

Κρυπτογράφηση: Το Α και το Ω της δικτυακής ασφάλειας

Σε νομικό και κοινωνικό επίπεδο, τίθεται ζήτημα προστασίας του απορρήτου σε όλες τις εκδοχές δικτυακής συναλλαγής (email, εμπορικές συναλλαγές, τραπεζικό και ιατρικό απόρρητο) και γενικότερα ζήτημα [προστασίας προσωπικών δεδομένων](#) του κάθε χρήστη του Internet.

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

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

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

Παρελθόν και μέλλον

Το παρελθόν: Ο αλγόριθμος του Καίσαρα

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

[Πίνακας αντιστοίχισης γραμμάτων](#)

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη secret, θα προκύψει το κρυπτογράφημα wignix. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται τρεις θέσεις αριστερά στο αλφάβητο. Δεν αρκεί να γνωρίζει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει λοιπόν το κλειδί, που σε αυτή την περίπτωση είναι ο αριθμός 3

Κρυπτογράφηση: Το A και το Ω της δικτυακής ασφάλειας

Το μέλλον: Κβαντική κρυπτογράφηση

Οι σημερινές τεχνολογίες κρυπτογράφησης, παρότι παρέχουν μεγάλο ποσοστό ασφάλειας, έχει αποδειχθεί ότι δεν είναι άτρωτες. Η απάντηση στο πρόβλημα είναι η χρήση της κβαντικής Φυσικής, όπως υποστηρίζει ο Νικολά Ζισίν, πρωτοπόρος της συγκεκριμένης τεχνολογίας στο Πανεπιστήμιο της Γενεύης. Εν συντομία, το σκεπτικό έχει ως εξής: οποιαδήποτε προσπάθεια παρατήρησης ενός κβαντικού συστήματος αυτόματα προκαλεί την "αλλοίωσή" του. Κατ' αυτό τον τρόπο, ακόμη και η παραμικρή προσπάθεια υποκλοπής γίνεται αμέσως αντιληπτή. Η κβαντική κρυπτογράφηση βρίσκεται εδώ και μια δεκαετία στο στάδιο των εργαστηριακών δοκιμών, αλλά σύντομα αναμένεται να εφαρμοστεί και εμπορικά.

Γιατί πρέπει να χρησιμοποιείται

Δεν είναι λίγοι αυτοί που πιστεύουν ότι η χρήση κρυπτογραφικών εργαλείων αφορά μόνο... κατασκόπους ή μανιώδεις χρήστες υπολογιστών. Στην πραγματικότητα, όταν κάποιος αποστέλλει ένα προσωπικό e-mail ή ανταλλάσσει εμπιστευτικές εμπορικές πληροφορίες για ένα έργο μέσω του ηλεκτρονικού ταχυδρομείου, οφείλει να γνωρίζει ότι, εάν δεν έχει κρυπτογραφηθεί, είναι σαν να το στέλνει με καρτ-ποστάλ: μπορεί να το διαβάσει σχεδόν οποιοσδήποτε.

Ένα e-mail, εκτός από τον αποστολέα και τον παραλήπτη, μπορεί να διαβαστεί εύκολα και από τους εργαζόμενους στον ISP (εταιρία παροχής Internet) του αποστολέα, τους εργαζόμενους στον ISP του παραλήπτη, από οποιονδήποτε ελέγχει τους routers από τους οποίους θα περάσουν τα "πακέτα" του μηνύματος και από οποιονδήποτε έχει πρόσβαση στον εξοπλισμό τηλεφωνίας στην τηλεφωνική εταιρία. Αν το μήνυμα αποστέλλεται ή παραλαμβάνεται από κινητό τηλέφωνο με σύνδεση στο Διαδίκτυο, τότε μπορεί να υποκλαπεί από άτομα με ειδικές συσκευές υποκλοπής συνομιλιών και μηνυμάτων κινητής τηλεφωνίας. Επιπλέον, είναι πολύ απλό να πλαστογραφηθεί η διεύθυνση αποστολής, ακόμα και με ένα τυπικό πρόγραμμα e-mail. Με λίγο περισσότερη δουλειά, κάποιος επιτήδειος μπορεί να αποκρύψει και άλλα σημάδια που δείχνουν από πού πραγματικά προέρχεται ένα μήνυμα.

Λύση στα παραπάνω προβλήματα δίνουν οι τεχνολογίες κρυπτογράφησης. Οι τεχνολογίες αυτές εξασφαλίζουν ότι το μήνυμα θα μπορεί να το διαβάσει μόνο ο παραλήπτης του, καθώς στα ενδιάμεσα στάδια το μήνυμα εμφανίζεται με ακατάληπτους χαρακτήρες, είναι δηλαδή μη αναγνώσιμο. Εκτός από την κρυπτογράφηση, μια άλλη τεχνολογία που παρέχει τέτοιου είδους ασφάλεια είναι η ηλεκτρονική υπογραφή, τομέας με τον οποίο έχουμε ήδη ασχοληθεί. Αξίζει, πάντως, να σημειώσουμε ότι είναι δυνατόν ένα μήνυμα να κρυπτογραφηθεί και ταυτόχρονα να υπογραφεί ηλεκτρονικά. Έτσι εξασφαλίζονται εξίσου η ασφάλεια στην επικοινωνία και η πιστοποίηση περιεχομένου και ταυτότητας αποστολέα.

Μέθοδοι κρυπτογράφησης

Συμμετρική κρυπτογράφηση

Στη συμμετρική κρυπτογράφηση χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, κατά συνέπεια, απαιτείται κάποιο ασφαλές μέσο για τη μετάδοσή του, όπως μια προσωπική συνάντηση, κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.

Μέθοδοι κρυπτογράφησης

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή, με πιο γνωστό τον Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Ηνωμένων Πολιτειών ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών

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

Ασύμμετρη κρυπτογράφηση

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

Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα

Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο

Η βασική αυτή αρχή της κρυπτογραφίας δημόσιου κλειδιού διατυπώθηκε το 1976 από τους Diffie και Hellman, ενώ το 1977 οι Rivest, Shamir και Adleman, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων, δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημόσιου κλειδιού.

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

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

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

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure - PKI) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών κρυπτογραφίας και υπηρεσιών, ο οποίος πιστοποιεί την εγκυρότητα του κάθε φυσικού προσώπου που εμπλέκεται σε μια συναλλαγή στο Διαδίκτυο, και παράλληλα προστατεύει την ασφάλεια της συναλλαγής.

Το PKI ενσωματώνει ψηφιακά πιστοποιητικά, κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα. Μια τυπική υλοποίηση του PKI περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες,

εξυπηρετητές (servers) και λογισμικό χρηστών. Παράλληλα προσφέρει σειρά εργαλείων για τη διαχείριση, ανανέωση και ανάκληση των πιστοποιητικών.

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη

Οι βασικές λειτουργίες/υπηρεσίες των Υποδομών Δημόσιου Κλειδιού είναι οι εξής:

Εμπιστευτικότητα (Confidentiality): Πρόκειται για την προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίησή τους. Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή τους. Η Υποδομή Δημόσιου Κλειδιού παρέχει κωδικοποίηση, αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από το συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization).

Ακεραιότητα (Integrity): Είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους. Παρέχεται από μηχανισμούς κρυπτογραφίας όπως οι ηλεκτρονικές υπογραφές.

Μη Άρνηση Αποδοχής (Non-Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας. Ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα. Η ασύμμετρη κρυπτογραφία παρέχει ηλεκτρονικές υπογραφές, κατά συνέπεια μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει τη συγκεκριμένη υπογραφή. Με αυτόν τον τρόπο, ο οποιοσδήποτε, και φυσικά ο παραλήπτης του μηνύματος, μπορεί να επιβεβαιώσει την ηλεκτρονική υπογραφή του αποστολέα.

Πιστοποίηση (Authentication): Πρόκειται για την επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής των πληροφοριών. Κάθε χρήστης που επιθυμεί να επιβεβαιώσει την ταυτότητα ενός άλλου προσώπου ή εξυπηρετητή με τον οποίο επικοινωνεί, βασίζεται στην πιστοποίηση. Οι παραδοσιακές μέθοδοι πιστοποίησης είναι οι εξής:

Με κάποιον κωδικό που γνωρίζουμε, όπως το PIN μιας τραπεζικής κάρτας ή το password ενός λογαριασμού

Με κάποιο αντικείμενο που έχουμε στην ιδιοκτησία μας, λόγω χάρη το κλειδί μιας πόρτας ή μια τραπεζική κάρτα

Με δακτυλικά αποτυπώματα, φωνή κ.λπ.

Το πιστοποιητικό (certificate) είναι ο τρόπος με τον οποίο η Υποδομή Δημόσιου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών ή πληροφορίες που σχετίζονται με αυτά, ή και τα δύο. Η εκδότρια αρχή των πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (Certificate Authority - CA). Οι Αρχές Πιστοποίησης διασφαλίζουν τη δημοσίευση και τη διανομή των δημόσιων κλειδιών και λαμβάνουν το δημόσιο κλειδί του ενδιαφερόμενου χρήστη. Εάν ο χρήστης ενεργεί στη συγκεκριμένη περίπτωση ως ιδιώτης, θα πρέπει να παραχωρήσει όλα τα απαραίτητα στοιχεία που αποδεικνύουν την ταυτότητά του. Σε αντίθετη περίπτωση, ο χρήστης θεωρείται ότι ενεργεί εκ μέρους κάποιας επιχείρησης, οπότε οφείλει να παραχωρήσει όλες τις νομικές πληροφορίες που απαιτούνται για την αξιοπιστία και τη νόμιμη λειτουργία της. Ουσιαστικά ένα ψηφιακό πιστοποιητικό αποτελεί μια ψηφιακά υπογεγραμμένη δήλωση από μια αρχή πιστοποίησης, η οποία:

Προσδιορίζει την αρχή πιστοποίησης που το εξέδωσε

Περιέχει το όνομα και κάποιες άλλες πληροφορίες του εγγεγραμμένου

Περιέχει το δημόσιο κλειδί του εγγεγραμμένου, το οποίο είναι ψηφιακά υπογεγραμμένο από την αρχή πιστοποίησης που το εξέδωσε

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη

Για την πιστοποίηση της ταυτότητας των συναλλασσομένων χρησιμοποιούνται τα πιστοποιητικά ασφαλείας, που επιπλέον εγγυώνται και την ασφάλεια ενός δικτυακού τόπου. Υπάρχουν δύο είδη πιστοποιητικών:

Τα προσωπικά πιστοποιητικά, τα οποία αποτελούν ένα είδος εγγύησης ότι ο χρήστης είναι αυτός που δηλώνει ότι είναι. Σε αυτά καταχωρούνται προσωπικές πληροφορίες, όπως όνομα χρήστη και κωδικός πρόσβασης. Στη συνέχεια, οι πληροφορίες αυτές αποθηκεύονται σε ένα πιστοποιητικό, το οποίο χρησιμοποιείται όταν στέλνονται προσωπικές πληροφορίες σε ένα διακομιστή ελέγχου ταυτότητας που απαιτεί πιστοποιητικό. Επίσης, ένα προσωπικό πιστοποιητικό επιτρέπει στο χρήστη να λαμβάνει κρυπτογραφημένα μηνύματα από τους υπόλοιπους χρήστες.

Τα πιστοποιητικά δικτυακών τόπων, τα οποία περιέχουν πληροφορίες που πιστοποιούν ότι η συγκεκριμένη ιστοσελίδα είναι γνήσια και ασφαλής. Αυτό διασφαλίζει ότι κανένα άλλο site δεν μπορεί να παρουσιαστεί με την ταυτότητα της γνήσιας, ασφαλούς τοποθεσίας. Επίσης, τα πιστοποιητικά δικτυακών τόπων χρονολογούνται κατά την έκδοσή τους. Όταν προσπαθείτε να συνδεθείτε με το website ενός οργανισμού, το πρόγραμμα ανάγνωσης επαληθεύει τη διεύθυνση Internet που είναι αποθηκευμένη στο πιστοποιητικό και ελέγχει την ημερομηνία λήξης του. Εάν οι πληροφορίες αυτές δεν είναι έγκυρες ή εάν έχει παρέλθει η ημερομηνία λήξης, εμφανίζεται προειδοποιητικό μήνυμα (Warning).

Έχουν αναπτυχθεί ή βρίσκονται υπό κατασκευή διάφορα πρωτόκολλα ασφαλείας που κάνουν χρήση των παραπάνω τεχνικών, όπως το SSL (Secure Sockets Layer), της Netscape, και το SET (Secure Electronic Transactions), που αναπτύχθηκε από τη Visa και τη MasterCard. Από αυτά σήμερα χρησιμοποιείται το SSL. Αρκετές ιστοσελίδες είναι εξοπλισμένες με προγράμματα που χρησιμοποιούν το πρωτόκολλο αυτό, αποτρέποντας έτσι τα μη εξουσιοδοτημένα πρόσωπα από την πρόσβασή τους σε δεδομένα που αποστέλλονται από και προς αυτές τις ιστοσελίδες. Τέτοια sites ονομάζονται "ασφαλή".

Οι πιο γνωστοί φυλλομετρητές ιστοσελίδων (browsers) υποστηρίζουν το πρωτόκολλο SSL και την κρυπτογράφηση που προσφέρει, ενώ ενημερώνουν το χρήστη ότι βρίσκεται σε ασφαλή τοποθεσία και μπορεί να στέλνει πληροφορίες ακίνδυνα. Με το πρωτόκολλο αυτό οι επικοινωνίες πραγματοποιούνται σε κωδικοποιημένη μορφή και επιπλέον γίνεται έλεγχος της αυθεντικότητας της ιστοσελίδας.

Η διαδικασία μιας ασφαλούς επικοινωνίας έχει ως εξής:

Ο φυλλομετρητής συνδέεται με τον ασφαλή δικτυακό τόπο.

Ο δικτυακός τόπος δηλώνει την ταυτότητά του, η οποία ελέγχεται με τα πιστοποιητικά που εκδίδονται από υπηρεσίες πιστοποίησης.

Η ασφαλής ιστοσελίδα και ο browser συμφωνούν στη χρήση συγκεκριμένου κλειδιού/αλγορίθμου που χρησιμοποιείται για την κρυπτογράφηση της υπόλοιπης επικοινωνίας

Τα δεδομένα που διακινούνται είναι κρυπτογραφημένα με το κλειδί/αλγόριθμο που συμφωνήθηκε στο προηγούμενο βήμα.

Η κρυπτογράφηση γίνεται με χρήση αλγορίθμου 40bit ή 128bit. Εάν έχει χρησιμοποιηθεί κρυπτογράφηση 40bit, τότε για να αποκρυπτογραφήσει κανείς τα δεδομένα που ανταλλάχθηκαν, θα πρέπει να δοκιμάσει περίπου 240 διαφορετικά κλειδιά, ενώ, εάν έχει χρησιμοποιηθεί κρυπτογράφηση 128bit, τότε θα πρέπει να δοκιμάσει περίπου 2.128 διαφορετικά κλειδιά.

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη

Με τη χρήση μεγάλης υπολογιστικής ισχύος, η αποκρυπτογράφηση του κλειδιού των 40bit μπορεί να επιτευχθεί σε μερικές ημέρες, ενώ η αποκρυπτογράφηση του κλειδιού των 128bit, με τα σημερινά δεδομένα, είναι πρακτικά αδύνατη. Θα πρέπει να

σημειωθεί ότι απαγορεύεται από τη νομοθεσία των ΗΠΑ η εξαγωγή και χρήση προγραμμάτων που υποστηρίζουν κωδικοποίηση 128bit εκτός των Ηνωμένων Πολιτειών και του Καναδά.

Στο πλαίσιο των προσπαθειών που καταβάλλονται για την ανάπτυξη των ηλεκτρονικών συναλλαγών, έχει επιτραπεί η χρήση της τεχνολογίας SGC (Server Gated Cryptography) ή International Step-Up Encryption, που αποτελεί επέκταση του πρωτοκόλλου SSL, από πιστωτικά ιδρύματα και άλλων χωρών. Η επέκταση αυτή επιτρέπει στα πιστωτικά ιδρύματα, εφόσον διαθέτουν το κατάλληλο πιστοποιητικό, να επικοινωνούν με τους πελάτες τους με κωδικοποίηση 128bit.

PGP (Pretty Good Privacy)

Στην αγορά κυκλοφορούν αρκετά προγράμματα λογισμικού κρυπτογράφησης. Είναι πολύ σημαντικό να γίνεται σωστή επιλογή του προϊόντος που θα χρησιμοποιηθεί. Υπάρχουν προγράμματα που είτε δεν χρησιμοποιούν αρκετά ασφαλείς αλγόριθμους είτε δημιουργούν σφάλματα (bugs) στην υλοποίηση της κρυπτογράφησης. Επίσης, θα πρέπει η τεχνική κρυπτογράφησης να ελέγχεται από ειδικούς, ενώ οι μέθοδοι πρέπει να είναι γνωστές και το λογισμικό που τις υλοποιεί υψηλής ποιότητας.

Για την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου και αρχείων, δημοφιλέστερο πρόγραμμα είναι το PGP (Pretty Good Privacy). Οι αλγόριθμοι του PGP είναι γνωστοί και ασφαλείς. Ο πηγαίος κώδικάς του είναι διαθέσιμος στο κοινό, γεγονός που επέτρεψε σε ειδικούς επιστήμονες των κλάδων της πληροφορικής και της κρυπτογραφίας να το εξετάσουν και να αναζητήσουν σφάλματα ή "κερκόπορτες" (back doors). Χρησιμοποιείται εδώ και αρκετά χρόνια, και οι ειδικοί της κρυπτογραφίας το θεωρούν σε μεγάλο βαθμό αξιόπιστο.

Το PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον καθηγητή Philip Zimmerman του MIT και χρησιμοποιεί τους αλγόριθμους για την κρυπτογράφηση και υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου. Όταν κυκλοφόρησε για πρώτη φορά, η αμερικανική κυβέρνηση προσπάθησε να απαγορεύσει τη διανομή του, με τη δικαιολογία ότι η υψηλής ποιότητας κρυπτογράφηση συμπεριλαμβάνεται στα... όπλα, και η κυβέρνηση έχει δικαίωμα να περιορίσει τη χρήση της.

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

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

Η υποδομή δημόσιου κλειδιού και η κρυπτογράφηση στην πράξη

Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί. Αυτή είναι μια μονόδρομη διαδικασία: αφού κρυπτογραφηθεί το μήνυμα, δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με το ιδιωτικό κλειδί. Για το λόγο αυτό, είναι σημαντικό να μη διαρρεύσει. Επειδή και το ιδιωτικό και το δημόσιο κλειδί μπορεί να

αποτελούν αρκετά μεγάλα σε όγκο αρχεία, το πρόγραμμα PGP αποθηκεύει το ιδιωτικό κλειδί στο δίσκο κρυπτογραφημένο. Κάθε φορά που ο χρήστης θέλει να το χρησιμοποιήσει, πρέπει να εισάγει την "passphrase", κωδικό που δεν αποθηκεύεται πουθενά αλλά έχει ο ίδιος απομνημονεύσει.

Κάθε χρήστης του PGP διατηρεί λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί (keyring). Για την προστασία της λίστας, την υπογράφει ο ίδιος με το ιδιωτικό του κλειδί. Κάθε κλειδί που προστίθεται στη λίστα είναι δυνατόν να φέρει έναν από τους παρακάτω χαρακτηρισμούς:

Απολύτως Έμπιστο (Completely Trusted)

Μερικώς Έμπιστο (Marginally Trusted)

Μη Έμπιστο (Untrusted)

Άγνωστο (Unknown)

Πάντως, αν και το PGP είναι σε μεγάλο βαθμό αξιόπιστο για εφαρμογές απλής ταυτοποίησης που εκτελούνται από απλούς χρήστες, δεν θεωρείται κατάλληλο για εφαρμογές ηλεκτρονικού εμπορίου και για όσες απαιτούν ισχυρή ταυτοποίηση. Τα πιστοποιητικά του PGP δεν είναι επεκτάσιμα και περιέχουν μόνο μία διεύθυνση ηλεκτρονικής αλληλογραφίας, την τιμή ενός δημόσιου κλειδιού και ένα χαρακτηρισμό βαθμού εμπιστοσύνης.

Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει ασφαλές μέσο προσδιορισμού της ταυτότητας ενός χρήστη, το PGP δεν μπορεί να παράσχει ισχυρή ταυτοποίηση (strong authentication). Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας. Επίσης, το συγκεκριμένο πρόγραμμα δεν υποστηρίζει μεθόδους επαλήθευσης και ανάκλησης των πιστοποιητικών. Οι διαδικασίες αυτές διεξάγονται αποκλειστικά με άμεση επικοινωνία των χρηστών. Επιπλέον, δεν παρέχει την επιλογή της ανωνυμίας, καθώς η χρήση μιας διεύθυνσης e-mail που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών.

X.509

Το X.509 είναι ένα πρότυπο κρυπτογράφησης το οποίο σχεδιάστηκε για να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου X.500 (LDAP). Το πρωτόκολλο X.500 αποτελεί μια ιεραρχική μέθοδο οργάνωσης ευρετηρίων (καταλόγων), η οποία σχεδιάστηκε από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization - ISO) και ενσωματώθηκε στο διαδικτυακό πρωτόκολλο LDAP (Lightweight Directory Access Protocol).

Η πρώτη έκδοση του X.509 δημοσιεύθηκε το 1988, καθιστώντας το την παλαιότερη πρόταση για μια παγκόσμια Υποδομή Δημόσιου Κλειδιού. Το γεγονός αυτό, σε συνδυασμό με την υποστήριξη του προτύπου από τον ISO και τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union - ITU), έχουν οδηγήσει στην υιοθέτηση του X.509 από μεγάλο αριθμό οργανισμών και κατασκευαστών.

Αρκετά χρηματοπιστωτικά ιδρύματα χρησιμοποιούν το X.509 για το πρότυπο ασφαλών συναλλαγών SET (Secure Electronic Transactions). Χρησιμοποιείται επίσης σε φυλλομετρητές ιστοσελίδων (browsers), εξυπηρετητές (servers).

Συμπεράσματα

Η ανάπτυξη ασφαλών συστημάτων που θα είναι φιλικά προς το χρήστη και στα οποία θα πραγματοποιείται η διακίνηση ευαίσθητων πληροφοριών χωρίς κίνδυνο υποκλοπής ή αλλοίωσης αναμένεται ότι θα συντελέσει στην αύξηση της χρήσης του

Internet τόσο στον τομέα των εμπορικών συναλλαγών όσο και γενικότερα στις επικοινωνίες.

Ειδικότερα, η προστασία των προσωπικών δεδομένων στο πλαίσιο λειτουργίας του ηλεκτρονικού εμπορίου αποτελεί κρίσιμο παράγοντα για την επιτυχημένη εκπλήρωση των στόχων του στην Κοινωνία της Πληροφορίας. Οι κίνδυνοι προσβολής της προσωπικότητας μπορούν να προστατευθούν με την εφαρμογή των κατάλληλων μέτρων προστασίας κάθε εμπλεκόμενου φορέα σε μια ηλεκτρονική συναλλαγή.

Τεχνικές που στοχεύουν στην ανωνυμοποίηση των καναλιών επικοινωνίας, τεχνολογίες ασφάλειας των πληροφοριών και προστασίας της ιδιωτικότητας (όπως η κρυπτογράφηση) είναι άμεσα συνδεδεμένες με ένα επιτυχημένο περιβάλλον ηλεκτρονικού επιχειρείν.

Μικρομεσαίες επιχειρήσεις που χρησιμοποιούν το Διαδίκτυο ή δραστηριοποιούνται σ' αυτό, δεν έχουν ουσιαστικά άλλη επιλογή από το να υιοθετούν σε μικρό ή μεγάλο βαθμό τεχνικές κρυπτογράφησης.

Πηγή: http://www.efarmoges.gr/store/gr/articles/kryptografisi_8.shtml