Ασφάλεια

Ηλεκτρονικό εμπόριο, έγκλημα και θέματα ασφάλειας

Καθώς το κυβερνοέγκλημα αυξάνεται η διαχείριση του Η.Ε. πρέπει να προετοιμαστεί να αντιμετωπίσει τις εγκληματικές επιθέσεις.

Ορισμοί και έννοιες

Ασφάλεια πληροφοριών (Information security, InfoSec)

Μπορεί να οριστεί ότι είναι η Εμπιστευτικότητα (Confidentiality), η Ακεραιότητα (Integrity) και η Διαθεσιμότητα (Availability) της πληροφορίας.

Εμπιστευτικότητα (Confidentiality)

Η πληροφορία μένει μυστική και μόνο τα εξουσιοδοτημένα άτομα έχουν πρόσβαση.

Η πληροφορία δεν πρέπει να είναι «ορατή» από κανέναν εκτός από τον προβλεπόμενο λήπτη.

Ακεραιότητα (Integrity)

Η πληροφορία που μεταφέρεται από μια οντότητα σε μια άλλη οντότητα δεν πρέπει να έχει αλλοιωθεί με κανένα τρόπο.

Η ακεραιότητα περιλαμβάνει και την ακεραιότητα της πηγής.

Υπάρχουν μηχανισμοί που ελέγχουν την μη δυντατότητα τροποποίησης και μηχανισμοί ανίχνευσης τροποποίησης.

Διαθεσιμότητα (Availability)

Η μη δυνατότητα πρόσβασης στην πληροφορία έστω και αν έχουν ικανοποιηθεί άλλα μέτρα ασφάλειας.

Επιθέσεις όπως η άρνηση υπηρεσίας (denial of service ή DoS) είναι ένα παράδειγμα.

Ταυτοποίηση (Identification)

Το χαρακτηριστικό του είναι η μοναδικότητα μέσα σε ένα πλαίσιο τοπικότητας και σκοπιμότητας.

Είναι το πρώτο βήμα πριν την αυθεντικοποίηση και εξουσιοδότηση στη διαδικασία πρόσβασης στην πληροφορία.

Αυθεντικοποίηση (Authenticity, Authentication)

Μέσω της αυθεντικοποίησης γίνεται έλεγχος και επιβεβαίωση της οντότητας που έχει κάνει την ταυτοποίηση.

Επιβεβαιώνεται δηλαδή ότι η οντότητα είναι πράγματι αυτή που ισχυρίζεται ότι είναι.

Αυτό μπορεί να γίνει με τους εξής τρόπους:

1. Τι γνωρίζεις (what you know)
2. Τι έχεις (what you have)
3. Τι είσαι (what you are)

Εξουσιοδότηση (Authorization)

Με την εξουσιοδότηση δίνονται δικαιώματα στην οντότητα σχετικά με το σε ποιές πληροφορίες μπορεί να έχει πρόσβαση και τι είδους πρόσβαση.

Είναι το τρίτο βήμα μετά την ταυτοποίηση και αυθεντικοποίηση.

Σημαντικό ρόλο έχει ο διαχειριστής του συστήματος.

Υπευθυνότητα (Accountability)

Αναφέρεται στη δυνατότητα καταγραφής και ιχνηλάτησης της οντότητας που κακόβουλα ίσως προκάλεσε πρόβλημα και η προσάρτηση ευθυνών σε αυτή.

Τα αρχεία log και audit trail είναι ένα παράδειγμα.

Μη αποκήρυξη ή Μη άρνηση (Nonrepudiation)

Η οντότητα που συμμετέχει στη συναλλαγή δεν μπορεί να αρνηθεί τις ενέργειές της.

Λειτουργίες και Εμπιστοσύνη (Functionality vs. Assurance)

Πως είμαστε σίγουροι ότι οι λειτουργίες είναι σωστές και ασφαλείς.

Ιδιωτικότητα (Privacy)

Τα προσωπικά στοιχεία δεν πρέπει να μοιράζονται σε τρίτους.

Αντιδράσεις στην εφαρμογή ασφάλειας στα πληροφοριακά συστήματα

Αν και η ασφάλεια είναι απαραίτητη και αναγκαία, υπάρχουν και «φωνές» που αντιδρούν για λόγους όπως:

Ευκολία χρήσης (Ease of use)

Τα μέτρα ασφάλειας κάνουν πιο δύσκολη την επικοινωνία μεταξύ πελάτη καταστήματος και αυτό σημαίνει λιγότερα κέρδη.

Δημόσια ασφάλεια (Public safety)

Δημόσιοι οργανισμού θέλουν να έχουν προσβαση στα προσωπικά στοιχεία για λόγους δημόσιας ασφάλειας.

Οι κύριες απειλές για την ασφάλεια του Η.Ε.

Οι πιο κύριες απειλές είναι:

Κακόβουλος κώδικας (viruses, worms, Trojan horses, ransomware, και bot networks)

Απειλεί την ακεραιότητα του συστήματος και την ομαλή λειτουργία του.

Botnet

Τεράστιος αριθμός υπολογιστών στο Διαδίκτυο που έχουν υποστεί πειρατεία και προωθούν κίνηση (spam, virus)

Δούρειος ίππος (trojan horse)

Πρόγραμμα που φαίνεται να εκτελεί χρήσιμη λειτουργία αλλά περιέχει επικίνδυνη κρυφή συνάρτηση.

Ιός ή σκουλήκι μακροεντολής (macro virus/ worm)

Εκτελούνται όταν ανοίγει ένα αντικείμενο εφαρμογής που περιέχει τη μακροεντολή ή εκτελείται μια συγκεκριμένη διαδικασία.

Ανεπιθύμητο λογισμικό (adware, spyware, κ.λπ.)

Επικίνδυνο λογισμικό που εγκαθίσταται στο σύστημά σας χωρίς να το γνωρίαεται ή χωρίς να έχετε δώσει την συγκατάθεσή σας.

Phishing

Παραπλανητικό ή απατηλό περιεχόμενο με σκοπό την απόσπαση εμπιστευτικής πληροφορίας για οικονομικό κέρδος.

Πειρατεία και κυβερνοβανδαλισμός (Hacking και cybervandalism)

Σκόπιμη διακοπή, αλλοίωση ή και καταστροφή ενός ιστότοπου.

Κλοπή ή ψευδής πιστωτική κάρτα (Credit card fraud/theft)

Ίσως η μεγαλύτερη απειλή για την οποία οι χρήστες είναι περισσότερο προσεκτικοί και επιφυλακτικοί.

Spoofing

Όταν κάποιος χάκερ προσπαθεί να εξαπατήσει με απόκρυψη της πραγματικής του ταυτότητας.

Pharming

Ανακατεύθυνση ενός λινκ σε ψευδείς (μεταμφιεσμένους) ιστότοπους.

Ψευδής ταυτότητα (Identity fraud)

Η μη εξουσιοδοτημένη χρήση προσωπικών δεδομένων άλλου ατόμου.

Άρνηση παροχής υπηρεσιών (DOS)

Ένα σύστημα βομβαρδίζεται από αιτήσεις για υπηρεσίες/πρόσβαση και καταρρέει ή δεν μπορεί να ανταποκριθεί.

Sniffing

Πρόγραμμα που «κρυφακούει» και καταγράφει πληροφορίες που διακινούνται στο διαδίκτυο.

Εκ των έσω

Αν και οι προσπάθειες γίνονται να κρατηθούν μακρυά οι εκτός του συστήματος εισβολείς και απειλές, ο μεγαλύτερος κίνδυνος προέρχεται «εκ των έσω».

Κακοσχεδιασμένο λογισμικό και σερβερ

Η ανάπτυξη της πολυπλοκότητας στο λογισμικό και τις ρυθμίσεις έφερε και πολλά κενά στην ασφάλεια.

Κοινωνικά δίκτυα

Τα κοινωνικά δίκτυα παρουσιάζουν πολλά θέματα ασφάλειας τα οποία μπορεί να οδηγήσουν σε μη ασφαλές Η.Ε.

Κινητή πλατφόρμα

Προσθέτει θέματα ασφάλειας μέσω της ασύρματης επικοινωνίας.

Cloud computing

Η νέα ιδέα φέρνει και νέα θέματα ασφάλειας προς θεώρηση.

Η προστασία της πληροφορίας στο διαδίκτυο

Ποιά είναι η προστασία που μπορεί να προσφέρει η τεχνολογία από τις απειλές που αναφέρθηκαν.

Κρυπτογραφία

Μεσω της κρυπτογραφίας το μήνυμα προς αποστολή κρυπτογραφείται και αποστέλεται κρυπτογραφημένο.

Η κρυπτογράφηση δεν αποτελεί πανάκεια αλλά μπορεί να καλύψει τους τέσσερεις παρακάτω κανόνες ασφάλειας.

1. Ακεραιότητα (Integrity)
2. Μη αποκήρυξη ή Μη άρνηση (Nonrepudiation)
3. Αυθεντικότητα (Authenticity)
4. Εμπιστευτικότητα (Confidentiality)

Συστατικά κρυπτογράφησης

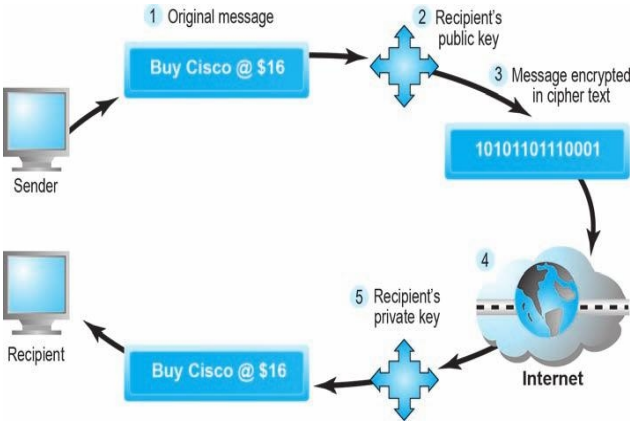
- Ακρυπτογράφητο κείμενο
- Αλγόριθμος κρυπτογράφησης
- Κλειδί
- Χώρος κλειδιού
- Κρυπτοκείμενο

Τεχνικές κρυπτογράφισης

Οι πιο γνωστές τεχνικές κρυπτογράφησης είναι:

Συμμετρική κρυπτογραφία

Και τα δύο μέρη μοιράζονται το ίδιο κλειδί κρυπτογράφησης και αποκρυπτογράφησης. Advanced Encryption Standard (AES).

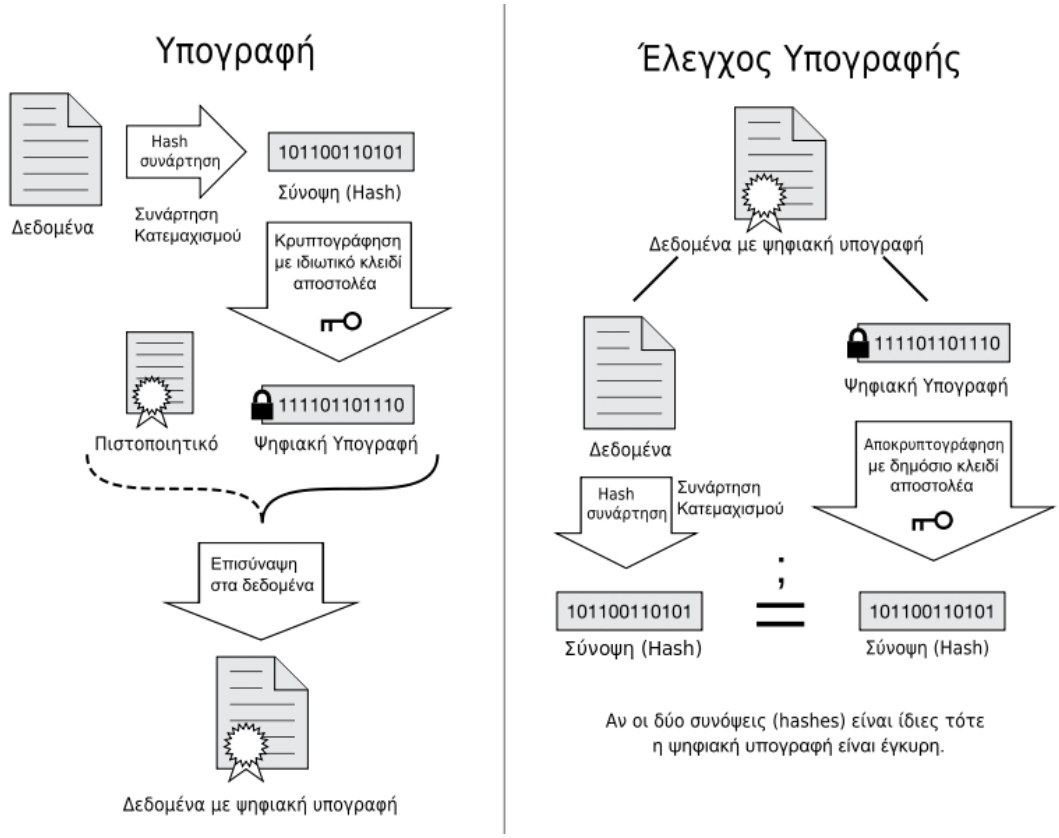


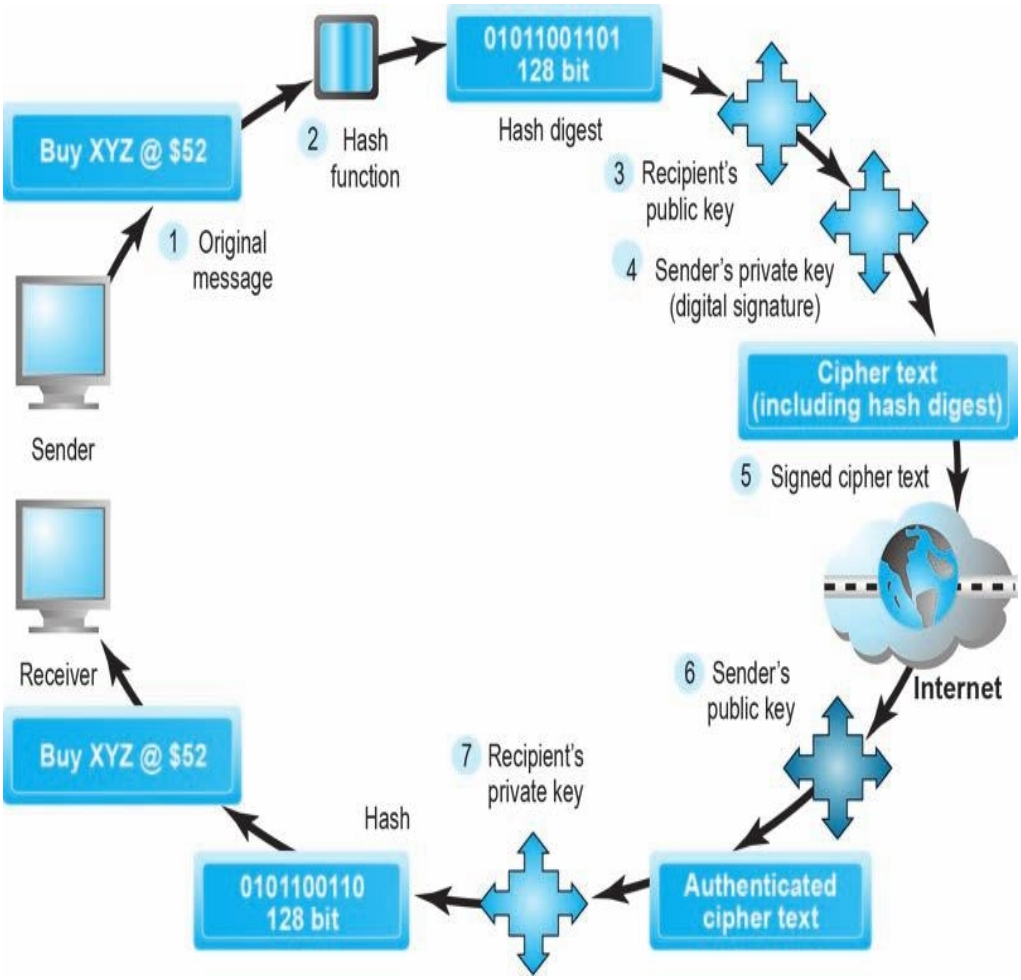
Ασύμμετρη κρυπτογραφία (Δημόσιο κλειδί)

Το μήνυμα κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη και μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί του παραλήπτη.

Ψηφιακές υπογραφές

Βασίζονται στα δημόσια κλειδιά για πιστοποίηση της ταυτότητας του αποστολέα μηνύματος ή μη τροποποίησης του αρχικού μηνύματος.


Υπογραφή
Δεδομένα
Hash συνάρτηση
Συνάρτηση Κατεμαχισμού
101100110101
Σύνοψη (Hash)
Κρυπτογράφηση με ιδιωτικό κλειδί αποστολέα
Πιστοποιητικό
111101101110
Ψηφιακή Υπογραφή
Επισύναψη στα δεδομένα
Δεδομένα με ψηφιακή υπογραφή
Έλεγχος Υπογραφής
Δεδομένα με ψηφιακή υπογραφή
111101101110
Ψηφιακή Υπογραφή
Δεδομένα
Αποκρυπτογράφηση με δημόσιο κλειδί αποστολέα
Hash συνάρτηση
Συνάρτηση Κατεμαχισμού
101100110101
Σύνοψη (Hash)
101100110101
Σύνοψη (Hash)
Αν οι δύο συνόψεις (hashes) είναι ίδιες τότε η ψηφιακή υπογραφή είναι έγκυρη.


Buy XYZ @ $52
1 Original message
Sender
2 Hash function
01011001101 128 bit
Hash digest
3 Recipient's public key
4 Sender's private key (digital signature)
Cipher text (including hash digest)
5 Signed cipher text
Internet
6 Sender's public key
Authenticated cipher text
7 Recipient's private key
0101100110 128 bit
Hash
Buy XYZ @ $52
Receiver

Άλλες τεχνικές / Εργαλεία
Εκτός από την κρυπτογράφηση, άλλα εργαλεία για την ασφαλή επικοινωνία είναι:

Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
Διασφαλίζει server authentication, client authentication, και message integrity για συνδέσεις TCP/IP.

Virtual private networks (VPNs)
Επιτρέπουν απομακρυσμένους χρήστες να επικοινωνούν με ασφάλεια μέσω του internet.

WPA2 και CCMP
Προσφέρουν ασφάλεια στις ασύρματες συσκευές. Χρησιμοποιούν τον αλγόριθμο AES για κρυπτογράφηση.

Firewalls
Λειτουργούν ως φίλτρα ανάμεσα στο διαδίκτυο και το ιδιωτικό δίκτυο μιας εταιρείας.

Proxies (gateway)
Περιορίζουν την πρόσβαση από «εσωτερικά» σε «εξωτερικά δίκτυα»

Κόμβος ενός δικτύου από λογισμικό και υλικό που απομονώνει ένα ιδιωτικό από ένα δημόσιο δίκτυο εξετάζοντας τα πακέτα δεδομένων που περνούν από αυτόν.

Intrusion detection and prevention systems (IDS/IDP)
Παρακολουθεί και προστατεύει από ύποπτες κινήσεις.

Λειτουργικά συστήματα (Operating system controls)
Εφαρμόζουν κανόνες ασφαλείας

Anti-virus λογισμικό
Αντι-ιικό λογισμικό.

Πολιτικές, διαδικασίες και νόμοι που επηρεάζουν την ασφάλεια

Καθε επιχείρηση πρέπει να εφαρμόζει πολιτικές και διαδικασίες όπως επίσης να λαμβάνει υπόψη τους νόμους που ισχύουν στη χώρα που δραστηριοποιείται.

Το πλάνο μπορεί να περιλαμβάνει:

1. Αξιολόγηση κινδύνου
2. Πολιτική ασφάλειας
3. Πλάνο υλοποίησης
4. Ομάδα ασφάλειας
5. Περιοδικοί έλεγχοι ασφάλειας