαγορεύσει τη συγκεκριμένη πρόσβαση. Εάν η πρόσβαση επιτρέπεται, το σύστημα προσθέτει τα αντίστοιχα κατηγορήματα περιορισμού στην αντίστοιχη εντολή (με την βοήθεια της SQL) με σκοπό τον έλεγχο της πρόσβασης σε επίπεδο δεδομένων.

Η διαδικασία Prolog που ενεργοποιείται είναι:

check-access(user-id, r, o, p)

όπου:

user-id: ο κωδικός του χρήστη που επιθυμεί να έχει το δικαίωμα (r, o, p)

r: τα επιτρεπόμενα είδη πρόσβασης για το σύνολο των δεδομένων του αντικειμένου πρόσβασης ο

o: το σύνολο των δεδομένων του αντικειμένου πρόσβασης στο οποίο ορίζεται η πρόσβαση

p: τα κατηγορήματα περιορισμών που καθορίζουν τις νόμιμες εμφανίσεις του συνόλου των δεδομένων του αντικειμένου πρόσβασης

Κατά την πραγματοποίηση μιας ανάκλησης ρόλου, το σύστημα ελέγχει εάν η ανάκληση έχει ισχύ, δηλαδή εάν η εξουσιοδότηση αυτή έχει γίνει από το χρήστη και προκαλεί συνεχείς ανακλήσεις όσον αφορά τους ρόλους και τους αντίστοιχους κανόνες πρόσβασης που έχουν σχέση με τον εξουσιοδοτημένο ρόλο.

Η διαδικασία ανάκλησης υλοποιείται μέσω της ακόλουθης διαδικασίας Prolog:

revoke-role (user-id-1, user-id-2, role)

-

όπου:

user-id-1: ο κωδικός του εξουσιοδότη

user-id-2: ο κωδικός του εξουσιοδοτούμενου

role: ο ρόλος που ο εξουσιοδότης θέλει να ανακαλέσει από τον εξουσιοδοτούμενο

Οταν ο χρήστης επιθυμεί να διακόψει την πρόσβαση του στο σύστημα (log-out), τότε οι κανόνες που βρίσκονται στο προσωρινό αρχείο καταχωρούνται στο αντίστοιχο αρχείο του συστήματος διαχείρισης πρόσβασης και στη συνέχεια διαγράφεται το προσωρινό αρχείο.

Η διαδικασία Prolog που χρησιμοποιείται για το σκοπό αυτό είναι η ακόλουθη:

unload-rules (user-id)

όπου:

user-id: ο κωδικός του χρήστη

Η επιλογή της Prolog για την υλοποίηση του συστήματος ελέγχου πρόσβασης έγινε με σκοπό την ανάπτυξη και δημιουργία μιας πρώτης έκδοσης του συστήματος μέσα στον κύκλο επεξεργασία / δοκιμή / διόρθωση (compile /test/edit cycle). Επίσης, η χρήση της Prolog μας επέτρεψε την εύκολη και αποτελεσματική χρήση των επαγωγικών κανόνων. Ομως, ένα βασικό μειονέκτημα της Prolog είναι η υποχρεωτική αντιγραφή της βάσης δεδομένων του συστήματος στην κύρια μνήμη, με αποτέλεσμα να απαιτείται κάθε φορά μεγάλη ποσότητα μνήμης [Far89, Bra89, Tak89]. Η αντιμετώπιση αυτού του προβλήματος μπορεί να γίνει με την επιλογή μιας εναλλακτικής στρατηγικής υλοποίησης, η οποία να βασίζεται σε άλλη κατάλληλη προσέγγιση (π.χ. γλώσσα C,C++) ή στη σύνδεση μεταξύ της Prolog και των συστημάτων διαχείρισης σχεσιακών βάσεων δεδομένων ή σε μια τεχνολογία ενεργής βάσης δεδομένων (active database) [Cer87, Far89,Moh94, Cha95].

-

5.11 Λειτουργία του συστήματος ελέγχου πρόσβασης

Η λειτουργία του συστήματος ελέγχου πρόσβασης μέσα σ' ένα πληροφοριακό σύστημα, που παρουσιάζεται στο σχήμα 6, πραγματοποιείται μέσα από την ακόλουθη αλγοριθμική διαδικασία :

Βήμα 1ï Πρόσβαση του χρήστη στο ΠΣΝ με τη βοήθεια του κωδικού του.

Βήμα 2ï Εάν ο κωδικός γίνει αποδεκτός τότε το σύστημα ελέγχου πρόσβασης συλλέγει όλους τους κανόνες που έχουν σχέση με το χρήστη και τους καταχωρεί σ' ένα προσωρινό αρχείο. Εάν ο κωδικός δεν γίνει αποδεκτός τότε πήγαινε στο βήμα 6. Εάν υπάρχει έστω και ένας κανόνας, δηλαδή το προσωρινό αρχείο δεν είναι κενό, τότε η διαδικασία συνεχίζεται στο επόμενο βήμα, αλλιώς, όταν δεν υπάρχει κανόνας που να σχετίζεται με τον χρήστη, πήγαινε στο βήμα 6.

Βήμα 3ï Εμφάνιση του βασικού μενού στο χρήστη. Εάν η επιλογή είναι 'Έξοδος' τότε πήγαινε στο βήμα 6. Σε οποιαδήποτε άλλη περίπτωση το σύστημα ελέγχου πρόσβασης εξετάζει εάν ο χρήστης έχει πρόσβαση στην επιλογή του.

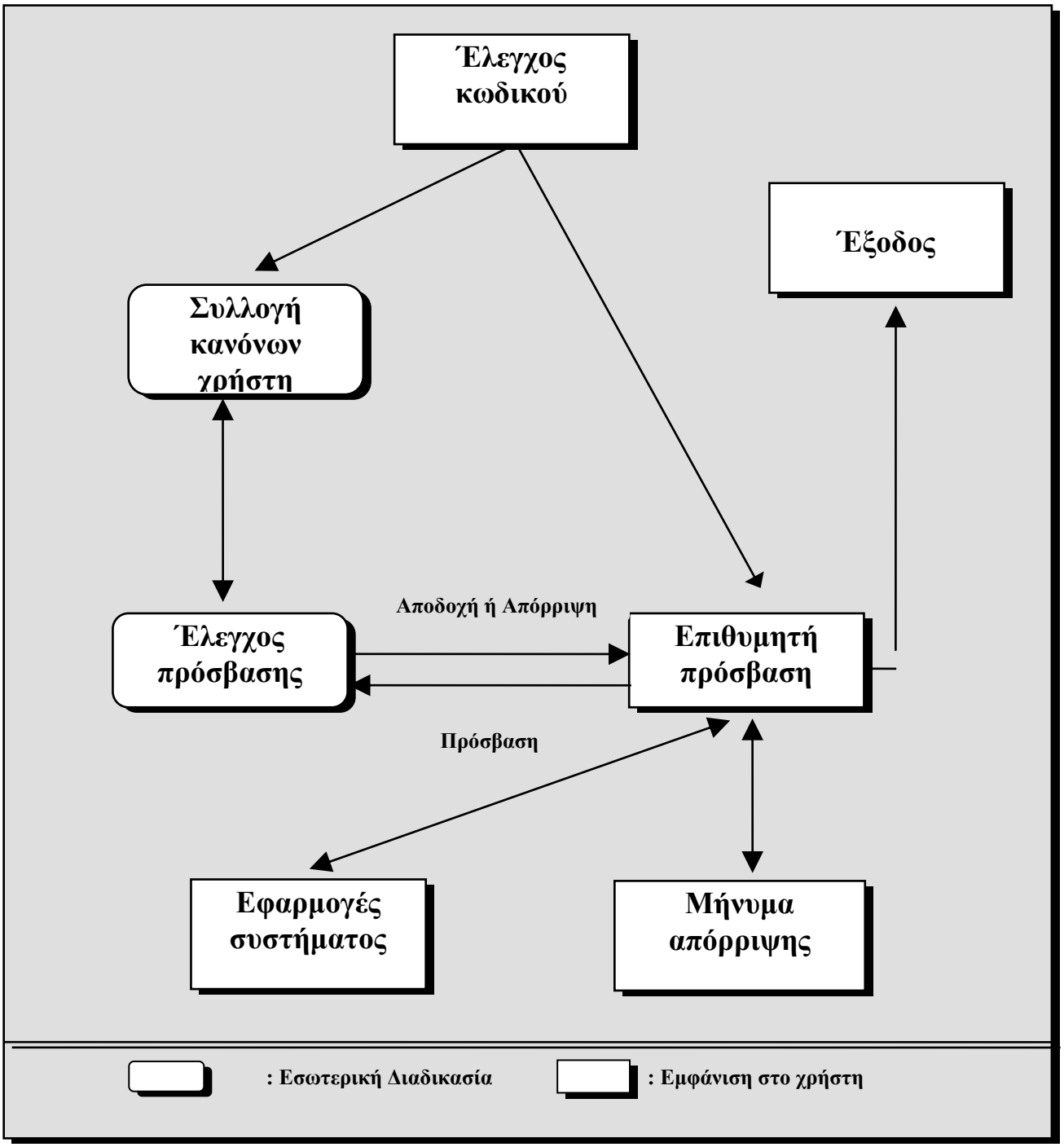
Βήμα 4ï Εάν η πρόσβαση επιτρέπεται τότε εμφανίζεται το αντίστοιχο μενού. Εάν είναι εφαρμογή τότε εμφανίζονται τα περιεχόμενα του. Εάν η πρόσβαση δεν επιτρέπεται τότε η διαδικασία επιστρέφει στο προηγούμενο μενού και στο βήμα 3.

Βήμα 5ï Επιλογή των επιθυμητών περιεχομένων. Οι κανόνες που είναι καταχωρημένοι στο προσωρινό αρχείο εξετάζουν εάν τα περιεχόμενα που ο χρήστης θέτει ικανοποιούν τις απαιτήσεις που υπάρχουν. Όταν ο χρήστης φύγει από τη φόρμα αυτή η διαδικασία επιστρέφει στο προηγούμενο μενού και στο βήμα 3.

-

Βήμα 6ï Επιλογή "Έξοδο" και το προσωρινό αρχείο διαγράφεται από τη μνήμη.

Βήμα 7ï Τέλος διαδικασίας.



Σχήμα 6. Λειτουργία του συστήματος πρόσβασης.

-

5.12 Διαχείριση του συστήματος ελέγχου πρόσβασης

Για την διαχείριση του συστήματος ελέγχου πρόσβασης θα είναι υπεύθυνο το γραφείο ασφάλειας του νοσοκομείου (hospital's security office) για τις ακόλουθες τρεις διαδικασίες:

- Καθορισμό και συντήρηση της βάσης του συστήματος ελέγχου πρόσβασης (δηλαδή καταχώρηση, διόρθωση και διαγραφή των κανόνων πρόσβασης καθώς και των αντίστοιχων δεδομένων),

- Έλεγχο ότι οι εφαρμογές του πληροφοριακού συστήματος και ο μηχανισμός ελέγχου πρόσβασης "επικοινωνούν" σωστά (δηλαδή οι εντολές "καλέσματος" έχουν ενσωματωθεί στα κατάλληλα σημεία), και

- Παροχή ασφάλειας στο σύστημα ελέγχου (δηλαδή κανείς άλλος χρήστης εκτός από τον υπεύθυνο του γραφείου δεν έχει πρόσβαση στους κανόνες και στα αντίστοιχα δεδομένα).

Η ορθή λειτουργία των δύο διαδικασιών επιβάλλει την άμεση συνεργασία του υπεύθυνου του γραφείου με τον υπεύθυνο ανάπτυξης των εφαρμογών του πληροφοριακού συστήματος, ώστε να διατηρείται η ισορροπία μεταξύ της απόδοσης του συστήματος, της ευκολίας των χρηστών και των περιορισμών ασφάλειας.

Η διαχείριση του ελέγχου πρόσβασης βασίζεται στην έννοια της **ιδιοκτησίας,** η οποία επιτρέπει στον κάτοχο ενός αντικειμένου την παροχή ή την ανάκληση του δικαιώματός του στο ή από το αντικείμενο αυτό σ' άλλους χρήστες και μπορεί να επεκταθεί, έτσι ώστε να επιτρέπει και τη μεταβίβαση της εξουσιοδότησης [Fug88, Woo80].

Στον προτεινόμενο μηχανισμό χρησιμοποιείται η εκτεταμένη προσέγγιση ιδιοκτησίας και ως μονάδα ιδιοκτησίας θεωρείται η εμφάνιση του συνόλου δεδομένων μιας φόρμας. Ο υπεύθυνος του γραφείου ασφάλειας καθορίζει τις συνθήκες που επιτρέπουν την μεταβίβαση του

δικαιώματος από έναν χρήστη σ' άλλον και έχει οριστεί ως εξουσιοδότης των κανόνων πρόσβασης που σχετίζονται με τους μόνιμους ρόλους ενός χρήστη.

Η προστασία του συστήματος ελέγχου πρόσβασης από μη εξουσιοδοτημένες ενέργειες (θελητά ή αθέλητα) αποτελεί επίσης σημαντική απαίτηση [Ste91]. Για το λόγο αυτό, η βάση έχει καταχωρηθεί σ’ ένα υπολογιστικό σύστημα και προστατεύεται με κρυπτογραφικούς μηχανισμούς αυθεντικοποίησης γνωστοί μόνο στο γραφείο ασφάλειας. Οι κανόνες ελέγχου πρόσβασης που μεταφέρονται στο σύστημα του κάθε χρήστη, όταν αυτός χρησιμοποιεί το πληροφοριακό σύστημα, προστατεύονται μέσω των μηχανισμών ασφάλειας του δικτύου.

5.13 Συμπεράσματα

Ένα σύστημα ασφάλειας, για να είναι ολοκληρωμένο και αποτελεσματικό, θα πρέπει να παρέχει προστασία στις πληροφορίες σε επίπεδο βάσης δεδομένων, πληροφοριακού συστήματος, λειτουργικού συστήματος και δικτύου, ενώ συγχρόνως θα πρέπει να λαμβάνεται υπόψη και η φυσική ασφάλεια.

Η ανάπτυξη και η υλοποίηση ενός συστήματος ασφάλειας απαιτεί τον καθορισμό των απαιτήσεων που προκύπτουν μέσα στο περιβάλλον. Η ανάλυση των απαιτήσεων αυτών οδηγεί στην εύρεση ενός πλαισίου το οποίο περιλαμβάνει την πολιτική ασφάλειας, τις στρατηγικές, το μοντέλο (ή τα μοντέλα) ασφάλειας καθώς και τους μηχανισμούς υλοποίησής τους. Η διαδικασία ελέγχου πρόσβασης των χρηστών θεωρείται από τις πιο βασικές διαδικασίες, που ένα σύστημα ασφάλειας θα πρέπει να παρέχει σε περιβάλλον βάσεων δεδομένων.

Διάφορα μοντέλα και μέθοδοι υλοποίησης έχουν προταθεί όσο αφορά τον έλεγχο πρόσβασης των χρηστών, ενώ οι ιδιαιτερότητες του κάθε περιβάλλοντος καθορίζουν σε μεγάλο βαθμό όχι μόνο τη δυνατότητα εφαρμογής τους, αλλά και την επιτυχή λειτουργία τους. Σ' ένα περιβάλλον νοσοκομείου οι ιδιαιτερότητες αυτές είναι πολλές και επειδή ο κύριος σκοπός είναι

η διασφάλιση της υγείας του ασθενή, ένα σύστημα ελέγχου προσβάσεων των χρηστών θα πρέπει να λειτουργεί σύμφωνα μ' αυτό.

Στο κεφάλαιο αυτό παρουσιάστηκε ένας μηχανισμός ελέγχου πρόσβασης χρηστών σε περιβάλλον βάσεων δεδομένων για ένα νοσοκομείο. Το σύστημα βασίζεται στο μοντέλο ασφάλειας ρόλου - χρήστη. Τα κύρια χαρακτηριστικά του συστήματος αυτού είναι:

1. Η δυνατότητα ενσωμάτωσης του συστήματος ελέγχου πρόσβασης σ' ένα ήδη υπάρχον πληροφοριακό σύστημα νοσοκομείου, χωρίς αυτό να απαιτεί μεγάλο προγραμματιστικό κόστος και σημαντικές παρεμβάσεις στο λογισμικό ή στο υλικό.

2. Ο έλεγχος πρόσβασης πραγματοποιείται στο επίπεδο εφαρμογών, ώστε οι κανόνες πρόσβασης να μπορούν να αλλάζουν δυναμικά, όταν αυτό απαιτείται από την πολιτική ασφάλειας του νοσοκομείου χωρίς να υπάρχει επίδραση στο υπόλοιπο σύστημα.

3. Η δυνατότητα παροχής ρόλων κατά εξουσιοδότηση (άμεσα ή έμμεσα) και η αυτόματη ανάκλησή τους όταν απαιτείται.

4. Στην περίπτωση ενσωμάτωσης σ' ένα πληροφοριακό σύστημα νοσοκομείου, το ίδιο το πληροφοριακό σύστημα του νοσοκομείου να μπορεί να λειτουργήσει σε διαφορετικά νοσοκομεία είτε αυτά έχουν την ίδια, είτε διαφορετική πολιτική ασφάλειας και απαιτήσεις.

Το προτεινόμενο μοντέλο ελέγχου πρόσβασης αντιστοιχεί στις απαιτήσεις ελέγχου πρόσβασης των χρηστών του Περιφερειακού Γενικού Νοσοκομείου Αθηνών "Γ. ΓΕΝΝΗΜΑΤΑΣ" και έχει υλοποιηθεί σε πειραματικό στάδιο με ενθαρρυντικά αποτελέσματα.

-

ΠΑΡΑΡΤΗΜΑ 1

ΥΛΟΠΟΙΗΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΠΡΩΤΟΚΟΛΛΩΝ

1. Εισαγωγή

Στο παράρτημα αυτό παρουσιάζονται ορισμένα κρυπτογραφικά πρωτόκολλα γνωστά ως παραλλαγές (variants) του πρωτοκόλλου των Diffie και Hellman (D-H) καθώς και διάφορες μορφές υλοποίησής τους. Πιο συγκεκριμένα, τα κρυπτογραφικά πρωτόκολλα που θα εξετασθούν είναι :

- των Diffie και Hellman [Dif76]
- του Yacobi [Yac91]
- των Matsumoto, Takashima και Imai [Mat86]
- Station to Station [Dif92,Dif93]
- των Alexandris, Burmester, Chrissikopoulos και Desmedt [Ale92,Ale93]

και αφορούν την επικοινωνία μεταξύ δύο χρηστών ενώ αποβλέπουν στον υπολογισμό ενός κοινού μυστικού κλειδιού, το οποίο μπορούν να χρησιμοποιήσουν ως κλειδί ενός συμμετρικού κρυπτογραφικού συστήματος για να κωδικοποιούν και αποκωδικοποιούν τα μηνύματα που ανταλλάσσουν μεταξύ τους.

-

2. Το Πρωτόκολλο των Diffie - Hellman

Το πρωτόκολλο των Diffie και Hellman [Dif76] δε θα παρουσιαστεί στο παράρτημα αυτό καθώς έχει γίνει εκτενή ανάλυση στο κεφάλαιο 1. Στην υλοποίηση που ακολουθεί, εξετάζεται η πρώτη έκδοση του πρωτοκόλλου των Diffie και Hellman όπου παρέχεται αυθεντικοποίηση των χρηστών. Η διαδικασία υλοποίησης της δεύτερης έκδοσης, όπου οι χρήστες χρησιμοποιούν τυχαίους αριθμούς, είναι παρόμοια με της πρώτης έκδοσης ενώ ο απαιτούμενος χρόνος της δεύτερης είναι διπλάσιος σε σχέση με της πρώτης έκδοσης και κατά συνέπεια δεν αναφέρεται στους πίνακες που ακολουθούν.

3. Παραλλαγές του πρωτοκόλλου των Diffie - Hellman

Σ' όλα τα κρυπτογραφικά πρωτόκολλα που θα περιγραφούν στη συνέχεια, κατά τη διαδικασία ένταξης ενός νέου χρήστη στο σύστημα ως εξουσιοδοτημένου χρήστη, επιλέγεται ένα μυστικό κλειδί *s*, όπου $1 < s < p-1$ και υπολογίζεται το δημόσιο κλειδί του *P*, που συνήθως είναι $P = a^S \bmod p$ σε συνεργασία με το κέντρο εμπιστοσύνης το οποίο είναι υπεύθυνο για την επιλογή των παραμέτρων α και *p*. Το δημόσιο κλειδί κάθε εξουσιοδοτημένου χρήστη του συστήματος είναι καταχωρημένο σ' ένα δημόσιο αρχείο-ευρετήριο μαζί με το ονοματεπώνυμό του, τη διεύθυνση του και άλλα χαρακτηριστικά και ονομάζεται συνήθως ευρετήριο δημοσίων κλειδιών (directory).

4. Το Πρωτόκολλο του Yacobi

Το πρωτόκολλο που έχει προταθεί από το Yacobi [Yac91] παρέχει αυθεντικοποίηση μεταξύ των δύο χρηστών. Σύμφωνα με το πρωτόκολλο αυτό το κέντρο εμπιστοσύνης είναι υπεύθυνο για το δημόσιο αρχείο - ευρετήριο και για την επιλογή των βασικών παραμέτρων α και

-

m, οι οποίες είναι δημόσια γνωστές. Η παράμετρος *m* είναι ένα *RSA modulus* (*m=p.q, p, q* πρώτοι αριθμοί) ενώ το *α* είναι ένα στοιχείο βάσης το οποίο παράγει ένα αρκετά μεγάλο δακτύλιο ακεραίων *modulo m*.

Εστω ότι οι χρήστες *A* και *B* με μυστικά κλειδιά s_A, s_B και δημόσια κλειδιά P_A, P_B αντίστοιχα, θέλουν να επικοινωνήσουν μεταξύ τους. Για τη δημιουργία ενός κοινού κλειδιού επικοινωνίας K θα πρέπει :

- Κάθε χρήστης *i* να επιλέξει έναν τυχαίο αριθμό R_i και στη συνέχεια να υπολογίζει τον αριθμό $X_i = a^{R_i} \bmod m$ τον οποίο να στέλνει στον άλλο χρήστη *j*.

- Κάθε χρήστης υπολογίζει το κλειδί επικοινωνίας σύμφωνα με τον ακόλουθο τύπο:

$$K_{ij} = P_j^{R_i}.X_j^{S_i} \bmod m = P_i^{R_j}.X_i^{S_j} \bmod m = a^{R_i S_j}.a^{R_j S_i} \bmod m = a^{R_i S_j + R_j S_i} \bmod m$$

Το πρωτόκολλο αυτό παρέχει τη δυνατότητα ανανέωσης του κλειδιού επικοινωνίας κάθε φορά που οι δύο χρήστες θέλουν να επικοινωνήσουν ενώ ο αριθμός των μηνυμάτων που ανταλλάσσουν είναι ο ελάχιστος (ένα).

Σύμφωνα με το Yacobi, ένας παθητικός αντίπαλος που γνωρίζει μόνο ότι είναι δημόσια γνωστό (α, m, P_A, P_B) καθώς και τα μηνύματα (X_A, X_B) που οι δύο χρήστες ανταλλάσσουν, δεν μπορεί να υπολογίσει το κοινό κλειδί επικοινωνίας. Επίσης, με την προϋπόθεση ότι δεν μπορεί να αποκτήσει καμιά πληροφορία τόσο για τα μυστικά κλειδιά των δύο χρηστών όσο και τους τυχαίους αριθμούς που επιλέγονται, ο υπολογισμός του κοινού μυστικού κλειδιού από έναν αντίπαλο χρήστη βασίζεται στην επίλυση του γνωστού προβλήματος των Diffie και Hellman. Στην περίπτωση που ο αντίπαλος έχει τη δυνατότητα να γνωρίζει ορισμένα προηγούμενα κοινά κλειδιά τότε, κατά την ανταλλαγή των μηνυμάτων μεταξύ των χρηστών *A* και *B*, μπορεί να επέμβει και να δημιουργήσει κοινά κλειδιά επικοινωνίας με κάθε χρήστη. Για να το πετύχει όμως αυτό θα πρέπει να γνωρίζει έναν πολυωνυμικού χρόνου αλγόριθμο ανακατασκευής

-

κλειδιών (η μέθοδος βασίζεται σε πρωτόκολλα μηδενικής γνώσης), του οποίου η μαθηματική απόδειξη περιγράφεται στο [Yac90]. Συνεπώς, το συγκεκριμένο πρωτόκολλο παρέχει ασφάλεια και στις δύο περιπτώσεις. Αντίθετη άποψη έχει εκφραστεί από τους Y. Desmedt και M. Burmester όπου έχουν αποδείξει ότι το συγκεκριμένο πρωτόκολλο δεν παρέχει ασφάλεια έναντι επίθεσης γνωστού κλειδιού [Des93]. Επίσης, ο M. Burmester έχει περιγράψει το σύστημα αυτό σε επίθεση γνωστού κλειδιού [Bur95b].

5. Το Πρωτόκολλο των Matsumoto, Takashima και Imai

Το κρυπτογραφικό πρωτόκολλο των Matsumoto, Takashima και Imai (MTI) [Mat86] δε θα παρουσιαστεί στο παράρτημα αυτό καθώς έχει γίνει εκτενή ανάλυση στο κεφάλαιο 1.

6. Το Πρωτόκολλο Station To Station

Το πρωτόκολλο Station to Station (STS) [Dif92, Dif93] είναι μία εξέλιξη του πρωτοκόλλου των Diffie και Hellman με τη χρήση των ηλεκτρονικών υπογραφών. Στο πρωτόκολλο υπάρχει ένα κέντρο ελέγχου (αντίστοιχο του κέντρου εμπιστοσύνης) το οποίο είναι υπεύθυνο για την επιλογή των βασικών παραμέτρων *α* και *p*. Το *α* είναι πρωτογενές στοιχείο του *GF(p)* και το *p* είναι ένας πρώτος αριθμός. Το πρωτόκολλο STS χωρίζεται σε τρεις φάσεις.

Στην πρώτη φάση, οι χρήστες *A* και *B* επιλέγουν από έναν τυχαίο αριθμό R_A και R_B αντίστοιχα και υπολογίζουν τα $a^{R_A} \bmod p$ και $a^{R_B} \bmod p$ τα οποία και ανταλλάσσουν μεταξύ τους. Στη συνέχεια ο κάθε χρήστης υπολογίζει το κοινό κλειδί που σύμφωνα με τον ακόλουθο τύπο:

$$K = \left(a^{R_B} \bmod p\right)^{R_A} = a^{R_B R_A} \bmod p = a^{R_A R_B} \bmod p = \left(a^{R_A} \bmod p\right)^{R_B}$$

-

Στη δεύτερη φάση, κάθε χρήστης με τη βοήθεια των ηλεκτρονικών υπογραφών υπογράφει τα δύο μηνύματα που έχουν ανταλλάξει με το μυστικό κλειδί του. Στη συνέχεια, με την χρήση ενός συμμετρικού αλγορίθμου και κλειδί το κοινό μυστικό κλειδί, κωδικοποιεί τα υπογεγραμμένα μηνύματα.

Στην τρίτη φάση, κάθε χρήστης για να επιβεβαιώσει ότι ο άλλος χρήστης έχει το ίδιο κοινό κλειδί και είναι πράγματι ο χρήστης αυτός, αποκωδικοποιεί το μήνυμα που έλαβε στη δεύτερη φάση χρησιμοποιώντας το κοινό κλειδί (για το συμμετρικό αλγόριθμο) και το δημόσιο κλειδί του άλλου χρήστη (για την ηλεκτρονική υπογραφή). Το αποτέλεσμα των δύο αποκωδικοποιήσεων πρέπει να είναι τα δύο μηνύματα που οι χρήστες αντάλλαξαν στην πρώτη φάση.

Το STS πρωτόκολλο έχει τα ακόλουθα πλεονεκτήματα :[Dif92, Dif93]

- Η ασφάλειά του βασίζεται στο πρόβλημα των Diffie και Hellman (πρόβλημα διακριτού λογάριθμου) και στην ασφάλεια της ηλεκτρονικής υπογραφής.

- Δε χρησιμοποιεί χρονικά όρια (timestamps) τα οποία έχουν βασικά μειονεκτήματα.

- Η διαδικασία της αυθεντικοποίησης ολοκληρώνεται όταν οι δύο χρήστες επιβεβαιώσουν ότι έχουν δημιουργήσει το ίδιο κοινό κλειδί επικοινωνίας που χρησιμοποιείται μέσα στη διαδικασία.

- Οι χρήστες έχουν τη δυνατότητα να δημιουργούν μόνοι τους τα μυστικά κλειδιά με αποτέλεσμα το πρωτόκολλο να παρέχει μεγαλύτερη ασφάλεια.

- Δεν περιέχει περιττά δεδομένα καθώς η χρήση της συμμετρικής κωδικοποίησης των ηλεκτρονικών υπογραφών, η ψηφιακή υπογράμμιση όλων των τιμών και ο μη διαχωρισμός της διαδικασίας αυθεντικοποίησης από αυτήν της δημιουργίας του κοινού κλειδιού επικοινωνίας αποτελούν απαραίτητα και αναγκαία συστατικά που θα πρέπει να υπάρχουν στο πρωτόκολλο ώστε να διατηρείται η ασφάλεια του.

-

7. Το Πρωτόκολλο των Alexandris, Burmester, Chrissikopoulos και Desmedt

Το κρυπτογραφικό πρωτόκολλο που έχει προταθεί από τους N. Alexandris, M. Burmester, V. Chrissikopoulos και Y. Desmedt (ABCD) επεκτείνει το πρωτόκολλο των Diffie και Hellman σε σύστημα αυθεντικοποίησης [Ale92, Ale93]. Το ABCD πρωτόκολλο έχει πολλά κοινά σημεία με τα κρυπτογραφικά πρωτόκολλα MTI [Mat86] και του Yacobi [Yac90].

Στο πρωτόκολλο αυτό, το Κέντρο Εμπιστοσύνης ονομάζεται Κέντρο Αυθεντικοποίησης Κλειδιού -KAK (Key Authentication Centre - KAC) το οποίο επιλέγει στην πρώτη φάση της διαδικασίας τις βασικές παραμέτρους, έναν πολύ μεγάλο πρώτο αριθμό p και ένα πρωταρχικό στοιχείο α του Zp, με τα οποία κάθε χρήστης δημιουργεί το δημόσιο κλειδί του P, $P = a^{-S} \bmod p$, όπου S το μυστικό του κλειδί το οποίο έχει επιλέξει μόνος του. Στη συνέχεια ο χρήστης ενημερώνει το KAK για το δημόσιο κλειδί του το οποίο καταχωρείται στο δημόσιο αρχείο - ευρετήριο.

Για τη δημιουργία ενός κοινού κλειδιού επικοινωνίας οι δύο χρήστες επιλέγουν από ένα τυχαίο αριθμό $R\ \left(R_A, R_B \in Z_{p-1}\right)$ και υπολογίζουν τους αριθμούς $X_A = R_A + S_A \bmod(p-1)$ και $X_B = R_B + S_B (\bmod\, p-1)$ τους οποίους ανταλλάσσουν. Το κοινό κλειδί επικοινωνίας είναι το:

$$K_{AB} = \left(P_B . a^{X_B}\right)^{R_A} = a^{R_B R_A} = a^{R_A R_B} = \left(P_A . a^{X_B}\right)^{R_B} = K_{BA}$$

Τα βασικά χαρακτηριστικά του πρωτοκόλλου ABCD είναι τα ακόλουθα :

- Οι βασικές αρμοδιότητες *του Κέντρου Αυθεντικοποίησης Κλειδιών KAK* είναι η επιλογή των βασικών παραμέτρων και η διαχείριση του ευρετηρίου των εξουσιοδοτημένων χρηστών. Η

-

επικοινωνία με τους χρήστες πραγματοποιείται για την ανάκληση των δικαιωμάτων κάποιου χρήστη οποιαδήποτε στιγμή θεωρείται απαραίτητο.

- *Διαφορετικά κλειδιά επικοινωνίας για κάθε επικοινωνία (freshness).*

- *Μικρή υπολογιστική πολυπλοκότητα, ελαχιστοποίηση των βημάτων που απαιτούνται και ασφάλεια αποδεδειγμένη* [Dif92].

- Η διαδικασία της αυθεντικοποίησης των δύο χρηστών ολοκληρώνεται με τη δημιουργία του κλειδιού επικοινωνίας (key distribution system).

- *Χρήση της τεχνικής κλίσης - απόκρισης (challenge - response)* για την αντιμετώπιση του προβλήματος της επανάληψης των μηνυμάτων.

Η ασφάλεια του πρωτοκόλλου ABCD έναντι παθητικών επιθέσεων είναι μαθηματικά αποδεδειγμένη και ανάγεται στη δυσκολία επίλυσης του προβλήματος των Diffie και Hellman. Το πρωτόκολλο όμως δεν προσφέρει ασφάλεια έναντι επίθεσης γνωστού κλειδιού. Επομένως, εάν πρόκειται να χρησιμοποιηθεί το πρωτόκολλο αυτό, τα κλειδιά αυτά πρέπει να φυλάσσονται σε ασφαλή θέση. Μια μέθοδος επίλυσης του προβλήματος αυτού είναι η καταχώρηση του μυστικού κλειδιού, του κοινού κλειδιού και των αλγορίθμων σε μία tamper proof συσκευή. Με τον τρόπο αυτό κανένας δεν μπορεί να αποκαλύψει το κοινό κλειδί K_{AB} (ούτε ακόμα και οι ίδιοι οι χρήστες). Σε σύγκριση με τα πρωτόκολλα που περιγράφηκαν στις προηγούμενες ενότητες, το πρωτόκολλο ABCD έχει χαμηλή υπολογιστικότητα (δύο εκθετικές πράξεις και έναν πολλαπλασιασμό).

Η ενίσχυση της ασφάλειας του πρωτοκόλλου ABCD επιτυγχάνεται με μια βελτιωμένη έκδοσή του, στην οποία αντιμετωπίζεται η περίπτωση όπου ο αντίπαλος μπορεί να έχει μη περιορισμένο αριθμό πληροφοριών από προηγούμενες επικοινωνίες. Για τη δημιουργία του κοινού κλειδιού επικοινωνίας οι δύο χρήστες επιλέγουν από ένα τυχαίο αριθμό

-

$R\left(R_A, R_B \in Z_{p-1}\right)$ και υπολογίζουν τα $X_A = a^{R_A} \bmod p$ και $X_B = a^{R_B} \bmod p$ τα οποία ανταλλάσσουν. Το κοινό κλειδί επικοινωνίας είναι το :

$$K_{AB} = \left(P_B^{R_A} . X_B^{S_A}\right) \bmod p = \left(a^{S_B}\right)^{R_A} . \left(a^{R_B}\right)^{S_A} \bmod p = a^{R_A S_B + R_B S_A} \bmod p = \left(a^{S_A}\right)^{R_B} \left(a^{R_A}\right)^{S_B} \bmod p = \left(P_A^{R_B} . X_A^{S_B}\right) \bmod p = K_{BA}$$

Το μειονέκτημα της μορφής αυτής, σε αντίθεση με την αρχική του μορφή, είναι η χρησιμοποίηση της εκθετικής πράξης αντί του πολλαπλασιασμού στη δημιουργία του μηνύματος το οποίο οι χρήστες ανταλλάσσουν, αυξάνοντας τον υπολογιστικό χρόνο και την πολυπλοκότητα.

Το πρωτόκολλο ABCD ικανοποιεί τις γενικές αρχές που πρέπει να διέπουν ένα ασφαλές πρωτόκολλο αυθεντικοποίησης σύμφωνα με τους W. Diffie, P. Van Oorschot και M. Wiener [Dif92]. Από όλα τα πρωτόκολλα που αναφέραμε συμπεραίνεται ότι η ενίσχυση της ασφάλειας συνεπάγεται την αύξηση του απαιτούμενου υπολογιστικού χρόνου.

8. Περιγραφή αλγορίθμων

Στην ενότητα αυτή περιγράφονται διάφοροι αλγόριθμοι υλοποίησης των πρωτοκόλλων που παρουσιάστηκαν στις προηγούμενες ενότητες. Οι αριθμοί που αναφέρονται στα πρωτόκολλα εκφράζονται ως συμβολοσειρές μήκους 180 και 360 χαρακτήρων (512 και 1024 bits αντίστοιχα), ενώ η γλώσσα προγραμματισμού που χρησιμοποιήθηκε είναι η ANSI C. Τα αποτελέσματα των προγραμμάτων έχουν μετρηθεί σε μικρο-υπολογιστή 286 (12 MHz) , 386DX (40 MHz) και 486 (66 MHz) με μαθηματικό επεξεργαστή.

-

Πίνακας 1. Απαιτούμενοι χρόνοι υπολογισμού του $x \bmod y$

x	**y**	**286**	**386 DX**	**486** **(μαθηματ. επεξεργ)**
800	500	00:01:10:25	00:00:20:98	00:00:05:98
800	400	00:01:33:64	00:00:27:96	00:00:07:69
800	200	00:02:17:97	00:00:40:98	00:00:11:21
600	300	00:00:52:79	00:00:15:60	00:00:04:56
600	150	00:01:17:77	00:00:23:01	00:00:06:43
500	250	00:00:36:69	00:00:10:87	00:00:03:24
400	200	00:00:23:56	00:00:07:03	00:00:01:87
300	150	00:00:13:35	00:00:04:01	00:00:01:04
200	100	00:00:06:04	00:00:01:81	00:00:00:49

Ο υπολογισμός του ισουπόλοιπου *(x mod y),* όπου το πλήθος των χαρακτήρων του *x* είναι ανεξάρτητο από το αντίστοιχο του *y*, γίνεται με τον αλγόριθμο[2] Ι. Ο αλγόριθμος αυτός έχει τη δυνατότητα να υπολογίζει συγχρόνως και το πηλίκο, όταν αυτό θεωρείται αναγκαίο. Στον Πίνακα 1 παρουσιάζονται οι αντίστοιχες μετρήσεις.

Ενας αντίστοιχος αλγόριθμος υπολογισμού του ισουπόλοιπου που περιγράφεται από τον Comba [Com90] είναι ταχύτερος από τον αλγόριθμο Ι, αλλά αφορά μόνο την περίπτωση όπου το πλήθος των χαρακτήρων του *x* είναι διπλάσιο από το αντίστοιχο πλήθος του *y*. Η χρησιμοποίηση μιας διαδικασίας υπολογισμού του ισουπόλοιπου, όταν το μήκος του *x* δεν είναι διπλάσιο από το μήκος του *y*, από τον αλγόριθμο του Comba επιτρέπει τη συνύπαρξη των δύο αλγορίθμων.

[2] Ο αλγόριθμος Ι όπως και οι αλγόριθμοι ΙΙ και ΙΙΙ που θα χρησιμοποιηθούν στην συνέχεια, παρουσιάζονται αναλυτικά στο τέλος του παραρτήματος.

-

Πίνακας 2. Απαιτούμενοι χρόνοι υπολογισμού του $x \bmod y$

x	y	Comba	Αλγόριθμος I (Παρ. Α)
362	181	00:00:05:00	00:00:06:00
724	362	00:00:18:00	00:00:23:00

Στον Πίνακα 2 παρουσιάζονται οι απαιτούμενοι χρόνοι υπολογισμού του $x \bmod y$ για τους δύο αλγορίθμους σε 386 DX μικροϋπολογιστή. Ο αλγόριθμος I εξαρτάται από τους χαρακτήρες των δύο αριθμών χωρίς όμως ο απαιτούμενος χρόνος να ξεπερνά τους χρόνους που αναφέρονται στο Πίνακα 2. Αντίθετα, ο αλγόριθμος του Comba απαιτεί σταθερό πλήθος επαναλήψεων το οποίο ισούται με το πλήθος των χαρακτήρων του *y*. Κάθε επανάληψη περιλαμβάνει έναν υπολογισμό ισουπόλοιπου, όπου το πλήθος των χαρακτήρων των αριθμών διαφέρει κατά ένα. Στην περίπτωση που πρέπει να υπολογίζεται το πηλίκο (είναι σημαντικό για τον υπολογισμό του $x^{-1} \bmod y$), ο χρόνος σχεδόν διπλασιάζεται αλλά δεν χρησιμοποιείται συχνά (το πολύ δύο φορές) χωρίς να επηρεάζει σε μεγάλο βαθμό τον συνολικό απαιτούμενο χρόνο.

Ο αλγόριθμος II για την επίλυση του $x^{-1} \bmod y$ βασίζεται στον τύπο :
$x^{-1} \bmod y = x^{\varphi(y)-1} \bmod y = x^{(y-1)-1} \bmod y = x^{y-2} \bmod y$ όταν ο *y* είναι πρώτος αριθμός [Seb89]. Ο αλγόριθμος αυτός ολοκληρώνεται σε πέντε το πολύ βήματα και απαιτεί μόνο τέσσερις υπολογισμούς σε σχέση με τους άλλους αλγόριθμους που ο απαιτούμενος αριθμός επαναλήψεων είναι μεγαλύτερος [Seb89].

Η εύρεση της τιμής του $x^t \bmod y$, όταν τα *x, t* είναι πολύ μεγάλοι αριθμοί βασίζεται στον υπολογισμό της τιμής του x^t σε όσο το δυνατόν λιγότερα βήματα [Kro79]. Η μέθοδος που χρησιμοποιείται, βασίζεται στην ανάλυση του *t* σε άθροισμα των δυνάμεων του

-

$2\left(2^0,2^1,2^2,2^3,\ldots\right)$, δηλαδή $t=2^{n_1}+2^{n_2}+\ldots+2^{n_i}, n_i=0,1,2,\ldots$. Ο υπολογισμός του n_i βασίζεται στον τύπο: $n_i=n_{i-1}+n_{i-1}$, ενώ για το t ισχύουν οι ακόλουθες δύο περιπτώσεις : (i) το t να ισούται με μία από τις δυνάμεις του 2 και (ii) το t να βρίσκεται ανάμεσα σε δύο δυνάμεις $\left(n_i<t<n_{i+1}\right)$. Στη δεύτερη περίπτωση για να υπολογιστεί το t θα πρέπει, γνωρίζοντας όλες τις προηγούμενες δυνάμεις $\left(n^k, k=0,1,2,\ldots,n_i\right)$, να αναλυθεί το $t-n_i$ σε άθροισμα των δυνάμεων αυτών. Ο τρόπος αυτός είναι αρκετά γρήγορος καθώς η εύρεση των δυνάμεων του 2 δεν αποτελεί χρονοβόρα διαδικασία.

Ο υπολογισμός του $x^t \bmod y$, όταν τα x και y παραμένουν σταθερά (αλλάζουν σε ειδικές περιπτώσεις), εξαρτάται από τις δυνατές τιμές $x^n \bmod y$ οι οποίες μπορούν να υπολογιστούν στην αρχή της όλης διαδικασίας μειώνοντας έτσι τον συνολικό απαιτούμενο χρόνο. Εάν ο ίδιος υπολογισμός επαναλαμβάνεται πολλές φορές με διαφορετικό t τότε όλες οι δυνατές τιμές $x^n \bmod y$ μπορούν να καταχωρηθούν σε ένα δημόσιο αρχείο, ώστε κάθε χρήστης να αναζητεί την τιμή που τον ενδιαφέρει. Στην περίπτωση αυτή ο συνολικός χρόνος και η πολυπλοκότητα μειώνονται, ενώ η ασφάλεια δεν επηρεάζεται καθώς η τιμή του t δεν μπορεί να προβλεφθεί, εάν είναι γνωστές οι τιμές των $x \bmod y$, $x^2 \bmod y$, $x^4 \bmod y$, ..., $x^{n-1} \bmod y$, $x^n \bmod y$. Καθώς στο αρχείο καταχωρούνται όλες οι δυνάμεις μέχρι το n να είναι μεγαλύτερο ή ίσο με το t ,το μόνο που αποκαλύπτεται είναι ότι το $t \in [n-1, n]$. Επομένως, ο αντίπαλος μπορεί να πληροφορηθεί τις δύο οριακές δυνάμεις *n-1* και *n* αλλά δεν μπορεί να αποκτήσει το t καθώς το διάστημα είναι πολύ μεγάλο. Για παράδειγμα, εάν το t είναι ένας είκοσι χαρακτήρων-ψηφίων αριθμός, τότε τα *n-1* και *n* έχουν τις τιμές που παρουσιάζονται στον Πίνακα 3.

Πίνακας 3.

n-1	**n**
009223372036854775808	018446744073709551616
018446744073709551616	036893488147419103232
036893488147419103232	073786976294838206464

-

Στην περίπτωση που δεν θέλουμε ο αντίπαλος να γνωρίζει το κλειστό διάστημα στο όποιο ανήκει το *t,* μπορεί κάθε φορά να υπολογίζεται μέχρι την μέγιστη δυνατή δύναμη που καθορίζεται από το πλήθος των χαρακτήρων του *t*. Εάν το *t* είναι δέκα χαρακτήρων αριθμός, τότε η μέγιστη δύναμη είναι *9999999999*. Το μέγεθος του αρχείου καταχώρησης των αποτελεσμάτων είναι σχετικό μικρό (π.χ. 80Ê) και εξαρτάται από το πλήθος και το είδος των δεδομένων που καταχωρούνται. Τέλος, η παραπάνω διαδικασία μπορεί να χρησιμοποιηθεί όταν το *x* δεν είναι σταθερό, αλλά ο χρήστης θα πρέπει να δημιουργεί προσωρινά το αρχείο καταχώρηση το οποίο να διαγράφει στο τέλος της διαδικασίας.

9. Υλοποίηση

Οπως έχει αναφερθεί και στο κεφάλαιο 2, ο απαιτούμενος συνολικός χρόνος είναι αποτελεί μια από τις βασικές παραμέτρους αποδοχής, τόσο για τα κρυπτογραφικά πρωτόκολλα, όσο και για τα συστήματα ασφαλείας. Στην ενότητα αυτή παρουσιάζονται διάφορες μορφές υλοποίησης των πρωτοκόλλων με τη βοήθεια των αλγορίθμων της προηγούμενης ενότητας. Οι απαιτούμενοι χρόνοι αναφέρονται στις δύο διαδοχικές διαδικασίες υλοποίησης των κρυπτογραφικών πρωτοκόλλων, της προετοιμασίας και της επικοινωνίας δύο χρηστών.

- Η **διαδικασία προετοιμασίας** αφορά κάθε δραστηριότητα του χρήστη ώστε να μπορεί να επικοινωνήσει μελλοντικά. Η διαδικασία αυτή πραγματοποιείται μόνο μία φορά, στο τέλος της διαδικασίας ένταξης του χρήστη στο σύστημα. Ο συνολικός χρόνος που απαιτείται δεν επηρεάζει τις πιθανές μελλοντικές επικοινωνίες του χρήστη με άλλους χρήστες. Φυσικά, δεν πρέπει να ξεπερνά κάποιο χρονικό διάστημα. Ο καθορισμός του χρονικού αυτού ορίου καθορίζεται κυρίως από τις ιδιαιτερότητες του χώρου, όπου εφαρμόζεται το πρωτόκολλο. Η μοναδική περίπτωση επανάληψης της διαδικασίας είναι όταν οι τιμές των βασικών παραμέτρων του συστήματος αλλάζουν για την εξασφάλιση μεγαλύτερης παροχής ασφάλειας.

-

- Η **διαδικασία επικοινωνίας** αφορά κάθε δραστηριότητα ενός χρήστη *A* από τη στιγμή που έχει αποφασίσει να επικοινωνήσει με ένα χρήστη *B*. Η διαδικασία αυτή είναι πιο σημαντική από την προηγούμενη καθώς ο απαιτούμενος συνολικός χρόνος είναι αυτός που οι δύο χρήστες χρειάζονται για να επικοινωνήσουν.

Η πιο απλή μορφή υλοποίησης είναι η εκτέλεση κάθε βήματος του πρωτοκόλλου ξεχωριστά, χωρίς να γίνεται καμία απαραίτητη προετοιμασία για τα επόμενα βήματα, με τη βοήθεια του αλγορίθμου Ι. Συνεπώς, στη διαδικασία προετοιμασίας δημιουργείται ένα αρχείο που περιλαμβάνει μόνο τα δεδομένα εκείνα που είναι απαραίτητα για τον υπολογισμό του δημοσίου κλειδιού του χρήστη. Για παράδειγμα, στο πρωτόκολλο ABCD το αρχείο περιλαμβάνει μόνο δυνάμεις που σχετίζονται με τον υπολογισμό του $a^{-s} \bmod p$.

Πίνακας 4. Επιδόσεις απλής μορφής υλοποίησης για 512 bits

ΠΡΩΤΟΚΟΛΛΟ	**ΔΙΑΔΙΚΑΣΙΑ ΠΡΟΕΤΟΙΜΑΣΙΑΣ**	**ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ**
Diffie - Hellman (D-H)	00:13:00.00	00:12:18.00
Randomized D-H 1ï	00:13:00.00	00:24:36.05
Randomized D-H 2o	00:13:00.00	00:12:18.05
Yacobi	00:13:00.00	00:28:19.00
ABCD	00:13:31.00	00:24:36.10
ABCD (N.V.)[3]	00:13:00.00	00:28:19.00
MTI	00:13:00.00	00:25:15.00

-

Πίνακας 5. Επιδόσεις απλής μορφής υλοποίησης για 1024 bits

ΠΡΩΤΟΚΟΛΛΟ	**ΔΙΑΔΙΚΑΣΙΑ ΠΡΟΕΤΟΙΜΑΣΙΑΣ**	**ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ**
Diffie - Hellman (D-H)	00:51:05.00	00:48:46.00
Randomized D-H 1ï	00:51:05.00	01:37:32.22
Randomized D-H 2o	00:51:05.00	00:48:46.22
Yacobi	00:51:05.00	01:52:01.00
ABCD	00:53:17.00	01:37:32.44
ABCD (N.V.)	00:51:05.00	01:52:01.00
MTI	00:51:05.00	01:39:44.32

Οι επιδόσεις της μορφής αυτής παρουσιάζονται στους Πίνακες 4 και 5 και έχουν μετρηθεί σε ένα 386 - DX (40), ενώ τα μήκη των αριθμών που χρησιμοποιήθηκαν είναι 180 (512 bits) και 360 (1024 bits) αντίστοιχα, εκτός από τους τυχαίους αριθμούς που το πλήθος των ψηφίων τους είναι 20. Η διαφορά του Randomized D-H 1ï και Randomized D-H 2ï είναι ότι στο πρώτο η διαδικασία δημιουργίας του κοινού κλειδιού επικοινωνίας επαναλαμβάνεται κάθε φορά στη διαδικασία επικοινωνίας. Στην περίπτωση όμως που οι χρήστες επικοινωνούν για πρώτη φορά (δηλ. δεν έχουν προηγούμενο κλειδί επικοινωνίας), ο χρόνος στο Randomized D-H 2ï είναι ο ίδιος με τον χρόνο στο Randomized D-H 1ï. Οσον αφορά τον χρόνο της διαδικασίας προετοιμασία είναι ίδιος για όλα τα πρωτόκολλα εκτός του πρωτοκόλλου ABCD επειδή είναι το μόνο που έχει αρνητική δύναμη στη δημιουργία του δημοσίου κλειδιού του χρήστη. Η διαφορά αυτή, ισχύει και στις επόμενες μορφές υλοποίησης που παρουσιάζονται στη συνέχεια.

Η δεύτερη μορφή υλοποίησης αφορά το πρωτόκολλο ABCD καθώς οι δυνάμεις που χρησιμοποιούνται είναι θετικές και αρνητικές αντίθετα με τα υπόλοιπα πρωτόκολλα που είναι όλες θετικές. Συνεπώς, εάν το αρχείο δεν περιέχει μόνο τις δυνάμεις υπολογισμού του δημοσίου κλειδιού, αλλά τόσο τις θετικές όσο και τις αρνητικές δυνάμεις που χρησιμοποιούνται στα επόμενα βήματα της διαδικασίας επικοινωνίας (και μπορούν να υπολογιστούν), τότε ο

[3] Το ABCD (N.V.) είναι η βελτιωμένη έκδοση του κρυπτογραφικού πρωτοκόλλου ABCD που περιγράφεται στην

-

συνολικός χρόνος επικοινωνίας θα μειωθεί. Στην περίπτωση των 512 bits ο αναμενόμενος χρόνος για τη διαδικασία επικοινωνίας μειώνεται στα 00:15:53:10 (μειώνεται κατά 00:08:43:00), ενώ ο χρόνος της διαδικασίας της προετοιμασίας αυξάνεται κατά 00:08:35:00 και φθάνει στα 00:22:06:00. Μία άλλη αύξηση είναι το μέγεθος του αρχείου το οποίο από 25.364 bytes γίνεται 38.012 bytes το οποίο όμως δεν επηρεάζει τον χρόνο προσπέλασής του. Αντίστοιχα για τα 1024 bits ο αναμενόμενος χρόνος για τη διαδικασία επικοινωνίας μειώνεται στα 01:02:43:44, ενώ ο χρόνος της διαδικασίας της προετοιμασίας αυξάνεται στα 01:29:05:00. Το μέγεθος του αρχείου, στην περίπτωση αυτή, είναι 75.752 bytes.

Στις παραπάνω μετρήσεις, τόσο στην περίπτωση των 512 bits όσο και των 1024 bits, δεν έγινε χρήση του αλγορίθμου που ορίζεται από τον Comba. Η τρίτη μορφή υλοποίησης είναι όμοια με την πρώτη, με μόνη διαφορά ότι γίνεται χρήση του αλγορίθμου που ορίζεται από τον Comba και παρουσιάζεται στον πίνακα 6. Η μείωση των χρόνων, που παρατηρείται, οφείλεται στο ότι η διαδικασία Comba είναι πιο γρήγορη (Πίνακας 2).

Πίνακας 6. Επιδόσεις με τη χρήση του αλγόριθμου Comba για 512 bits

ΠΡΩΤΟΚΟΛΛΟ	**ΔΙΑΔΙΚΑΣΙΑ ΠΡΟΕΤΟΙΜΑΣΙΑΣ**	**ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ**
Diffie - Hellman (D-H)	00:11:16.69	00:08:25.00
Randomized D-H 1ï	00:11:16.69	00:16:50.11
Randomized D-H 2o	00:11:16.69	00:08:25.11
Yacobi	00:11:16.69	00:19:22.00
ABCD	00:11:58.00	00:16:50:22
ABCD (N.V.)	00:11:16.69	00:19:22.00
MTI	00:11:16.69	00:17:37.31

Η τέταρτη μορφή υλοποίησης είναι όμοια με τη δεύτερη με μόνη διαφορά ότι χρησιμοποιείται ο αλγόριθμος που ορίζεται από τον Comba. Ο απαιτούμενος χρόνος της

ενότητα 7

διαδικασίας επικοινωνίας μειώνεται στα 00:10:51:22, ενώ ο απαιτούμενος χρόνος για την διαδικασία προετοιμασίας αυξάνεται στα 00:18:04:00. Μία άλλη αλλαγή που μειώνει το χρόνο στην διαδικασία επικοινωνίας, αλλά αυξάνει το χρόνο στην διαδικασία προετοιμασίας, είναι όταν στο αρχείο καταχωρούνται περισσότερες δυνάμεις του 2. :2^0,2^1,2^4,2^6,2^8,2^{12},2^{16},... (Αλγόριθμος ΙΙΙ) και αποτελεί την πέμπτη μορφή υλοποίησης. Η μείωση του συνολικού χρόνου οφείλεται στη μείωση του πλήθους των επαναλήψεων που απαιτούνται για τον υπολογισμό του $x^t \bmod y$ (προηγούμενη ενότητα). Η ασφάλεια δεν επηρεάζεται ενώ τα πιθανά διαστήματα μέσα στα οποία ο αντίπαλος μπορεί να αναζητήσει το *t* είναι περισσότερα αλλά με μικρότερο εύρος. Οπως και στον πίνακα 3, όταν το *x* είναι ένας αριθμός είκοσι χαρακτήρων τότε τα *n-1* και *n* έχουν τις τιμές που παρουσιάζονται στον πίνακα 7.

Πίνακας 7. Οριακές τιμές των *n-1* και *n* όταν το *t* είναι είκοσι ψηφίων αριθμός.

n-1	n
009223372036854775808	013835058055282163712
013835058055282163712	018446744073709551616
018446744073709551616	027670116110564327424
027670116110564327424	036893488147419103232
036893488147419103232	055340232221128654848
055340232221128654848	073786976294838206464

Ενα άλλο πλεονέκτημα της πέμπτης μορφής υλοποίησης είναι ότι αυξάνει τις πιθανότητες ταύτισης του *t* με μία από τις δυνάμεις που είναι καταχωρημένες στο αρχείο. Στον Πίνακα 8 παρουσιάζονται οι επιδόσεις της πέμπτης μορφής υλοποίησης όταν τα μήκη των αριθμών είναι 180 (512 bits), το αρχείο περιλαμβάνει μόνο τις δυνάμεις που είναι απαραίτητες για τον υπολογισμό του δημοσίου κλειδιού και χρησιμοποιείται ο αλγόριθμος του Comba.

-

Πίνακας 8. Επιδόσεις της πέμπτης μορφής υλοποίησης με τη βοήθεια του αλγόριθμου Comba για 512 bits

ΠΡΩΤΟΚΟΛΛΟ	ΔΙΑΔΙΚΑΣΙΑ ΠΡΟΕΤΟΙΜΑΣΙΑΣ	ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ
Diffie - Hellman (D-H)	00:18:23.69	00:08:25.00
Randomized D-H 1ï	00:18:23.69	00:16:50.11
Randomized D-H 2o	00:18:23.69	00:08:25.11
Yacobi	00:18:23.69	00:19:22.00
ABCD	00:19:19:00	00:16:50.22
ABCD (N.V.)	00:18:23.69	00:19:22.00
MTI	00:18:23.69	00:17:37.31

Παρατηρούμε στον Πίνακα 8 ότι ο χρόνος της διαδικασίας επικοινωνίας έχει παραμείνει ο ίδιος σχετικά με τον Πίνακα 6, ενώ ο χρόνος της διαδικασίας προετοιμασίας έχει αυξηθεί. Αυτό συμβαίνει γιατί η αύξηση των πιθανών τιμών στο αρχείο δεν επηρεάζει τη διαδικασία επικοινωνίας, αλλά τη διαδικασία προετοιμασίας. Αντίθετα, όταν το αρχείο περιλαμβάνει και άλλες δυνάμεις εκτός από αυτές που απαιτούνται για τον υπολογισμό του δημοσίου κλειδιού του χρήστη (έκτη μορφή υλοποίησης), ο χρόνος της διαδικασίας επικοινωνίας μειώνεται περίπου κατά 6.0 min, από 00:16:50:22 σε 00:10:50:22 ενώ ο χρόνος της διαδικασίας προετοιμασίας αυξάνεται στα 00:32:12:00. Το μέγεθος του αρχείου στην περίπτωση αυτή είναι 77.701 bytes.

Στον Πίνακα 9 αναφέρονται οι απαιτούμενοι χρόνοι για τις διαδικασίες προετοιμασίας και επικοινωνίας με τη μέθοδο Comba, όταν το αρχείο περιλαμβάνει θετικές και αρνητικές δυνάμεις, οι αριθμοί είναι 512 bits και χρησιμοποιείται μικροϋπολογιστής 486 με μαθηματικό επεξεργαστή.

-

Πίνακας 9. Επιδόσεις της έκτης μορφής υλοποίησης σε 486 PC

ΠΡΩΤΟΚΟΛΛΟ	**ΔΙΑΔΙΚΑΣΙΑ ΠΡΟΕΤΟΙΜΑΣΙΑΣ**	**ΔΙΑΔΙΚΑΣΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ**
Diffie - Hellman (D-H)	00:05:59:00	00:01:54.00
Randomized D-H 1ï	00:05:59:00	00:03:48.05
Randomized D-H 2ο	00:05:59:00	00:01:54.05
Yacobi	00:05:59:00	00:04:45.00
ABCD	00:10:32:00	00:03:49.10
ABCD (N.V.)	00:05:59:00	00:04:45.00
MTI	00:05:59:00	00:04:00.00

Μία άλλη μορφή υλοποίησης, η έβδομη, η οποία είναι εύκολο να υλοποιηθεί, βασίζεται στην ακόλουθη σχέση: $x^t \bmod y = x^{t_1} \bmod y . x^{-t_2} \bmod y$ εάν $t = t_1 - t_2$. Μπορεί, όμως να εφαρμοστεί μόνο για το πρωτόκολλο ABCD και για αυτό το λόγο δεν παρουσιάζεται [Kro79].

Η επιλογή της μορφής υλοποίησης καθορίζεται κυρίως από τις ιδιαιτερότητες του χώρου εφαρμογής του πρωτοκόλλου. Για παράδειγμα, εάν ο υπεύθυνος του συστήματος δεν μπορεί να αντιγράφει το αρχείο σε κάθε νέο χρήστη και οι βασικοί παράμετροι του πρωτοκόλλου πρέπει να αλλάζουν συχνά για μεγαλύτερη ασφάλεια, τότε πρέπει να ληφθεί υπόψη ο απαιτούμενος χρόνος των διαδικασιών προετοιμασίας και επικοινωνίας. Εάν οι παράμετροι δεν αλλάζουν συχνά, ο χρόνος της διαδικασίας επικοινωνίας είναι σημαντικότερος από το χρόνο της διαδικασίας προετοιμασίας, ενώ, το μέγεθος του χώρου αποθήκευσης που ανήκει σε κάθε χρήστη καθορίζει την επιλογή αλγορίθμου που θα χρησιμοποιηθεί για την δημιουργία του αρχείου.

Τέλος ο τρόπος αναζήτησης των τιμών στα αρχεία είναι ο δυαδικός. Ο χρόνος που απαιτείται είναι *log2n* όπου *n* το πλήθος των δυνατών τιμών, ενώ σε κάθε επανάληψη το πλήθος των δυνατών τιμών μειώνεται στο μισό [Kro79].

-

10. Συμπεράσματα

Στο παράρτημα αυτό παρουσιάστηκαν ορισμένα κρυπτογραφικά πρωτόκολλα που χαρακτηρίζονται ως παραλλαγές του πρωτοκόλλου Diffie-Hellman. Κατά την παρουσίαση η έμφαση δόθηκε στην ασφάλεια κάθε πρωτοκόλλου και στις διάφορες μορφές υλοποίησής τους σε μικροϋπολογιστή.

Η υλοποίησή τους βασίζεται στη χρήση ενός αρχείου που περιέχει τις πιθανές τιμές που είναι απαραίτητες για τον υπολογισμό του κοινού κλειδιού επικοινωνίας. Το αρχείο δημιουργείται στη διαδικασία προετοιμασίας και τα δεδομένα του καθορίζονται από το πρωτόκολλο που χρησιμοποιείται. Οταν το πρωτόκολλο είναι το ABCD, τότε περιέχει όλες τις δυνατές τιμές των $x^t \bmod y$ και $x^{-t} \bmod y$, ενώ για οποιοδήποτε άλλο πρωτόκολλο περιέχει τις δυνατές τιμές του $x^t \bmod y$ που υπολογίζονται με τη βοήθεια του αλγόριθμου III ή της μεθόδου που παρουσιάζεται στην ενότητα 3. Ειδικότερα, όταν το κρυπτογραφικό πρωτόκολλο που χρησιμοποιείται είναι ένα από τα D-H, Randomized D-H, ABCD (N.V.), Yacobi ή MTI η δομή του αρχείου είναι:

πεδίο 1ϊ	**πεδίο 2ϊ**
δύναμη t	$x^t \bmod y$

ενώ στην περίπτωση του πρωτοκόλλου ABCD η δομή του αρχείου είναι

πεδίο 1ϊ	**πεδίο 2ϊ**	**πεδίο 3ϊ**
δύναμη t	$x^t \bmod y$	$x^{-t} \bmod y$

Η χρήση αρχείου δεν μειώνει την ασφάλεια του πρωτοκόλλου αντιθέτως μειώνει το συνολικό απαιτούμενο χρόνο. Επιπλέον όταν το σύστημα μπορεί να παρέχει την αντιγραφή του αρχείου αυτού σε κάθε νέο εξουσιοδοτημένο χρήστη χωρίς παρεμβάσεις, τότε κάθε χρήστης δεν χρειάζεται να το δημιουργήσει, αλλά ο υπεύθυνος του συστήματος μπορεί να το αντιγράφει στο

ευρετήριο του κάθε χρήστη μηδενίζοντας σχεδόν το χρόνο που απαιτείται για τη διαδικασία προετοιμασίας. Βασιζόμενοι σ' αυτό, μια πιθανή αύξηση του πλήθους των καταχωρημένων τιμών στο αρχείο μπορεί να μειώσει ακόμα περισσότερο το απαιτούμενο χρόνο στη διαδικασία της επικοινωνίας.

Επίσης παρουσιάστηκε ένας αλγόριθμος εύρεσης του $x^{-1} \bmod y$ (αλγόριθμος I) ο οποίος σε σταθερό πλήθος επαναλήψεων υπολογίζει το αποτέλεσμα σε σχέση με άλλους, που ο αριθμός των επαναλήψεων δεν είναι σταθερός.

-

Αλγόριθμος I

---

1. If α < p then α mod p = α , stop.
2. If α = p then α mod p = 0 , stop.
3. If α > p then { p1=p;
   while (p1 < α)
   p1 = p1 * 10 ;
   }
4. While { α = α - p1 ;
   If α < p then α mod p = α , stop.
   If α=p then α mod p = 0 , stop.
   If α > p then { while (p1 > p)
   p1 = p1 / 10 ;
   }
   }

Αλγόριθμος II

---

1. Εάν p είναι πρώτος αριθμός τότε $a^p \bmod p = a \bmod p$ για κάθε α
2. $a^p \bmod p = a^{p-2+2} \bmod p = \left(a^{p-2} \bmod p\right)\left(a^2 \bmod p\right) \bmod p$
3. Σύμφωνα με το [1] έχουμε $z_1 = a^p \bmod p = a \bmod p$
4. Εάν $z_2 = a^2 \bmod p$ και $z_3 = a^{p-2} \bmod p$ έχουμε σύμφωνα με την [2] $z_1 = z_2 * z_3 \bmod p$. Τα z_1 και z_2 μπορούν να υπολογιστούν.
5. Σύμφωνα με τον γνωστό τύπο του modulo έχουμε :

   $z_1 = z_2 * z_3$ ή $kp + z_1 = z_2 * z_3$ όπου k =0,1,2,3,4,... Η πρώτη μορφή ισχύει εάν $z_2 \bmod z_1 = 0$ δηλαδή το z_1 διαιρείται ακριβώς με το z_2

   Η δεύτερη μορφή ισχύει όταν δεν ισχύει η πρώτη. Πιο συγκεκριμένα έχουμε:

   $z_3 = \left(k * p + z_1\right) / z_2$. Εστω ότι $n = p + z_1 \bmod z_2$. Τότε η λύση θα βρεθεί εάν $k = n + 1$.

-

Αλγόριθμος III

---

1. counter = 1

2. power = 2^0 /* power = 1 * /

3. { if counter < 4 { power1 = power
power = power + power
}
if counter = 4 { power1 = power1 + power }
if counter > 4 { power1 = power1 + power1
power = power + power
}
counter = counter +1

} while power1 < max-power /* max-power = μέγιστη δυνατή τιμή */

-

ΒΙΒΛΙΟΓΡΑΦΙΑ

-

[Αλε89] Αλεξανδρής, Ν. και Χρυσικόπουλος, Β. (1989) *Θεωρία Πληροφοριών*, Εκδόσεις Α. Σταμούλης, Πειραιάς.

[Αλε95] Αλεξανδρής, Ν., Χρυσικόπουλος, Β. και Πεππές, Δ. (1995) Ασφάλεια Δικτύων Υπολογιστικών Συστημάτων, *Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά Θέματα,* ΕΠΥ, 61-78.

[Αλε95b] Αλεξανδρής, Ν., Burmester, Μ. και Χρυσικόπουλος, Β. (1995) Η Κρυπτολογία στην Ασφάλεια Πληροφοριών, *Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά Θέματα,* ΕΠΥ, 231-248.

[Βασ90] Βασιλακόπουλος, Γ. και Χρυσικόπουλος, Β. (1990) *Πληροφοριακά Συστήματα Διοίκησης-Ανάλυση και Σχεδιασμός,* Εκδόσεις Α. Σταμούλης, Πειραιάς.

[Βασ91] Βασιλακόπουλος, Γ. (1991) *Σχεδιασμός Βάσεων Δεδομένων και dBASE IV/SQL*, Εκδόσεις Α. Σταμούλης, Πειραιάς.

[Δου93] Δουκίδης, Γ., Φραγκοπούλου, Α. και Αναγνωστόπουλος, Ι. (1993) *EDI Η πληροφορική στις Σύγχρονες Επιχειρήσεις*, Εκδόσεις Α. Σταμούλης, Πειραιάς - Αθήνα.

[Μαρ95] Μαρούλης, Δ. Γρίτζαλης, Δ. και Κάτσικας, Σ. (1995) Ο ρόλος της Εμπιστης Τρίτης Οντότητας στην ασφάλεια δικτύων, *Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά Θέματα,* ΕΠΥ, 261-272.

[Μελ95] Μελετίου, Γ. (1995) Μαθηματική Κρυπτογραφία, Διοφαντική Πολυπλοκότητα και το Πρόβλημα του Διακριτού Λογάριθμου, *Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά Θέματα,* ΕΠΥ, 273-279.

[Παγ95] Πάγκαλος, Γ. (1995) Ασφάλεια των Συστημάτων Βάσεων Δεδομένων, *Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά Θέματα,* ΕΠΥ, 79-104.

[Παπ95] Παπανικολάου, Κ. (1995) Ασφάλεια πληροφοριών και συστημάτων πληροφορικής - Ενέργειες της Ευρωπαϊκής Επιτροπής κατά την περίοδο 1992-1994, *Ασφάλεια Πληροφοριών, Τεχνικά, Νομικά και Κοινωνικά Θέματα,* ΕΠΥ, 281-299.

[Στα69] Σταμάτης Ε. (1969) *Αι Μυστικαί Τηλεπικοινωνίαι των Αρχαίων Ελλήνων*, Εκδόσεις Κ. Νικολάου, Αθήνα.

[Adl77] Adleman, L., Manders,K.M. and Miller, G.M. (1977) On taking roots in finite fields, *Annual Symposium on Foundations of Computer Science,* **18**, 175-178.

-

[Ale92] Alexandris, N. , Burmester, M. and Chrissikopoulos V. (1992) An Efficient Public Key Distribution System. *IFIP 12th World Computer Congress*, North Holland, Madrid Spain, 532 - 539.

[Ale93] Alexandris, N., Burmester, M., Chrissikopoulos V. and Desmedt, Y. (1993) A Secure Key Distribution System. *Proc. 3rd Symposium on State and Progress of Research in Cryptology*, Rome, Italy, 30 -34.

[ANS81] ANSI X3.93, (1981) American National Standard for Data Encrytpion Algorithm (DEA). American National Standards Institute.

[Aue94] Aue, A. and Breu, M. (1994) Distributed Information Systems: An Advanced Methodology, *IEEE Transactions on Software Engineering*, **20** (8), 594-605.

[Bak84] Bakker, A. and Mol, J. (1984) Hospital Information Systems. *Effective health Care*, **1** (4), 215-221.

[Bak92] Bakker, R. (1992) Trends in Modern Hospital Information Systems. *Medinfo 92*, K.C. Lun et al. (eds), North-Holland (Elsevier), 182-187.

[Bar91] Barber, B., Jensen, O., Lamberts, H., Roger France, F., De Schouwer, P. and Zollner, H. (1991) The Six Safety First Principles of Health Information Systems: A programme of Implementation Part 1 Safety and Security, *Data protection and confidentiality in Health Informatics*, CEC DG XIII/F AIM (eds.), IOS Press, 296-314.

[Bar92] Barber, B. and Davey, J. (1992) The Use of the CCTA Risk Analysis and Management Methodology [CRAMM] in Health Information Systems. *Medinfo 92*, K.C. Lun et al. (eds.), North-Holland (Elsevier), 1589-1593.

[Bau90] Bauspiess, F. and Knobloch, H.J. (1990) How to Keep Authenticity Alive in a Computer Network. *Advances in Cryptology-Eurocrypt '89, Lecture Notes in Computer Science #434*, J.J. Quisquater and J. Vandewalle (eds.), Springer-Verlag, 36-46.

[Bel76] Bell, D. and LaPadula, L. (1976) Secure Computer System: Unified Exposition and Multics Interpretation. *Technical Report* MTR-2997. MITRE Copr. Bedford Mass.

[Bel94] Bellare, M. and Rogaway P. (1994) Entity authentication and key distribution, in *Advances in Cryptology - Crypto '93, Lecture Notes in Computer Science #773,* D.R. Stinson (ed.), Springer-Verlag, 232-249.

[Ben91] Bengio, S., Brassard, G., Desmedt, Y., Goutier, C. and Quisquater, J.J. (1991) Secure implementations of identification systems. *Journal of Cryptology*, **4**(2), 175-184.

[Ber70] Berlekamp, E.R. (1970) Factoring polynomials over large finite fields. *Mathematics of Computation*, **24**(11), 713-735.

[Ber94] Bertino, E. and Weigard, H. (1994) An approach to authorisation modelling in object-oriented database systems, *Data & Knowledge Engineering* , **12**, 1-29.

[Bet91] Beth, T. and Knobloch, H.J. (1991) Open network authentication without online server. *Proc. Symposium on Computer Security, CS 90,* Rome 1990, 160-165.

[Bir92] Bird, R., Gopal, I., Herzberg, A., Jansen, P., Kutten, S., Molva, R. and Yung, M. (1992) Systematic design of two-party authentication protocols, in *Advances in Cryptology - Crypto '91, Lecture Notes in Computer Science #576,* J. Feigenbaum, (ed.), Springer-Verlag, 44 -61.

[Bis88] Biskup, J. and Bruggemann, H. (1988) The Personal Model of Data: Towards a Privacy-Oriented Information System. *Computers & Security*, North-Holland (Elsevier), **7**

[Bis89] Biskup, J. and Bruggemann, H. (1989) The Personal Model of Data: Towards a Privacy-Oriented Information System (extended abstract). *Proc. of the 5th International Conference on Data Engineering (ICDE),* IEEE Computer Society, 348-355.

[Bis91] Biskup, J. (1991) Medical Database Security. *Data Protection and Confidentiality in Health Informatics CEC DG XIII/F AIM,* 214-230.

[Ble92] Bleich, L. and Slack, V. (1992) Design a Hospital Information System: A Comparison between Interfaced and Integrated Systems. *Medinfo 92,* K.C. Lun et al. (eds), North-Holland (Elsevier), 174-177.

[Blu84] Blum, M. and Micali, S. (1984) How to generate cryptographically strong sequences of pseudo-random bits, *Siam J. Comput.,* **13**, 850 - 864.

[Blu93] Blundo,C., De Santis,A., Herzberg, A., Kutten, S., Vaccaro, U. and Yung, M. (1993) Perfectly-secure key distribution for dynamic conferences. *Advances in Cryptology-Cypto '92, Lecture Notes in Computer Science #740,* E. Brickell (ed.), Springer-Verlag, 471-487.

[Bra86] Brassard, G. and Crepeau, C. (1986) Non Transitive Transfer of Confidence: A perfect Zero-Knowledge Interactive protocol for SAT and Beyond, *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, 188-195.

[Bra87] Brassard G., Modern Cryptology - A Tutorial, *Lecture Notes in Computer Science # 325,* G.Goos, and J.Hartmanis (eds), Springer-Verlag, 1987.

[Bra88] Brassard, G., Chaum, D. and Crepeau, C. (1988) Minimum Disclosure Proofs of Knowledge, *Journal of Computer and Systems Sciences,* **37** (2), 156-189.

[Bra89] Brayshaw, M., Bree, D., Burgwal, K., Hoevenaars, M., Papegaaij, B., Schreinemakers, J., Sirks, J. and Smit, A. (1989) Integrating Expert Systems and Relational Databases: Results of an Initial Case Study using a User/Task-oriented Design Framework, *Data and Knowledge Base Integration, Proceedings of the Knowledge Base Integration,* Keele, England, 4-5 October, 200-223.

[Bra89a] Brandt, J., Damgard, I., Landrock, P. and Pedersen, T. (1989) Zero-knowledge authentication scheme with secret key exchange. *Advances in Cryptology- Crypto '88, Lecture Notes in Computer Science #403,* S. Goldwasser (ed.), Springer-Verlag, 583-588.

[Bur94] Burmester, M (1994) On the Risk of Opening Distributed Keys. *Advances in Cryptology-Crypto '94, Lecture Notes in Computer Science #839,* E. Brickell (ed.), Springer-Verlag, 308-317.

[Bur94a] Burmester, M. (1994) Cryptoanalysis of the Chang-Wu-Chen key distribution system, *Advances in Cryptology-Eurocrypt'93, Lecture Notes in Computer Science #765,* T. Helleseth ed., Springer-Verlag, 440-442.

[Bur95] Burmester, M. and Desmedt, Y. (1995) A Secure and Efficient Conference Key Distribution System, *Advances in Cryptology-Eurocrypto '94,* A. DeSantis (ed.), Springer-Verlag, 275-286.

-

[Bur95a] Burmester, M., , Alexandris, N., Chrissikopoulos, V. and Peppes, D. (1995) Πρωτόκολλα συμφωνίας κλειδιού: Δύο αποτελεσματικά μοντέλα αποδεδειγμένης ασφάλειας, *5ϊ Πανελλήνιο Συνέδριο Πληροφορικής, Τόμος 1,* ΕΠΥ , 177 - 186.

[Bur95b] Burmester, M. Weaknesses of key distribution systems for which authentication is implicit. Submitted to Crypto '94.

[Bur96] Burmester, M., Alexandris, N., Chrissikopoulos, V. and Peppes, D. (1996) Efficient and provably secure key agreement, *Proc. IFIP/SEC 96, Information Systems Security, Facing the information society of the 21st century,* S.K. Katsikas, D. Gritzalis (eds.), Chapman and Hall, 227-236.

[Car92] Carroll, T. (1992) The costs and benefits of a Hospital Information System. *Medinfo 92,* K.C. Lun et al. (eds), North-Holland (Elsevier), 1216-1220.

[Cas95] Castano, S., Fugini, M., Martella, G. and Samarati, P. (1995) *Database Security*, ACM Press.

[Cer87] Ceri, S., Gottlob, G. and Wiederhold, G. (1987) Interfacing Relational Databases and Prolog Efficiently. *Expert Databases Systems*, L. Kerschberg (ed.), 207-223.

[Cha87] Chaum, D., Evertse, J.-H., van de Graaf, J. and Peralta, R. (1987) Demonstrating possession of a discrete logarithm without revealing it. *Advances in Cryptology-Crypto '86, Lecture Notes in Computer Science #263,* A. Odlyzko (ed.), Springer-Verlag, Berlin, 200-212.

[Cha87a] Chaum, D. (1987) Demonstrating That a Public Predicate can be satisfied without revealing any information about how. *Advances in Cryptology-Crypto '86, Lecture Notes in Computer Science #263, ,* A. Odlyzko (ed.), Springer-Verlag, Berlin, 159-199.

[Cha95] Chakravarthy, S. (1995) Architectures and monitoring techniques for active databases: An evaluation. *Data & Knowledge Engineering*, **16**, 1-26.

[Chr95] Chrissikopoulos, V. and Peppes, D. (1995) A Practical Conference Key Distribution System, *Information Security - the Next Decade*, *Proceeding IFIP/SEC'95, The 11th International Information Security Conference*, J.Eloff and S.Somls (eds.), 167-175.

[Com90] Comba, P. (1990) Exponentiation cryptosystems on the IBM PC, *IBM Systems Journal*, **29** (4), 526-538.

-

[Com93] Commission of the European Communities (1993) *Guidelines on a Medical Devices Vigilance System.*, Directorate-General, Industry, Brussels.

[Cop86] Coppersmith, D., Odlyzko, A. and Schroeppel, R. (1986) Discrete Logarithms in GF(p), *Algorithmica*, 1-15.

[Cop87] Coppersmith, D. (1987) Cryptography, *IBM Journal Res. Develop*., **31** (2), 244-248.

[Cou88] Coulouris, G. and Dollimore, J. (1988) *Distributed Systems Concepts and Design*, Addison-Wesley.

[Cou90] Council Directive 90/385/EEC. (1990) Official Journal of the European Communities L 189.

[Cou93] Council Directive 93/42/EEC. (1993) Official Journal of the European Communities L 169, **36**.

[Dat90] Date, C.J. (1990) *An Introduction to Database Systems*, 5th edn. Addison-Wesley.

[Den79] Denning, D.E. and Denning, P.J. (1979) Data Security, *ACM Surveys* , **11** (3).

[Den83] Denning, D.E. (1983) *Cryptography and Data Security*, Addison-Wesley.

[Dep77] Department of Commerce (1977), National Bureau of Standards, *Data Encryption Standard*, FIPS Publication **46**.

[Des88] Desmedt, Y., Goutier, C. and Bengio, S. (1988) Special uses and abuses of the Fiat-Shamir passport protocol. *Advances in Cryptology-Crypto '87, Lecture Notes in Computer Science #293,* C. Pomerance (ed.), Springer-Verlag, 21-39.

[Des93] Desmedt, Y. and Burmester, M. (1993) Towards practical proven secure authenticated key distribution, *Proceedings of the 1st ACM Conference on Computer and Communication Security*, Fairfax, Virginia, ACM Press, 228-231.

[Dif76] Diffie, W. and Hellman, M. (1976) New directions in cryptography, *IEEE Trans. Inform. Theory*, **IT-22**,644-654.

[Dif92] Diffie, W., Van Oorschot, P. and Wiener, M. (1992) Authentication and Authenticated Key Exchanges. *Designs, Codes and Cryptography*, **2**, 107-125.

[Dif93] Diffie, W. (1993) Objectives and Costs in Peer Entity Negotiation, *Proc. 3rd Symposium on State and Progress of Research in Cryptology,* Rome, Italy, 9-15.

[Dob79] Dobkin, D.A., Jones, A.J. and Lipton, R. (1979) Protection against user influence, *ACM Transactions on Database Systems* , **4** (1), 97-106.

-

[DoD85] DoD, Department of defence, Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, 1985.

[Dus92] Dusserre, L. and Allaert, A. (1992) Expert systems and medical liability, *Medinfo 92*, K.C. Lun et al. (eds.), North-Holland (Elsevier), 1576-1581.

[EEC91] EEC/DGXII, (1991) *Data Protection and Confidentiality in health informatics*, IOS press.

[Ehl89] Ehlers, C. (1989) Communication in a Hospital Information System-Improvement by ISDN, *Medinfo 89*, B. Barber et al. (eds.), North-Holland (Elsevier), 1085-1088.

[Eic92] Eichinger, S. and Pernul, G. (1992) Design Environment for a Hospital Information System: Meeting the Data Security Challenge. *Medinfo 92,* K.C.Lun et al (eds.), Elsevier Science Publishers B.V. (North-Holland), 1582-1588.

[ElG87] El-Gamal, S. and Ghoneim, M. (1987) A Specialised hospital information system. *Medical Informatics*, **12** (3), 203-215.

[EUR95] EUROMEDIES (EUROpean MEdical Device Information Exchange System) (1995) concerted action. Project number A2122. AIM Programme Intermediate report.

[Fag78] Fagin, R. (1978) On an Authorization Mechanism. *ACM Transactions on Database systems*, **3** (3), 310-319.

[Far89] Farris, C. and Singleton, P. (1989) Combining Prolog with an RDBMS for Applications in Software Configuration Management, *Data and Knowledge Base Integration, Proceedings of the Knowledge Base Integration*, Keele, England, 4-5 October, 169-180.

[Fia87] Fiat, A. and Shamir, A. (1987) How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology-Crypto '86, Lecture Notes in Computer Science, #263,*A. Odlyzko (ed.) Springer-Verlag, Berlin, 186-194.

[Fis92] Fischer, M. and Wright, R. (1992) Multiparty Secret Key Exchange Using a Random Deal of Cards, *Advances in Cryptology-Crypto '91, Lecture Notes in Computer Science #576*, J.Feigenbaum (ed), 141-155.

[Fok83] Fokkens, O. (1983) Patient privacy and Professional privacy, *Medinfo 83, Seminars*, O.Fokkens et al. (eds.), North-Holland, 67-70.

[Fug87] Fugini, M. and Martella, G. (1987) Conceptual Modeling of Authorization in database Systems. *The Journal of Systems and Software*, **7**, 3-13.

[Fug88] Fugini, M. (1988) Secure Database Development Methodologies. *Database Security: Status and prospects*, C.E. Landwehr (ed.), 103-129.

[Gas88] Gasser, M. (1988) *Building A Secure Computer System*, Van Nostrand Reinhold, New York.

[Ger89] Gerdin-Jelger, U. and Peterson, H, (1989) *Medinfo 89*, B. Barber et al. (eds.), North-Holland (Elsevier), 14-16.

[Gol84] Goldwasser, S. and Micali, S. (1984) Probabilistic encryption, *Journal of Computer and System Sciences*, **28**, 270-299.

[Gol85] Goldwasser,S., Micali, S. and Rackoff,C. (1985) The Knowledge Complexity of Interactive Proof Systems. *Proceedings of the 17th ACM Symposium on the Theory of Computing*, 291-304.

[Gol87] Goldreich,O., Micali, S. and Wigderson, A. (1987) How to prove all NP statements in Zero Knowledge and a Methodology of Cryptographic Protocol Design. *Advances in Cryptology-Crypto '86, Lecture Notes in Computer Science #263,* A. Odlyzko (ed.), Springer-Verlag, Berlin, 171-185.

[Gol88] Goldwasser, S., Micali, S. and Rivest, R. (1988) A digital signature scheme secure against adaptive chosen-message attacks, *Siam J. Comput.*, **17**, 281-308.

[Gon90] Gong, L. and Wheeler, D. (1990) A matrix key distribution scheme, *Journal of Cryptology*, **2**, 51-59.

[Gon93] Gong, L. (1993) Increased Availability and Security of an Authentication Service, *IEEE Journal on Selected Areas in Communications,* **11** (5), 657-662.

[Gon94] Gong, L. (1994) Efficient Network Authentication Protocols: Lower Bounds and Optimal Implementations, *SRI International SRI-CSL-94-15*, 1-33.

[Gri76] Griffiths, P. and Wade, B. (1976) An Authorization Mechanism for a Relational Database System. *ACM Transactions on Database Systems,* **1** (3), 242-255.

[Gri91] Gritzalis, D. and Kastikas, S. (1991) Protection of personal information: aims, principles, technical issues, *Governmental and Municipal Information Systems, II* , R.Traunmuller (ed.), North-Holland (Elsevier), 73-81.

[Gri91b] Gritzalis, D., Kastikas, S., Keklikoglou, J. and Tomaras, A. (1991) Data security in medical information systems: technical aspects of a proposed legislation, *Medical Informatics*, **16** (4), 371-383.

[Gri91c] Gritzalis, D., Tomaras, A., Kastikas, S. and Keklikoglou, J., (1991) Data Security in Medical Information Systems: The Greek Case, *Computers & Security*, **10**, 141-159.

[Gri92] Gritzalis, D. and Kastikas, S. (1992) Data Confidentiality and User Access Rights in Medical Information Systems, *Medinfo 92*, K.C. Lun et al. (eds.), North-Holland (Elsevier), 1566-1571.

[Gri93] Gritzalis, D., Katsikas, S. and Pangalos, G. (1993) A methodology for the development of secure health information systems, *Proceedings of 11th International Congress of the European Federation for medical Informatics*, Reichert et al. (eds.), Jerusalem, Israel, 402-409.

[Gun90] Gunther, C.G. (1990) An identity-based key exchange protocol. *Advances in Cryptology-Eurocrypt '89, Lecture Notes in Computer Science #434*, J.J. Quisquater and J. Vandewalle (eds.), Springer-Verlag, 29-37.

[Hin88] Hinke, T. (1988) DBMS Technology vs. Threats, *Database Security: Status and Prospects* , C.E. Landwehr (ed.), 57-87.

[Hoe91] Hoevenaars, M. (1991) Integrating Expert Systems and Relational Databases. *Expert Systems Integration*, S.W.I.F.T. (ed.), 57-66.

[Ing82] Ingemarsson, I., Tang, D. and Wong, C. (1982) A Conference Key Distribution System, *IEEE Journal on Selected Areas in Communications*, **IT-28** (5), 714-719.

[ING91] INGRES/SQL Reference Manual for the UNIX and VMS Operating Systems, Release 6.4, December 1991.

[ISO89] ISO/IEC 7492-2 (1989) Information Technology - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

[ISO95] ISO/IEC CD11770-3 (1995) Draft Directory. Information Technology - Security Techniques - Key Management, Part 3: Mechanisms using asymmetric techniques. Key Agreement Mechanism 5.

[ITS91] Information Technology Evaluation Criteria (ITSEC), Ver. 1.2, EEC Document, Brussels, June 1991.

-

[ITS92] Information Technology Security Evaluation Manual (ITSEM). Draft Ver. 0.2, EEC Draft Document, April 1992.

[Jan91] Janson, P. and Molva, R. (1991) Security In Open Networks and Distributed Systems, *Computer Networks and ISDN Systems*, **22**,323-346.

[Kah76] Kahn,D. (1976) *The Codebreakers. The story of secret writing*, MacMillian Publishing Co, Inc., New York.

[Ker90] "*Guide to Kerberos*", *System and Network Management Vol. 4*, ULTRIX Ver 4.0, 1990.

[Kir89] Kirkpatrick, K. (1989) Modeling A LAN Security Server. *Lecture Notes in Computer Science # 396, Local Area Network Security*, T.A. Berson & T.Beth (eds), Springer-Verlag , 113 -137.

[Kno88] Knobloch, H.J. (1988) A Smart Card Implementation of the Fiat-Shamir Identification Scheme. *Advances in Cryptology - Eurocrypt 88,* 87-95.

[Koh91] Kohl, J. (1991) "The Evolution of the Kerberos Authentication Service", *EurOpen Conference Norway*.

[Kohl] Kohl, J. and Newmann, B.C., *The kerberos network authentication service*, MIT Project, Athena, Version 5.

[Kohl93] Kohl, J. (1993) The Kerberos Network Authentication Service (V5), *RFC 1510, Digital Equipment Corp. & C.Neuman ISI.*

[Koy88] Koyama, K. and Ohta, K. (1988) Identify Based Conference Key Distribution Systems, *Advances in Cryptology-Crypto '87, Lecture Notes in Computer Science # 293*, C.Pomerance (ed), 175-184.

[Kro79] Kronsjo, L. (1979) *Algorithms, their Complexity and Efficiency*. Second Edition, John Wiley & Sons, Inc.

[Lec90] Lecler, M. and Steinacker, M. (1990) Extending Kerberos' Functionality, *CS'90 Symposium on Computer Security*,Italy, 133-139.

[Lee83] Leenen, H. (1983) Legal Aspects of the Use of Information Systems in Health Care, *Medinfo 83 Seminars*, O.Fokkens et al. (eds.), North-Holland, 51-54.

[Lei94] Leighton, T. and Micali, S. (1994) Secret-key agreement without public-key cryptography, in *Advances in Cryptology - Crypto '93, Lecture Notes in Computer Science #773,* D. Stinson (ed.),Springer - Verlag, 456-479.

[Loc88] Lochovsky, F. and Woo, C. (1988) Role-Based Security in Database Management Systems. *Database Security: Status and prospects,* C.E. Landwehr (ed.), 209-222.

[Man88] Manola, F. (1988) A Personal view of DMBS Security, *Database Security : Status and Prospects*, C.E. Landwehr (ed.) , North-Holland (Elsevier), 23-34.

[Mat86] Matsumoto, T., Takashima, Y., and Imai, H. (1986) On seeking smart public key distribution systems, *The Transactions of the IECE of Japan,* **E69**, 99-106.

[Med90] *Medical Informatics Computer Applications in Health Care* (1990) E. Shortliffe et al (eds.), Addison-Wesley Publ.

[Men91] Menezes, A., Vanstone,S. and Okamoto, T. (1991) Reducing Elliptic Curve logarithms to logarithms in a finite field, In *Proceedings of the Twenty Third Annual ACM Symp. Theory of Computing,* STOC, 80-89.

[Mil92] Milian, J. and Munt, E. (1992) A Modern Fully Integrated Hospital Information System. *Medinfo 92,* K.C. Lun et al. (eds), North-Holland (Elsevier), 236-240.

[Mil93] Miller, D. (1993) Implementing Healthcare Information Security Programs, *Toward an Electronic Patient Record '93, Ninth Annual International Symposium on the Computerisation of Medical Records and North American Conference on Patient Cards,* San Antonio, Texas, 279-281.

[Moh94] Mohammed, I. and Dilts, D. (1994) Design for dynamic user-role-based security, *Computers & Security*, **13**, 661-671.

[Moi89] Moidu, K. and Wigertz, O. (1989) Computer Based Information Systems in Primary health Care-Why? *Journal of Medical Systems*, **13** (2), 59-65.

[Ned78] Needham, R. and Schroeder, M.D. (1978) Using encryption for authentication in large networks of computers", *Commun. ACM*, **21**, 993-999.

[Nist800] Public-Key Cryptography, Security Technology Group, National Institute of Standards and Technology, Special Publication 800-2, April 1991

[Not91] Notargiacomo, L. and Graubart, D. (1991) Health Delivery: The Problem Solved ?. *Database Security, IV : Status and Prospects*, S. Jajodia and C.E. Landwehr (eds.), 13-26.

[Odl84] Odlyzko, A. (1984) Discrete Logs in a Finite Field and their Cryptographic Significance, *Advances in Cryptology-Eurocrypt '84, Lecture Notes in Computer Science #209,* N.beth and I.Ingermarsson (eds), Springer-Verlag, 224-314.

[Oka89] Okamoto, E. and Tanaka, K. (1989) Key Distribution System Based on Identification Information,*IEEE Journal on Selected Areas in Communications,* SAC-**7**(4),481-485.

[Oko88] Okamoto, E. (1988) Key distribution systems based on identification information. *Advances in Cryptology-Crypto '87, Lecture Notes in Computer Science #293,* C. Pomerance (ed.), Springer-Verlag, 194-202.

[Oln93] Olnes, J. (1993) EDIFACT security made simple-the EDIMED approach, *Computers & Security,* **12**, 765-774.

[Pan93] Pangalos, G. (1993) Medical Database Security Evaluation. *Medical Informatics,* **18** (4), 283-292.

[Pan93b] Pangalos, G. (1993) Medical Database Security Policies. *Methods of Information in Medicine*, **32** (5), 349-356.

[Pan95] Pangalos, G., Gritzalis, D., Khair, M. and Bozios, L. (1995) Improving the security of medical database systems. *Proceedings of the IFIP TC11 International conference on information security, IFIP/Sec' 95, Cape Town,* 11-25.

[Par84] Parker, D.B. (1984) The many faces of data vulnerability, *IEEE Spectrum* , **21** (5).

[Per95] Pernul, G. (1995) Information Systems Security: Scope, State-of-the-art, and Evaluation of the Techniques. *Journal of Information Management,* **15** (3), 165-180.

[Pif91] Pfitzmann, A. and Pfitzmann, B. (1991) Security in Medical Networks. *Data protection and Confidentiality in health informatics, IOS press*, 231-248.

[Pra95] Pramataris, K., Giaglis, G., Papamichail, G., Doukidis, G. and Pallikarakis, N. (1995) The Potential of EDI in Health: The EUROMEDIES case, *Proceedings of Health Telematics 95* [To appear].

[Rab80] Rabin. M. (1980) Probabilistic Algorithms in Finite Fields. *SIAM Journal on Computing*, **9**(2), 273-280.

-

[Rab91] Rabitti, F., Bertino, E., Kim, W. and Woelk D. (1991) A Model of Authorization for Next-Generation Database Systems. *ACM Transactions on Database Systems,* **16** (1), 88-131.

[Riv78] Rivest, R.L., Shamir, A. and Adleman, L.(1978) A Method for obtaining Digital Signature and Public key Cryptosystems,*Communications of the ACM,***21**(2),120-126.

[Riv92] Rivest, R.L (1992) The MD5 Message-Digest Algorithm, *RFC 1321, MIT LCS & RSA Data Security, Inc.*

[Rob92] Robinson, M. (1992) A Legal Examination of Format, Signature and Confidentiality Aspects of Computerized health Information, *Medinfo 92,* K.C. Lun et al. (eds.), North-Holland (Elsevier), 1554-1560.

[Rog91] Roger France, F. (1991) The European Challenge in Health Information Systems, *Data protection and confidentiality in Health Informatics*, CEC DG XIII/F AIM (eds.), IOS Press, 65-70.

[Sak93] Sakurai,K. and Itoh,T. (1993) On the discrepancy between serial and parallel of zero-knowledge protocols, *Advances in Cryptology-Crypto '92, Lecture Notes in Computer Science #740,* E.F. Brickell (ed.), Springer-Verlag, 246-259.

[San93] Sanders, P. and Furnell, S. (1993) Data Security in Medical Information Systems using a generic model, *Proceedings of 11th International Congress of the European Federation for medical Informatics,* Reichert et al. (eds.), Jerusalem, Israel, 410-414.

[Sch91] Schnorr, C. (1991) Efficient Signature Generation by Smart Cards", *Journal of Cryptology,* **4**, 161-174.

[Sch94] Schneier, B. (1994) *Applied Cryptography, Protocols, Algorithms and Source Code in C*, John Wiley & Sons, Inc.

[Seb89] Seberry, J. and Pieprzyk, J. (1989) *Cryptography, An Introduction to Computer Security*, Advances in Computer Science Series, Richard P.Brent - Editor.

[Sha85] Shamir, A. (1985) Identity-based cryptosystems and Sifgnatures Schemes. *Advances in Cryptology-Crypto '84, Lecture Notes in Computer Science # 196,* Springer-Verlag, 46-53.

[Sha91] Sharrott, L. (1991) Centralized and Distributed Information Systems: Two Architecture Approaches for the 90s, *Healthcare Information Management Systems*, M.J.Ball et al. (eds.), Springer-Verlag, 306-315.

[Sim91] *Contemporary Cryptology, The Science of Information Integrity*, (1991) G.Simmons ed, IEEE PRESS.

[Ste91] Steinke, G. (1991) Design Aspects of Access Control in a Knowledge Base System. *Computers & Security*, **10**, 612-625.

[Sto88] Stonebraker, M., Hanson, E. and Potamianos, S. (1988) The POSTGRES Rule Manager. *IEEE Transactions on Software Engineering*, **14** (7), 897-907.

[Sto89] Stonebraker, M. (1989) Future Trends in Database Systems, *IEEE Transactions on Knowledge and Data Engineering*, **1** (1), 33-44.

[Sto92] Stonebraker, M. (1992) The Integration of Rule Systems and Database Systems. *IEEE Transactions on Knowledge and Data Engineering*, **4** (5), 415-423.

[Str94] Strous, L. (1994) Security Evaluation Criteria, *Computers and Security*, **13**, 379-384.

[SYB] SYBASE SQL Server Release 10.0

[Tak89] Takizawa, M. and Katsumata, M. (1989) Integration of Database Systems at the Navigational Level by using Prolog, *Data and Knowledge Base Integration, Proceedings of the Knowledge Base Integration*, Keele, England, 4-5 October, 181-199.

[Tak92] Takeda, H, Matsumura, Y., Kondo, H. and Inoue, M. (1992) Development of a totally integrated hospital information system: An intelligent hospital in Osaka university, *Medinfo 92*, K.C. Lun et al. (eds), North-Holland (Elsevier), 241-246.

[Tan94] Tang, P. (1994) Information Systems (Synopsis), *Yearbook of Medical Informatics 1994*, 215-217.

[Tin88] Ting, T. (1988) A User-Role Based Data Security Approach. *Database Security: status and prospects*, C.E. Landwehr (ed.), 187-208.

[Tin92] Ting, T., Demurjian, S. and Hu, M. (1992) Requirements, Capabilities and Functionalities of User-Role Based Security for an Object-Oriented Design Model, *Database Security, V : Status and Prospects*, C.E. Landwehr and S. Jajodia (eds.) , North-Holland (Elsevier), 275-296.

[Tre93] Treacher, A., Barber, B. and Osborne, D. (1993) Training for health information security: an approach to cultural change. *Healthcare computing*, 80-87.

[Tsu89] Tsujii, S. and Otoh, T. (1989) An ID Based Cryptosystem Based on the Discrete Logarithm Problem, *IEEE Journal on Selected Areas in Communications,* SAC-**7** (4), 467-473.

[Vas96] Vassilacopoulos, G., Chrissikopoulos, V. and Peppes, D. (1996) Security Enforcement in a European Medical Device Vigilance System Network, *Proc. IFIP/SEC 96, Information Systems Security, Facing the information society of the 21st century,* S.K. Katsikas, D. Gritzalis (eds.), Chapman and Hall, 377-386.

[Vas96a] Vassilacopoulos, G., and Peppes, D. (1996) A Front End Authorization Mechanism For Hospital Information Systems, *Medical Informatics,* Vol. 21 (**2)**, 93-103

[Wil91] Williamson, J. and Draper, J. (1991) EDI Security - Today and Tomorrow. *Information Security,* D. Lindsay and W. Price (eds.), IFIP, 361-374.

[Wil97] Wilson, S., Johnson, D. and Menezes, A. (1997) Key Agreement Protocols and their Security Analysis, *6th IMA International Conference on Cryptography and Coding*, Cirencester England, 17-19 Dec. (To appear)

[Woo80] Wood, C., Fernandez, E.B. and Summers, R.C. (1980) Data Base Security: Requirements, Policies and Models. *IBM Systems Journal,* **19** (2).

[Yac90] Yacobi, Y. and Shmuely,Z. (1990). On key distribution systems. *Advances in Cryptology-Crypto '89, Lecture Notes in Computer Science #435,* G. Brassard (ed.), Springer-Verlag, Berlin 344-355.

[Yac91] Yacobi, Y. (1991) A Key Distribution Paradox", *Lecture Notes in Computer Science #537, Advances in Cryptology-Crypto '90,* A.Menezes and S.Vanstone (eds), Springer - Verlag, 268-273.

[Yah93] Yahalom, R. Klein B. and Beth, T. (1993) Trust Based Navigation in Distributed Systems, *European Institute for System Security,* Karlsruhe University, Report 93/4.

[Yao82] Yao, A. (1982) Theory and applications of trapdoor functions, in *23th Annual Symp. on Foundations of Computer Science (FOCS),* IEEE Computer Society Press, 80-91.