ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

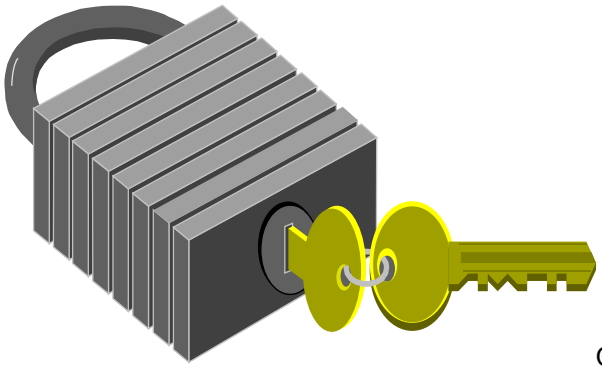
Δ Ι Α Τ Μ Η Μ Α Τ Ι Κ Ο Π Ρ Ο Γ Ρ Α Μ Μ Α Μ Ε Τ Α Π Τ Υ Χ Ι Α Κ Ω Ν Σ Π Ο Υ Δ Ω Ν Σ Τ Η Ν Δ Ι Ο Ι Κ Η Σ Η Ε Π Ι Χ Ε Ι Ρ Η Σ Ε Ω Ν (EXECUTIVE MBA)

Εργασία στα πλαίσια του μεταπτυχιακού μαθήματος

Π λ η ρ ο φ ο ρ ι α κ ά σ υ σ τ ή μ α τ α δ ι ο ί κ η σ η ς / Η λ ε κ τ ρ ο ν ι κ ό Ε μ π ό ρ ι ο

Διδάσκων : Οικονομίδης Α.

Τίτλος εργασίας : **Ασφάλεια στο Η/Ε**
Security for E-commerce



Θεσσαλονίκη Μαΐος 2002

Μεταπτυχιακές φοιτήτριες :Θρήσκου Χρυσάνθη Α.Μ. 1/01
Μήλιου Αικατερίνη Α.Μ. 32/01

Περιεχόμενα

Contents

Summary

The electronic trade is a new way of exchange of products that actualized via the internet. This nature of Internet has rendered permanently increasing the need of protection of data after the not permitted access in the trafficked in information is relatively easy, has potentially calamitous consequences for the order operation of organisms of (finances, militarymen, policies) and states and moreover is detected with difficulty.

The safety in the electronic trade has created crowd of discussions and research, thing that renders circumspect a big part the purchasing and enterprising world.

The basic dangers that threaten the electronic transactions have to do with the integrity, the confidentiality of data, the non repudiation and the verification of genuineness.

The requirements of safety in the electronic trade are focused in:

- Authentication (Control of authenticity)

This process aims at the verification of identity of user

- Authorization (Authorisation)

Includes the control of access in concrete information and services when the identity of user is ascertained

- Confidentiality (Confidentiality)

The confidentiality is interwoven with the reject of not permitted modification of information. It is provided via encryption and is essential element of privatization of user. Mainly for the electronic trade, it constitutes of big importance component so much in the protection of finances of data, in the protection of information of growth, organisational structures and other personal information from not permitted access .

- Integrity (Integrity)

The integrity has to make with the sure transport of data in the network. This means that with no way it should not exists, not permitted modification of data and this is ensured with various methods (eg digital signatures).

Non-repudiation (not refusal of responsibility)

Constitutes a very important sector in the safety in the electronic trade. In order to be completed a transaction it will be supposed that somebody cannot claim that he did not participate in this.

The Internet is known as for his devotion in open sea models. This support in the open sea models, in combination with the open exchange of information above the Internet, perhaps leads to the thought that Internet and safety are terms reciprocal excluded. Such thing abstains from the reality. The Internet has been equipped with variety standards that they cover many levels of networking, from safety in level of parcel up to safety in level of applications.

The secure HTTP was developed with a view to provide sure mechanisms of communication between HTTP of customers and agents and give them the possibility for sure commercial transactions.

The companies of credit cards in collaboration with economic organisms, tradesmen and holders of cards develop sure and pioneering solutions for electronic trade (e-commerce). From games as computers, from flowers as the clothes, the persons might him buy online with confidence. This moment exist two types of reliable technologies of safety, the SSL and the SET™ that are available for online purchases.

When we make transactions with tradesmen that we know, then we can use SSL in order to protect the secrecy of our transaction. The Secure Sockets Layer (SSL) provides well-founded protection of secrecy with the encryption of channel between the consumer and the tradesman. In order to find if our transaction is ensured by the SSL, we can check the intact key or the closed symbol of lock in the frame of our window browser. We still can check URL of tradesman - it will be supposed to change from “http” in “https” when we processed sure transactions. So much the Netscape Navigator and the Microsoft Internet Explorer use SSL.

Technology SET (Secure Electronic Transaction) was developed for the biggest online safety that makes capable consumers and the tradesmen ascertain the genuineness of other before a transaction.

Almost in all the environments of distributed systems, the electronic post (e-mail) is the multi-used network application. With the amounting dependence of use of electronic post for any aim can no one conceive, that exists a increasing need for services verification of genuineness (authentication) and confidentiality (confidentiality). Two forms dominate today in the sector of safety in the electronic post: **the Pretty Good**

Privacy (PGP) and the **Private-Enhanced Mail (PEM).**

The electronic system of payments should be supported from the suitable cryptographic techniques of state of key. Basic element of mechanisms of safety constitute also the digital signatures as well as the publication and utilisation of digital certificates. Without these elements many are the dangers and the threats that can result. However once again results a additive basic question to resolution. It shouldn't do exist somebodies restrictions and somebodies governing lines in the concretisation of all these processes? Naturally it should.

One of the widespreadest ways of safety of network is the use of firewall. Firewall is a mechanism that is used in order to checks the access from and to the network with final aim the protection of network. Firewall it functions as a gate from which passes all the movement from and to the network. With the use of Firewall the communication between in the protected network and in any other network is limited.

Some basic principles of safety and secrecy of personal data exist that should not be overlooked and that are internationally acceptable. Taking into consideration these principles and knowing the need for common with the European partners policies, it should head for the development of policy of safety. The choice of somebodies of important entities can help or complicate this effort of development of policy

Περίληψη

Το ηλεκτρονικό εμπόριο είναι ένας νέος τρόπος ανταλλαγής προϊόντων που πραγματοπιείται μέσω του διαδικτύου. Η φύση αυτή του Διαδικτύου έχει καταστήσει διαρκώς αυξανόμενη την ανάγκη προστασίας των δεδομένων αφού η μη εξουσιοδοτημένη πρόσβαση στις διακινούμενες πληροφορίες είναι σχετικά εύκολη, έχει ενδεχομένως καταστρεπτικές συνέπειες για την εύρυθμη λειτουργία οργανισμών (οικονομικών, στρατιωτικών, πολιτικών) και κρατών και επιπλέον ανιχνεύεται δύσκολα.

Η ασφάλεια στο ηλεκτρονικό εμπόριο έχει δημιουργήσει πλήθος συζητήσεων και έρευνας, πράγμα που καθιστά επιφυλακτικό ένα μεγάλο μέρος του αγοραστικού και επιχειρηματικού κόσμου.

Οι βασικοί κίνδυνοι που απειλούν τις ηλεκτρονικές συναλλαγές έχουν να κάνουν με την ακεραιότητα, την εμπιστευτικότητα των δεδομένων ,την άρνηση υπηρεσίας και την εξακρίβωση της γνησιότητας.

Οι απαιτήσεις ασφάλειας στο ηλεκτρονικό εμπόριο επικεντρώνονται στα :

- Authentication (Έλεγχος αυθεντικότητας)

  Η διαδικασία αυτή έχει στόχο την εξακρίβωση της ταυτότητας του χρήστη.

- Authorization (Εξουσιοδότηση)

  Περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί.

- Confidentiality (Εμπιστευτικότητα)

  Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας. Παρέχεται μέσω κρυπτογράφησης και είναι απαραίτητο στοιχείο της ιδωτικότητας του χρήστη. Κυρίως για το ηλεκτρονικό εμπόριο, αποτελεί υψίστης σημασίας συστατικό τόσο στην προστασία των οικονομικών δεδομένων, όσο και στην προστασία πληροφοριών ανάπτυξης, οργανωτικών δομών και άλλων προσωπικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση.

- Integrity (Ακεραιότητα)

Η ακεραιότητα έχει να κάνει με την ασφαλή μεταφορά των δεδομένων στο δίκτυο. Αυτό σημαίνει ότι με κανένα τρόπο δεν πρέπει να υπάρξει, μη εξουσιοδοτημένη τροποποίηση των δεδομένων και αυτό διασφαλίζεται με διάφορες μεθόδους (π.χ. ψηφιακές υπογραφές).

- Non-repudiation (Μη αποποίηση της ευθύνης)

Αποτελεί ένα πολύ σημαντικό τομέα στην ασφάλεια στο ηλεκτρονικό εμπόριο. Για να ολοκληρωθεί μια συναλλαγή θα πρέπει να μην μπορεί κάποιος να ισχυρισθεί ότι δεν συμμετείχε σε αυτή.

Το Διαδίκτυο είναι γνωστό για την αφοσίωσή του σε ανοιχτά πρότυπα. Αυτή η υποστήριξη στα ανοιχτά πρότυπα, σε συνδυασμό με την ανοιχτή ανταλλαγή πληροφορίας πάνω από το Διαδίκτυο, ίσως οδηγήσει στη σκέψη ότι Διαδίκτυο και ασφάλεια είναι όροι αμοιβαία αποκλειόμενοι. Κάτι τέτοιο απέχει από την πραγματικότητα. Το Διαδίκτυο έχει εξοπλιστεί με ποικιλία στάνταρτ που καλύπτουν πολλά επίπεδα δικτύωσης, από ασφάλεια σε επίπεδο πακέτου μέχρι ασφάλεια σε επίπεδο εφαρμογών.

Το secure HTTP αναπτύχθηκε με σκοπό να παρέχει ασφαλείς μηχανισμούς επικοινωνίας μεταξύ HTTP πελατών και εξυπηρετητών και να τους δώσει τη δυνατότητα για ασφαλείς εμπορικές συναλλαγές

Οι εταιρείες πιστωτικών καρτών σε συνεργασία με οικονομικούς οργανισμούς, εμπόρους και κατόχους καρτών αναπτύσσουν ασφαλείς και πρωτοποριακές λύσεις για το ηλεκτρονικό εμπόριο (e-commerce). Από παιχνίδια ως υπολογιστές, από λουλούδια ως ρούχα, οι άνθρωποι θα μπορούν να τα αγοράζουν online με εμπιστοσύνη. Αυτή τη στιγμή υπάρχουν δύο τύποι αξιόπιστων τεχνολογιών ασφαλείας, το SSL και το SET^{TM}, που είναι διαθέσιμες για online αγορές.

Όταν κάνουμε συναλλαγές με εμπόρους που γνωρίζουμε, τότε μπορούμε να χρησιμοποιήσουμε SSL για να προστατέψουμε την μυστικότητα της συναλλαγής μας. Το Secure Sockets Layer (SSL) παρέχει βάσιμη προστασία μυστικότητας με την κρυπτογράφηση του καναλιού μεταξύ του καταναλωτή και του εμπόρου. Για να βρούμε εάν η συναλλαγή μας διασφαλίζεται από το SSL, μπορούμε να ελέγξουμε το άθικτο κλειδί ή το κλειστό σύμβολο κλειδαριάς στο πλαίσιο του παραθύρου του browser μας. Μπορούμε ακόμα να ελέγξούμε το URL του εμπόρου- θα πρέπει να αλλάξει από "http" σε "https" όταν επεξεργαζόμαστε ασφαλείς συναλλαγές. Τόσο το Netscape Navigator όσο και ο Microsoft Internet Explorer χρησιμοποιούν SSL.

Η τεχνολογία **SET (Secure Electronic Transaction)** αναπτύχθηκε για τη μέγιστη online ασφάλεια που κάνει ικανούς τους καταναλωτές και τους εμπόρους να εξακριβώνουν τη γνησιότητα του άλλου πριν από μια συναλλαγή.

Σχεδόν σε όλα τα περιβάλλοντα κατανεμημένων συστημάτων, το ηλεκτρονικό ταχυδρομείο (e-mail) είναι η πιο πολυχρησιμοποιούμενη δικτυακή εφαρμογή. Με την ανερχόμενη εξάρτηση της χρήσης του ηλεκτρονικού ταχυδρομείου για οποιοδήποτε σκοπό μπορεί κανείς να αντιληφθεί, υπάρχει μία αυξανόμενη ανάγκη για υπηρεσίες εξακρίβωση γνησιότητας (authentication) και εμπιστευτικότητας (confidentiality). Δύο σχήματα κυριαρχούν σήμερα στον τομέα της ασφάλειας στο ηλεκτρονικό ταχυδρομείο: **το Pretty Good Privacy (PGP)** και το **Private-Enhanced Mail (PEM)**.

Το ηλεκτρονικό σύστημα πληρωμών θα πρέπει να υποστηρίζεται από τις κατάλληλες **κρυπτογραφικές τεχνικές** δημόσιου κλειδιού. Βασικό στοιχείο των μηχανισμών ασφάλειας αποτελούν και οι **ψηφιακές υπογραφές** καθώς και η έκδοση και χρησιμοποίηση **ψηφιακών** πιστοποιητικών. Δίχως αυτά τα στοιχεία πολλοί είναι οι κίνδυνοι και οι απειλές που μπορούν να προκύψουν. Όμως και πάλι προκύπτει ένα πρόσθετο βασικό ζήτημα προς επίλυση. Δεν πρέπει να υπάρξουν κάποιοι περιορισμοί και κάποιες κατευθυντήριες γραμμές στην υλοποίηση όλων αυτών των διαδικασιών; Φυσικά και πρέπει.

Ένας από τους πιο διαδεδομένους τρόπους ασφαλείας ενός δικτύου είναι η χρήση firewall. Firewall είναι ένας μηχανισμός που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το δίκτυο με απώτερο σκοπό την προστασία του δικτύου. Ένα firewall λειτουργεί σαν μία πύλη από την οποία περνάει όλη η κίνηση από και προς το δίκτυο. Με την χρήση ενός Firewall περιορίζεται η επικοινωνία ανάμεσα στο προστατευόμενο δίκτυο και ένα οποιοδήποτε άλλο δίκτυο.

Υπάρχουν κάποιες **βασικές αρχές ασφάλειας και μυστικότητας** των προσωπικών δεδομένων που δεν πρέπει να παραβλέπονται και που είναι διεθνώς αποδεκτοί. Με γνώμονα αυτές τις αρχές και γνωρίζοντας την ανάγκη για κοινές με τους Ευρωπαίους εταίρους πολιτικές, πρέπει να πορευτούμε για την εκπόνηση μιας πολιτικής ασφάλειας. Η επιλογή κάποιων σημαντικών οντοτήτων μπορεί να βοηθήσει ή να δυσκολέψει την προσπάθεια εκπόνησης αυτής της πολιτικής.

ΣΗΜΑΣΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

ΕΙΣΑΓΩΓΗ

Η ραγδαία διάδοση του Διαδικτύου (Internet), έχει συμβάλλει κατά πολύ στη διαμόρφωση της σύγχρονης κοινωνίας. Τα αποτελέσματα αυτής της διάδοσης τα ζούμε καθημερινά, σε όλους τους τομείς και όχι μόνο σε μια κλειστή ομάδα ανθρώπων που χρησιμοποιούν τους υπολογιστές. Με βάση αυτό ως δεδομένο αναμενόμενο και λογικό ήταν, η εξέλιξη αυτή να επηρεάσει σημαντικά και έναν καθοριστικό τομέα της ζωής μας, που είναι το εμπόριο.

Έτσι, δημιουργήθηκε ένας καινούριος τρόπος ανταλλαγής προϊόντων, το **ηλεκτρονικό εμπόριο.**

Τι είναι το ηλεκτρονικό εμπόριο ;

Ηλεκτρονικό εμπόριο είναι η ικανότητα να πραγματοποιούνται συναλλαγές, που σχετίζονται με την ανταλλαγή αγαθών ή υπηρεσιών, μεταξύ δύο ή περισσότερων χρησιμοποιώντας ηλεκτρονικά εργαλεία και τεχνικές.

Το χαμηλό κόστος, η εύκολη πρόσβαση, η γρήγορη και συνεχής ενημέρωση, είναι μερικοί μόνο από τους παράγοντες που βοήθησαν στην ανάπτυξη του ηλεκτρονικού εμπορίου.

Είναι ένας τρόπος εμπορίου, ο οποίος μπορεί να υιοθετηθεί από όλες τις επιχειρήσεις, ανεξαρτήτως κατηγορίας. Δεν υπάρχει πλέον το πλεονέκτημα των μεγάλων επιχειρήσεων σε σχέση με τις μικρές και μικρομεσαίες. Το κόστος, όπως προαναφέραμε είναι χαμηλό, έτσι παρέχεται η δυνατότητα σε όλους να το εκμεταλλευθούν και να αυξήσουν τις πωλήσεις τους.

Μέχρι εδώ παρουσιάσαμε μόνο θετικά στοιχεία για το ηλεκτρονικό εμπόριο και δεν αναφέραμε τα μειονεκτήματά του. Αυτά είναι και τα οποία φράζουν την εξάπλωσή του και εμποδίζουν την περαιτέρω εξέλιξή του. Το πιο σημαντικό από όλα τα προβλήματα, και το πιο καίριο είναι η ασφάλεια των συναλλαγών.

Ο δισταγμός των περισσότερων επιχειρήσεων αλλά και των καταναλωτών οφείλεται κυρίως στην ανησυχία για την ασφάλεια του δικτύου αλλά και των συναλλαγών που πραγματοποιούνται σ' αυτό.

Αυτό είναι και το μείζον πρόβλημα που πρέπει να αντιμετωπισθεί και να καθησυχάσει έτσι τόσο τους επιχειρηματίες, όσο και τους υποψήφιους πελάτες.

Είναι γνωστές πολλές περιπτώσεις καταστροφής δεδομένων, εξαπάτησης ή κλοπής χρημάτων, υποκλοπής προσωπικών ή οικονομικών πληροφοριών (π.χ. αριθμοί πιστωτικών καρτών) κλπ.

Με βάση αυτά ως δεδομένα διαπιστώνουμε ότι ασφάλεια στο ηλεκτρονικό εμπόριο σημαίνει εξασφάλιση στον καταναλωτή ότι οι συναλλαγές που πραγματοποιεί μέσω του δικτύου είναι απόρρητες και δεν μπορούν να επεξεργασθούν από κανένα τρίτο πρόσωπο. Επίσης, να γνωρίζει ότι η συγκεκριμένη σελίδα του Web που επισκέπτεται ανήκει στη συγκεκριμένη εταιρεία και ότι Δε θα δει τα προσωπικά του στοιχεία δημοσιευμένα κάπου στο Internet.

Ένα σύστημα ηλεκτρονικού εμπορίου για να είναι επιτυχημένο θα πρέπει να είναι ασφαλές. Αυτός είναι ο κύριος παράγοντας που το κρίνει. Για να μπορέσει όμως το σύστημα να είναι ασφαλές, θ πρέπει να είναι καταγραμμένα με πλήρη σαφήνεια τα σημεία στα οποία είναι ευάλωτο και με συγκεκριμένες τεχνικές να τα αντιμετωπίσει με επιτυχία.

Οι κυριότερες απειλές και επιθέσεις στις οποίες οι εμπορικές δραστηριότητες σε δικτυωμένα περιβάλλοντα είναι ευάλωτα και χρειάζονται επισήμανση είναι τα εξής :

- Πρόσβαση χωρίς εξουσιοδότηση σε δικτυακούς πόρους.
- Καταστροφή πληροφοριών και πόρων.
- Μεταβολή πληροφοριών ή εισαγωγή νέων.
- Αποκάλυψη πληροφοριών σε μη εξουσιοδοτημένα άτομα.
- Πρόκληση διάρρηξης και διακοπής δικτυακών υπηρεσιών.
- Κλοπή πληροφοριών και δικτυακών πόρων.
- Άρνηση λήψης υπηρεσιών και άρνηση λήψης ή αποστολής πληροφοριών.
- Κατοχή υπηρεσιών χωρίς άδεια.
- Αποκάλυψη σε τρίτους κατά τη διάρκεια της συναλλαγής εμπιστευτικών στοιχείων.

Θεωρείται ίσως το πλέον σημαντικό στοιχείο η κατανόηση αυτών των προβλημάτων. Μόνο με αυτό τον τρόπο μπορούν οι εφαρμογές και οι τεχνολογίες του ηλεκτρονικού εμπορίου να αντιμετωπίσουν τα θέματα αυτά. Με βάση αυτό μπορεί ο διαχειριστής του συστήματος ή ο υπεύθυνος ασφαλείας μιας επιχείρησης να επιλέξει κατάλληλα και με καλή απόδοση συστήματα που ελέγχουν και προστατεύουν τις πληροφορίες που είναι κρίσιμες για το τομέα αυτό.

Οι πλέον διαδεδομένοι μέθοδοι προστασίας είναι οι εξής :

- Σύστημα password.
- Απόκρυψη των στοιχείων.
- Ασφάλεια βασισμένη στην εμπιστοσύνη.

Για να μπορέσει το ηλεκτρονικό εμπόριο να διαδοθεί ευρέως και να αναπτυχθεί θα πρέπει να δοθεί ιδιαίτερη σημασία στην εγγυημένη ασφάλεια. Μόνο έτσι θα μπορέσει να ανταγωνισθεί το συμβατικό εμπόριο.

Σε αυτό ακριβώς το σημείο βρίσκεται και η μεγάλη πρόκληση για τους υποστηρικτές του ηλεκτρονικού εμπορίου. Πως θα μπορέσει η ασφάλεια του απλού εμπορίου, που βασίζεται στο χαρτί και στην αμοιβαία εμπιστοσύνη εμπόρου - καταναλωτή, να μεταβεί και στο ηλεκτρονικό εμπόριο. Και για να είμαστε και πιο ακριβείς, πρέπει να πεισθεί και ο υποψήφιος καταναλωτής του αγαθού ή της παρεχόμενης υπηρεσίας για την ασφάλεια και αξιοπιστία του συστήματος ηλεκτρονικού εμπορίου, για να δεχθεί να ολοκληρώσει τη συνδιαλλαγή και να δώσει τα προσωπικά του στοιχεία και δεδομένα.

ΑΠΕΙΛΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ WEB

Ο πίνακας 1-1 παρέχει μια περίληψη των τύπων των απειλών ασφάλειας που υπάρχουν στο Web. Ένας τρόπος για ομαδοποίηση αυτών των απειλών είναι σε παθητικές και ενεργές επιθέσεις. Οι παθητικές επιθέσεις περιλαμβάνουν την υποκλοπή (eavesdropping) στη δικτυακή κίνηση μεταξύ του browser και του server, και την πρόσβαση σε ένα Web site που υποτίθεται ότι είναι περιορισμένη. Οι ενεργές επιθέσεις περιλαμβάνουν το να υποδύεσαι κάποιον άλλο χρήστη, την αλλαγή του περιεχομένου μηνυμάτων μεταξύ client και server, και την αλλαγή των πληροφοριών σε ένα Web site.

	Απειλές	Συνέπειες	Αντίμετρα
Ακεραιότητα	▪ Τροποποίηση των δεδομένων του χρήστη ▪ Trojan Horse browser ▪ Τροποποίηση της μνήμης ▪ Τροποποίηση της κίνησης (traffic) των μηνυμάτων κατά τη μεταφορά	▪ Απώλεια πληροφορίας ▪ Συμβιβασμός της μηχανής ▪ ευπάθεια σε όλες τις άλλες απειλές	Κρυπτογραφικά checksums
Εμπιστευτικότητα	▪ Υποκλοπή στο Δίκτυο ▪ Κλοπή πληροφορίας από τον server ▪ Κλοπή δεδομένων από τον client ▪ Πληροφορίες σχετικές με τη διαμόρφωση του δικτύου ▪ Πληροφορία για το ποιος client μιλά στο server	▪ Απώλεια πληροφορίας ▪ Απώλεια μυστικότητας	Κρυπτογράφηση, Web proxies
Αρνηση Υπηρεσίας	▪ Καταστροφή των user threads ▪ Πλημμύρισμα μηχανής με ψεύτικες απειλές ▪ Γέμισμα δίσκου ή μνήμης ▪ Απομόνωση μηχανής από επιθέσεις DNS	▪ Διασπαστικό ▪ Ενοχλητικό ▪ Εμποδίζει το χρήστη να τελειώσει την δουλειά του	Δύσκολο να εμποδιστεί
Εξακρίβωση γνησιότητας	▪ Προσωποποίηση νόμιμων χρηστών ▪ Παραχάραξη δεδομένων	▪ Διαστρέβλωση του χρήστη ▪ Πεποίθηση ότι λάθος πληροφορίες είναι έγκυρες	Κρυπτογραφικές τεχνικές

Πίνακας 1-1: **Σύγκριση των Απειλών στο Web**

Ένας άλλος τρόπος για ταξινόμηση των απειλών έχει να κάνει με την τοποθεσία της απειλής: στο Web server, το Web browser, και τη δικτυακή κίνηση μεταξύ browser και server. Το θέμα της ασφάλειας της κυκλοφορίας είναι στην κατηγορία της δικτυακής ασφάλειας που μας ενδιαφέρει περισσότερο.

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Μέχρι εδώ έχει γίνει σαφές ότι η ασφάλεια στο ηλεκτρονικό εμπόριο είναι το πιο σημαντικό δεδομένο που πρέπει να αντιμετωπισθεί σοβαρά για την υλοποίηση ενός ασφαλούς συστήματος.

Υπάρχουν διάφορες απαιτήσεις για τη δημιουργία του, οι οποίες σε γενικές γραμμές μπορούν να χωρισθούν στα παρακάτω θέματα :

- Authentication (Έλεγχος αυθεντικότητας)

Η διαδικασία αυτή έχει στόχο την εξακρίβωση της ταυτότητας του χρήστη.

Όλα τα μέρη που εμπλέκονται στη συναλλαγή πρέπει να αισθάνονται σίγουρα ότι επικοινωνούν με άλλα μέλη που συνεργάζονται και όχι με κάποιον που ισχυρίζεται ότι είναι κάποιος άλλος. Ο έλεγχος αυτός πραγματοποιείται πριν την έναρξη οποιασδήποτε ηλεκτρονικής συναλλαγής και υλοποιείται με τη χρήση διαφόρων τεχνολογιών. Συγκεκριμένα, ο χρήστης παρέχει πληροφορίες για τη ταυτότητά του και συγκρίνονται με αυτές που το σύστημα ήδη γνωρίζει για το χρήστη. Αν το σύστημα λάβει από το χρήστη τις σωστές πληροφορίες (δηλαδή, ταυτίζονται με αυτές που έχει καταχωρημένες), τότε αναγνωρίζει το χρήστη και τον πιστοποιεί σαν το μέλος του συστήματος με τα συγκεκριμένα στοιχεία. Οι μέθοδοι που ακολουθούνται για την πιστοποίηση βασίζονται στα εξής χαρακτηριστικά :

- Επιβεβαίωση κάποιου τύπου ιδιοκτησιακών πληροφοριών, όπως login name και password.
- Κατοχή κάποιας πληροφορίας όπως ένα κλειδί ή μια κάρτα.
- Απόδειξη ότι ένα τρίτο έμπιστο μέλος (π.χ. administrator) έχει ήδη εγκαταστήσει πιστοποίηση γι' αυτόν που τη διεκδικεί.

Για να εξακριβωθεί η ταυτότητα ενός χρήστη, τα χαρακτηριστικά αυτά θα πρέπει να συνδυάζονται παρά να τα λαμβάνουμε υπόψη ξεχωριστά. Μερικοί κοινοί τρόποι σε συστήματα ασφαλείας δικτύων, που χρησιμοποιούνται για την αυθεντικοποίηση των χρηστών περιλαμβάνουν passwords, προσωπικούς αριθμούς αναγνώρισης (Personal Identification Numbers - PINs) και διάφορα άλλα.

- <u>Authorization (Εξουσιοδότηση)</u>

Το θέμα αυτό περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί. Στην πράξη εξουσιοδότηση σημαίνει παραχώρηση δικαιωμάτων στο χρήστη από τον ιδιοκτήτη. Για παράδειγμα κλασσική περίπτωση αποτελεί η εξουσιοδότηση από τον πελάτη στον έμπορο ο έλεγχος των στοιχείων της πιστωτικής του κάρτας και αν τα χρήματα στο λογαριασμό καλύπτουν το ποσό των συναλλαγών. Έτσι, περιορίζονται οι χειρισμοί, οι ενέργειες κάποιου χρήστη στο περιβάλλον αυτό. Η εξουσιοδότηση αποτελείται από μηχανισμούς ελέγχου πρόσβασης, δικτυακούς πόρους και δικαιώματα πρόσβασης.

Αυτά περιγράφουν προνόμια πρόσβασης ή άδειες σχετικά με τις συνθήκες κάτω από τις οποίες διάφορες οντότητες μπορούν να έχουν πρόσβαση σε δικτυακούς πόρους και πως επιτρέπεται να μπουν σ' αυτούς τους δικτυακούς πόρους. Τέτοια παραδείγματα αδειών, είναι :

- Δημιουργία ή καταστροφή
- Διάβασμα ή γράψιμο
- Προσθήκη, διαγραφή ή μετατροπή κειμένου.
- Εισαγωγή - εξαγωγή
- Εκτέλεση

Τα δικαιώματα αυτά ελέγχονται από μια λίστα πρόσβασης. Αυτή καταγράφει τις άδειες των χρηστών. Οι υπηρεσίες πρόσβασης επιβάλλοντα αρχικά από τις υπηρεσίες ελέγχου πρόσβασης.

- <u>Confidentiality (Εμπιστευτικότητα)</u>

Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας. Παρέχεται μέσω κρυπτογράφησης και είναι απαραίτητο στοιχείο της ιδωτικότητας του

χρήστη. Κυρίως για το ηλεκτρονικό εμπόριο, αποτελεί υψίστης σημασίας συστατικό τόσο στην προστασία των οικονομικών δεδομένων, όσο και στην προστασία πληροφοριών ανάπτυξης, οργανωτικών δομών και άλλων προσωπικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση.

Είναι χρήσιμη ακόμη και σε πληροφορίες που η δημοσιοποίησή τους εξαρτάται από το χρόνο. Αυτό αφορά για λίστες τιμών ή για κάποια αναφορά που ίσως για κάποιο συγκεκριμένο χρονικό διάστημα να είναι απόλυτα εμπιστευτικές και μετά από αυτό απόλυτα διαθέσιμες στον οποιονδήποτε. Για να καλυφθούν και να συμβιβαστούν αυτές οι ανάγκες και πολιτικές ελέγχου ροής της πληροφορίας, απαραίτητο είναι να περιλαμβάνονται στην εμπιστευτικότητα καθώς και στον έλεγχο της αυθεντικότητας.

Η εμπιστευτικότητα πρέπει να εξασφαλίζει τα εξής :

(1) η πληροφορία δεν μπορεί να διαβαστεί, αντιγραφεί, μετατραπεί ή αποκαλυφθεί χωρίς την απαραίτητη εξουσιοδότηση και

(2) οι επικοινωνίες μέσω των δικτύων δεν μπορούν να διακοπούν. Τεχνικές κρυπτογράφησης και κωδικοποίησης έχουν σχεδιαστεί για να ικανοποιούν αυτές τις απαιτήσεις.

- Integrity (Ακεραιότητα)

  Η ακεραιότητα έχει να κάνει με την ασφαλή μεταφορά των δεδομένων στο δίκτυο. Αυτό σημαίνει ότι με κανένα τρόπο δεν πρέπει να υπάρξει, μη εξουσιοδοτημένη τροποποίηση των δεδομένων και αυτό διασφαλίζεται με διάφορες μεθόδους (π.χ. ψηφιακές υπογραφές). Υπάρχουν συγκεκριμένοι μέθοδοι που ελέγχουν αν ένα μήνυμα έχει μεταβληθεί τη στιγμή της μεταφοράς. Στα συστήματα ηλεκτρονικού εμπορίου απαραίτητο είναι η εφαρμογή τέτοιων μεθόδων ώστε να μπορεί να διασφαλισθεί ο χρήστης ότι τα δεδομένα που έστειλε φθάνουν στον προορισμό τους αναλλοίωτα, δηλαδή χωρίς την προσθήκη, αφαίρεσης ή αναδιάταξης μερών των δεδομένων.

- Non-repudiation (Μη αποποίηση της ευθύνης)

Αποτελεί ένα πολύ σημαντικό τομέα στην ασφάλεια στο ηλεκτρονικό εμπόριο. Για να ολοκληρωθεί μια συναλλαγή θα πρέπει να μην μπορεί κάποιος να ισχυρισθεί ότι δεν συμμετείχε σε αυτή. Απαραίτητη είναι η διασφάλιση όλων των πλευρών ότι η συνδιαλλαγή τους θα ολοκληρωθεί και από τη στιγμή αυτή, δεν μπορεί κανείς να παρέμβει και να ισχυρισθεί το αντίθετο. Καθίσταται σαφές ότι οι υπηρεσίες μη αποποίησης της ευθύνης θα πρέπει ανά πάσα στιγμή να μπορούν να αποδείξουν την προέλευση, μεταφορά, παράδοση και μετάδοση των δεδομένων, αν φυσικά τους ζητηθεί από κάποιο εξουσιοδοτημένο μέλος. Απαραίτητο είναι να αναφέρουμε ότι η ανάγκη για τέτοιες υπηρεσίες, αντικατοπτρίζει τις ατέλειες που έχει κάθε περιβάλλον επικοινωνίας, και φανερώνει το γεγονός ότι πρέπει να υπάρξουν κατάλληλοι μηχανισμοί ασφαλείας για την ολοκλήρωση των συναλλαγών και των επικοινωνιών.

ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Υπάρχουν πολλά διαφορετικά είδη απειλών τα οποία διακυβεύουν την ασφάλεια στο ηλεκτρονικό εμπόριο. Προκειμένου να εξουδετερωθούν αυτές οι απειλές, έχει αναπτυχθεί ένας ικανός αριθμός πρωτοκόλλων και εφαρμογών βασισμένων σε τεχνικές κρυπτογράφησης που ήδη αναλύθηκαν.

Το Διαδίκτυο είναι γνωστό για την αφοσίωσή του σε ανοιχτά πρότυπα. Αυτή η υποστήριξη στα ανοιχτά πρότυπα, σε συνδυασμό με την ανοιχτή ανταλλαγή πληροφορίας πάνω από το Διαδίκτυο, ίσως οδηγήσει στη σκέψη ότι Διαδίκτυο και ασφάλεια είναι όροι αμοιβαία αποκλειόμενοι. Κάτι τέτοιο απέχει από την πραγματικότητα. Το Διαδίκτυο έχει εξοπλιστεί με ποικιλία στάνταρτ που καλύπτουν πολλά επίπεδα

δικτύωσης, από ασφάλεια σε επίπεδο πακέτου μέχρι ασφάλεια σε επίπεδο εφαρμογών. Αν επιμένει κανείς να θεωρεί το Διαδίκτυο ανασφαλές μέσο λόγω της αποκεντρωμένης φύσης του, αξίζει να σημειωθεί ότι τα δεδομένα που εμπλέκονται σε συναλλαγές μπορούν να διασφαλιστούν κάνοντας χρήση ενός ικανού αριθμού στάνταρτ.

Πρότυπα ασφάλειας για το Διαδίκτυο		
Πρότυπο	***Λειτουργία***	***Εφαρμογή***
Secure HTTP (S-http)	Καθιστά ασφαλείς τις web συναλλαγές	Browsers, web servers και Internet εφαρμογές
Secure Sockets Layer (SSL)	Παρέχει ασφάλεια σε πακέτα δεδομένων στο επίπεδο δικτύου	Browsers, web servers και Internet εφαρμογές
Secure MIME (S/MIME)	Καθιστά τα προσαρτημένα σε μηνύματα ηλεκτρονικού ταχυδρομείου αρχεία ασφαλή (secure mail attachments)	Πακέτα ηλεκτρονικού ταχυδρομείου με RSA κρυπτογράφηση και ψηφιακές υπογραφές
Secure Electronic Transactions (SET)	Εγγυάται ασφάλεια σε συναλλαγές με πιστωτικές κάρτες	Έξυπνες κάρτες, Transaction Servers

Σχήμα 1: Πρότυπα ασφαλείας.

Τα στάνταρτ που καλύπτονται εδώ κατηγοριοποιούνται σύμφωνα με το αν παρέχουν ασφάλεια σύνδεσης ή ασφάλεια εφαρμογών. Στάνταρτ όπως το **Secure Sockets Layer (SSL)** έχουν σχεδιαστεί με σκοπό να επιτύχουν ασφαλή επικοινωνία στο Διαδίκτυο, αν και το SSL χρησιμοποιείται κυρίως για web εφαρμογές. Το **Secure HTTP (S-HTTP)** και το **Secure MIME (S/MIME)**, από την άλλη πλευρά, στοχεύουν στην παροχή αυθεντικοποίησης και εμπιστευτικότητας στις εφαρμογές (το S-HTTP για web εφαρμογές και το S/MIME για ηλεκτρονικό ταχυδρομείο και συναφείς εφαρμογές). Το SET προχωρά ένα βήμα περισσότερο προσφέροντας ασφάλεια στις συναλλαγές ηλεκτρονικού εμπορίου.

ΑΣΦΑΛΕΙΑ ΣΤΟ WEB

Secure HTTP

Το secure HTTP αναπτύχθηκε με σκοπό να παρέχει ασφαλείς μηχανισμούς επικοινωνίας μεταξύ HTTP πελατών και εξυπηρετητών και να τους δώσει τη δυνατότητα για ασφαλείς εμπορικές συναλλαγές. Είναι ένα ασφαλές, προσανατολισμένο σε μηνύματα πρωτόκολλο, που σχεδιάστηκε για χρήση σε συνδυασμό με το απλό HTTP. Παρέχει ένα πλήθος από μηχανισμούς ασφάλειας και στους πελάτες και στους εξυπηρετητές, με συμμετρικές υπηρεσίες και δυνατότητες και για τους δύο, ενώ παράλληλα διατηρεί το μοντέλο επικοινωνίας και τα χαρακτηριστικά του HTTP.

Το S-HTTP παρέχει ασφαλείς από άκρο-εις-άκρο συναλλαγές, αντίθετα με τους μηχανισμούς εξουσιοδότησης στο HTTP, καθώς οι πελάτες ωθούνται στο να αρχίζουν ασφαλείς συναλλαγές χρησιμοποιώντας πληροφορίες στις επικεφαλίδες των μηνυμάτων. Με το S-HTTP καμιά «ευαίσθητη» πληροφορία δεν είναι ανάγκη να μεταδοθεί στο δίκτυο ανέλεγκτα. Επίσης το S-HTTP παρέχει πλήρη ευελιξία σε αλγορίθμους κρυπτογράφησης και παραμέτρους.

Το μοντέλο επεξεργασίας

Προετοιμασία μηνύματος

Η δημιουργία ενός S-HTTP μηνύματος γίνεται από τον αποστολέα ενσωματώνοντας τις δικές του κρυπτογραφικές επιλογές με αυτές του παραλήπτη. Το αποτέλεσμα είναι μία λίστα από κρυπτογραφικές εμπλουτίσεις και κλειδιά, έτοιμα να εφαρμοστούν. Για να γίνει αυτό, μπορεί να χρειαστεί η μεσολάβηση του χρήστη. Για παράδειγμα, μπορεί να παρέχονται πολλά κλειδιά για να υπογραφεί το μήνυμα. Με βάση αυτά τα δεδομένα, ο αποστολές εφαρμόζει τις εμπλουτίσεις στο κείμενο του μηνύματος και δημιουργεί ένα S-HTTP μήνυμα.

Ανάκτηση μηνύματος

Ο αποστολέας μπορεί ήδη να έχει δηλώσει ότι θα εκτελέσει κάποιες κρυπτογραφικές λειτουργίες πάνω στο μήνυμα. Για να ανακτήσει το S-HTTP μήνυμα, ο παραλήπτης πρέπει να διαβάσει τις επικεφαλίδες για να

ανακαλύψει ποιες κρυπτογραφικοί μετασχηματισμοί έγιναν στο μήνυμα, μετά να αφαιρέσει τους μετασχηματισμούς, χρησιμοποιώντας κάποιο συνδυασμό των κλειδιών του αποστολέα και του παραλήπτη, ενώ παράλληλα θα σημειώνει ποιες εμπλουτίσεις έγιναν. Ο παραλήπτης μπορεί επίσης να επιλέξει να επικυρώσει ότι οι εφαρμοσμένες εμπλουτίσεις ταιριάζουν τόσο με τις εμπλουτίσεις που ο αποστολέας είπε ότι θα εφάρμοζε όσο και με αυτά που ο παραλήπτης ζήτησε, καθώς και με τις τρέχουσες κρυπτογραφικές προτιμήσεις, για να δει αν το S-HTTP μήνυμα μετασχηματίστηκε κατάλληλα. Αυτή η διαδικασία μπορεί να απαιτεί αλληλεπίδραση με το χρήστη για να επικυρώσει ότι οι εμπλουτίσεις είναι αποδεκτές στο χρήστη.

Διαπραγμάτευση

Για να προσφέρουν ευελιξία στα κρυπτογραφικές εμπλουτίσεις που χρησιμοποιούνται, ο πελάτης και ο εξυπηρετητής διαπραγματεύονται τις εμπλουτίσεις που ο καθένας προτίθεται να χρησιμοποιήσει, δεν προτίθεται να χρησιμοποιήσει, ή θα απαιτήσει να χρησιμοποιηθούν. Τα μπλοκ διαπραγμάτευσης αποτελούνται από τέσσερα μέρη: *ιδιότητα*, *τιμή, κατεύθυνση* και *ένταση*. Εάν οι πράκτορες δεν είναι ικανοί να ανακαλύψουν ένα κοινό σύνολο αλγορίθμων θα πρέπει να γίνουν οι κατάλληλες ενέργειες. Η συνεχής αίτηση μιας αρνούμενης επιλογής θεωρείται αναποτελεσματική και ακατάλληλη.

Προστασία του μηνύματος

Η προστασία του μηνύματος μπορεί να παρέχεται σε τρεις άξονες:

- Υπογραφή
- Εξακρίβωση γνησιότητας
- Κρυπτογράφηση

Πολλαπλοί μηχανισμοί διαχείρισης κλειδιού υποστηρίζονται, συμπεριλαμβανομένου διαμοιραζόμενων μυστικών, με στυλ κωδικών, ανταλλαγή δημοσίου κλειδιού και διανομή εισιτηρίου (ticket) στον Κέρβερο. Συγκεκριμένα έχει γίνει πρόβλεψη για προκαθορισμένα συμμετρικά session κλειδιά με σκοπό να σταλούν εμπιστευτικά μηνύματα σε αυτούς που δεν έχουν ζευγάρι δημόσιου/ιδιωτικού κλειδιού. Επιπρόσθετα ένας μηχανισμός απόκρισης-πρόκλησης («nonce») παρέχεται για να επιτρέπει σε όσους θέλουν να επιβεβαιωθούν για το ότι η συναλλαγή έχει γίνει πρόσφατα.

Υπογραφή

Αν εφαρμόζεται ο εμπλουτισμός της ηλεκτρονικής υπογραφής, είτε ένα κατάλληλο πιστοποιητικό μπορεί να προσαρτηθεί στο μήνυμα, είτε ο αποστολέας μπορεί να αναμένει από τον παραλήπτη να αποκτήσει το απαιτούμενο πιστοποιητικό ανεξάρτητα.

Ανταλλαγή κλειδιών και κρυπτογράφηση

Για την υποστήριξη της bulk κρυπτογράφησης, το S-HTTP ορίζει δύο μηχανισμούς μεταφοράς κλειδιού, έναν που χρησιμοποιεί ανταλλαγή κρυπτογραφημένου κλειδιού και έναν άλλο με κλειδιά που είναι κανονισμένα εξωτερικά. Στην πρώτη περίπτωση, η παράμετρος του συστήματος συμμετρικής κρυπτογράφησης περνιέται κρυπτογραφημένη με το δημόσιο κλειδί του παραλήπτη. Στην άλλη περίπτωση κρυπτογραφούμε το περιεχόμενο χρησιμοποιώντας ένα καθορισμένο session κλειδί με τις πληροφορίες αναγνώρισης κλειδιού να ορίζονται σε μία από τις γραμμές της επικεφαλίδας. Τα κλειδιά μπορούν ακόμα να εξαχθούν από τα εισιτήρια του Κέρβερου.

Γνησιότητα μηνύματος και Αποστολέα

Το S-HTTP παρέχει ένα τρόπο για να επικυρώνει την ακεραιότητα του μηνύματος και την εξακρίβωση γνησιότητας του αποστολέα για ένα μήνυμα μέσω του υπολογισμού ενός κωδικού εξακρίβωσης γνησιότητας μηνύματος (**Message Authentication Code** – **MAC**), που υπολογίζεται σαν ένα hash κλειδιού πάνω από το κείμενο, χρησιμοποιώντας ένα διαμοιραζόμενο μυστικό-το οποίο θα μπορούσε να έχει κανονιστεί με διάφορους τρόπους. Αυτή η τεχνική δεν απαιτεί ούτε τη χρήση κρυπτογραφίας δημοσίου κλειδιού, ούτε κρυπτογράφησης.

Ανανέωση

Το πρωτόκολλο παρέχει ένα απλό μηχανισμό απόκρισης/πρόκλησης, επιτρέποντας και στα δύο μέρη να επιβεβαιώσουν ότι οι μεταδόσεις έγιναν πρόσφατα. Επιπρόσθετα, η προστασία της ακεραιότητας που

παρέχεται στις επικεφαλίδες του HTTP, αποδέχεται οι υλοποιήσεις να θεωρούν την επικεφαλίδα «Date:» ως ένα δείκτη ανανέωσης, όπου είναι δυνατό.

Nonces

Τα Nonces είναι αδιαφανείς, προσωρινοί, προσανατολισμένοι-στη-σύνοδο (session-oriented) identifiers, που μπορούν να χρησιμοποιηθούν για να παρέχουν μία ένδειξη ανανέωσης. Οι τιμές των nonces είναι ένα θέμα τοπικό, αν και μπορεί απλά να είναι τυχαίοι αριθμοί που παράγονται από τον αποστολέα. Η τιμή παρέχεται απλά για να επιστραφεί από τον παραλήπτη.

Μορφή του μηνύματος

Η σύνταξη του S-HTTP επίτηδες μιμείται τη σύνταξη του HTTP σε μία προσπάθεια να διευκολύνει την ενσωμάτωση στα συστήματα που ήδη χρησιμοποιούν το HTTP. Επιπλέον, ορισμένες HTTP επικεφαλίδες γίνονται S-HTTP επικεφαλίδες, γιατί παρέχουν χρήσιμες λειτουργίες που έχουν προεκτάσεις στην ασφάλεια.

Ένα S-HTTP μήνυμα αποτελείται από μία γραμμή αίτησης ή κατάστασης (όπως και στο HTTP) ακολουθούμενη από τις επικεφαλίδες που καθορίζονται στο RFC-822, ακολουθούμενα από ένα κρυμμένο κείμενο. Όταν ανακτάται το περιεχόμενο του κειμένου, μπορεί να είναι είτε ένα άλλο S-HTTP μήνυμα, είτε απλά δεδομένα.

Επικεφαλίδες

Οι επικεφαλίδες που έχουν προστεθεί περιγράφονται στον παρακάτω πίνακα Το S-HTTP παρέχει διάφορες δυνατότητες για το στάνταρ που θα ακολουθηθεί στη μορφή του μηνύματος από τους πελάτες και τους εξυπηρετητές, αλλά κυρίως χρησιμοποιούνται το [PKCS-7] και το [MOSS].

Όνομα παραμέτρου	**προαιρετική/ απαιτούμενη**	**Ερμηνεία**	**πιθανές τιμές**
Content-Privacy-domain	απαιτούμενη	μορφή ενθυλακωμένου περιεχομένου	‘MOSS’,”PKCS-7’
Content-Transfer-Encoding	προαιρετική	μέθοδος κωδικοποίησης	‘BASE64’, ‘8BIT’ και όλες οι κωδικοποιήσεις του MOSS
Content-Type	απαιτούμενη	τύπος	application/http application/shttp
Prearranged-Key-Info	προαιρετική	πληροφορία σχετική με το κλειδί που χρησιμοποιείται στην ενθυλάκωση του μηνύματος, για την ανταλλαγή κλειδιών	εσωτερικό (inband), εξωτερικό (outband), Κέρβερου
MAC-info	προαιρετική	ένα κωδικός (MAC) για την εξακρίβωση της γνησιότητας του μηνύματος	-

Πίνακας 1.2 **Οι επικεφαλίδες του μηνύματος στο S-HTTP**

Ορισμένες HTTP ευκολίες, και ιδιαίτερα εκείνες που αναφέρονται με το caching και τους αντιπροσώπους (proxies), απαιτούν ειδική θεώρηση, όταν εφαρμόζεται S-HTTP επεξεργασία. Το S-HTTP παρέχει ειδική μεταχείριση για αυτά τα χαρακτηριστικά, αντιγράφοντας τις σχετικές HTTP επικεφαλίδες με S-HTTP σύνταξη. Οι επικεφαλίδες που έχουν εισαχθεί από το HTTP φαίνονται στον παρακάτω πίνακα.

Όνομα παραμέτρου	**Ερμηνεία**
Connection: Keep-Alive	Σχεδιασμένο για να επιτρέπει επίμονες συνδέσεις μεταξύ πελάτη/αντιπροσώπου και αντιπροσώπου/εξυπηρετητη
IF-Modified-Since	μπορεί να χρησιμοποιηθεί από τον αντιπρόσωπο για να δείξει ότι το έγγραφο μπορεί να βρίσκεται στην προσωρινή του μνήμη

Content-MD5	χρησιμοποιείται από τους εξυπηρετητές για να δίνουν τη δυνατότητα στους αντιπροσώπους να ανιχνεύουν αν έγιναν έγκυρες προσπελάσεις της ενδιάμεσης μνήμης.

Πίνακας 1.3.: **Οι επικεφαλίδες που έχουν εισαχθεί από το HTTP**

Μια θεώρηση του αντιπροσώπου (Proxy)

Η χρήση του S-HTTP παρουσιάζει και κάποια θέματα υλοποίησης στη χρήση των HTTP αντιπροσώπων. Ενώ είναι απλό να επιτρέπεις στον αντιπρόσωπο να προωθεί τις αιτήσεις, θα ήταν προτιμότερο να μπορούσαν οι S-HTTP αντιπρόσωποι να κρατάνε σε προσωρινή μνήμη (Cache) τις απαντήσεις, τουλάχιστο σε ορισμένες περιπτώσεις. Επιπλέον, το S-HTTP παρέχει εξακρίβωση γνησιότητας σε πελάτη και σε αντιπρόσωπο.

Εξακρίβωση γνησιότητας πελάτη αντιπροσώπου

Όταν ένας S-HTTP αντιπρόσωπος παραλαμβάνει μία αίτηση (S-HTTP ή HTTP) που απαιτεί να εξακριβωθεί η προέλευσή της, επιστρέφει τον κωδικό κατάστασης 422. Ο πελάτης, που λαμβάνει την απάντηση αυτή διαβάζει τις κρυπτογραφικές επιλογές που έστειλε ο αντιπρόσωπος και αν είναι πρόθυμος να παρέχει αυτές τις εμπλουτίσεις στο μήνυμα, ενθυλακώνει το προηγούμενο μήνυμα, χρησιμοποιώντας τις ζητούμενες επιλογές.Προσωρινή αποθήκευση (caching) στον αντιπρόσωπο

Αν και είναι καλό να αποφεύγεται η προσωρινή αποθήκευση (caching) για λόγους ασφάλειας και εμπιστευτικότητας, αυτό συμβαίνει μόνο σε ορισμένες περιπτώσεις, π.χ. όταν η εμπιστευτικότητα χρησιμοποιείται για να περιορίσει την πρόσβαση ορισμένων χρηστών σε μία κλάση εγγράφων.

Για να ζητήσει δεδομένα που έχουν αποθηκευτεί προσωρινά στον αντιπρόσωπο, ο πελάτης στέλνει στον αντιπρόσωπο ολόκληρη τη γραμμή του URL για να του δώσει να καταλάβει ότι ζητούνται αποθηκευμένα δεδομένα. Ο αντιπρόσωπος πρέπει να αναγνωρίζει ποια URLs βρίσκονται στην προσωρινή του μνήμη και να ελέγχει την επικεφαλίδα **Content-MD5** για να είναι σίγουρος ότι συνέβη μία έγκυρη αίτηση στην προσωρινή μνήμη.

Socket Secure Layer (SSL)

Το SSL προήλθε από την Netscape. Όταν ήρθε η ανάγκη για τυποποίηση στο Internet, η ομάδα TLS σχηματίστηκε στην IETF για να αναπτύξει ένα κοινό πρότυπο.

SSL αρχιτεκτονική

Το SSL έχει σχεδιαστεί ώστε να κάνει χρήση του TCP και να παρέχει αξιόπιστη end-to-end ασφαλή υπηρεσία. Μάλιστα, το SSL δεν είναι ένα πρωτόκολλο αλλά δύο επίπεδα πρωτοκόλλων, όπως φαίνεται στο παρακάτω σχήμα.

<table>
<tr><td>SSL Handshake Protocol</td><td>SSL Change Ciphert Spec Protocol</td><td>SSL Alert Protocol</td><td>HTTP</td></tr>
<tr><td colspan="4">SSL Record Protocol</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

Σχήμα 1-4: **SSL Protocol Stack**

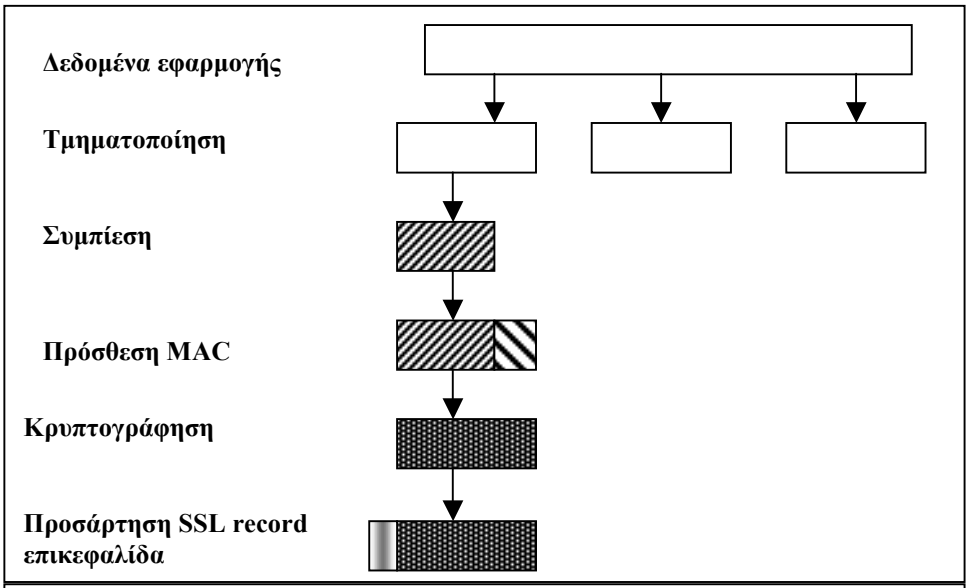
Το **SSL Record Protocol** παρέχει βασικές υπηρεσίες ασφάλειας σε διάφορα πρωτόκολλα υψηλότερων επιπέδων, όπως το HTTP. Τρία πρωτόκολλα υψηλότερων επιπέδων ορίζονται ως μέρη του SSL: το *Handshake Protocol*, το *Change Cipher Spec Protocol* και το *Alert Protocol*. Αυτά τα SSL-specific πρωτόκολλα χρησιμεύουν στη διαχείριση των SSL ανταλλαγών.

SSL Record Protocol

Το SSL Record Protocol παρέχει δύο υπηρεσίες για SSL συνδέσεις:

- *εμπιστευτικότητα*: Το Handshake Protocol ορίζει ένα διαμοιραζόμενο μυστικό κλειδί που χρησιμεύει στη συμβατική κρυπτογράφηση των SSL payloads.
- *ακεραιότητα μηνύματος*: Το Handshake Protocol επίσης ορίζει ένα διαμοιραζόμενο μυστικό κλειδί που χρησιμοποιείται για το σχηματισμο του **message authentication code** (**MAC**).

Το σχήμα 6-3 φανερώνει τη λειτουργία του SSL Record Protocol. Το Record Protocol παίρνει το μήνυμα της εφαρμογής που θα μεταδοθεί, τμηματοποιεί τα δεδομένα σε εύχρηστα blocks, προαιρετικά συμπιέζει τα δεδομένα, εφαρμόζει ένα MAC, κρυπτογραφεί, προσθέτει μια επικεφαλίδα, και μεταδίδει το αποτέλεσμα αυτό σε ένα TCP segment. Τα δεδομένα που λαμβάνονται αποκρυπτογραφούνται, επιβεβαιώνονται, αποσυμπιέζονται, επανασυγκεντρώνονται και διανέμονται στους χρήστες των ανώτερων επιπέδων.



Σχήμα 1-5: **Λειτουργία του SSL Record Protocol**

Το πρώτο βήμα είναι η τμηματοποίηση. Κάθε μήνυμα υψηλότερού επιπέδου τμηματοποιείται σε blocks των 214 bytes (16384 bytes) ή λιγότερο. Η συμπίεση εφαρμόζεται προαιρετικά. Το επόμενο βήμα είναι να υπολογιστεί το message authentication code πάνω από τα συμπιεσμένα δεδομένα. Για αυτό το σκοπό χρησιμοποιείται ένα διαμοιραζόμενο μυστικό κλειδί. Στη συνέχεια, το αποτέλεσμα κρυπτογραφείται χρησιμοποιώντας συμμετρική κρυπτογράφηση. Οι παρακάτω αλγόριθμοι είναι επιτρεπτοί:

Clock Cipher		**Stream Cipher**	
Αλγόριθμος	**Μέγεθος κλειδιού**	**Αλγόριθμος**	**Μέγεθος κλειδιού**
IDEA	128	RC4-40	40
RC2-40	40	RC4-128	128
DES-40	40		
DES	56		
3DES	168		
Fortezza	80		

Πίνακας 1-6: **Αλγόριθμοι του SSL record protocol**

Για την κρυπτογράφηση ρεύματος, το συμπιεσμένο μήνυμα μαζί με το MAC κρυπτογραφούνται. Για block κρυπτογράφηση, μπορεί να προστεθεί padding μετά το MAC πριν τη κρυπτογράφηση. Το τελικό βήμα της επεξεργασίας του SSL Record Protocol είναι η προσθήκη μιας επικεφαλίδας με τα ακόλουθα στοιχεία:

- Τύπος περιεχομένου,

- Κύρια έκδοση,
- Δευτερεύουσα έκδοση,
- Συμπιεσμένο μήκος.

Change Cipher Spec Protocol

Είναι το απλούστερο από τα τρία SSL-specific πρωτόκολλα που χρησιμοποιούν το SSL Record Protocol. Αποτελείται από ένα απλό μήνυμα μήκους ενός byte με τιμή ίση με 1. Ο μόνος σκοπός αυτού του μηνύματος είναι να προκαλέσει την εκκρεμή κατάσταση να αντιγραφεί στην τρέχουσα κατάσταση που ενημερώνει το cipher suite να χρησιμοποιηθεί σε αυτή τη σύνδεση.

Alert Protocol

Χρησιμοποιείται για να μεταφέρει συναγερμούς στην ομότιμη οντότητα. Κάθε μήνυμα στο πρωτόκολλο αποτελείται από δύο bytes. Το πρώτο byte παίρνει την τιμή **προειδοποίηση** (1) ή **μοιραίο** (2) για να μεταφέρει τη σημασία του μηνύματος. Το δεύτερο byte περιέχει ένα κώδικα που ορίζει το συγκεκριμένο συναγερμό.

Handshake Protocol

Το πιο περίπλοκο τμήμα του SSL είναι το Handshake Protocol. Αυτό το πρωτόκολλο επιτρέπει στον server και τον client να εξακριβώσουν την γνησιότητα του άλλου, να διαπραγματευτούν τον αλγόριθμο κρυπτογράφησης και MAC, και τα κλειδιά κρυπτογράφησης που θα προστατέψουν τα δεδομένα στο SSL record. Το handshake protocol χρησιμοποιείται πριν μεταδοθούν τα δεδομένα. Αποτελείται από μια σειρά μηνυμάτων που ανταλλάσσονται μεταξύ του client και του server. Κάθε μήνυμα έχει τρία πεδία:

- Τύπος (1 byte),
- Μήκος (3 bytes) και
- Περιεχόμενο (>1 byte).

Η ανταλλαγή μηνυμάτων μπορεί να θεωρηθεί ότι έχει τέσσερις φάσεις.

Φάση 1. Εγκατάσταση Ικανοτήτων Ασφάλειας

Η φάση αυτή χρησιμοποιείται για να αρχικοποιήσει μια λογική σύνδεση και να εγκαταστήσει τις ικανότητες ασφάλειας που θα συνδεθούν με αυτή. Αυτή η ανταλλαγή αρχικοποιείται από τον client, που στέλνει μήνυμα **client_hello** με τις ακόλουθες παραμέτρους: έκδοση, random, session ID, Cipher Suite, μέθοδο συμπίεσης. Αφού σταλεί το μήνυμα αυτό, ο client περιμένει το μήνυμα **server_hello**, που έχει τις ίδιες παραμέτρους με αυτές του **client_hello**.

Φάση 2. Εξακρίβωση γνησιότητας Server και Ανταλλαγή κλειδιών

Ο server ξεκινά αυτή τη φάση στέλνοντας το πιστοποιητικό του, εάν χρειάζεται να εξακριβωθεί η γνησιότητά του. Το μήνυμα **certificate** απαιτείται για οποιαδήποτε συμφωνημένη μέθοδο ανταλλαγής, εκτός από τη μέθοδο anonymous Diffie-Hellman. Στη συνέχεια, ένα μήνυμα **server_key_exchange** μπορεί να σταλεί αν αυτό απαιτείται. Μετά ένας non-anonymous server μπορεί να απαιτήσει ένα πιστοποιητικό από τον πελάτη. Το μήνυμα **certificate_request** περιλαμβάνει δύο παραμέτρους: τύπο πιστοποιητικού και εξουσιοδοτήσεις πιστοποιητικού. Το τελικό μήνυμα της φάσης 2 είναι το **server_done**, που σηματοδοτεί το τέλος του μηνύματος **hello**.

Φάση 3. Εξακρίβωση γνησιότητας Client και Ανταλλαγή κλειδιών

Εάν ο server έχει απαιτήσει πιστοποιητικό, ο client αρχίζει τη φάση αυτή στέλνοντας μήνυμα **certificate**. Στη συνέχεια είναι το μήνυμα **client_key_exchange** που πρέπει να σταλεί σε αυτή την φάση. Τέλος, ο client μπορεί να στείλει ένα μήνυμα **certificate_verify** για να παρέχει επικύρωση του πιστοποιητικού.

Φάση 4. Τέλος

Αυτή η φάση ολοκληρώνει την εγκατάσταση μιας ασφαλούς σύνδεσης. Ο client στέλνει μήνυμα **change_cipher_spec** και αντιγράφει το εκκρεμές CipheSpec στο τρέχον CipherSpec. Μετά, ο client στέλνει το μήνυμα **finished** που επικυρώνει ότι οι διεργασίες ανταλλαγής κλειδιών και εξακρίβωσης γνησιότητας ήταν επιτυχημένες. Σε απάντηση αυτών των δύο μηνυμάτων, ο server στέλνει το δικό του μήνυμα **change_cipher_spec**, μεταφέρει το εκκρεμές CipherSpec στο τρέχον CipherSpec, και στέλνει το μήνυμα **finished**. Σε αυτό το σημείο το handshake έχει ολοκληρωθεί και ο client με τον server μπορούν να ξεκινήσουν να την ανταλλαγή δεδομένων του επιπέδου εφαρμογής.

Κλειδιά στο SSL

Υπάρχει ένας αριθμός από κλειδιά που χρησιμοποιούνται: το **δημόσιο κλειδί** του server, το **server-write-key**, και το **client-write-key**. Το server-write-key, και το client-write-key παράγονται μέσω μιας hash από το master key, ένα ordinal χαρακτήρα, την πρόκληση και το id της σύνδεσης.

ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ -SET

Το SET είναι μια ανοικτή προδιαγραφή κρυπτογράφησης και ασφάλειας που σχεδιάστηκε για να προστατέψει τις συναλλαγές με πιστωτικές κάρτες σε ένα ανοικτό δίκτυο, όπως το Internet. Από τον Απρίλιο του 1997, προγράμματα SET λαμβάνουν χώρα σε 39 χώρες παγκοσμίως όπως τις Η.Π.Α, Νότια Αφρική, Αυστραλία, Μαλαισία, Χονγκ-Κονγκ, Κορέα, Μεγάλη Βρετανία και Καναδά. Μάλιστα, νέες αγορές έρχονται στο προσκήνιο.

Το SET δεν είναι από μόνο του ένα σύστημα πληρωμής, αλλά ένα σύνολο από πρωτόκολλα και τυποποιήσεις που βοηθάνε τους χρήστες να χρησιμοποιήσουν την υπάρχουσα υποδομής πληρωμής με πιστωτικές κάρτες στο Internet, με ασφαλή τρόπο. Βασικά το SET προσφέρει τρεις υπηρεσίες:

- Παρέχει ένα ασφαλές κανάλι επικοινωνίας μεταξύ όλων των συμμέτοχων στη συναλλαγή.
- Παρέχει εμπιστοσύνη με τη χρήση των ηλεκτρονικών πιστοποιητικών (digital certificates) X.509v3 για να επιβεβαιώσει ότι οι καταναλωτές και οι έμποροι εξουσιοδοτούνται να χρησιμοποιούν και να δέχονται αντίστοιχα πιστωτικές κάρτες. Αυτό είναι το ηλεκτρονικό ισοδύναμο ενός καταναλωτή που ψάχνει την επιγραφή της πιστωτικής του εταιρείας στη βιτρίνα ενός καταστήματος, και του εμπόρου που ελέγχει την υπογραφή του καταναλωτή στο πίσω μέρος της πιστωτικής του κάρτας.
- Εγγυάται την μυστικότητα επειδή η πληροφορία είναι διαθέσιμη στους ενδιαφερομένους μόνο όταν και όπου αυτό είναι αναγκαίο. Έτσι η πληροφορία της κάρτας πληρωμής του καταναλωτή προστατεύεται έως ότου φτάσει στον οικονομικό οργανισμό. *Ο έμπορος δεν μπορεί να διαβάσει αυτή την πληροφορία στη συναλλαγή πληρωμής.*

ΓΕΝΙΚΗ ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ SET

ΑΠΑΙΤΗΣΕΙΣ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

Το SET ορίζει τις παρακάτω απαιτήσεις για ασφαλή επεξεργασία πληρωμής με πιστωτικές κάρτες πάνω από το Internet:

- Παρέχει εμπιστευτικότητα στις πληροφορίες πληρωμής και παραγγελίας.
- Εγγυάται την ακεραιότητα των μεταδιδόμενων δεδομένων.
- Παρέχει πιστοποίηση ότι ο κάτοχος της κάρτας είναι νόμιμος χρήστης του λογαριασμού της πιστωτικής κάρτας.
- Παρέχει πιστοποίηση ότι ο έμπορος μπορεί να δεχτεί συναλλαγές με πιστωτική κάρτα μέσω της συνεργασίας του με κάποιο οικονομικό οργανισμό.
- Εγγυάται τη χρήση των καλύτερων πρακτικών ασφαλείας και τεχνικών σχεδίασης συστημάτων για να προστατέψει όλους τους νόμιμους συμμέτοχους στη συναλλαγή ηλεκτρονικού εμπορίου.
- Δημιουργεί ένα πρωτόκολλο που δεν εξαρτάται από τους μηχανισμούς μεταφοράς ασφαλείας ούτε εμποδίζει την χρήση τους.
- Διευκολύνει και ενθαρρύνει την αλληλεπίδραση μεταξύ software και network providers.
-

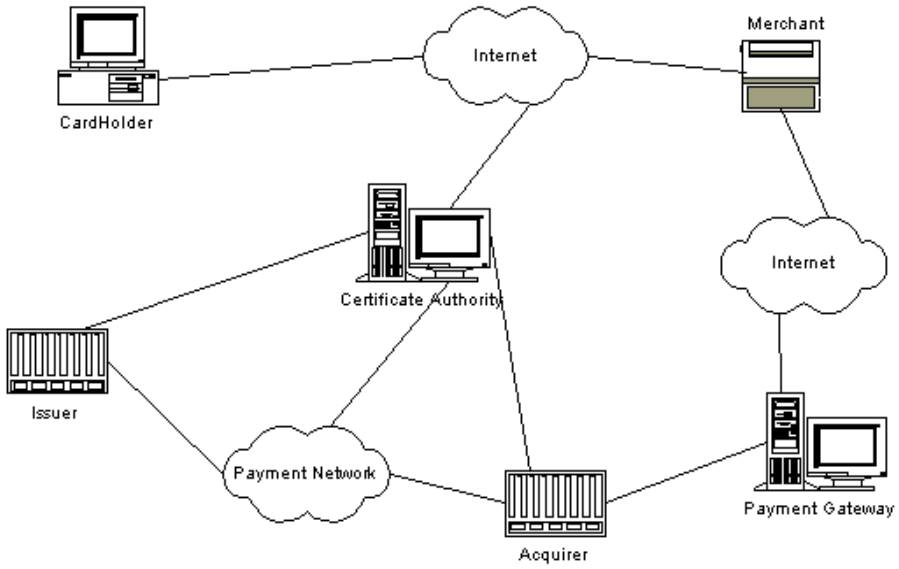
Το SET ενσωματώνει τα ακόλουθα χαρακτηριστικά:

- Εμπιστευτικότητα της πληροφορίας
- Ακεραιότητα των δεδομένων
- Εξακρίβωση γνησιότητας του λογαριασμού του κατόχου της κάρτας
- Εξακρίβωση γνησιότητας του εμπόρου

Οι συμμέτοχοι του SET

Η εικόνα 6.1 δείχνει τους συμμέτοχους στο σύστημα SET:

- **Κάτοχος της κάρτας**.
- **Έμπορος**.
- **Πάροχος (Issuer)**: Είναι οικονομικός οργανισμός, όπως μια τράπεζα, που παρέχει την πιστωτική κάρτα στον κάτοχο αυτής.
- **Acquirer**: Είναι οικονομικός οργανισμός που ανοίγει ένα λογαριασμό με ένα έμπορο και επεξεργάζεται τις πληρωμές και τις εξουσιοδοτήσεις πληρωμής των καρτών.
- **Payment Gateway**: Είναι μια λειτουργία που επιτελείται από τον acquirer ή κάποιο τρίτο, και επεξεργάζεται τα μηνύματα πληρωμής του εμπόρου.
- **Υπηρεσία πιστοποίησης** (**Certificate Authority**): Είναι μια οντότητα που εκδίδει X.509v3 πιστοποιητικά δημοσίου-κλειδιού σε κατόχους κάρτας, εμπόρους, και payment gateways.



Εικόνα 1-7 Συμμέτοχοι στο σύστημα SET

Η συναλλαγή στο SET

Περιγράφουμε την ακολουθία των γεγονότων που απαιτούνται για μια συναλλαγή.

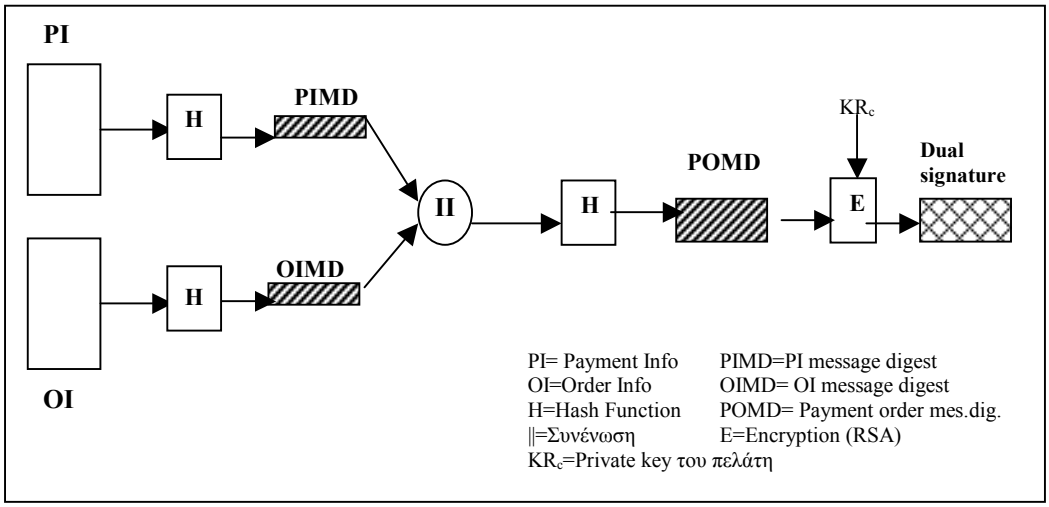
1. Ο πελάτης αποκτά το ηλεκτρονικό πορτοφόλι (digital wallet), το software που επικοινωνεί με το SET software του εμπόρου αυτόματα για να επιβεβαιώσει το πιστοποιητικό του εμπόρου και τη σχέση του με ένα έμπιστο οικονομικό οργανισμό.
2. Ο πελάτης ανοίγει ένα λογαριασμό, από μια τράπεζα που υποστηρίζει ηλεκτρονική πληρωμή και SET.
3. Ο πελάτης λαμβάνει ένα X.509v3 ηλεκτρονικό πιστοποιητικό, το οποίο επιβεβαιώνει το δημόσιο-κλειδί RSA του πελάτη και την ημερομηνία λήξης του πιστοποιητικού.
4. Οι έμποροι έχουν τα δικά τους πιστοποιητικά: ένα πιστοποιητικό δημοσίου-κλειδιού για την υπογραφή μηνυμάτων και ένα άλλο για την ανταλλαγή κλειδιού.

5. Ο πελάτης κάνει μια παραγγελία.
6. Ο έμπορος επιβεβαιώνεται, δηλαδή στέλνει ένα αντίγραφο του πιστοποιητικού του στον πελάτη.
7. Η παραγγελία και η πληρωμή στέλνονται στον έμπορο, μαζί με το πιστοποιητικό του πελάτη.
8. Ο έμπορος ζητά εξουσιοδότηση πληρωμής από το payment gateway, δηλαδή ότι η πίστωση του πελάτη είναι επαρκής για την αγορά.
9. Ο έμπορος επιβεβαιώνει την παραγγελία στον πελάτη.
10. Ο έμπορος παρέχει τα αγαθά ή την υπηρεσία.

Ο έμπορος απαιτεί την πληρωμή από το payment gateway, που χειρίζεται την επεξεργασία πληρωμών.

ΚΑΙΝΟΤΟΜΙΑ ΤΟΥ SET : Η διπλή υπογραφή

Μια σημαντική καινοτομία που εισάγεται στο SET είναι η διπλή υπογραφή (dual signature). Ο σκοπός της είναι να συνδέσει δύο μηνύματα που απευθύνονται σε δύο διαφορετικούς παραλήπτες. Ο πελάτης θέλει να στείλει την *πληροφορία παραγγελίας* (**Order Information - OI**) στον έμπορο και την *πληροφορία πληρωμής* (**Payment Information - PI**) στην τράπεζα, και του παρέχεται επιπλέον προστασία σε μυστικότητα για να κρατήσει ξεχωριστά αυτά τα δύο αντικείμενα. Ο σύνδεσμος χρειάζεται έτσι ώστε ο πελάτης να μπορεί να αποδείξει ότι αυτή η πληρωμή προορίζεται για τη συγκεκριμένη παραγγελία και όχι για άλλα αγαθά ή υπηρεσία.
Ας υποθέσουμε ότι ο πελάτης στέλνει δύο μηνύματα στον έμπορο- ένα υπογεγραμμένο OI και ένα υπογεγραμμένο PI - και ότι ο έμπορος δίνει το PI στην τράπεζα. Αν ο έμπορος μπορεί να αποκτήσει άλλο OI από τον πελάτη θα μπορούσε να ισχυριστεί ότι το δεύτερο OI πηγαίνει με το PI αντί για το γνήσιο OI.
Η παρακάτω εικόνα δείχνει την κατασκευή της διπλής υπογραφής. Ο πελάτης παίρνει το hash του PI και το hash του OI. Αυτά τα δύο hashes συνενώνονται και το αποτέλεσμα το κάνουμε hash. Ο πελάτης κρυπτογραφεί το τελικό hash με το ιδιωτικό του κλειδί, δημιουργώντας έτσι την διπλή υπογραφή.



Εικόνα 1-8

Ετσι, ο έμπορος όταν λάβει το OI και τη διπλή υπογραφή (DS) μπορεί να την επιβεβαιώσει. Η τράπεζα όταν λάβει το PI και το DS μπορεί να επιβεβαιώσει την υπογραφή. Ο πελάτης έχει συνδέσει το OI και το PI και μπορεί να αποδείξει το σύνδεσμο.
Από τους τύπους συναλλαγών του SET οι πιο σημαντικοί είναι οι παρακάτω:

Τύποι Συναλλαγών

ΑΙΤΗΣΗ ΑΓΟΡΑΣ (PURCHASE REQUEST)

Η ανταλλαγή αίτησης αγοράς αποτελείται από τέσσερα μηνύματα: Initiate Request, Initiate Response, Purchase Request, και Purchase Response. Ο κάτοχος της κάρτας πρέπει να έχει αντίγραφα των πιστοποιητικών του εμπόρου και του payment gateway, οπότε και ζητά τα πιστοποιητικά αυτά στο μήνυμα **Initiate Request** προς τον έμπορο. Ο έμπορος αποκρίνεται και υπογράφει με το ιδιωτικό του κλειδί. Το **Initiate Response** μήνυμα περιλαμβάνει τα πιστοποιητικά του εμπόρου και του payment gateway. Ο κάτοχος της κάρτας επιβεβαιώνει τα πιστοποιητικά μέσω των αντίστοιχων CA υπογραφών τους, και στη συνέχεια

δημιουργεί το OI και το PI. Μετά, ετοιμάζει το **Purchase Request** μήνυμα, και για αυτό το σκοπό παράγει ένα one-time συμμετρικό κλειδί κρυπτογράφησης, το K_s. Το μήνυμα περιλαμβάνει τα ακόλουθα:

- Πληροφορία σχετική με την αγορά. Αυτή η πληροφορία θα προωθηθεί στο payment gateway από τον έμπορο.
- Πληροφορία σχετικά με την παραγγελία. Αυτή η πληροφορία χρειάζεται από τον έμπορο.
- Πιστοποιητικό του κατόχου της κάρτας. Αυτό περιέχει το δημόσιο κλειδί του κατόχου, και χρειάζεται από τον έμπορο και το payment gateway.

Όταν ο έμπορος λάβει το μήνυμα Purchase Request, εκτελεί τις παρακάτω ενέργειες:

- Επιβεβαιώνει τα πιστοποιητικά του κατόχου της κάρτας.
- Επιβεβαιώνει τη διπλή υπογραφή, χρησιμοποιώντας το δημόσιο κλειδί του πελάτη.
- Επεξεργάζεται την παραγγελία και προωθεί την πληροφορία πληρωμής στο payment gateway.
- Στέλνει μήνυμα purchase response στον κάτοχο της κάρτας.

ΜΗΝΥΜΑ ΑΠΟΚΡΙΣΗΣ ΑΓΟΡΑΣ (PURCHASE RESPONSE)

Αποτελείται από ένα block απόκρισης που αναγνωρίζει την παραγγελία και αναφέρει τον κατάλληλο αριθμό συναλλαγής. Όταν το software του κατόχου της κάρτας λάβει το μήνυμα, επιβεβαιώνει το πιστοποιητικό του εμπόρου και την υπογραφή στο block απόκρισης.

ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΠΛΗΡΩΜΗΣ (PURCHASE AUTHORIZATION)

Η εξουσιοδότηση πληρωμής εγγυάται ότι η συναλλαγή έγινε δεκτή από τον issuer, δηλαδή ότι ο έμπορος θα πληρωθεί. Στη συνέχεια ο έμπορος μπορεί να παρέχει τις υπηρεσίες ή τα αγαθά στον πελάτη.
Ο έμπορος στέλνει ένα μήνυμα **Authorization Request** στο payment gateway που αποτελείται από

- Πληροφορίες σχετικές με την αγορά
- Πληροφορίες σχετικές με την εξουσιοδότηση
- Πιστοποιητικά

Το payment gateway έχοντας αποκτήσει την εξουσιοδότηση από τον issuer, επιστρέφει μήνυμα Authorization Response στον έμπορο, που περιλαμβάνει τα ακόλουθα:

- Πληροφορίες σχετικές με την εξουσιοδότηση
- Capture token πληροφορία. Αυτή η πληροφορία θα χρησιμοποιηθεί για να πραγματοποιηθεί η πληρωμή αργότερα.
- Πιστοποιητικό του gateway

ΑΠΟΚΤΗΣΗ ΠΛΗΡΩΜΗΣ (PAYMENT CAPTURE)

Για να πληρωθεί ο έμπορος, ανταλλάσσει με το payment gateway ένα μήνυμα capture request και ένα μήνυμα capture response. Το **Capture Request** μήνυμα περιλαμβάνει το ποσό πληρωμής, το id της συναλλαγής και το capture token από το Authorization Response. Όταν το payment gateway λάβει το μήνυμα αφού ελέγξει για τη συνέπεια μεταξύ του capture request και του capture token, δημιουργεί ένα αίτημα συμψηφισμού που στέλνεται στον issuer, και έτσι μεταφέρονται τα χρήματα στο λογαριασμό του εμπόρου. Εν συνεχεία, το gateway ειδοποιεί τον έμπορο για την πληρωμή με ένα μήνυμα **Capture Response**.

Πρέπει να τονιστεί ότι το SET δεν επηρεάζει την απόδοση του συστήματος ή της συναλλαγής. Μελέτη του Gartner Group το 1998, δείχνει ότι η απόδοση των εγκαταστάσεων SET™ είναι περισσότερο από επαρκής για απαιτήσεις μεγάλου όγκου συναλλαγών

Ασφάλεια στο ηλεκτρονικό ταχυδρομείο: PEM, S/MIME και PGP

Όσον αφορά, τώρα, την προστασία των ηλεκτρονικών ταχυδρομείων ενδεικτικά αναφέρουμε τα εξής standards:

- Privacy Enhanced Mail (PEM) το οποίο όμως έχει ιστορική αξία πλέον,
- MOSS, το οποίο δεν έτυχε ιδιαίτερης εμπορικής υποστήριξης,

- Pretty Good Privacy (PGP), το οποίο αποτελείται από πέντε υπηρεσίες: κρυπτογράφηση μηνύματος, ψηφιακή υπογραφή, συμπίεση, e-mail συμβατότητα, κατάτμηση

PRIVACY ENHANCED MAIL (PEM)

Το **Privacy Enhanced Mail (PEM)** είναι ένα στάνταρτ για την ασφάλεια ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας συμμετρική ή ασύμμετρη κρυπτογραφία. Το PEM έχει φθίνουσα πορεία διότι αδυνατεί να διαχειριστεί το νεώτερο πολυμελές ηλεκτρονικό ταχυδρομείο (multipart e-mail) το οποίο υποστηρίζεται από το MIME (Multipurpose Internet Mail Extensions), ενώ απαιτεί αυστηρή ιεραρχία αρχών πιστοποίησης για να εκδώσει κλειδιά.

S/MIME (Multipurpose Internet Mail)

Το S/MIME είναι ένα standard για αποστολή αρχείων με binary attachments μέσω του internet.Το Secure/MIME είναι μια επέκταση του MIME standard για την αναγνώριση των κρυπτογραφημένων e-mail.Αντίθετα από το PGP ,το S/MIME δεν εφαρμόσθηκε σαν ένα αυτόνομο πρόγραμμα , αλλά σαν ένα εργαλείο που σχεδιάστηκε για να προστίθεται σε διάφορα πακέτα ηλεκτρονικού ταχυδρομείου .Επειδή το εργαλείο προέρχεται από την RSA Data Security και περιλαμβάνει άδειες για όλους τους απαιτούμενους αλγόριθμους και όλες τις πατέντες , και επειδή οι μεγαλύτερες εταιρείες που πουλούν συστήματα e-mail ήδη έχουν επιχειρηματική σχέση με την RSA Data Security , είναι πιθανό το S/MIME να υιοθετηθεί περισσότερο από το PGP, από τους πωλητές e-mail προγραμμάτων.

Το S/MIME προσφέρει εμπιστευτικότητα , εξαιτίας του ότι ο κρυπτογραφικός αλγόριθμος καθορίζεται από τον χρήστη. Προσφέρει ακεραιότητα , εξαιτίας του ότι η συνάρτηση αποσύνθεσης καθορίζεται από τον χρήστη. Προσφέρει αναγνώρισης γνησιότητας με την χρήση των X.509 v3 δημοσίου κλειδιού πιστοποιητικών και προσφέρει και απαγόρευση απάρνησης λόγω των κρυπτογραφικά υπογεγραμμένων μηνυμάτων. Το σύστημα μπορεί να χρησιμοποιηθεί με δυνατή ή αδύνατη κρυπτογράφηση .

Για να στείλουμε κρυπτογραφημένα μηνύματα σε κάποιον με το S/MIME ,πρέπει να έχουμε ένα αντίγραφο του δημόσιου κλειδιού του . Τα περισσότερα προγράμματα που χρησιμοποιούν το S/MIME κάνουν χρήση των X.509 v3 Public Key Infrastructures σαν και αυτές που δημιουργούνται από την VeriSign και άλλες αρχές πιστοποίησης .

Pretty Good Privacy (PGP)

Εισαγωγή

Το PGP είναι ένα φαινόμενο, αφού πρόκειται για τη δουλειά ουσιαστικά ενός μόνο ανθρώπου, του Phil Zimmerman και παρέχει τις υπηρεσίες της εμπιστευτικότητας (confidentiality) και της εξακρίβωσης γνησιότητας (authentication) που μπορούν να χρησιμοποιηθούν στις εφαρμογές ηλεκτρονικού ταχυδρομείου και αποθήκευσης αρχείων. Από τη στιγμή της γέννησης του και πέρα το PGP χρησιμοποιείται ευρύτατα και αυτό εξαιτίας των παρακάτω λόγων:

- Είναι διαθέσιμο παντού και μπορεί να τρέξει σε οποιαδήποτε πλατφόρμα.
- Βασίζεται σε αλγορίθμους που είναι ευρέως αποδεκτοί σαν απόλυτα ασφαλείς.
- Είναι κατάλληλο για ένα ευρύ φάσμα εφαρμογών.
- Δεν αναπτύχθηκε, ούτε ελέγχεται από κυβερνητικό ή άλλο οργανισμό για τυποποιήσεις.

Περιγραφή της λειτουργίας του PGP

Η λειτουργία του PGP αποτελείται από πέντε υπηρεσίες, οι οποίες συνοψίζονται στον παρακάτω πίνακα: **εξακρίβωση γνησιότητας**, **εμπιστευτικότητα**, **συμπίεση**, **συμβατότητα ηλ. ταχυδρομείου** (e-mail) και **τμηματοποίηση**.

Λειτουργία	Αλγόριθμοι	Περιγραφή
Εμπιστευτικότητα-Κρυπτογράφηση μηνύματος	IDEA, RSA	Ένα μήνυμα κρυπτογραφείται χρησιμοποιώντας τον IDEA με ένα μιας χρήσεως session key, που δημιουργείται από τον αποστολέα. Το session key κρυπτογραφείται χρησιμοποιώντας τον RSA με το public key του παραλήπτη και συμπεριλαμβάνεται στο μήνυμα

Εξακρίβωση γνησιότητας-Ηλεκτρονική υπογραφή	RSA, MD5	Ένας hash κωδικός του μηνύματος δημιουργείται, χρησιμοποιώντας τον MD5. Αυτό το message digest κρυπτογραφείται χρησιμοποιώντας τον RSA με το private key του αποστολέα και συμπεριλαμβάνεται στο μήνυμα
Συμπίεση	ZIP	Ένα μήνυμα μπορεί να συμπιεστεί για αποθήκευση ή μετάδοση, χρησιμοποιώντας τον ZIP
E-mail συμβατότητα	Radix-64 μετατροπή	Για την παροχή διαφάνειας σε e-mail εφαρμογές, ένα κρυπτογραφημένο μήνυμα μπορεί να μετατραπεί σε ένα αλφαριθμητικό ASCII, χρησιμοποιώντας radix-64 μετατροπή
Τμηματοποίηση	-	Για την παροχή μέγιστου μεγέθους mail, το PGP εκτελεί τμηματοποίηση και συναρμολόγηση

Πίνακας 1-9: **Περίληψη των λειτουργιών του PGP**

Εξακρίβωση γνησιότητας (authentication)

Για την εξακρίβωση γνησιότητας (authentication) πρώτα ο αποστολέας στέλνει το μήνυμα. Στη συνέχεια ο MD5 χρησιμοποιείται για να παράγει ένα 128-bit hash code του μηνύματος. Ο κωδικός αυτός κρυπτογραφείται χρησιμοποιώντας RSA και το private key του αποστολέα και το αποτέλεσμα προσκολλάται στο μήνυμα. Ο παραλήπτης του μηνύματος χρησιμοποιεί με τη σειρά τον RSA με το public key του αποστολέα για να αποκρυπτογραφήσει και να βρει τον hash code. Τέλος, ο παραλήπτης παράγει ένα νέο hash code για το μήνυμα και το συγκρίνει με το αποκρυπτογραφημένο hash code που έχει βρει. Αν ταιριάζουν, τότε δέχεται το μήνυμα ως αυθεντικό.
Όπως βλέπουμε, ο συνδυασμός του MD5 και του RSA παρέχουν έναν αποτελεσματικό σχήμα ηλεκτρονικής υπογραφής (digital signature). Ακόμα, μπορούν να υποστηριχθούν υπογραφές που παράγονται και μεταδίδονται ξεχωριστά από το μήνυμα.

Εμπιστευτικότητα (Confidentiality)

Αυτή παρέχεται με την κρυπτογράφηση των μηνυμάτων προτού αποσταλούν ή αποθηκευτούν σαν αρχεία. Και στις δύο περιπτώσεις χρησιμοποιείται ο αλγόριθμος IDEA, και συγκεκριμένα η 64-bit cipher feedback (CFB) mode του IDEA με πίνακα αρχικοποίησης (initialization vector) όλο μηδενικά.
Στο PGP κάθε συμβατικό (conventional) κλειδί χρησιμοποιείται μόνο μία φορά, οπότε για κάθε μήνυμα παράγεται με τυχαίο τρόπο ένα κλειδί 128-bits. Για την προστασία του, το κλειδί αυτό, προτού μεταδοθεί, κρυπτογραφείται με βάση το public key του παραλήπτη. Η σειρά των γεγονότων έχει ως εξής: Ο αποστολέας παράγει ένα μήνυμα και ένα τυχαίο 128-bit αριθμό για να χρησιμοποιηθεί σαν session key για το μήνυμα αυτό μόνο. Στη συνέχεια το μήνυμα κρυπτογραφείται χρησιμοποιώντας το IDEA μαζί με το session key. Το session key κωδικοποιείται με RSA, χρησιμοποιώντας το public key του παραλήπτη και προσδένεται στο μήνυμα. Τέλος, ο παραλήπτης χρησιμοποιεί RSA με το δικό του private key, για να βρει το session key, το οποίο χρησιμοποιεί για να αποκρυπτογραφήσει το μήνυμα.
Για το μέγεθος του κλειδιού που θα χρησιμοποιήσει ο RSA, υπάρχουν οι δυνατότητες του Συνήθους (Casual - 384 bits), του Εμπορικού (commercial - 512 bits) και του στρατιωτικού (Military – 1024 bits) κλειδιού.

Εμπιστευτικότητα και Εξακρίβωση γνησιότητας

Όταν και οι δύο υπηρεσίες χρησιμοποιούνται, αρχικά, ο αποστολέας παράγει μία ηλεκτρονική υπογραφή το μήνυμα, με βάση το private key του, και την τοποθετεί στο τέλος του μηνύματος. Στη συνέχεια, το μήνυμα μαζί με την υπογραφή κρυπτογραφείται χρησιμοποιώντας τον IDEA και ένα session key και το session key κρυπτογραφείται χρησιμοποιώντας τον RSA και το public key του παραλήπτη.

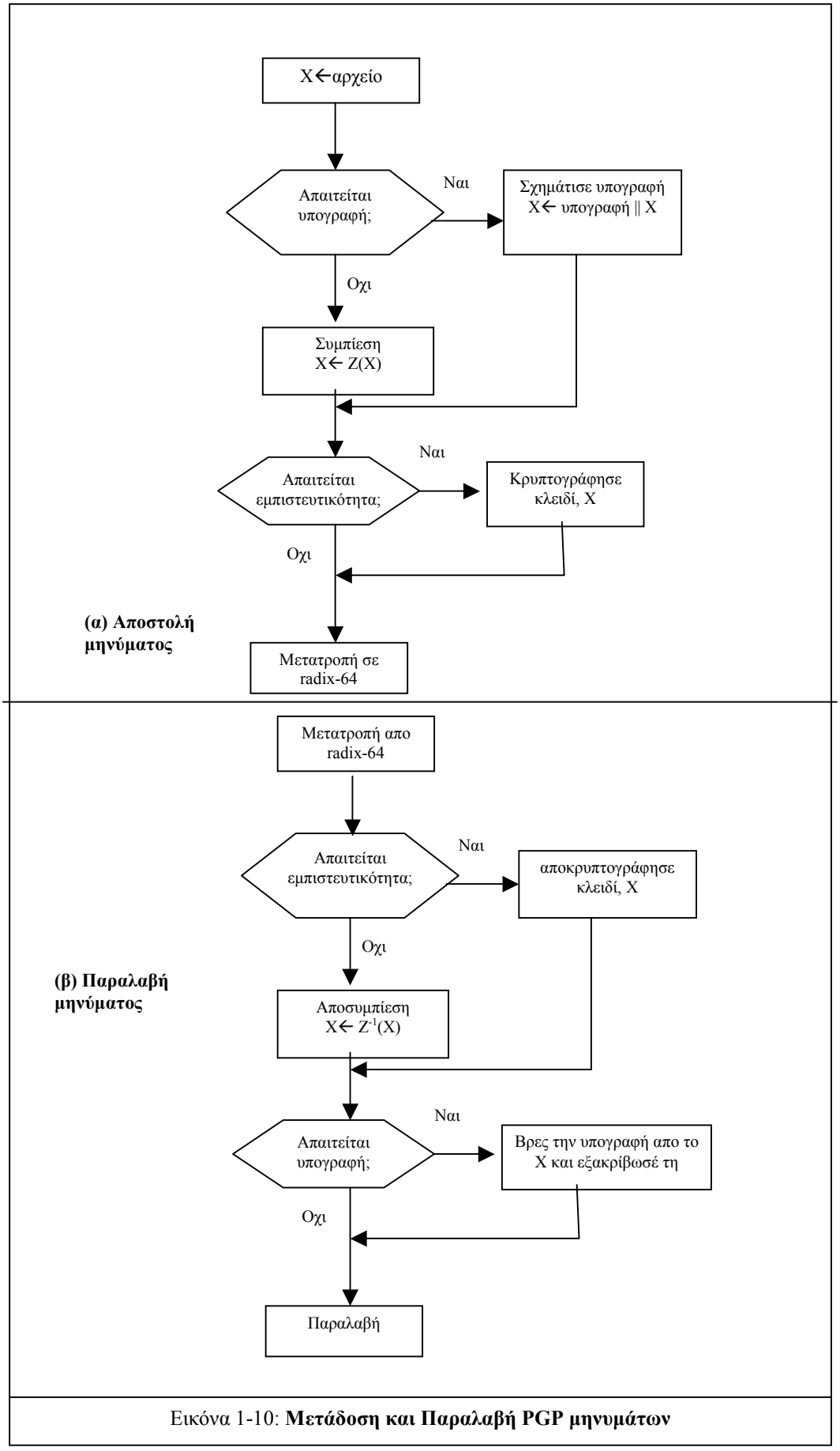
Συμπίεση (Compression)

Το PGP συμπιέζει από μόνο του το μήνυμα αφού τοποθετηθεί η υπογραφή και πριν κρυπτογραφηθεί. Έτσι κερδίζουμε χώρο και κατά την μετάδοση και κατά την αποθήκευση του μηνύματος. Ο αλγόριθμος που χρησιμοποιείται είναι ο ZIP.

Συμβατότητα ηλεκτρονικού ταχυδρομείου

Όταν χρησιμοποιείται PGP, ολόκληρο ή τουλάχιστον ένα μέρος του block που αποστέλλεται είναι κρυπτογραφημένο και αποτελείται από μία σειρά από τυχαία 8-bit octets. Λόγω του περιορισμού που υπάρχει σε ορισμένα συστήματα ηλεκτρονικού ταχυδρομείου για μόνο ASCII text μηνύματα, το PGP παρέχει μία υπηρεσία που μετατρέπει τη σειρά αυτή σε εκτυπώσιμους ASCII χαρακτήρες. Για το σκοπό αυτό

χρησιμοποιείται η **radix-64 μετατροπή**, που παίρνει κάθε ομάδα τριών octets και τα μετατρέπει σε 4 χαρακτήρες ASCII, καθώς επίσης προσθέτει στο τέλος ένα CRC, για την ανίχνευση τυχόν λαθών.
Το PGP ακόμα, μπορεί να μετατρέπει σε radix-64 μορφή μόνο το μέρος όπου υπάρχει η υπογραφή, ώστε ο αποστολέας να μπορεί να διαβάζει τα μηνύματα, χωρίς να χρησιμοποιεί PGP, και μόνο αν θέλει να πιστοποιήσει την υπογραφή να χρειάζεται το PGP.
Η εικόνα 4.1.1 δείχνει τη σχέση μεταξύ των παραπάνω υπηρεσιών. Κατά τη μετάδοση, αν αυτό απαιτείται, σχηματίζεται μία υπογραφή χρησιμοποιώντας ένα hash κωδικό του συμπιεσμένου κειμένου. Μετά το κείμενο μαζί με την υπογραφή συμπιέζονται και αν χρειάζεται η *εμπιστευτικότητα*, το όλο μπλοκ κρυπτογραφείται με το RSA-κρυπτογραφημένο κλειδί κρυπτογράφησης. Τέλος, ολόκληρο το μπλοκ αυτό μετασχηματίζεται στην radix-64 μορφή.
Κατά τη λήψη του μηνύματος, το εισερχόμενο μπλοκ πρώτα μετατρέπεται από την radix-64, στην αρχική δυαδική μορφή του και, αν είναι κρυπτογραφημένο, ο παραλήπτης ανακτά το session κλειδί και αποκρυπτογραφεί το μήνυμα. Το τελικό μπλοκ αποσυμπιέζεται και αν είναι υπογεγραμμένο, ο παραλήπτης ανακτά τον hash code που έχει μεταδοθεί και το συγκρίνει με αυτόν που έχει υπολογίσει αυτός.



Εικόνα 1-10: **Μετάδοση και Παραλαβή PGP μηνυμάτων**

Μια δημοφιλής εφαρμογή που αναπτύχθηκε με σκοπό την ασφάλεια μηνυμάτων και αρχείων είναι το **Pretty Good Privacy (PGP)**. Είναι ίσως η ευρύτερα διαδεδομένη εφαρμογή ασφαλείας για ηλεκτρονικό ταχυδρομείο στο Διαδίκτυο. Το PGP (Pretty Good Privacy) είναι πακέτο λογισμικού που παρέχει ρουτίνες κρυπτογράφησης για e-mail και εφαρμογές αποθήκευσης αρχείων. Το PGP απαρτίζεται από υπάρχοντα κρυπτοσυστήματα και πρωτόκολλα κρυπτογράφησης. Τρέχει σε διάφορες πλατφόρμες. Προσφέρει κρυπτογράφηση μηνύματος, ψηφιακές υπογραφές, συμπίεση δεδομένων και e-mail συμβατότητα.

Η τελευταία έκδοσή του για χρήστες εκτός των ΗΠΑ παρέχει έναν εύκολο τρόπο κρυπτογράφησης, διαχείρισης κλειδιών μέσα από γραφικό περιβάλλον. Το PGP συνδυάζει και τους δύο τρόπους κρυπτογράφησης, μεταφέροντας με ασφαλή τρόπο το ιδιωτικό κλειδί μέσα από τεχνικές δημόσιου κλειδιού. Μετά την εγκατάσταση του προγράμματος και κατά τη διαδικασία δημιουργίας του δημόσιου κλειδιού ο χρήστης καλείται να δώσει το επιθυμητό μέγεθος του κλειδιού. Εδώ πρέπει να τονιστεί ότι χρησιμοποιείται συμμετρικός αλγόριθμος για να μεταδώσει με ασφαλή τρόπο το ιδιωτικό κλειδί, το οποίο χρησιμοποιείται τελικά για την κρυπτογράφηση του κυρίως μηνύματος. Το PGP προσφέρει 3 συμμετρικούς αλγορίθμους, οι οποίοι είναι οι: CAST και IDEA με 128 bits μέγεθος κλειδιού, καθώς και ο Triple-DES με 168 bits μέγεθος κλειδιού. Εκτός από την κρυπτογράφηση, το PGP επιτρέπει στο χρήστη να υπογράψει ψηφιακά οποιοδήποτε κείμενο αποστέλλει, καθώς επίσης και να ελέγξει την πατρότητα του ψηφιακά υπογεγραμμένου κειμένου που έχει λάβει. Το PGP σχεδιάστηκε γύρω από την ιδέα ενός αξιόπιστου web το οποίο θα επιτρέπει στους χρήστες να μοιράζονται τα κλειδιά τους χωρίς να απαιτείται η ιεραρχία των αρχών πιστοποίησης.

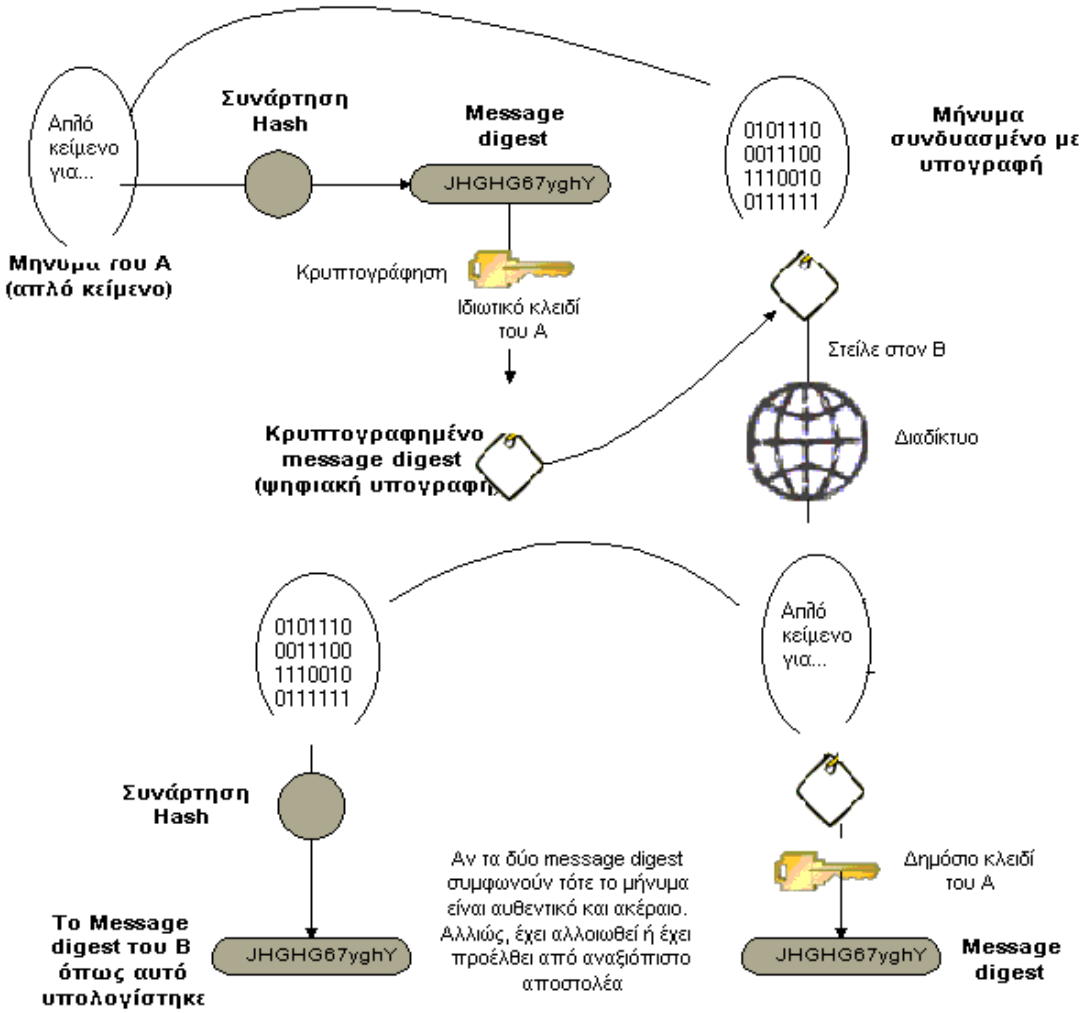
ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Η ψηφιακή υπογραφή (digital signature) θεωρείται ως το ηλεκτρονικό ισοδύναμο της συμβατικής υπογραφής και είναι μια συμβολοσειρά που προκύπτει από το συνδυασμό των δυαδικών ψηφίων ενός μηνύματος και αυτών ενός μυστικού κλειδιού.

Η χρησιμοποίηση της ψηφιακής υπογραφής σε ένα σύστημα ασφαλείας ενός δικτύου είναι απαραίτητη καθώς παρέχει αυθεντικοποίηση του αποστολέα, εμπιστευτικότητα και ακεραιότητα του μηνύματος.

Οι ασύμμετροι αλγόριθμοι είναι υπολογιστικά αργοί για την κρυπτογράφηση ενός ολόκληρου μηνύματος. Έστω λοιπόν ότι ο Α επιθυμεί να στείλει υπογεγραμμένο έγγραφο ή μήνυμα στον Β. Το πρώτο βήμα είναι γενικά να εφαρμόσει μια hash συνάρτηση στο μήνυμα και να δημιουργήσει ένα **message digest**. Το message digest είναι συνήθως αισθητά μικρότερο από το πρωτότυπο μήνυμα. Ουσιαστικά η δουλειά της hash συνάρτησης είναι να πάρει ένα μήνυμα οποιουδήποτε μεγέθους και να το συρρικνώσει σε προκαθορισμένο μέγεθος. Για να δημιουργήσει κανείς μια **ψηφιακή υπογραφή** κρυπτογραφεί συνήθως το message digest και όχι το ίδιο το μήνυμα (μ' άλλα λόγια το κρυπτογραφημένο message digest είναι η ψηφιακή υπογραφή του αποστολέα). Ο Α στέλνει στον Β το κρυπτογραφημένο message digest και το μήνυμα κρυπτογραφημένο ή όχι. Προκειμένου ο Β να αυθεντικοποιήσει την υπογραφή κάνει τα εξής**:**

- Εφαρμόζει, πρώτα απ' όλα, την ίδια hash συνάρτηση με τον Α στο μήνυμα που παρέλαβε (το οποίο επαναλαμβάνουμε είναι κρυπτογραφημένο ή απλό κείμενο). Δημιουργεί έτσι τη δική του εκδοχή για το ορθό message digest.
- Στη συνέχεια αποκρυπτογραφεί τη ψηφιακή υπογραφή την οποία παρέλαβε συνημμένη με το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Α. Η διαδικασία αυτή οδηγεί στην αναπαραγωγή του message digest το οποίο δημιούργησε ο Α.
- Ο Β έχει τώρα στη διάθεση του δύο message digests. Τα συγκρίνει και αν ταιριάζουν, αυθεντικοποίησε επιτυχώς τη ψηφιακή υπογραφή του Α. Αν όχι, υπάρχουν λίγες πιθανές εξηγήσεις. Είτε κάποιος προσποιείται τον Α, ή το μήνυμα μεταβλήθηκε από τη στιγμή που το υπέγραψε ο Α, ή υπήρξε λάθος στη μετάδοση.



Σχήμα 1-11: Ψηφιακή υπογραφή.

ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Είναι γεγονός αναμφισβήτητο ότι η απόκτηση εμπιστοσύνης που επιτυγχάνεται κατά τις συμβατικές συναλλαγές μέσω της οπτικής επαφής των δύο συναλλασσομένων μερών δεν είναι δυνατή όταν πρόκειται για συναλλαγές μέσω Web. Έτσι, είναι αναγκαία η ύπαρξη ενιαίας υποδομής, η οποία θα προστατεύει τις ιδιωτικές πληροφορίες από τρίτους (Privacy). Η πληροφορία που ανταλλάσσεται ανάμεσα στα δύο μέρη (αποστολέας και παραλήπτης, πελάτης και έμπορος) δεν πρέπει να καταλήγει σε τρίτους. Εξίσου σημαντικό στοιχείο είναι η επικύρωση της ταυτότητας (authentication) των επικοινωνούντων μερών. Ο αποστολέας πρέπει να γνωρίζει ότι οι πληροφορίες που στέλνει έχουν ως παραλήπτη το συγκεκριμένο πρόσωπο. Ο Α πρέπει να είναι σίγουρος ότι ο Β, με τον οποίο επικοινωνεί, είναι όντως αυτός που ισχυρίζεται ότι είναι. Άλλο σημαντικό θέμα είναι η διασφάλιση της ακεραιότητας των δεδομένων που αποστέλλονται. Τα στοιχεία μιας συναλλαγής πρέπει να φτάσουν στον προορισμό τους αυτούσια. Ακόμα κι αν πέσουν σε χέρια τρίτων, να είναι έτσι κρυπτογραφημένα ώστε να τους είναι άχρηστα - να μην μπορούν να τα εκμεταλλευτούν. Τα συναλλασσόμενα μέρη πρέπει να μην έχουν τη δυνατότητα άρνησης της συμμετοχής τους σε μια συναλλαγή.

Το ηλεκτρονικό εμπόριο και οι ηλεκτρονικές τραπεζικές συναλλαγές πρέπει να αναγνωρίζονται από το νομικό καθεστώς της χώρας στην οποία πραγματοποιείται. Μια ψηφιακή υπογραφή σε ένα κείμενο πρέπει να έχει την ίδια βαρύτητα με τη φυσική υπογραφή σε μια νομική αρχή, σε ένα δικαστήριο. Η ασφάλεια των αριθμών των πιστωτικών καρτών είναι βασική προϋπόθεση για την ευρεία διάδοση του ηλεκτρονικού εμπορίου. Οι πελάτες θέλουν να είναι σίγουροι ότι οι πληροφορίες των πιστωτικών καρτών τους είναι ασφαλείς καθώς μεταβιβάζονται μέσω Internet και ότι έχουν ως αποδέκτη έναν νόμιμο πωλητή ή αρχή. Αντίστοιχα, οι έμποροι πρέπει να γνωρίζουν ότι οι πληροφορίες που λαμβάνουν αντιστοιχούν σε νόμιμους κατόχους πιστωτικών καρτών. Η υποδομή αυτή στηρίζεται στην κρυπτογράφηση. Με τη συμμετρική κρυπτογράφηση επιτυγχάνεται η διασφάλιση του απορρήτου και της ακεραιότητας των πληροφοριών που

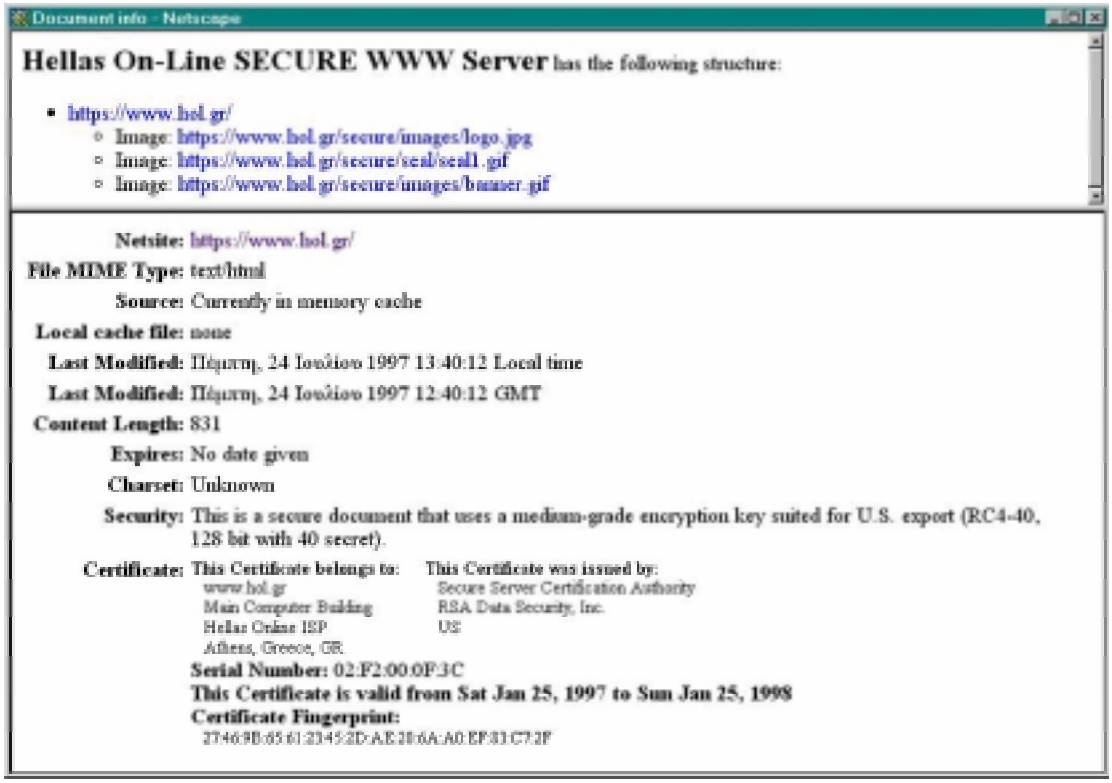
στέλνονται μεταξύ των συναλλασσόμενων μερών. Έτσι, αν βρεθούν στα χέρια τρίτων, θα τους είναι άχρηστες, αφού οι τελευταίοι δε θα μπορούν να αντιληφθούν το περιεχόμενό τους.

Για την επίτευξη της ταυτοποίησης χρησιμοποιείται κρυπτογράφηση δημόσιου κλειδιού. Με αυτό τον τρόπο κάθε συναλλασσόμενο μέρος αναγνωρίζεται ως τέτοιο με βάση το ψηφιακό πιστοποιητικό (Digital ID) που έχει αποκτήσει. Το ψηφιακό πιστοποιητικό είναι αντίστοιχο με την ταυτότητα, το δίπλωμα οδήγησης, το διαβατήριο και την πιστωτική κάρτα και εκδίδεται από αρχές πιστοποίησης (Certification Authorities, CA). Η ακεραιότητα διασφαλίζεται και με τη χρήση των ψηφιακών υπογραφών. Ο αποστολέας υπογράφει ψηφιακά την πληροφορία με το ιδιωτικό κλειδί του και την αποστέλλει. Όταν ο παραλήπτης λάβει το μήνυμα, ελέγχει την ψηφιακή υπογραφή του αποστολέα. Αν όντως υπάρχει, το μήνυμα έχει φτάσει ακέραιο, διαφορετικά έχει αλλάξει κατά τη μεταφορά του.

Τι χρειαζόμαστε όμως, στην πράξη τα προσωπικά πιστοποιητικά; Οι browsers χρησιμοποιούν το πιστοποιητικό για να αποκρυπτογραφήσουν πληροφορία που στέλνεται προς εμάς. Με τη δημιουργία του πιστοποιητικού δημιουργούμε ένα ζεύγος κλειδιών (δημόσιο και ιδιωτικό). Όποιος θέλει να μας στείλει εμπιστευτικές πληροφορίες τις κρυπτογραφεί με το δημόσιο κλειδί μας, οπότε μόνο εμείς με το ιδιωτικό κλειδί μας μπορούμε να τις αποκρυπτογραφήσουμε. Μπορούμε επίσης να στείλουμε πληροφορία κρυπτογραφημένη μέσω e-mail, χρησιμοποιώντας το πρωτόκολλο S/MIME. Επίσης μπορούν να χρησιμοποιηθούν για την είσοδό μας σε sites με ελεγχόμενη πρόσβαση, σε sites ηλεκτρονικών καταστημάτων, τραπεζών κλπ. Πολλά sites, μάλιστα, για διευκόλυνσή μας, συλλέγουν πληροφορίες με βάση την ταυτότητά μας για να δημιουργήσουν προφίλ με τις προτιμήσεις μας - οπότε, αν ξαναμπούμε στο συγκεκριμένο site, ανακτάται το προφίλ μας και εμφανίζονται πληροφορίες που ουσιαστικά εμείς θέλουμε να δούμε, σύμφωνα με τα στοιχεία που είχαμε δώσει την πρώτη φορά.

Η συνεχής εξέλιξη των πρωτοκόλλων ασφαλείας στο Internet αποτελεί την καλύτερη εγγύηση αλλά και την πιο ικανοποιητική απάντηση στο ερώτημα αν οι πραγματοποίηση τραπεζικών συναλλαγών μέσω του Διαδικτύου είναι σίγουρη και ασφαλής.

Βλέποντας ένα πιστοποιητικό ενός site:



ΚΡΥΠΤΟΓΡΑΦΙΑ

Η κρυπτογραφία είναι η τέχνη ή η επιστήμη που παρέχει ασφάλεια στην πληροφορία.
Έχει καταστεί εξαιρετικά σημαντική και αποτελεί πλέον δομικό στοιχείο της λειτουργίας οργανισμών και επιχειρήσεων, καθώς και εργαλείο προστασίας προσωπικών δεδομένων ιδιωτών. Αγοροπωλησίες, συναλλαγές, μεταφορά πληροφορίας και άλλες λειτουργίες έχουν εδραιωθεί ως αξιόπιστες βάσει της τεχνολογικής ανάπτυξης της κρυπτογραφίας.

Παραδοσιακά, η κρυπτογραφία περιλαμβάνει διάφορες τεχνικές για την απόκρυψη της πληροφορίας κατά τη διακίνηση και αποθήκευσή της, όπως είναι η συγχώνευση λέξεων με εικόνες, οι εικόνες σε σμίκρυνση μεγέθους τελείας στιγμής (microdots) κ.ά. Ωστόσο, σήμερα, η κρυπτογραφία σχετίζεται περισσότερο με το scrabbling (μετατροπή της πληροφορίας σε μη αναγνώσιμη), μια διαδικασία η οποία είναι ευρέως γνωστή ως κρυπτογράφηση, και την αντίστροφη διαδικασία της μετατροπής ενός κρυπτογραφήματος σε αναγνώσιμο κείμενο (αποκρυπτογράφηση). Η κρυπτογράφηση και η αποκρυπτογράφηση κάνουν συνήθως χρήση ενός κλειδιού, και η μέθοδος κωδικοποίησης πρέπει να είναι τέτοια έτσι ώστε η αποκρυπτογράφηση να είναι εκτελέσιμη μόνο αν υπάρχει γνώση του κατάλληλου αυτού κλειδιού.

Η κρυπτογραφία έχει τέσσερις αντικειμενικούς σκοπούς:
Εμπιστευτικότητα: η πληροφορία δεν πρέπει να γίνεται κατανοητή από κανέναν, πλην του πραγματικά επιδιωκόμενου παραλήπτη της.
Ακεραιότητα: η πληροφορία δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της πραγματοποιηθείσας αλλοίωσης. Αυτό ισχύει και στην περίπτωση που είναι αποθηκευμένη σε μια αποθήκη υλικού και στην περίπτωση που διακινείται από τον αποστολέα στον παραλήπτη.
Μη αποκήρυξη: Ο δημιουργός/ αποστολέας της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της δημιουργίας ή μετάδοσης της πληροφορίας.
Πιστοποίηση: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητες τους καθώς και την αρχή και τον προορισμό της πληροφορίας.

Η κρυπτογραφία είναι στενά συνδεδεμένη με τις αρχές της κρυπτανάλυσης και της κρυπτολογίας. Κρυπτανάλυση είναι η τέχνη της αποκωδικοποίησης των κρυπτογραφημάτων (παράγει το καθαρό κείμενο - plaintext) χωρίς τη γνώση του κατάλληλου κλειδιού. Η κρυπτολογία είναι ο κλάδος των μαθηματικών που μελετά όλες τις μαθηματικές θεμελιώσεις των κρυπτογραφικών μεθόδων και περιλαμβάνει και την κρυπτογραφία και την κρυπτανάλυση.

ΑΝΑΓΚΕΣ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ –ΑΠΟΚΡΥΨΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η κρυπτογραφία από τα αρχαία χρόνια, οπότε και πρωτοχρησιμοποιήθηκε, είχε ένα κύριο στόχο, την **απόκρυψη της πληροφορίας** κάποιου κειμένου από μη επιθυμητά πρόσωπα. Αυτή η ανάγκη προέκυψε για δύο λόγους. Ο πρώτος λόγος ήταν η ανάγκη επικοινωνίας και μεταφοράς μυστικών, ιδιαίτερα σε περιόδους πολέμου. Ο δεύτερος λόγος ήταν η πρόθεση κάποιων να αποκρύψουν πληροφορίες – γνώσεις από τους υπολοίπους. Συνήθως επρόκειτο για ιερείς ή αξιωματούχους που ήθελαν να αποκρύψουν πληροφορίες ή γνώσεις από το λαό. Σήμερα η ανάγκη αυτή έχει επεκταθεί από την προστασία των απλών προσωπικών δεδομένων μέχρι την προστασία βιομηχανικών και κρατικών μυστικών.

Καθώς η κρυπτολογία αναπτύσσεται ο αριθμός των στόχων της έχει επεκταθεί, όπως και ο αριθμός των εργαλείων που είναι διαθέσιμα για την επίτευξη αυτών των στόχων. Η κρυπτολογία παρέχει τρόπους με τους οποίους μπορεί να βοηθήσει κάποιον να αναπτύξει εμπιστοσύνη κατά τις επικοινωνίες του και να τους δώσει τις επιθυμητές ιδιότητες, παρά τις προσπάθειες των κακόβουλων χρηστών για το αντίθετο.

Έτσι εκτός από την **απόκρυψη της πληροφορίας** ή αλλιώς την **ιδιωτικότητα (privacy)** η κρυπτογραφία ικανοποιεί και μια σειρά από άλλες ανάγκες, οι οποίες περιγράφονται με συντομία παρακάτω.

Ταυτοποίηση (authentication)

Πρέπει να είναι δυνατό για τον παραλήπτη ενός μηνύματος να επιβεβαιώσει τον αποστολέα του και να μην μπορεί ένας εισβολέας να πάρει τη θέση κάποιου άλλου χρήστη.

Απόδειξη γνησιότητας-υπογραφές (signatures)

Ο παραλήπτης του μηνύματος μπορεί να πείσει κάποιον τρίτο ότι το μήνυμα που έλαβε προέρχεται από αυτόν που το υπογράφει και ο υπογράφων να πείσει για την ταυτότητά του.

Ακεραιότητα –(Integrity)

Πρέπει να μπορεί ο παραλήπτης ενός μηνύματος να επιβεβαιώσει ότι το μήνυμα δεν έχει τροποποιηθεί κατά τη διαδρομή του και ένας εισβολέας να μην μπορεί να αντικαταστήσει ένα κανονικό μήνυμα με ένα πλαστό.

Μη δυνατότητα άρνησης (nonrepudiation)

Ένας αποστολέας πρέπει να μην μπορεί να αρνηθεί ψευδώς ότι έστειλε κάποιο μήνυμα.

Μινιμαλισμός (minimality)

Τίποτα δεν μεταδίδεται σε τρίτους εκτός από αυτό που σαφώς έχει οριστεί πως πρέπει να μεταδοθεί.

Ταυτόχρονη ανταλλαγή (simultaneous exchange)

Τίποτα με αξία (π.χ. μια υπογραφή σε ένα συμβόλαιο) δεν μεταδίδεται πριν κάτι άλλο με αξία (π.χ. η υπογραφή του άλλου μέρους) δεν παραληφθεί.

Συντονισμός (coordination)

Σε μια επικοινωνία με πολλά μέρη, οι συμμετέχοντες μπορούν να συντονίσουν τις δραστηριότητές τους προς ένα κοινό σκοπό ακόμα και με την παρουσία ανεπιθύμητων – εχθρικών μερών.

Οριο συνεργασίας (Collaboration Threshold)

Σε μια επικοινωνία πολλών μερών οι επιθυμητές ιδιότητες διατηρούνται μέχρι ο αριθμός των ανεπιθύμητων – εχθρικών μερών δεν υπερβαίνει ένα συγκεκριμένο όριο.

Όλες αυτές είναι βασικές απαιτήσεις για κοινωνικές αλληλεπιδράσεις μέσω των υπολογιστών, που είναι ανάλογες αυτών που ισχύουν για τις διαπροσωπικές σχέσεις.

Η χρήση της κρυπτογράφησης

Από τη στιγμή που άρχισαν να μεταφέρονται πληροφορίες ξεκίνησε και η ιδέα της κρυπτογράφησης ή του κώδικα για να ασφαλιστούν τα μηνύματα . Το παρόν σύστημα αποστολής μηνυμάτων μέσω του internet βασίζεται στην ίδια γενική ιδέα κρυπτογράφησης που έχει χρησιμοποιηθεί εδώ και αιώνες .

Η διαφορά μεταξύ των προηγούμενων και των τωρινών μορφών κρυπτογράφησης βρίσκεται στο κλειδί που αποκρυπτογραφεί τον κώδικα. Στο παρελθόν ο παραλήπτης για να μπορεί να επαναφέρει το μήνυμα ξανά σε αναγνώσιμη μορφή , χρειαζόταν το κλειδί του μυστικού κώδικα. Το σύστημα δούλευε θαυμάσια τις περισσότερες φορές , επειδή σε κάποιο σε κάποιο σημείο τα δυο μέρη συναντιόντουσαν προσωπικά και μπορούσαν να ανταλλάξουν κώδικα , ώστε να ήταν σίγουρο ότι θα είναι μυστικός . Αν μια προσωπική συνάντηση δεν ήταν δυνατή , τα δυο μέρη έχουν τον κίνδυνο να υποκλαπεί ο μυστικός κώδικας και να αντιγραφεί .

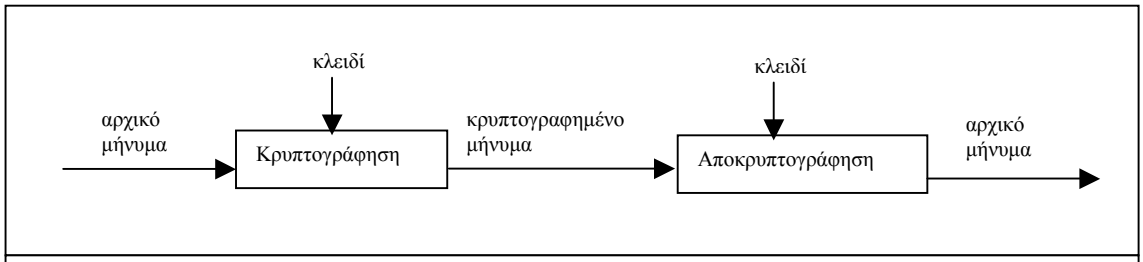
ΚΡΥΠΤΟΓΡΑΦΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ

Υπάρχουν δύο τύποι αλγορίθμων που βασίζονται σε κλειδιά: οι **συμμετρικοί** ή **μυστικού κλειδιού** και οι **μη συμμετρικοί** ή **δημόσιου κλειδιού**. Οι συμμετρικοί αλγόριθμοι διαιρούνται σε δύο κατηγορίες. Μερικοί λειτουργούν στο αρχικό κείμενο σε ένα bit τη φορά και καλούνται **stream** αλγόριθμοι. Άλλοι λειτουργούν πάνω σε μια ομάδα από bits οπότε καλούνται **block** αλγόριθμοι. Παρακάτω παρουσιάζονται ορισμένοι αντιπροσωπευτικοί αλγόριθμοι των παραπάνω κατηγοριών.

Αλγόριθμοι μυστικού κλειδιού

Οι αλγόριθμοι μυστικού κλειδιού (ή **συμμετρικοί αλγόριθμοι**) χρησιμοποιούν το ίδιο κλειδί, το οποίο καλείται και *μυστικό* (secret key), για την κρυπτογράφηση και αποκρυπτογράφηση. Σ' αυτούς τους αλγορίθμους απαιτείται και από τον αποστολέα και από τον παραλήπτη να συμφωνήσουν πάνω σε πιο κλειδί θα επικοινωνούν με ασφάλεια. Η ασφάλεια των αλγορίθμων μυστικού κλειδιού έγκειται στην προστασία του κλειδιού: όποιος κατέχει το κλειδί μπορεί να κρυπτογραφήσει και να αποκρυπτογραφήσει μηνύματα. Παρακάτω παρουσιάζονται ορισμένοι από τους πιο δημοφιλείς αλγορίθμους μυστικού κλειδιού.

Εδώ παρουσιάζεται σχηματικά πως κρυπτογραφείται ένα μήνυμα με αλγόριθμο μυστικού κλειδιού.



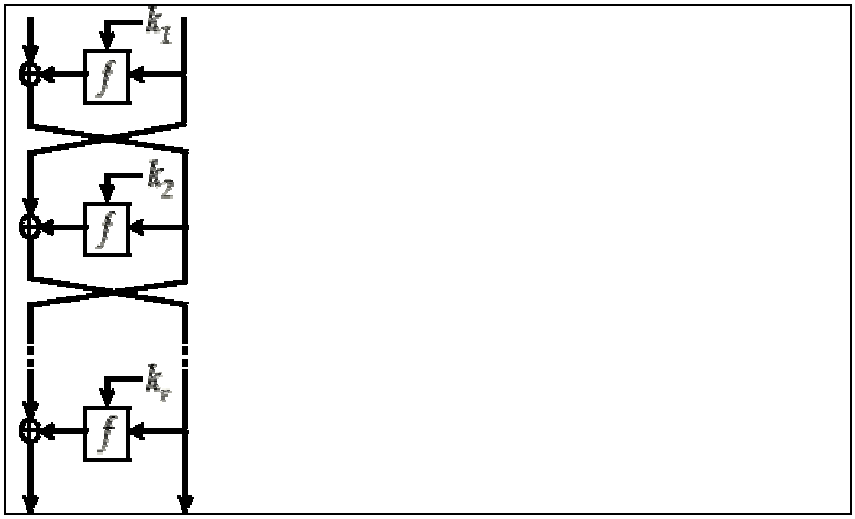
Σχήμα 1-12: **Κρυπτογράφηση μυστικού κλειδιού**

Οι αλγόριθμοι Feistel είναι μια ειδική τάξη επαναληπτικών block αλγορίθμων κρυπτογράφησης, όπου το κρυπτογραφημένο κείμενο υπολογίζεται από το κανονικό με επαναλαμβανόμενες εφαρμογές του ίδιου μετασχηματισμού ή συνάρτησης.

Σε έναν Feistel αλγόριθμο, το κείμενο που κρυπτογραφείται χωρίζεται σε δύο ίσα μέρη. Μια συνάρτηση *f* εφαρμόζεται στο ένα μέρος χρησιμοποιώντας ένα *υποκλειδί* και η έξοδος της *f* γίνεται XOR με το άλλο μέρος. Τα δύο μέρη μετά εναλλάσσονται. Κάθε γύρος ακολουθεί την ίδια διαδικασία εκτός από τον τελευταίο όπου τα μέρη δεν εναλλάσσονται (βλ. εικόνα 2.1.1).

Ένα ενδιαφέρον χαρακτηριστικό ενός Feistel αλγορίθμου είναι ότι η κρυπτογράφηση και η αποκρυπτογράφηση είναι ίδιες, λαμβάνοντας υπόψη τα υποκλειδιά που χρησιμοποιούνται για κάθε γύρο παίρνονται με την αντίστροφη σειρά στην αποκρυπτογράφηση.

Είναι δυνατόν να σχεδιαστούν επαναληπτικοί αλγόριθμοι οι οποίοι δεν είναι Feistel και η κρυπτογράφηση και η αποκρυπτογράφησή τους είναι δομικά η ίδια. Ένα τέτοιο παράδειγμα είναι και ο IDEA.



Εικόνα 1-13: **Αλγόριθμος κρυπτογράφησης Feistel**

Data Encryption Standard (DES)

Ο DES (Data Encryption Standard) είναι ένας block αλγόριθμος κρυπτογράφησης ο οποίος ορίστηκε από την κυβέρνηση των Η.Π.Α. το 1977 σαν επίσημο πρότυπο. Αρχικά ο DES αναπτύχθηκε από την IBM, έχει μελετηθεί εκτενώς από την μέρα της δημοσίευσής του και είναι το πιο γνωστό και ευρέως χρησιμοποιούμενο κρυπτοσύστημα στον κόσμο.

Ο DES έχει μέγεθος block 64-bit και χρησιμοποιεί ένα 56-bit κλειδί για την κρυπτογράφηση. Είναι ένας 16 γύρων Feistel αλγόριθμος κρυπτογράφησης και αρχικά σχεδιάστηκε για υλοποίηση στο hardware.

Ο DES μπορεί να χρησιμοποιηθεί και για κρυπτογράφηση σε συστήματα ενός χρήστη όπως στην αποθήκευση κρυπτογραφημένων αρχείων σε έναν σκληρό δίσκο.

RC2 και RC4

Ο RC2 είναι ένας μεταβλητού-μεγέθους-κλειδιού block αλγόριθμος κρυπτογράφησης ο οποίος σχεδιάστηκε από τον Rivest για την RSA Data Security. Τα αρχικά RC σημαίνουν "Rod's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και σχεδιάστηκε σαν αντικαταστάτης του DES. Μπορεί να φτιαχτεί ως λιγότερο ή περισσότερο ασφαλής από τον DES ενάντια στο "εξαντλητικό ψάξιμο κλειδιού" χρησιμοποιώντας κατάλληλο μέγεθος κλειδιού κάθε φορά. Το μέγεθος του block είναι 64-bits και είναι δύο με τρεις φορές γρηγορότερος από τον DES υλοποιημένος σε λογισμικό. Ο αλγόριθμος είναι μυστικός και είναι ιδιοκτησία της RSA Data Security.

Μια συμφωνία μεταξύ της Software Publishers Association (SPA) και της αμερικάνικης κυβέρνησης δίνει στους RC2 και RC4 ειδική μεταχείριση με το να επιτρέπει απλούστερη και γρηγορότερη έγκριση εξαγωγής τους από τους συνηθισμένους κρυπτογραφικούς αλγορίθμους. Ωστόσο, για να μπορεί να εγκριθεί η σύντομη εξαγωγή ενός προϊόντος πρέπει το μέγεθος του RC2 και RC4 κλειδιού να μην υπερβεί τα 40 bits. Κλειδιά με 56 bit επιτρέπονται μόνο σε γραφεία αμερικανικών επιχειρήσεων που βρίσκονται σε ξένες χώρες. Μία πρόσθετη συμβολοσειρά (40 με 88 bits μέγεθος) η οποία καλείται και *αλάτι* μπορεί να χρησιμοποιηθεί στο να αποθαρρύνει τρίτους που προσπαθούν να προ-υπολογίσουν ένα μεγάλο look-up πίνακα με πιθανές κρυπτογραφήσεις. Το αλάτι προστίθεται στο τέλος του κλειδιού και το επιμηκυμένο κλειδί χρησιμοποιείται στην κρυπτογράφηση του μηνύματος. Το αλάτι στέλνεται μη κρυπτογραφημένο μαζί με το μήνυμα. Οι RC2 και RC4 χρησιμοποιούνται ευρέως από ανθρώπους που θέλουν να εξάγουν τα προϊόντα τους, ενώ ο DES σχεδόν ποτέ δεν εγκρίνεται για εξαγωγή.

International Data Encryption Algorithm (IDEA)

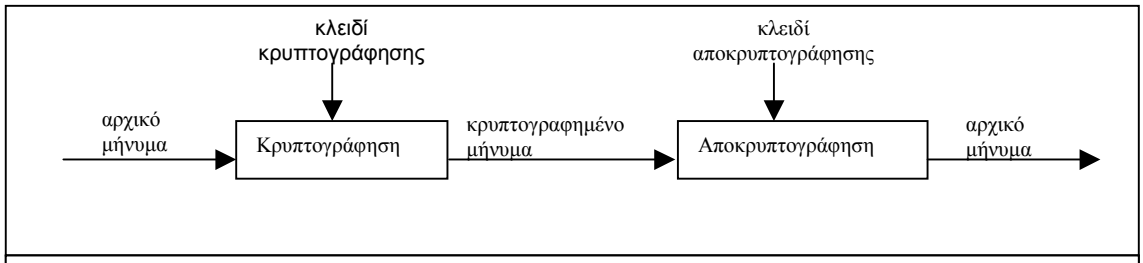
Ο IDEA (International Data Encryption Algorithm) είναι η δεύτερη έκδοση ενός block αλγόριθμου κρυπτογράφησης ο οποίος σχεδιάστηκε και παρουσιάστηκε από τους Lai και Massey. Είναι ένας 64-bit επαναληπτικός αλγόριθμος με ένα 128-bit κλειδί και 8 γύρους. Η δομή του αλγορίθμου έχει σχεδιαστεί για την εύκολη υλοποίηση τόσο στο λογισμικό όσο και στο υλικό, και η ασφάλεια του έγκειται στην χρησιμοποίηση τριών ασύμβατων τύπων αριθμητικών πράξεων πάνω σε λέξεις των 16 bit. Η ταχύτητα του IDEA είναι ίδια στο λογισμικό με αυτή του DES.

Το πιο σημαντικό κρυπταναλυτικό αποτέλεσμα οφείλεται στον Daemen. Αυτός βρήκε μια μεγάλη τάξη από 2^{51} αδύνατα κλειδιά για τα οποία η χρήση ενός από αυτά κατά την διάρκεια της κρυπτογράφησης μπορούσε να ανιχνευθεί και το κλειδί να βρεθεί. Ωστόσο, επειδή υπάρχουν 2^{128} πιθανά κλειδιά το προηγούμενο αποτέλεσμα δεν έχει επιπτώσεις στην ασφάλεια του αλγορίθμου. Ο IDEA γενικά θεωρείται ασφαλής και τόσο η ανάπτυξη του αλγορίθμου όσο και η θεωρητική του βάση έχουν ανοιχτά και ευρέως συζητηθεί.

Αλγόριθμοι δημόσιου κλειδιού

Οι αλγόριθμοι δημοσίου κλειδιού (public key) (ή αλλιώς μη-συμμετρικοί αλγόριθμοι) σχεδιάζονται έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από αυτό της αποκρυπτογράφησης. Ακόμα, το κλειδί της αποκρυπτογράφησης δεν μπορεί να υπολογισθεί γρήγορα από το κλειδί της κρυπτογράφησης. Αυτοί οι αλγόριθμοι ονομάζονται δημοσίου κλειδιού διότι το κλειδί της κρυπτογράφησης μπορεί να είναι δημόσιο. Ένας ξένος μπορεί να χρησιμοποιήσει το κλειδί της κρυπτογράφησης για να κρυπτογραφήσει ένα μήνυμα, αλλά μόνο ένα συγκεκριμένο άτομο με το αντίστοιχο κλειδί αποκρυπτογράφησης μπορεί να αποκρυπτογραφήσει το μήνυμα. Σε τέτοια συστήματα το κλειδί της αποκρυπτογράφησης ονομάζεται *ιδιωτικό* (private key) και το κλειδί της κρυπτογράφησης *δημόσιο* (public key) (βλ. σχήμα 2-2).

Επιπροσθέτως οι αλγόριθμοι δημοσίου κλειδιού δεν χρησιμοποιούνται μόνο για κρυπτογράφηση αλλά και για εξακρίβωση γνησιότητας (ηλεκτρονικές υπογραφές).



Σχήμα 1-14: **Αλγόριθμος δημόσιου κλειδιού**

Παρακάτω δίνονται δύο παραδείγματα κρυπτογράφησης και εξακρίβωσης γνησιότητας (authentication), χρησιμοποιώντας αλγόριθμο δημοσίου κλειδιού.

Κρυπτογράφηση

Όταν η Ελένη θέλει να στείλει ένα μυστικό μήνυμα στον Νίκο κοιτάζει το δημόσιο κλειδί του Νίκου και το χρησιμοποιεί για να κρυπτογραφήσει το μήνυμα και στην συνέχεια το στέλνει. Με την σειρά του ο Νίκος χρησιμοποιεί το ιδιωτικό του κλειδί για να αποκρυπτογραφήσει το μήνυμα και το διαβάζει.

Ηλεκτρονική υπογραφή

Για την υπογραφή ενός μηνύματος, η Ελένη κάνει έναν υπολογισμό εμπεριέχοντας το ιδιωτικό της κλειδί και το μήνυμα το ίδιο. Το αποτέλεσμα λέγεται ηλεκτρονική υπογραφή και επικολλάται στο μήνυμα, το οποίο και στέλνεται. Ο Νίκος για να επιβεβαιώσει την υπογραφή, κάνει έναν υπολογισμό χρησιμοποιώντας το μήνυμα, την υπογραφή της Ελένης και το δημόσιο κλειδί της Ελένης. Αν το αποτέλεσμα δείξει ότι το μήνυμα υπολογισμένο με το δημόσιο κλειδί της Ελένης είναι ίδιο με την υπογραφή της τότε το μήνυμα είναι αυθεντικό, διαφορετικά υπάρχει περίπτωση αλλοίωσης του μηνύματος.

Συνεπώς η κρυπτογράφηση και η εξακρίβωση γνησιότητας λαμβάνουν χώρα χωρίς το διαμοιρασμό ιδιωτικών κλειδιών, κάθε άτομο χρησιμοποιεί μόνο τα δημόσια κλειδιά του άλλου και το δικό του ιδιωτικό κλειδί. Καθένας μπορεί να στείλει κρυπτογραφημένα μηνύματα ή να επιβεβαιώσει ένα υπογεγραμμένο μήνυμα, χρησιμοποιώντας μόνο δημόσια κλειδιά, αλλά μόνο κάποιος ο οποίος έχει στην κατοχή του το σωστό ιδιωτικό κλειδί μπορεί να κρυπτογραφήσει και να υπογράψει ένα μήνυμα.

Στη συνέχεια παρουσιάζονται οι πιο δημοφιλείς αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού.

RSA

Ο RSA είναι ένα κρυπτοσύστημα δημοσίου κλειδιού για κρυπτογράφηση και εξακρίβωση γνησιότητας. Εφευρέθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman. Δουλεύει ως εξής: Παίρνουμε δύο μεγάλους πρώτους αριθμούς, p και q και βρίσκουμε το γινόμενό τους $n=pq$, το n λέγεται διαιρέτης. Διαλέγουμε έναν αριθμό e ο οποίος είναι μικρότερος από τον n και σχετικά πρώτος με το $(p-1)(q-1)$, δηλαδή ο e και το $(p-1)(q-1)$ δεν έχουν κοινούς διαιρέτες εκτός από το 1. Βρίσκουμε άλλον έναν αριθμό d τέτοιος ώστε το $(ed-1)$ να είναι διαιρέσιμο από το $(p-1)(q-1)$. Οι τιμές e και d ονομάζονται **δημόσιοι** και **ιδιωτικοί δείκτες** αντίστοιχα. Το δημόσιο κλειδί είναι το ζευγάρι (n,e) και το ιδιωτικό το (n,d). Οι παράγοντες p και q μπορεί να κρατηθούν μαζί με το ιδιωτικό κλειδί ή να καταστραφούν.

Είναι δύσκολο πιθανώς να βρεθεί το ιδιωτικό κλειδί *d* από το δημόσιο *(n,e)*. Εάν κάποιος μπορέσει να αναλύσει το *n* σε p και q, θα μπορέσει να πάρει την τιμή *d*. Η ασφάλεια του RSA βασίζεται στην θεώρηση ότι η ανάλυση σε παράγοντες γινομένου είναι δύσκολη. Μια μέθοδος εύκολης ανάλυση σε παράγοντες γινομένου ή κάποια άλλη εφικτή επίθεση θα μπορούσε να "σπάσει" τον RSA.

Παρακάτω παρουσιάζεται ένα απλουστευμένο παράδειγμα για το πώς δουλεύει ο αλγόριθμος για κρυπτογράφηση και εξακρίβωση γνησιότητας:

RSA κρυπτογράφηση: Ας υποθέσουμε ότι η Αλίκη θέλει να στείλει ένα μήνυμα *m* στον Μπομπ. Η Αλίκη δημιουργεί το κρυπτογραφημένο μήνυμα *c* ως εξής : $c=m^e \bmod n$, όπου *e* και *n* είναι του Μπομπ το δημόσιο κλειδί και το στέλνει στον Μπομπ. Για την αποκρυπτογράφηση ο Μπομπ κάνει το εξής: $m=c^d \bmod n$, η σχέση μεταξύ *e* και *d* εξασφαλίζει ότι ο Μπομπ θα αποκρυπτογραφήσει σωστά το *m*. Εφόσον μόνο ο Μπομπ κατέχει το *d*, μόνο αυτός μπορεί να το αποκρυπτογραφήσει.

RSA εξακρίβωση γνησιότητας: Τώρα ας υποθέσουμε ότι η Αλίκη θέλει να στείλει ένα μήνυμα *m* στον Μπομπ έτσι ώστε αυτός να είναι σίγουρος ότι το μήνυμα είναι αυθεντικό και προέρχεται από την Αλίκη. Η Αλίκη δημιουργεί μια ηλεκτρονική υπογραφή *s* ως εξής: $s=m^d \bmod n$, όπου *d, n* είναι το ιδιωτικό κλειδί της Αλίκης, και στέλνει τα *m, s* στον Μπομπ. Για να γίνει η επιβεβαίωση της υπογραφής ο Μπομπ ελέγχει το μήνυμα *m* που πήρε με αυτό που βγαίνει από την πράξη $s^e \bmod n$, όπου *e,n* είναι το δημόσιο κλειδί της Αλίκης.

Diffie-Hellman

Ο αλγόριθμος Diffie-Hellman είναι ένα πρωτόκολλο συμφωνίας που επιτρέπει την ανταλλαγή ενός μυστικού κλειδιού χρησιμοποιώντας τεχνικές των αλγορίθμων δημοσίου κλειδιού. Αναπτύχθηκε από τους Diffie και Hellman το 1976.

Το πρωτόκολλο έχει δύο παραμέτρους συστήματος *p* και *g*. Είναι και οι δύο δημόσιες και μπορούν να χρησιμοποιηθούν από όλους τους χρήστες σε ένα σύστημα. Η παράμετρος *p* είναι ένας πρώτος αριθμός και η παράμετρος *g* είναι ένας ακέραιος μικρότερος του *p*, ο οποίος είναι ικανός να παράγει κάθε αριθμό από το *1* έως το *p-1* όταν πολλαπλασιαστεί με τον εαυτό του ορισμένες φορές modulo τον πρώτο *p*.

Ας υποτεθεί ότι η Ελένη και ο Νίκος θέλουν να συμφωνήσουν σε ένα μυστικό κλειδί χρησιμοποιώντας το παραπάνω πρωτόκολλο. Προχωρούν ως ακολούθως: Πρώτα η Ελένη παράγει μια τυχαία ιδιωτική τιμή *α* και ο Νίκος παράγει μια τυχαία ιδιωτική τιμή *b*. Έπειτα και οι δύο παράγουν τις δημόσιες τιμές χρησιμοποιώντας τις παραμέτρους *p* και *g* και τις ιδιωτικές τους τιμές. Η δημόσια τιμή της Ελένης είναι η $g^a \bmod p$ και του Νίκου $g^b \bmod p$. Στη συνέχεια ανταλλάσσουν τις δημόσιες τιμές τους. Τελικά, η Ελένη υπολογίζει $k_{ab}=(g^b)^a \bmod p$ και ο Νίκος $k_{ba}=(g^a)^b \bmod p$. Εφόσον $k_{ab}=k_{ba}=k$, η Ελένη και ο Νίκος τώρα έχουν μοιραστεί ένα μυστικό κλειδί *k*.

Η ασφάλεια του πρωτοκόλλου εξαρτάται πάνω στο πρόβλημα του διακριτού λογάριθμου. Υποτίθεται ότι είναι υπολογιστικά μη πρακτικό να υπολογιστεί το κοινό μυστικό κλειδί *k* όταν δοθούν δύο δημόσιες τιμές $g^a \bmod p$ και $g^b \bmod p$ όταν ο πρώτος *p* είναι αρκετά μεγάλος.

Το πρωτόκολλο Diffie-Hellman είναι ευάλωτο σε μια *επίθεση παρεμβαλλόμενου προσώπου.* Σε αυτή την επίθεση ένας αντίπαλος η Κάρολ, εμποδίζει την δημόσια τιμή της Αλίκης να σταλεί στον Μπομπ και στέλνει την δική της σ' αυτόν. Όταν ο Μπομπ στέλνει την δική του τιμή, η Κάρολ την αντικαθιστά με την δική της και την στέλνει στην Αλίκη. Η Κάρολ και η Αλίκη συμφωνούν σε ένα μυστικό κλειδί και η Κάρολ και ο Μπομπ συμφωνούν σε άλλο. Μετά την ανταλλαγή αυτή η Κάρολ μπορεί να αποκρυπτογραφήσει οποιοδήποτε μήνυμα στέλνεται από τους άλλους δύο και πιθανόν να το αλλάξει και να το επαναμεταδώσει στους αντίστοιχους παραλήπτες. Η αδυναμία του αλγορίθμου οφείλεται στο γεγονός ότι το πρωτόκολλο δεν πιστοποιεί τους συμμετέχοντες σ' αυτήν την διαδικασία. Ορισμένες πιθανές λύσεις συμπεριλαμβάνουν την χρήση ηλεκτρονικών υπογραφών και άλλων ειδών πρωτοκόλλων.

Digital Signature Algorithm και Digital Signature Standard

Ο DSA είναι ένας αλγόριθμος ηλεκτρονικών υπογραφών και τα αρχικά του σημαίνουν **Digital Signature Algorithm**. Ο DSA δημοσιεύθηκε από το NIST στα πλαίσια του **Digital Signature Standard** (**DSS**), ενός σχεδίου για την κυβέρνηση των Η.Π.Α.

Ο DSA είναι βασισμένος επάνω στο πρόβλημα του διακριτού λογάριθμου και προέρχεται από τα κρυπτοσυστήματα που προτάθηκαν από τους Schnorr και ElGamal. Είναι μόνο για εξακρίβωση γνησιότητας. Ο αλγόριθμος γενικά θεωρείται ασφαλής όταν το κλειδί του είναι αρκετά μεγάλο. Το πρότυπο DSS αρχικά προτάθηκε για μέγεθος κλειδιού 512-bit αλλά μετά από αρκετή κριτική λόγω του ότι δεν ήταν ασφαλής αναθεωρήθηκε το πρότυπο DSS με χρήση κλειδιού μεγέθους μέχρι 1024-bits.

Στον DSA η δημιουργία της υπογραφής είναι πιο γρήγορη από την επιβεβαίωσή της, αντίθετα με τον RSA όπου εκεί η επιβεβαίωση της υπογραφής είναι πιο γρήγορη από την δημιουργία της.
Μια σύντομη περιγραφή του αλγορίθμου είναι η εξής:

11. Επιλέγεται ένας μεγάλος πρώτος αριθμός p μεταξύ 512 και 1024 bits.
12. Βρίσκεται ένας πρώτος παράγοντας q του p-1 160 bits.
13. Υπολογίζεται $g=h^{(p-1)/q} \bmod p$, όπου h ένας αριθμός μικρότερος από p-1.
14. Διαλέγουμε έναν άλλο αριθμό x<q ως το private key του αποστολέα.
15. Υπολογίζεται $y=g^x \bmod p$ και χρησιμοποιείται ως το public key του αποστολέα.
16. Ο αποστολέας υπογράφει το μήνυμα με το ζευγάρι (r,s) όπου $r=(g^k \bmod p) \bmod q$ και $s=(k^{-1}(SHA1(m)+xr)) \bmod q$, όπου m το μήνυμα, k ένας τυχαίος αριθμός και SHA1 η συνάρτηση για message digest.

Το παρόν κρυπτοσύστημα είναι αρκετά καινούργιο και δεν έχει γίνει αρκετή μελέτη πάνω σ' αυτό έτσι ώστε οι χρήστες να είναι πεπεισμένοι για την ασφάλειά του. Η πιστοποίηση της υπογραφής του DSA είναι αρκετά αργή. Η ύπαρξη ενός δεύτερου προτύπου πιστοποίησης θα ταλαιπωρήσει τις βιομηχανίες υπολογιστών διότι έχουν ήδη δεχθεί ως πρότυπο τον RSA.

Συναρτήσεις κατακερματισμού (Hash Functions)

Μια συνάρτηση κατακερματισμού *H* είναι ένας μετασχηματισμός ο οποίος παίρνει μία μεταβλητού μεγέθους είσοδο *m* και επιστρέφει ένα σταθερού μεγέθους string, το οποίο ονομάζεται τιμή κατακερματισμού *h,* δηλαδή *(h=H(m))*. Αυτές οι συναρτήσεις με μόνο αυτή την ιδιότητα έχουν μια ποικιλία από πολλές γενικού περιεχομένου εφαρμογές αλλά όταν χρησιμοποιούνται στην κρυπτογραφία τότε επιλέγονται με κάποιες επιπρόσθετες ιδιότητες.

Οι βασικές απαιτήσεις για μια κρυπτογραφική συνάρτηση κατακερματισμού είναι:

- Η είσοδος μπορεί να έχει οποιοδήποτε μέγεθος
- Η έξοδος έχει σταθερό μέγεθος
- Η *H(x)* είναι εύκολο να υπολογισθεί για οποιοδήποτε *x*
- Η *H(x)* είναι μιας κατεύθυνσης: Μια συνάρτηση κατακερματισμού λέγεται μιας κατεύθυνσης αν είναι δύσκολο να αντιστραφεί, δηλαδή αν δοθεί μια τιμή κατακερματισμού *h* τότε είναι δύσκολο να βρούμε αυτό το x για το οποίο θα ισχύει *H(x)=h*.
- Η *H(x)* δεν έχει συγκρούσεις: Μια συνάρτηση *H(x)* δεν έχει συγκρούσεις αν είναι υπολογιστικά μη πρακτικό να βρούμε δύο εισόδους *x* και *y* τέτοιες ώστε *H(x)=H(y)*.

Μια τιμή κατακερματισμού αντιπροσωπεύει με λιτό τρόπο ένα μεγαλύτερο μήνυμα ή κείμενο από το οποίο υπολογίστηκε. Παραδείγματα από γνώστες συναρτήσεις κατακερματισμού είναι οι MD2, MD5 και SHA.

Επειδή οι συναρτήσεις κατακερματισμού είναι γρηγορότερες από τους αλγορίθμους ηλεκτρονικών υπογραφών, συνηθίζεται αντί να υπολογίζεται η ηλεκτρονική υπογραφή ενός κειμένου, να υπολογίζεται η ηλεκτρονική υπογραφή της τιμής κατακερματισμού του που είναι και πιο μικρή από το ίδιο το κείμενο.

MD2, MD4 και MD5

Οι MD2, MD4 και MD5 είναι αλγόριθμοι *σύνοψης μηνυμάτων* (message digest) και αναπτύχθηκαν από τον Rivest. Ο προορισμός τους είναι για εφαρμογές ηλεκτρονικών υπογραφών όπου ένα μεγάλο μήνυμα πρέπει να συμπιεστεί με ασφάλεια προτού υπογραφθεί με το ιδιωτικό κλειδί. Και οι τρεις αλγόριθμοι παίρνουν ένα μήνυμα με αυθαίρετο μέγεθος και παράγουν μια 128-bit σύνοψή του. Παρόλο που οι δομές και των τριών αλγορίθμων μοιάζουν κάπως, ο σχεδιασμός του MD2 διαφέρει λίγο από τους υπόλοιπους δύο και έχει βελτιστοποιηθεί για μηχανές των 8-bit, ενώ οι MD4 και MD5 προορίζονται για 32-bit μηχανές.

Στον MD2 το μήνυμα πρώτα "γεμίζεται" στο τέλος με bytes έτσι ώστε το μέγεθος του σε bytes να είναι διαιρέσιμο με το 16. Έπειτα ένα 16-byte άθροισμα ελέγχου προστίθεται στο τέλος και στη συνέχεια υπολογίζεται πάνω σ' αυτό η τιμή κατακερματισμού του.

Στον MD4 το μήνυμα "γεμίζεται" στο τέλος με bits έτσι ώστε να εξασφαλισθεί ότι το μέγεθός του σε bits είναι διαιρέσιμο με το 512 αν προσθέσουμε και το 448. Μια 64-bit αναπαράσταση του αρχικού μήκους του μηνύματος προστίθεται με το μήνυμα. Ύστερα το μήνυμα επεξεργάζεται σε 512-bit μέρη στην επαναληπτική δομή των Damgard-Merkle και κάθε μέρος επεξεργάζεται σε τρεις διακεκριμένους γύρους. Γρήγορα ανακαλύφθηκαν διάφορες επιθέσεις γι' αυτόν τον αλγόριθμο και ο Dobbertin έδειξε πως μπορούν να βρεθούν

συγκρούσεις σε χρόνο μικρότερο από ένα λεπτό σε ένα τυπικό PC. Έτσι ο MD4 σήμερα θεωρείται ότι έχει σπαστεί.

Ο MD5 είναι ένας MD4 με ζώνες ασφαλείας. Είναι πιο αργός από τον MD4 αλλά και πιο ασφαλής. Ο αλγόριθμος αποτελείται από τέσσερις διακεκριμένους γύρους οι οποίοι έχουν λίγο διαφορετική σχεδίαση απ' αυτούς του MD4. Το μέγεθος του συνοπτικού μηνύματος καθώς και οι απαιτήσεις "γεμίσματος" παραμένουν οι ίδιες.

Secure Hash Algorithm (SHA)

Ο SHA, που σημαίνει Secure Hash Algorithm, καθορίστηκε στο **Secure Hash Standard** (**SHS**) και αναπτύχθηκε από το NIST. Ο σχεδιασμός του μοιάζει αρκετά με αυτούς της οικογένειας των συναρτήσεων κατακερματισμού του MD4.

Ο αλγόριθμος παίρνει έναν μήνυμα μικρότερο από 2^{64} bits σε μέγεθος και παράγει ένα συνοπτικό μήνυμα των 160 bit. Ο αλγόριθμος είναι λίγο αργότερος από τον MD5 αλλά το μεγαλύτερο συνοπτικό μήνυμα τον κάνει πιο ασφαλή απέναντι σε brute-force συγκρούσεις και επιθέσεις αντιστροφής.

Στεγανογραφία

Η στεγανογραφία είναι η τεχνική του να κρύβονται μυστικά μηνύματα μέσα σε άλλα μηνύματα, έτσι ώστε η παρουσία των μυστικών μηνυμάτων να μη γίνεται αντιληπτή. Ιστορικά κόλπα περιλαμβάνουν αόρατα μελάνια, πολύ μικρές διατρήσεις πάνω σε επιλεγμένους χαρακτήρες, μικρές διαφορές μεταξύ χειρόγραφων χαρακτήρων, σημάδια από μολύβι πάνω σε χαρακτήρες τυπωμένους, κομμάτια που καλύπτουν το μεγαλύτερο μέρος του μηνύματος εκτός από ορισμένους χαρακτήρες κ.ο.κ. Τελευταία συνηθίζεται να κρύβονται μυστικά μηνύματα πάνω σε γραφικές εικόνες.

Firewalls

Ένας από τους αποτελεσματικότερους τρόπους για την προστασία του δικτύου από πιθανούς παραβάτες είναι η χρήση ενός συστήματος Firewall μεταξύ του τοπικού δικτύου και του Internet. Το **Firewall** εξασφαλίζει ότι όλη η επικοινωνία μεταξύ του δικτύου μιας επιχείρησης και το Διαδίκτυο είναι σύμφωνη με την πολιτική ασφάλειας της επιχείρησης. Για να το πετύχει αυτό, ένα Firewall πρέπει να εντοπίζει και να ελέγχει τη ροή επικοινωνίας που περνάει μέσα από αυτό. Για να πετύχει τον έλεγχο των υπηρεσιών που βασίζονται στο TCP/IP, αν δηλαδή θα επιτρέψει, απορρίψει, κρυπτογραφήσει ή καταγράψει την επικοινωνία, το Firewall πρέπει να λαμβάνει, αποθηκεύει και να διαχειρίζεται πληροφορία που προέρχεται από όλα τα επίπεδα επικοινωνίας και από άλλες εφαρμογές. Οι συσκευές Firewall ενώ συχνά είναι απαραίτητες για την προστασία του site, αποτελούν επίσης και πηγή κινδύνου, γιατί, πρώτον οι χρήστες πιστεύουν ότι από την στιγμή που αγοράσθηκε το προϊόν, η ασφάλεια έχει εξασφαλισθεί, πράγμα που απέχει πολύ από την αλήθεια, και δεύτερον, γιατί ο ίδιος ο κώδικας είναι πιθανόν να μην συμπεριφέρεται όπως θα έπρεπε, με αποτέλεσμα να αφήνει τις πίσω πόρτες ανοικτές.

Ένα firewall αποτελείται από τρεις ομάδες συνιστωσών:

- *φίλτρα* για μπλοκάρισμα και/ή παρακολούθηση μετάδοσης συγκεκριμένου είδους μηνυμάτων (καθορισμένα από τον τύπο, τον προορισμό τους ή συνδυασμό και των δύο),
- *gateways* για προώθηση των αποδεκτών μηνυμάτων από τη μια μεριά του firewall στην άλλη,
- *application proxies* που εκτελούν έλεγχο ειδικής πρόσβασης σε εφαρμογές, παρακολούθηση και αναφορά.

Από κει και πέρα, για την επίτευξη της ασφάλειας σε μεμονωμένες περιπτώσεις χρήσης διαφόρων υπηρεσιών το πιο συνηθισμένο μέτρο ασφάλειας είναι τα γνωστά μας Ids και Passwords, τα οποία όμως δεν αποτελούν εγγύηση καθώς πολλοί χρήστες προτιμούν ένα ευκολομνημόνευτο password που όμως είναι πολύ εύκολο να βρεθεί από έναν αποφασισμένο hacker. Επίσης, θα πρέπει να γνωρίζουμε ότι οι περισσότερες απειλές (το 80% σύμφωνα με έρευνες) προέρχονται από νόμιμους χρήστες με έγκυρο password.

Μεγαλύτερη ασφάλεια προσφέρουν τα συστήματα που κάνουν χρήση των έξυπνων καρτών. Σε αυτά τα συστήματα, ο χρήστης για να μπει στο λογαριασμό του δεν χρειάζεται να είναι κάτοχος του password μόνο, άλλα και της προσωπικής του κάρτας. Τα επόμενα χρόνια επίσης θα είμαστε μάρτυρες μιας ραγδαίας ανάπτυξης βιομετρικών τεχνικών, όπως αυθεντικοποίηση με την ίριδα των ματιών, της φωνής, των αποτυπωμάτων κτλ.

Ένα άλλο μέτρο είναι η χρήση κρυπτογραφικών μεθόδων. Ένα ευρύτατα χρησιμοποιούμενο εργαλείο για την προστασία της μυστικότητας είναι αυτό που οι κρυπτογράφοι αποκαλούν «μυστικό κλειδί». Τα passwords σύνδεσης και οι αριθμοί PIN των πιστωτικών καρτών είναι παραδείγματα μυστικών κλειδιών. Οι καταναλωτές μοιράζονται αυτά τα κλειδιά μόνο με τους τρίτους που θέλουν να επικοινωνήσουν, όπως on-

line υπηρεσίες συνδρομής και τράπεζες. Έτσι οι προσωπικές πληροφορίες αποκρύβονται και μόνο μία από τις δυο πλευρές που έχει το μυστικό κλειδί στην κατοχή της μπορεί να τις αποκρυπτογραφήσει.

Όμως, το παραπάνω σύστημα, παρά την ευρεία χρήση του, παρουσιάζει κάποιους περιορισμούς. Από τη μία, λόγω της τεράστιας εξάπλωσης του διαδικτύου, είναι άβολο για τους χρήστες να δημιουργούν και να θυμούνται διαφορετικά passwords για κάθε περίσταση. Από την άλλη, κατά την αποστολή του, το password μπορεί να πέσει σε λάθος χέρια ή κάποια από τις δυο πλευρές να το χρησιμοποιήσει σε «υποχθόνιες» πράξεις και μετά να αρνηθεί το όλο συμβάν. Έτσι πάμε στην τεχνολογία ψηφιακών ταυτοτήτων η οποία λύνει αυτά τα προβλήματα γιατί δεν βασίζεται στη διαμοίραση μυστικών κλειδιών.

Ο σχεδιασμός ασφαλείας πρέπει να αποτελεί μέρος κάθε εφαρμογής ηλεκτρονικού εμπορίου. Είναι σημαντικό όμως να λαμβάνεται υπόψη από την αρχή του σχεδιασμού της εφαρμογής, γιατί είναι πολύ πιο δαπανηρό να προστεθεί ασφάλεια κατά τη διάρκεια της. Υπάρχουν πέντε βασικά βήματα για το σχεδιασμό της ασφάλειας των συστημάτων ηλεκτρονικού εμπορίου:

Καθορισμός της πολιτικής ασφαλείας.

Προσθήκη των απαραίτητων μηχανισμών ασφαλείας στην εφαρμογή.

Σχεδιασμός της ασφάλειας του φυσικού, δικτυακού και υπολογιστικού περιβάλλοντος του συστήματος.

Ανάπτυξη μηχανισμών ανάδρασης, επίβλεψης και περιοδικού ελέγχου για παρατήρηση της ορθής λειτουργίας του συστήματος.

Χρήση των αποτελεσμάτων της ανάδρασης, επίβλεψης και περιοδικού ελέγχου για βελτίωση του σχεδιασμού, υλοποίησης και λειτουργίας του συστήματος.

ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Καθορισμός της πολιτικής ασφαλείας

Το πρώτο βήμα στο σχεδιασμό ασφαλείας είναι ο καθορισμός της πολιτικής ασφαλείας. Η πολιτική θα πρέπει να καλύπτει όλο το σύστημα, περιλαμβάνοντας συστήματα πληροφοριών (δίκτυα και υπολογιστές), δεδομένα (πληροφορίες ανάπτυξης, παραγωγής και αποθήκευσης) και ανθρώπινο δυναμικό (χειριστές, προσωπικό συντήρησης, πελάτες). Η πολιτική θα πρέπει να περιέχει αναφορές για το τι προστατεύεται, τι είδος προστασίας χρειάζεται, ποιος είναι υπεύθυνος για τα διάφορα μέρη του συστήματος, για την απαραίτητη εκπαίδευση, και τι είδος επίβλεψης και περιοδικού ελέγχου απαιτείται.

Σχεδιασμός του περιβάλλοντος

Το δεύτερο βήμα είναι ο σχεδιασμός του περιβάλλοντος της εφαρμογής. Ο σχεδιασμός του περιβάλλοντος περιλαμβάνει όλες τις συνιστώσες έξω από την ίδια την εφαρμογή, όπως είναι οι υπολογιστές, τα λειτουργικά συστήματα, τα δίκτυα και οι φυσικές εγκαταστάσεις. Συχνά το περιβάλλον μπορεί να παρέχει κάποιες δυνατότητες προστασίας της εφαρμογής, έτσι ώστε η εφαρμογή να μη χρειάζεται να τις αντιγράψει. Αξίζει να σημειωθεί όμως ότι τέτοιες δυνατότητες πρέπει να καταγράφονται έτσι ώστε η εφαρμογή να μπορεί να επαναδημιουργηθεί οπουδήποτε εμφανισθεί ανάγκη. Σε άλλες περιπτώσεις το ίδιο το περιβάλλον πρέπει να δεσμεύει την εφαρμογή με διάφορους τρόπους ή να απαιτεί ειδικές μεθόδους ασφαλείας να λαμβάνονται από την εφαρμογή αν δεν περιλαμβάνονται από το περιβάλλον. Για παράδειγμα, ας υποτεθεί ότι μια εφαρμογή λειτουργεί σε συστήματα προστατευμένα με δυνατή φυσική ασφάλεια. Επιπλέον, οι χειριστές εκτελούν όλες τις εργασίες τους τοπικά. Σ' αυτήν την περίπτωση, η εφαρμογή θα δώσει λιγότερη προσοχή στον έλεγχο πιστοποίησης και στον έλεγχο πρόσβασης σε λειτουργίες διαχείρισης, γιατί μπορεί να υποθέσει ότι οι χειριστές έχουν την απαραίτητη πιστοποίηση από την αρχή όταν απέκτησαν πρόσβαση. Όμως σε μια εφαρμογή όπου η διαχείριση της είναι σχεδιασμένη να πραγματοποιείται εξ αποστάσεως έχει διαφορετικές απαιτήσεις. Γενικά είναι καλή πρακτική για την εφαρμογή να έχει τα δικά της μέσα για έλεγχο πιστοποίησης και πρόσβασης γιατί είναι πιθανόν οι μηχανισμοί φυσικής ασφαλείας να «κρεμάσουν».

Στην πράξη ο σχεδιασμός του περιβάλλοντος και ο σχεδιασμός των μηχανισμών ασφαλείας της εφαρμογής θα πρέπει να αλληλεπιδρούν με χρήσιμο τρόπο. Μερικά προβλήματα ασφαλείας είναι ευκολότερο να λυθούν από την εφαρμογή παρά από το περιβάλλον και το αντίστροφο. Σε μερικές περιπτώσεις, ειδικά στο σχεδιασμό των προϊόντων, η εφαρμογή μπορεί να επιβάλλει κάποιες απαιτήσεις στο περιβάλλον στο οποίο θα χρησιμοποιηθεί. Τελικά το πιο σημαντικό θέμα κατά την ανάπτυξη του σχεδίου ασφαλείας είναι ο σχεδιασμός ολόκληρου του συστήματος (εφαρμογής και περιβάλλοντος).

Σχεδιασμός των μηχανισμών ασφαλείας της εφαρμογής

Το τρίτο βήμα στο σχεδιασμό ασφαλείας είναι η παροχή μηχανισμών ασφαλείας για την ίδια την εφαρμογή. Ο γενικός σχεδιασμός της εφαρμογής μαζί με την πολιτική ασφαλείας θα πρέπει να παρέχει τις απαιτήσεις για το τι προστατεύεται και να δίνει μια καθοδήγηση για το είδος της προστασίας που χρειάζεται. Το σχέδιο ασφαλείας τότε μπορεί να χρησιμοποιήσει διάφορες συνιστώσες τεχνολογιών όπως συστήματα κρυπτογράφησης, πιστοποίησης και εξουσιοδότησης. Επιπρόσθετα σ' αυτούς τους γενικούς μηχανισμούς για έλεγχο της πρόσβασης στις πληροφορίες, μπορεί να υπάρχουν και κάποιες ειδικές απαιτήσεις της ίδιας της εφαρμογής. Για παράδειγμα, αν πρόκειται για εφαρμογή πωλήσεων λογισμικού πάνω από το δίκτυο, το σύστημα ασφαλείας μπορεί να περιέχει ειδικά κλειδιά που επιτρέπουν το λογισμικό να τρέχει μόνο στο συγκεκριμένο υπολογιστή του πελάτη.

Επίβλεψη και περιοδικός έλεγχος

Πέρα από τις ειδικές απαιτήσεις της εφαρμογής, η ασφάλεια απαιτεί μηχανισμούς ανάδρασης ώστε να εξασφαλίζεται ότι οι μηχανισμοί ασφαλείας λειτουργούν σωστά, μηχανισμούς αποθήκευσης ώστε να περιορίζεται η έκταση της ζημιάς, και μηχανισμούς ανάκτησης όταν παρουσιάζεται το πρόβλημα. Στο φυσικό κόσμο, είναι απαραίτητος ο νυχτοφύλακας που διασφαλίζει ότι οι πόρτες των χώρων είναι κλειδωμένες. Στον ηλεκτρονικό χώρο, αυτοί οι έλεγχοι αναλαμβάνονται από μηχανισμούς παρακολούθησης, ελέγχου ταχύτητας και υπηρεσίες πελατών. Η πληροφορία που παρέχεται από αυτούς τους μηχανισμούς μπορεί να χρησιμοποιηθεί με διάφορους τρόπους: για επαναλειτουργία σε περίπτωση προβλήματος, για έλεγχο ώστε να εξασφαλίζεται ότι οι επιθέσεις ήταν ανεπιτυχείς, για επιβεβαίωση ότι η λειτουργία συμφωνεί με την πολιτική ασφαλείας, και για αξιολόγηση αν η πολιτική ασφαλείας, ο σχεδιασμός και οι μηχανισμοί είναι αποτελεσματικοί για την εφαρμογή.

Ειδικοί στην ασφάλεια υπολογιστών συχνά επισημαίνουν ότι η ασφάλεια πρέπει να περικλείει ολόκληρο το σύστημα. Οι σχεδιαστές και οι χειριστές μιας υπηρεσίας πρέπει να λαμβάνουν σοβαρά υπόψη τους θέματα σχετικά με την εφαρμογή και τους κινδύνους πριν αποφασίσουν για το επίπεδο της ασφάλειας που θα παρέχεται, και εσωτερικά σε κάθε επίπεδο πρέπει να σκεφθούν τη σχετιζόμενη δύναμη των μηχανισμών ασφαλείας που θα αναπτυχθούν.

Ανάθεση ρόλων και υπευθυνοτήτων

Πολύ σημαντικό μέρος του σχεδιασμού της πολιτικής ασφαλείας είναι οι ρόλοι και οι αντίστοιχες υπευθυνότητες (του κάθε ρόλου) που πρέπει να ανατεθούν σε πρόσωπα-κλειδιά για την ορθή λειτουργία ενός συστήματος ηλεκτρονικού εμπορίου.

- Υπεύθυνος Ασφαλείας

Ο ρόλος του Υπεύθυνου Ασφαλείας περιλαμβάνει:

-την έγκαιρη και αποτελεσματική αντιμετώπιση περιστατικών ασφαλείας και ατυχημάτων ή έκτακτων γεγονότων.

-τη διαχείριση των δικαιωμάτων προσπέλασης.

-τη δημιουργία σχεδίου για την εκπαίδευση και ενημέρωση του υπόλοιπου προσωπικού.

-τη σύνταξη αναφορών για την ασφάλεια του συστήματος ανά τακτά χρονικά διαστήματα.

-την έγκαιρη ενημέρωση του σχετικά με οποιεσδήποτε αλλαγές που μπορούν να επηρεάσουν την ασφάλεια του συστήματος όπως διακοπές για συντήρηση ή επισκευή, πρόσληψη προσωπικού, αλλαγές στον εξοπλισμό κ.λπ.

- Διαχειριστής Συστήματος

Ο Διαχειριστής Συστήματος έχει τις ακόλουθες υπευθυνότητες:

-τη διαχείριση του υλικού και του εξοπλισμού του συστήματος και την καταγραφή του.

-τη διαχείριση (σε συνεργασία με τον Υπεύθυνο Ασφαλείας) των δικαιωμάτων προσπέλασης.

-την επίβλεψη του συστήματος για την ορθή του λειτουργία και το χειρισμό σε περίπτωση δυσλειτουργιών.

-την έγκαιρη ενημέρωση του σχετικά με οποιεσδήποτε αλλαγές που μπορούν να επηρεάσουν την ασφάλεια του συστήματος όπως διακοπές για συντήρηση ή επισκευή, πρόσληψη προσωπικού, αλλαγές στον εξοπλισμό κ.λπ.

- Διοικητικός Υπεύθυνος

Πρόκειται για το πρόσωπο που επικοινωνεί με τη διοίκηση και το προσωπικό του συστήματος. Έτσι παράλληλα με τις διάφορες διοικητικές του αρμοδιότητες είναι υπεύθυνος για:

-την επίβλεψη του Υπεύθυνου Ασφαλείας και του Διαχειριστή Συστήματος.
-τη μεταφορά των οδηγιών της διοίκησης στο υπόλοιπο προσωπικό.
-την παρακολούθηση της σωστής ολοκλήρωσης των προβλεπόμενων διαδικασιών.
-τη διατήρηση του ηθικού του προσωπικού σε ικανοποιητικό επίπεδο, ενός πολύ σημαντικού παράγοντα για την ασφάλεια του συστήματος.

- Χειριστές Συστήματος

Είναι υπεύθυνοι για την εκπλήρωση των καθηκόντων που τους ανατίθενται από τον Υπεύθυνο Ασφαλείας και το Διαχειριστή Συστήματος. Άλλες υπευθυνότητες τους είναι:
αναφορά περιστατικών σχετικών με την ασφάλεια του συστήματος και συνεισφορά τους στην επίλυση τους.
ενημέρωση για θέματα ασφαλείας.
η ακριβής τήρηση των κανονισμών του συστήματος.
η αποφυγή δραστηριοτήτων που μπορούν να επιφέρουν δυσλειτουργίες στο σύστημα.

Πλάνο Ασφαλείας

Το πλάνο ασφαλείας πρέπει να είναι πλήρες ώστε να ικανοποιεί όλες τις απαιτήσεις ασφαλείας που αναφέρθηκαν παραπάνω σε όποιο σημείο της υλοποίησης του συστήματος και αν εμφανίζονται αυτές.

Αναγνώριση και έλεγχος αυθεντικότητας
Αναγνωριστικά χρηστών
Με τη βοήθεια των αναγνωριστικών εξασφαλίζεται η ταυτοποίηση κάθε χρήστη ότι πραγματοποίησε μια ενέργεια.
Επιλογή συνθηματικών
Τα συνθηματικά (passwords) που υιοθετούν οι χρήστες πρέπει να έχουν αρκετό μήκος και να επιλέγονται με τέτοιο τρόπο, ώστε να είναι δύσκολο για κάποιον εισβολέα να τα μαντέψει ή να τα αποκρυπτογραφήσει από το αρχείο συνθηματικών.
Αποθήκευση συνθηματικών
Τα συνθηματικά των χρηστών θα πρέπει να αποθηκεύονται σε κατάλληλη μορφή, ώστε κανείς, ακόμα και ο Διαχειριστής του συστήματος να μην μπορεί να τα διαβάσει.
Συχνότητα αλλαγής των συνθηματικών
Τα συνθηματικά θα πρέπει να αλλάζουν αρκετά συχνά, ώστε να διασφαλίζεται η εμπιστευτικότητα τους.

Έλεγχος πρόσβασης
Δικαιώματα πρόσβασης
Για κάθε νέο λογαριασμό χρήστη θα πρέπει να καθορίζονται τα δικαιώματα πρόσβασης στους πόρους του συστήματος.
Αδρανής σταθμός εργασίας
Οι σταθμοί εργασίας θα πρέπει να κλειδώνονται όταν μένουν αδρανείς για κάποιο χρονικό διάστημα (προτεινόμενος χρόνος 10 λεπτά) ώστε να περιοριστεί η πιθανότητα ένας μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση.
Διαχείριση δικαιωμάτων
Κατάλληλος μηχανισμός επιτρέπει την πρόσβαση σε ιδιαίτερες λειτουργίες του συστήματος μόνο σε χρήστες που πρέπει να έχουν πρόσβαση σ' αυτές.
Πολιτική ελέγχου πρόσβασης
Πρόκειται για την απαραίτητη ύπαρξη καταγεγραμμένης πολιτικής για τον έλεγχο πρόσβασης.
Ασφάλεια του λογισμικού εφαρμογών
Η πρόσβαση στα αρχεία του λογισμικού εφαρμογών θα πρέπει να ελέγχεται με τη βοήθεια κατάλληλων προγραμμάτων.

Απόδοση ευθυνών
Καταγραφή των γεγονότων
Πρόκειται για την καταγραφή όλων των περιστατικών (γεγονότων ή λειτουργιών) που λαμβάνουν χώρα στο σύστημα κάθε χρονική στιγμή, ώστε κάθε επεισόδιο να μπορεί να διερευνηθεί και να αποδοθούν ευθύνες.
Διατήρηση των αρχείων καταγραφής γεγονότων
Θα πρέπει να διατηρείται κατάλληλο αρχείο καταγραφής γεγονότων για αρκετό χρονικό διάστημα. Επίσης θα πρέπει να υπάρχει ο κατάλληλος χώρος για την αποθήκευση του αρχείου καταγραφής γεγονότων.
Επιθεώρηση των αρχείων καταγραφής γεγονότων

Τα αρχεία καταγραφής γεγονότων θα πρέπει να επιθεωρούνται ανά τακτά χρονικά διαστήματα, ώστε να εξασφαλίζεται ότι όλοι οι χρήστες εκτελούν τις εργασίες για τις οποίες είναι εξουσιοδοτημένοι.
Διερεύνηση επεισοδίων
Όταν κάποια επεισόδια ανιχνεύονται ή υπάρχουν υποψίες γι' αυτά, πρέπει να διερευνούνται σε βάθος.

Προστασία από ιούς
Πρόληψη και αποτροπή
Θα πρέπει να ελαχιστοποιηθεί η πιθανότητα να προσβληθεί το σύστημα από ιούς οποιασδήποτε μορφής.
Ανίχνευση
Το σύστημα θα πρέπει να περιλαμβάνει μηχανισμούς περιοδικού ελέγχου για ιούς.
Αντιμετώπιση
Τέλος, θα πρέπει να υπάρχουν κατάλληλοι μηχανισμοί απομόνωσης και καταστροφής των ιών.

Διαχείριση ασφάλειας δικτύου
Διαχείριση δικτύου
Η διαχείριση των δικτύων πρέπει να γίνεται με ασφαλή τρόπο. Για οποιαδήποτε προβλήματα θα πρέπει να ενημερώνεται ο Υπεύθυνος Ασφαλείας.
Παρακολούθηση του δικτύου
Η κατάσταση του δικτύου θα πρέπει να παρακολουθείται, ώστε να διευκολύνεται η έγκαιρη ανίχνευση των προβλημάτων.
Εμπιστευτικότητα δεδομένων στο δίκτυο
Η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω δικτύου θα πρέπει να προστατεύεται.

Έλεγχος πρόσβασης μέσω δικτύου
Έλεγχος αυθεντικότητας εφαρμογών
Η επικοινωνία μεταξύ εφαρμογών θα πρέπει να γίνεται με ασφαλή τρόπο.
Απομακρυσμένη πρόσβαση σε μη ενεργές πόρτες
Μόνο οι είσοδοι (ports) που χρησιμοποιούνται θα πρέπει να είναι ενεργές και οι υπόλοιπες πρέπει να είναι κλειδωμένες.
Firewalls
Θα πρέπει να υπάρχει διαχωρισμός μεταξύ των δικτύων και προστασία τους με τη χρήση firewalls.

Ηλεκτρονικό Εμπόριο και Προσωπικά Δεδομένα

Οι έμποροι προκειμένου να μετρήσουν τις καταναλωτικές προτιμήσεις του κοινού με σκοπό να προσαρμόσουν στη βάση ζήτησης τις γραμμές παραγωγής τους και να προωθήσουν τις πωλήσεις τους μέσω του διαδικτύου, δημιουργούν νέους τρόπους συλλογής, επεξεργασίας και διασύνδεσης των προσωπικών δεδομένων. Τα προσωπικά δεδομένα συνήθως συλλέγονται κατά την αρχική φάση σύνδεσης του πελάτη με το δικτυακό χώρο του πωλητή και στην συνέχεια χρησιμοποιούνται σύγχρονες τεχνικές εξόρυξης δεδομένων (data mining) για την περαιτέρω ανάλυσή τους. Αποτέλεσμα της παραπάνω διαδικασίας είναι η δημιουργία βάσεων καταναλωτικών προφίλ των πελατών. Προφίλ ενός ατόμου νοείται ως μια συλλογή δεδομένων που μπορεί μοναδικά να προσδιορίσει την ταυτότητα του ατόμου αυτού.

Οι οντότητες οι οποίες τυπικά εμπλέκονται στην εγκατάσταση μιας ηλεκτρονικής σύνδεσης, με έμφαση στων πραγματοποίηση ηλεκτρονικών συναλλαγών και οι οποίες είναι ταυτόχρονα η πηγή και ο αποδέκτης των προσωπικών δεδομένων των χρηστών είναι οι εξής:

1. **Χρήστης**: Ο ενδιαφερόμενος για την απόκτηση μιας υπηρεσίας του διαδικτύου, την απόκτηση ενός προϊόντος με χρήση τεχνολογιών που βοηθούν στην ανάπτυξη του ηλεκτρονικού εμπορίου κ.λ.π.
2. **Παροχέας Υπηρεσιών Διαδικτύου**, **ΠΥΔ,** (Internet Service Provider, ISP): Η οντότητα που παρέχει, τυπικά σε χρήστες, το υλικό (hardware) και πιθανώς λογισμικό (software), για την απόκτηση πρόσβασης στις βασικές υπηρεσίες του διαδικτύου.
3. **Παροχέας Φυσικού Μέσου επικοινωνίας, ΠΦΜ**, (Carrier Provider): Η οντότητα που παρέχει το φυσικό τεχνολογικό μέσο μετάδοσης και επικοινωνίας δεδομένων π.χ. αναλογικές ή/και ψηφιακές

γραμμές, εξοπλισμός αναμετάδοσης σημάτων με χρήση ψηφιακών κέντρων, δορυφόρων κ.λ.π. Οι οντότητες αυτές τυπικά αντιπροσωπεύονται από μεγάλους τηλεπικοινωνιακούς οργανισμούς π.χ. ΟΤΕ.

4. **Παροχέας Τελικής Υπηρεσίας ΠΤΥ**. Η οντότητα που παρέχει με χρήση κάποιου πρωτοκόλλου επικοινωνίας, την ζητούμενη από τον χρήστη υπηρεσία π.χ. αναζήτηση πληροφοριών με χρήση μηχανών αναζήτησης (search machines), αγορά προιόντων με χρήση τεχνολογιών ανάπτυξης ηλεκτρονικού εμπορίου κ.λ.π.

Δύο επιπλέον οντότητες που παίζουν σημαντικό ρόλο στην διεκπεραίωση των ηλεκτρονικών συναλλαγών αλλά δεν εμπλέκονται, συνήθως, άμεσα σε αυτές είναι:

1. **Έμπιστες Τρίτες Οντότητες (ΕΤΟ)**: αυτές είναι έμπιστες οντότητες οι οποίες δεν εμπλέκονται άμεσα στην συναλλαγή αλλά μπορούν να καταφύγουν οι εμπλεκόμενοι μιας συναλλαγής σε περιπτώσεις διενέξεων, για την επαλήθευση των στοιχείων της συναλλαγής. Τυπικό έργο των οντοτήτων αυτών είναι η έκδοση και διαχείριση ψηφιακών πιστοποιητικών (digital certificates). Οι ΕΤΟ συναντούνται στην βιβλιογραφία και με τον όρο Αρχές Πιστοποίησης (ΑΠ).
2. **Λοιποί ενδιάμεσοι**: αυτές είναι τυπικά οι Τράπεζες που εμπλέκονται στην εκκαθάριση των πληρωμών είτε αυτές πραγματοποιούνται με τεχνολογίες ψηφιακού χρήματος είτε με χρήση πιστωτικών καρτών.

Στην Ελλάδα το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και 2774/99 (Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα) με τον οποίο η Αρχή Προστασίας Δεδομένων και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχουν αντίστοιχες αρμοδιότητες όπως ο νόμος αυτός ορίζει. Κάθε συλλογή και επεξεργασία στοιχείων των χρηστών του διαδικτύου (π.χ. ηλεκτρονική διεύθυνση αλληλογραφίας, διεύθυνση διαδικτύου κ.λ.π) εμπίπτουν στις διατάξεις των παραπάνω νόμων. Οποιαδήποτε χρήση των τηλεπικοινωνιακών υπηρεσιών όπως ορίζονται στο νόμο 2774/99 προστατεύεται από τις ρυθμίσεις για το απόρρητο των επικοινωνιών. Η άρση του απορρήτου σε δημόσιες αρχές είναι επιτρεπτή μόνο για τους λόγους και υπό τους όρους και διαδικασίες που ορίζει ο Ν. 2225/94 όπως ισχύει.

Οι κίνδυνοι

Ο χώρος του ηλεκτρονικού εμπορίου κρύβει πολλούς κινδύνους για τον ανυποψίαστο χρήστη. Οι περιπτώσεις όπου διακριτά καταγράφονται προσωπικά δεδομένα διακρίνονται στις παρακάτω κατηγορίες:

1. Όταν **με τη συγκατάθεσή του** ο χρήστης δίνει τα προσωπικά του στοιχεία, όποτε για παράδειγμα επιθυμεί να αγοράσει κάποιο προϊόν /υπηρεσία ή να κατεβάσει (download) κάποιο πρόγραμμα στον προσωπικό του υπολογιστή ή και να εγγραφεί σε κάποια υπηρεσία του διαδικτύου. Προσωπικά δεδομένα, όπως στοιχεία ταυτότητας, στοιχεία επαγγελματικά, στοιχεία εκπαίδευσης ή και ακόμα οικονομικά στοιχεία όπως είναι ο αριθμός της πιστωτικής κάρτας.
2. Όταν **χωρίς την συγκατάθεσή του** χρήστη, συλλέγονται προσωπικά στοιχεία μέσω των λεγόμενων προγραμμάτων cookies τα οποία καταγράφουν και επεξεργάζονται την συμπεριφορά του χρήστη κατά την πλοήγησή του στο διαδίκτυο (πχ προτιμήσεις).
3. Όταν στα πλαίσια του παροχέα υπηρεσιών πρόσβασης στο Internet τηρείται αρχείο με τα προσωπικά στοιχεία του χρήστη και κατ΄ επέκταση στοιχεία των ηλεκτρονικών διευθύνσεων (ιστοσελίδες) τις οποίες επισκέπτεται, τον ακριβή χρόνο και τη διάρκεια της επίσκεψης.

ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Άλλο ένα θεμελιώδες θέμα ασφαλείας συνίσταται στη διαφύλαξη του προσωπικού απορρήτου, το οποίο πλέον αποτελεί ένα ακανθώδες ζήτημα στο Internet. Ένας μεγάλος όγκος πληροφοριών μπορεί να συλλεχθεί σχετικά με τους χρήστες του Δικτύου και πολλές φορές δεν είναι ξεκάθαρο ποιος ή με ποιο τρόπο θα χρησιμοποιήσει αυτές τις πληροφορίες. Συγκεκριμένα, δύο από τις σημαντικότερες τεχνολογίες που σχετίζονται με το θέμα είναι: **α)** τα cookies και **β**) το Web tracking,.

Μέσω των Internet passports, διασφαλίζεται το προσωπικό απόρρητο του χρήστη, ενώ ταυτόχρονα επιτρέπεται στα Web sites να συλλέγουν πληροφορίες που χρειάζονται για να προσφέρουν εξειδικευμένες υπηρεσίες στους επισκέπτες τους. Η πιο κοινή χρήση των δεδομένων αυτών είναι η 'διευκόλυνση' της εισόδου των χρηστών σε Web sites που ζητούν όνομα χρήστη και password.

Το cookie που βρίσκεται στο σκληρό δίσκο περιλαμβάνει το όνομα του χρήστη και το password, με αποτέλεσμα να μη χρειάζεται να δηλώνονται κάθε φορά, αφού τα στέλνει στον server και ο χρήστης εισέρχεται στο site ελεύθερα. Τα cookies μπορεί να περιλαμβάνουν σχεδόν κάθε είδος πληροφοριών, όπως την τελευταία φορά που ένας χρήστης επισκέφθηκε κάποιο site, τα αγαπημένα του sites και άλλες παρόμοιες πληροφορίες. Μπορούν, επίσης, να χρησιμοποιηθούν για την παρακολούθηση των χρηστών όσο βρίσκονται σε κάποιο site και τη συλλογή πληροφοριών σχετικών με τις σελίδες που προτιμούν να επισκέπτονται.

Εκτός από τα cookies, υπάρχουν και άλλες μέθοδοι παρακολούθησης του τρόπου με τον οποίο οι χρήστες χρησιμοποιούν ένα Web site. Μία από αυτές προτείνει τη λεπτομερή εξέταση του ημερολογίου λειτουργίας του Web server. Η εξέταση αυτή επιτρέπει τον προσδιορισμό των δημοφιλέστερων σελίδων του site, των sites που μόλις επισκέφτηκαν οι χρήστες , του αριθμού των σελίδων που διαβάζουν σε μία τυπική επίσκεψη και άλλων σχετικών πληροφοριών.

Άλλες μέθοδοι στηρίζονται στη χρήση ορισμένων προγραμμάτων λογισμικού, ονόματι sniffers, τα οποία εξετάζουν κάθε πακέτο που εισέρχεται ή εξέρχεται από ένα Web site. Για τη διαφύλαξη του ιδιωτικού απορρήτου έχουν αναπτυχθεί αρκετές τεχνολογίες και πρότυπα. Σε αυτά περιλαμβάνονται τα Platform for Privacy Preferences (P3P), Internet Content and Exchange standard (ICE) και Open Profiling Standard (OPS). Οι τεχνολογίες αυτές ονομάζονται γενικά Internet passports. Τα Internet passports επιτρέπουν στους χρήστες να ελέγχουν ποιες προσωπικές πληροφορίες θα γίνουν διαθέσιμες στα Web sites, καθώς και τον τρόπο με τον οποίον αυτά θα τις χρησιμοποιήσουν. Επιτρέπουν, επίσης , στους χρήστες να ελέγχουν το είδος των πληροφοριών που θα συλλέξει το site κατά τη διάρκεια της πλοήγησής τους και το πώς θα τις χρησιμοποιήσει.

Επίλογος

Με βάση αυτά ως δεδομένα διαπιστώνουμε ότι τελικά ακόμη και η ασφάλεια σε έναν χώρο όπως αυτός του Διαδικτύου, μπορεί να υπάρξει.

Το Διαδίκτυο ξεκίνησε ως το απόλυτο εκφραστικό μέσο της ελευθερίας της επικοινωνίας των ανθρώπων. Σύντομα όμως πολλοί προσπάθησαν να εκμεταλευθούν αυτή την ελευθερία εις βάρος άλλων. Πλέον η τεχνολογία έχει φθάσει στο σημείο να μπορεί να μας εξασφαλίζει ότι οι συνδιαλλαγές μας στο Διαδίκτυο είναι ασφαλείς. Μπορούμε πλέον να αγοράζουμε οτιδήποτε από το χώρο αυτό με την ίδια ασφάλεια που θα ψωνίζαμ από το κατάστημα της γειτονιάς μας.

ΠΗΓΕΣ

- **"E-Business και Προστασία Προσωπικών Δεδομένων: σεβασμός του πολίτη στην Ψηφιακή Εποχή "** *Κωνσταντίνος Μουλίνος , Κωνσταντίνα Καμπουράκη Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα*

- Η προστασία του καταναλωτή ως ασθενέστερου, Η προστασία του ασθενέστερου στο δίκαιο Αλεξανδρίδου Ελίζα (εκδόσεις Σάκκουλα, 1997)
- Β΄Γνωμοδοτήσεις – Μελέτες «Η πρόταση της οδηγίας της ΕΕ για το ηλεκτρονικό εμπόριο και προστασία του καταναλωτή» Αλεξανδρίδου Ελίζα (περιοδικό «Δίκαιο Επιχειρήσεων & Εταιριών» έτος 6ο, αρ. τεύχους 58, σ. 113)
- Εισαγωγή στο Δίκαιο του Ηλεκτρονικού Εμπορίου Θεόδωρος Γ. Σιδηρόπουλος (εκδόσεις Αδελφών Κυριακίδη Α.Ε.) α.ε.
- Ηλεκτρονικό Εμπόριο Αρσένης Πασχόπουλος και Παναγιώτης Σκαλτσάς Εκδόσεις Κλειδάριθμος.
- SHTTP: The Protocol: http://cis.nyu.edu/xiaodong/security/protocol.html
- Visa Security FAQ: http://www.visa.com/nt/ecomm/faq.html
- The World Wide Web Security FAQ: http://www.w3.org/Security/faq/wwwsf1.html
- e-Επιχειρείν Πλήρης Οδηγός Ανάλυσης Τεχνικών Και Εμπορικών Θεμάτων Εκδότης Μ. Γκιούρδας 2001 McGraw Hill Companies.
- Web Commerce Technology Handbook Daniel Minoli –Emma Minoli McGraw Hill Series
- PC Magazine , "Secure Sockets Layer –SSL 3.0 ", May 26, 1998
- Pc Magazine, "S/Mime keeps e-mail communication secure-usually", September 1 ,1998
- http://www.telstra.com.au/info/security.html
- http://www.alw.nih.gov./Security/security.html
- PGP FAQ: http://www.cam.ac.uk.pgp.net/pgpnet/pgp-faq/
- An Overview of SSL : http://www.homeport.org./~adam/ssl.html
- Cryptography –An Overview : http://www.hack.gr/users/dij/crypto/
- SHTTP: The Protocol : http://cis.nyu.edu./xiaodong/security/protocol.html
- Visa Security FAQ: http://www.visa.com/nt/ecomm/faq.html
- The World Wide Web Security FAQ : http://www.w3.org/Security/faq/wwwsf1.html