Εισαγωγή στην ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Γιώργος Καμπουράκης

“Do not figure on opponents not attacking; worry about your own lack of preparation”

The Book of Five Rings

Περιεχόμενα

- Βασικές έννοιες
- Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα (CIA)
- Τύποι απειλών
- Ευπάθειες, Απειλές, Έλεγχοι
- Επιτιθέμενοι
- Μέθοδοι άμυνας
- Κρυπτογραφία
- Ψηφιακές υπογραφές
- Ψηφιακά πιστοποιητικά
- Αρχές ασφαλείας

Βασικές έννοιες

- Computer Security:
  - Διαφύλαξη υπολογιστικών πόρων από μη εξουσιοδοτημένη χρήση
  - Προστασία πληροφορίας από ακούσια ή σκόπιμη βλάβη, αποκάλυψη ή τροποποίησή της

- Communication Security:
  - Προστασία δεδομένων κατά τη μετάδοση σε δίκτυα και κατανεμημένα συστήματα

"Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction".

Βασικές έννοιες

- **Απόλυτη ασφάλεια δεν είναι δυνατόν να υπάρξει**
  - *To decide whether a computer system is "secure", you must first decide what "secure" means to you, then identify the threats you care about.*

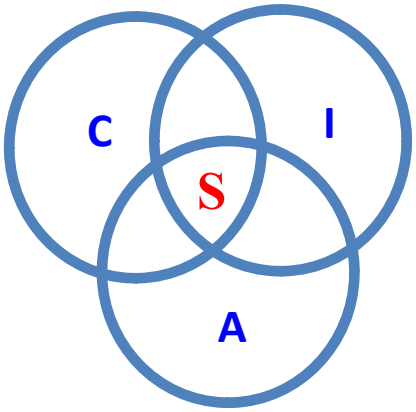
- Απειλή (Threat): Οντότητα που μπορεί να προκαλέσει ζημιά ή παραβίαση σε τμήμα ή στο σύνολο του δικτύου (κλίμακα: local, shared, national)
- Επίθεση (Attack): Είναι η εκμετάλλευση μιας αδυναμίας (vulnerability) από εισβολέα για την πραγματοποίηση απειλής (Exploit = επιτυχής επίθεση)
- Αντίμετρα (Countermeasures): Μηχανισμός ή διαδικασία με στόχο τον περιορισμό ή την εξάλειψη επιπτώσεων απειλής

"Threats are realized through attacks which can materialize through certain vulnerabilities if they have not been mitigated with appropriate countermeasures".

Confidentiality, Integrity, Availability (CIA)

CIA

- Εμπιστευτικότητα (Confidentiality): *Who is authorized to use data?*
- Ακεραιότητα (Integrity): *Is data "good"?*
- Διαθεσιμότητα (Availability): *Can access data whenever need it?*



S = Secure

CIA ή CIAAAN…

μερικά επιπρόσθετα στοιχεία ασφάλειας

- Πιστοποίηση Ταυτότητας (Authentication)
- Εξουσιοδότηση (Authorization)
- Μη-αποποίηση (Non-repudiation)
- Λογιστική καταγραφή (Accounting)

Αλληλεξάρτηση στοιχείων CIA

- Παράδειγμα 1: C vs. I+A
  - Αποσυνδέουμε τους υπολογιστές από το Διαδίκτυο ώστε να αυξήσουμε την εμπιστευτικότητα
  - Δημιουργούμε πρόβλημα στη διαθεσιμότητα και πιθανώς στην ακεραιότητα (lost updates)

- Παράδειγμα 2: I vs. C+A
  - Ενεργοποιούμε πολλαπλούς ελέγχους (άνθρωποι / μηχανές) για να αυξήσουμε την ακεραιότητα
  - Προκαλούμε πρόβλημα στην εμπιστευτικότητα μιας και η πληροφορία γίνεται διαθέσιμη σε περισσότερες οντότητες
  - Ομοίως στη διαθεσιμότητα μιας και οι περισσότεροι έλεγχοι (μέχρις ότου ολοκληρωθούν) απαγορεύουν την πρόσβαση στα δεδομένα

Εμπιστευτικότητα

- Εγγυάται ότι τα δεδομένα δεν αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες

- Π.χ. για την ασφάλεια επικοινωνιών

  – Εμπιστευτικότητα Σύνδεσης (Connection Confidentiality Service). Παρέχει εμπιστευτικότητα στα προς μετάδοση δεδομένα

  – Εμπιστευτικότητας μη Εγκατεστημένης Σύνδεσης (Connectionless Confidentiality Service). Παρέχει εμπιστευτικότητα μεμονωμένων τμημάτων δεδομένων

"Doctor-patient confidentiality doesn't extend to massage therapists."

Εμπιστευτικότητα

- Υπηρεσία Εμπιστευτικότητας Επιλεγμένου Πεδίου (Selected Field Confidentiality Service). Παρέχει εμπιστευτικότητα συγκεκριμένων πεδίων στα δεδομένα μιας σύνδεσης ή σε μεμονωμένα τμήματά τους

- Υπηρεσία Εμπιστευτικότητας Ροής Κίνησης (Traffic Flow Confidentiality Service). Παρέχει προστασία από επιθέσεις τύπου ανάλυσης κυκλοφορίας

Ακεραιότητα Δεδομένων

- Εξασφαλίζει τη μη τροποποίηση των δεδομένων από μη-εξουσιοδοτημένους χρήστες. Π.χ. για την ασφάλεια επικοινωνιών διακρίνουμε σε:
  - Υπηρεσία Ακεραιότητας Σύνδεσης με αποκατάσταση (Connection Integrity Service With Recovery). Εξασφαλίζει ακεραιότητα και παρέχει παράλληλα δυνατότητα ανάκτησης
  - Υπηρεσία Ακεραιότητας Σύνδεσης Χωρίς Αποκατάσταση (Connection Integrity Service Without Recovery). Παρέχει μόνον ακεραιότητα δεδομένων

Ακεραιότητα Δεδομένων

- Υπηρεσία Ακεραιότητας Σύνδεσης Επιλεγμένου Πεδίου (Selected Field Connection Integrity Service). Παρέχει ακεραιότητα μεμονωμένων πεδίων δεδομένων

- Υπηρεσία Ακεραιότητας Άνευ Εγκατάστασης Σύνδεσης (Connectionless Integrity Service). Παρέχει ακεραιότητα μεμονωμένων τμημάτων δεδομένων

- Υπηρεσία Ακεραιότητας Επιλεγμένου Πεδίου Άνευ Εγκατάστασης Σύνδεσης (Selected Field Connectionless Integrity Service). Παρέχει ακεραιότητα συγκεκριμένων πεδίων σε μεμονωμένα τμήματα δεδομένων

Πιστοποίηση ταυτότητας

- Στοχεύει να αποδεικνύει την ταυτότητα οντότητας και να εξασφαλίζει τη γνησιότητα μηνυμάτων που ανταλλάσσονται σε μια επικοινωνία. Διακρίνουμε σε:
  - Αυθεντικοποίηση Ομότιμης Οντότητας (Peer Entity Authentication). Μία οντότητα δεν μπορεί να προσποιηθεί ότι είναι μία άλλη
  - Αυθεντικοποίηση Προέλευσης δεδομένων (Data Origin Authentication). Η πηγή προέλευσης μηνύματος είναι αυτή που ισχυρίζεται.

Εξουσιοδότηση / Έλεγχος προσπέλασης

- Παρέχει προστασία χρήσης πόρων του συστήματος, από μη εξουσιοδοτημένες οντότητες.
- Συνεργάζεται με τις υπηρεσίες αυθεντικοποίησης.

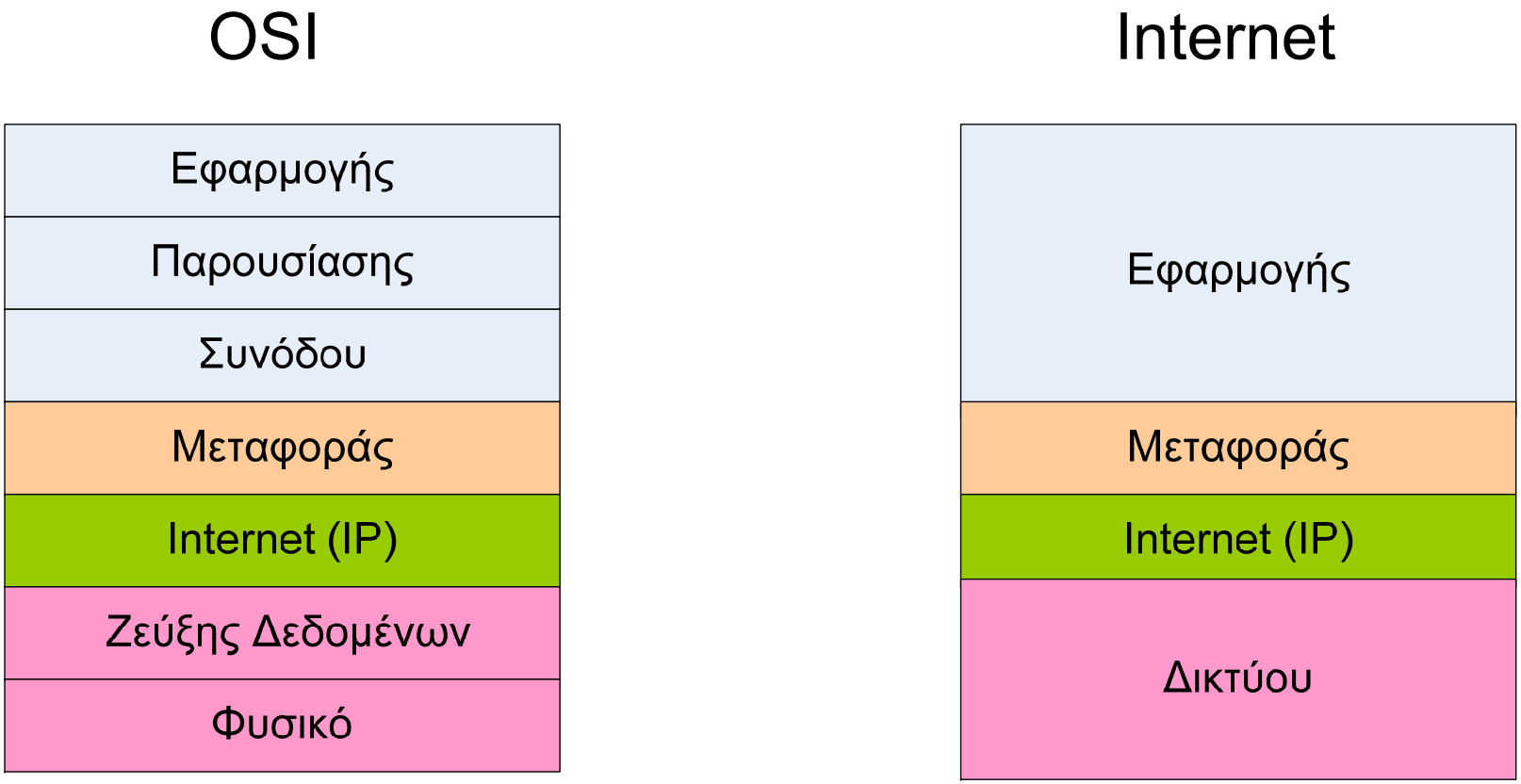
"The pharmacist is on the phone, trying to secure prior authorization. Do you want to wait? He shouldn't be more than an hour."

(Μη) Αποποίηση

- Π.χ. για την ασφάλεια επικοινωνιών
  - Μη αποποίηση με Απόδειξη Προελεύσεως (Non-Repudiation With Proof Of Origin). Παρέχει πιστοποίηση προέλευσης των ληφθέντων μηνυμάτων
  - Μη αποποίηση με Απόδειξη Παραδόσεως (Non-Repudiation With Proof Of Delivery). Παρέχει πιστοποίηση παράδοσης μηνυμάτων στον αποστολέα

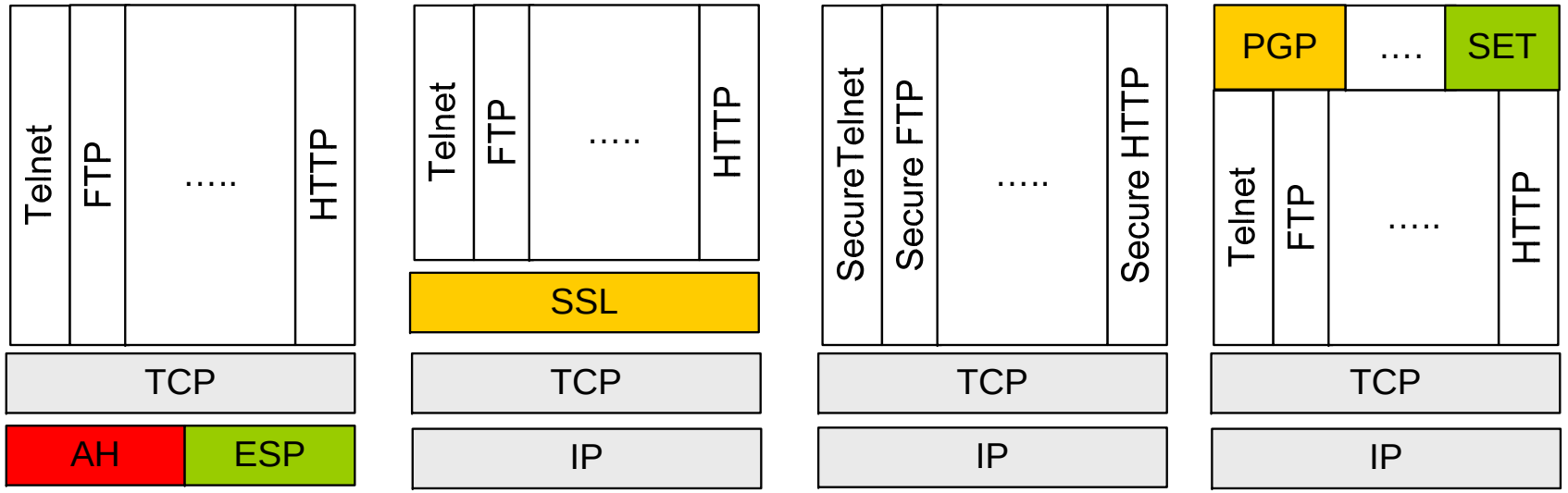
"I see you're still in denial."

Το μοντέλο του Internet



Σε ποιο ή ποια επίπεδα θέλουμε να παρέχουμε ασφάλεια;

Σχέσεις πρωτοκόλλων ασφαλείας και στοίβας OSI



Επίπεδο Δικτύου *Επίπεδο Μεταφοράς* *Επίπεδο Εφαρμογής* *Πάνω από το επίπεδο Εφαρμογής*

Υπηρεσίες Ασφάλειας ανά επίπεδο OSI

Επίπεδο	Υπηρεσία
7. Εφαρμογής (Application)	Αυθεντικοποίηση Έλεγχος Προσπέλασης Ακεραιότητα δεδομένων Εμπιστευτικότητα Δεδομένων Μη αποποίηση
6. Παρουσίασης (Presentation)	Εμπιστευτικότητα Δεδομένων
5. Συνόδου (Session)	----------
4. Μεταφοράς (Transport)	Αυθεντικοποίηση Έλεγχος Προσπέλασης Ακεραιότητα δεδομένων Εμπιστευτικότητα Δεδομένων
3. Δικτύου (Network)	Αυθεντικοποίηση Έλεγχος Προσπέλασης Ακεραιότητα δεδομένων Εμπιστευτικότητα Δεδομένων
2. Ζεύξης Δεδομένων (Data Link)	Αυθεντικοποίηση Έλεγχος Προσπέλασης Ακεραιότητα δεδομένων Εμπιστευτικότητα Δεδομένων
1. Φυσικό (Physical)	Εμπιστευτικότητα Δεδομένων

Είδη Απειλών

- Είδη απειλών [passive / active]:
  - Interception
    - Μη εξουσιοδοτημένη οντότητα καταφέρνει να προσπελάσει κάποιο πόρο
  - Interruption
    - Ένας πόρος καταστρέφεται, ή δεν είναι προσπελάσιμος
  - Modification
    - Μη εξουσιοδοτημένη οντότητα μεταβάλλει την κατάσταση ενός πόρου
  - Fabrication
    - Μη εξουσιοδοτημένη οντότητα φαλκιδεύει έναν πόρο

Παραδείγματα;

Interception: wiretapping to capture data in a network or the illicit copying of files, Interruption: destruction of a piece of hardware, or cutting of a communication line, Modification: changing values in a data file or modifying the contents of a message being transmitted over a network, Fabrication: insertion of spurious messages in a network or the addition of records to a file.

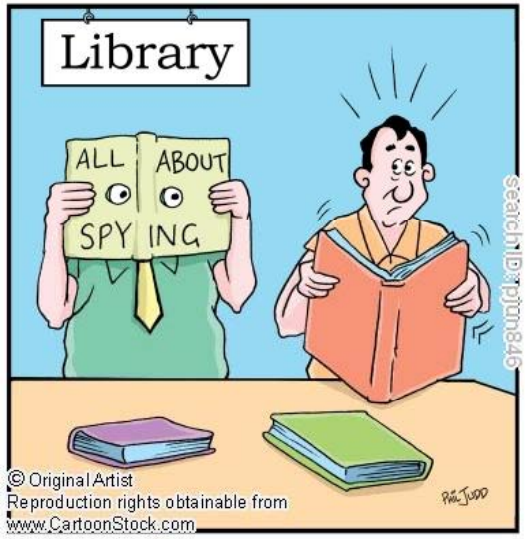
Είδη Απειλών

- Για τους πόρους (resources)
- Για τα δεδομένα (data)
  - τοποθετείται πάνω από το s/w, μιας και τα δεδομένα χρησιμοποιούνται από το s/w
- Για το λογισμικό (s/w)
  - τοποθετείται πάνω από το h/w, μιας και το s/w εκτελείται σε h/w
- Για το υλικό (h/w)

Είδη Απειλών: H/W

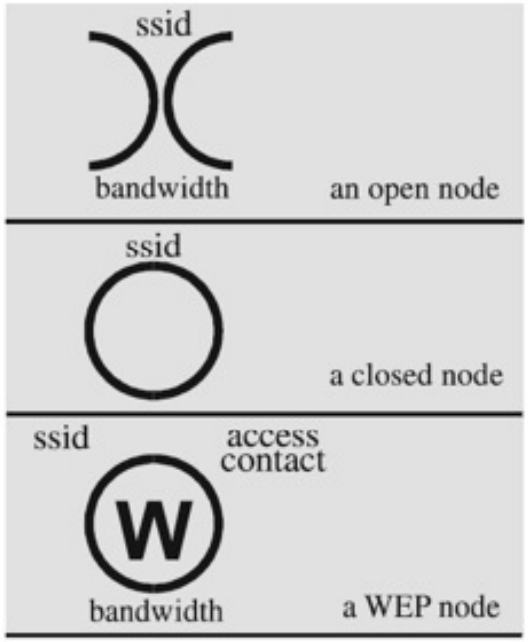
- Εγκατάσταση / αφαίρεση μιας συσκευής
  - Π.χ.: Snooping, wiretapping

    Snoop: to look around a place secretly in order to discover things about it or the people connected with it. [Cambridge Dictionary of American English]
  - Π.χ.: Modification, alteration
  - ...
- Φυσικές απειλές/επιθέσεις στο h/w
  - Αθέλητες ή εσκεμμένες
  - Κλοπή / Καταστροφή
    - Πρόκληση ζημιάς στη μηχανή (καφές, ποντίκια, *ζωύφια*)
    - Κλοπή
    - "Machinicide": Axe / hammer the machine
    - ...
  - Απαιτούνται αντίμετρα: φύλακες, κλειδαριές, επιτήρηση χώρου



Snooping: Wardriving / Warwalking, Warchalking

- Wardriving/warwalking:
  - driving/walking around with a wireless-enabled notebook looking for unsecured wireless LANs
- Warchalking:
  - using chalk markings to show the presence and vulnerabilities of wireless networks nearby
    - E.g., a circled "W" -- indicates a WLAN protected by Wired Equivalent Privacy (WEP) encryption



Είδη Απειλών: S/W

- Deletion
  - Κατά λάθος διαγραφή
  - Αντίμετρα: χρήση *Configuration Management Software* *(tracking and controlling changes in the software)*
- Modification
  - Trojan Horses, , Viruses, Logic Bombs, Trapdoors, Information Leaks, ...
- Theft
  - Παράνομη αντιγραφή
    - P2P

"I'm waiting for them to work out the bugs first."

Κακόβουλο λογισμικό

- Bacterium (rabbit programs): *A specialized form of virus which does not attach to a specific file. A type of malware that create many instances of themselves, or run many times simultaneously in order to consume large amounts of system resources.*

- Logic bomb: *Malicious [program] logic that activates when specified conditions are met. Usually intended to cause denial of service or otherwise damage system resources.*

- Trapdoor: *A hidden computer flaw known to an intruder, or a hidden computer mechanism (usually software) installed by an intruder, who can activate the trap door to gain access to the computer without being blocked by security services or mechanisms.*

Κακόβουλο λογισμικό

- Trojan horse: *A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.*
- Virus: *A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.*
- Worm: *A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.*

Είδη Απειλών: Data

- Πόσο πολύτιμα είναι τα δεδομένα;
  - Αριθμός πιστωτικής κάρτας vs. Αριθμός τηλεφώνου
  - Πηγαίος κώδικας
  - Τι βλέπω; vs. Ποια η σημασία;
    - "4798" -> πρόθεμα τηλεφωνικού αριθμού ή τμήμα Α.Φ.Μ.?
- Επαρκής προστασία
  - Κρυπτογραφία
    - Χρονικοί περιορισμοί (αναθεώρηση)
- Identity Theft
  - http://www.consumer.gov/idtheft/
  - *Bank employee indicted for stealing depositors' information to apply over the Internet for loans*
  - *$7M loss, Florida: Stole 12,000 cards from restaurants via computer networks and social engineering*

"Remember when your identity was stolen? I just bought it back on ebay."

Απειλές

Μη εξουσιοδοτημένη χρήση (masquerade): Μη εξουσιοδοτημένος χρήστης προσπαθεί να αποκτήσει πρόσβαση σε διαθέσιμους πόρους

Αποποίηση (repudiation): Κάποια οντότητα αποποιείται τη συμμετοχή της σε μία επικοινωνία

Ανάλυση επικοινωνίας (traffic analysis): Υποκλοπή πληροφορίας σχετικά με διακίνηση δεδομένων μεταξύ οντοτήτων, με στόχο την έμμεση εξαγωγή συμπερασμάτων

Ενεργός παρακολούθηση (active tapping): Τροποποίηση δεδομένων των

Κακόβουλο λογισμικό / data-driven attacks: (Viruses, Trojan horses, worms)

Επανεκπομπή μηνυμάτων (replay): Καταγραφή έγκυρων μηνυμάτων με στόχο μεταγενέστερη επανεκπομπή τους

Άρνηση Παροχής Υπηρεσίας (denial of service): Παρεμπόδιση ομαλής λειτουργίας του συστήματος

Μη ενεργός ή παθητική παρακολούθηση (passive tapping): Παρακολούθηση δεδομένων που διακινούνται μεταξύ χρηστών δικτύου

Είδη επιθέσεων: Data CIA

- Αποκάλυψη (Disclosure)
  - Επίθεση κατά της εμπιστευτικότητας
- Μη-εξουσιοδοτημένη μεταβολή (modification) / εξαπάτηση (deception)
  - Π.χ., παροχή εσφαλμένων δεδομένων (επίθεση κατά της ακεραιότητας)
- Παρεμπόδιση (Disruption)
  - DoS (επίθεση κατά της διαθεσιμότητας)
- Σφετερισμός (Usurpation)
  - Μη-εξουσιοδοτημένη χρήση υπηρεσιών (επίθεση κατά της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας)

Είδη επιθέσεων: Data CIA

- Παραδείγματα επιθέσεων κατά της εμπιστευτικότητας
  - Tapping / snooping
- Παραδείγματα επιθέσεων κατά της ακεραιότητας
  - Modification: salami attack
    - Π.χ., από κάθε λογαριασμό καταθέσεων μιας τράπεζας αποκόπτω λεπτά του € και τα καταθέτω στο δικό μου λογαριασμό
  - Fabrication: replay data
    - Κάνω την ίδια κατάθεση στο λογαριασμό μου δύο ή περισσότερες φορές
- Παραδείγματα επιθέσεων κατά της διαθεσιμότητας
  - Delay vs. "full" DoS
- Παραδείγματα επιθέσεων: Αποποίηση (repudiation)
  - Data origin repudiation: *"ποτέ δεν το έστειλα"*

    Repudiation = μη παραδοχή (δεν αποδέχομαι να τηρήσω μια συμφωνία ή να αναγνωρίσω ένα χρέος, μια συναλλαγή κλπ.
  - Data receipt repudiation: *"ποτέ δεν το έλαβα"*

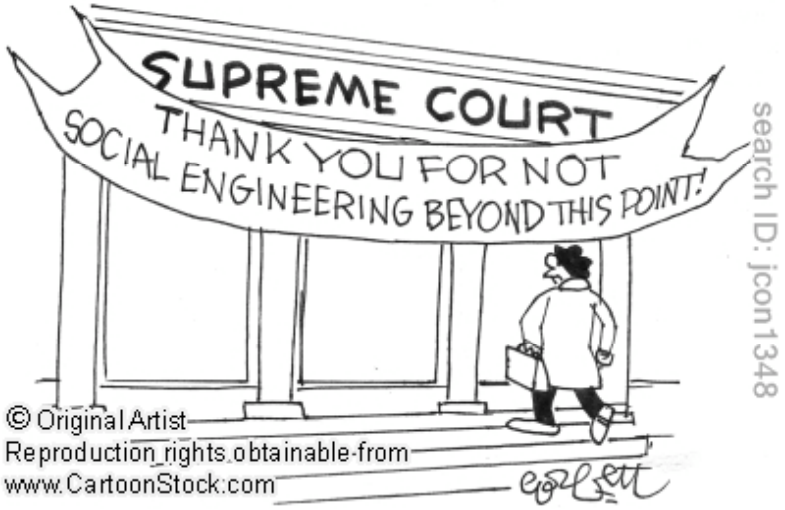
"My client pleads not guilty by reason of still being in denial."

Αδυναμίες / Απειλές

- Network vulnerabilities / threats
  - Οφείλονται σε:
    - πολυπλοκότητα
    - Δίνουν στους επιτιθέμενους τη δυνατότητα συνεργασίας
  - Ασύρματα δίκτυα
- Access vulnerabilities / threats
  - Κλοπή κύκλων επεξεργαστή, εύρους ζώνης
  - Κακόβουλη φυσική πρόσβαση
  - DoS στους εξουσιοδοτημένους χρήστες
- People vulnerabilities / threats
  - Πολύ συχνά το πιο αδύναμο σημείο ασφάλειας
  - Social engineering
  - Δυσαρεστημένοι υπάλληλοι

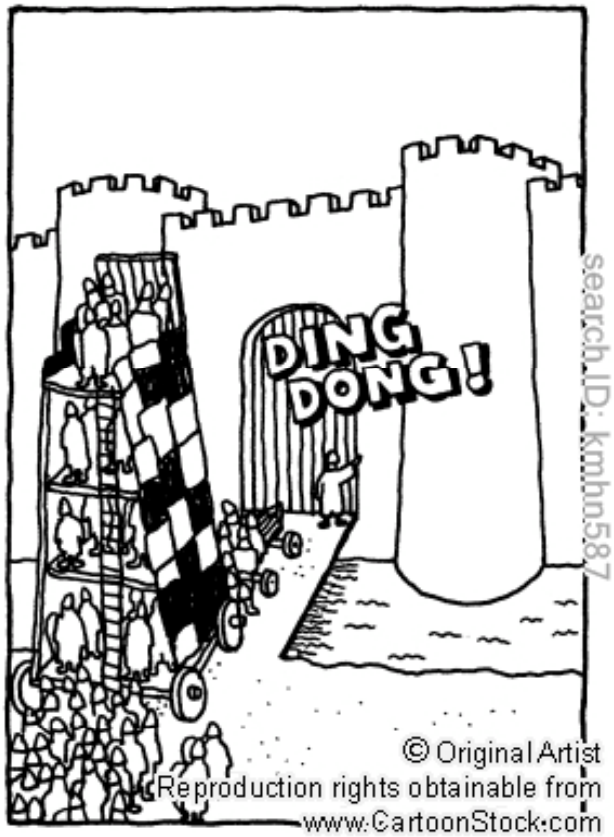
Social Engineering

- Social Engineering
  - Phishing
  - Baiting
  - Quid pro quo
  - Virus hoaxes
  - Dumpster diving
  - Reverse social engineering
  - Pretexting
  - …



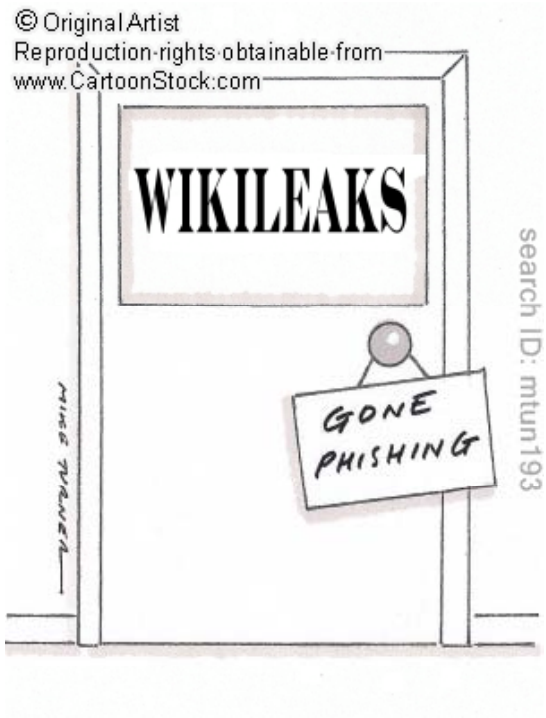
Επιτιθέμενοι

- Χρειάζονται MOM
  - Μέθοδο (Method)
    Skill, knowledge, tools …
  - Ευκαιρία (Opportunity)
    χρόνο και πρόσβαση
  - Κίνητρο (Motive)



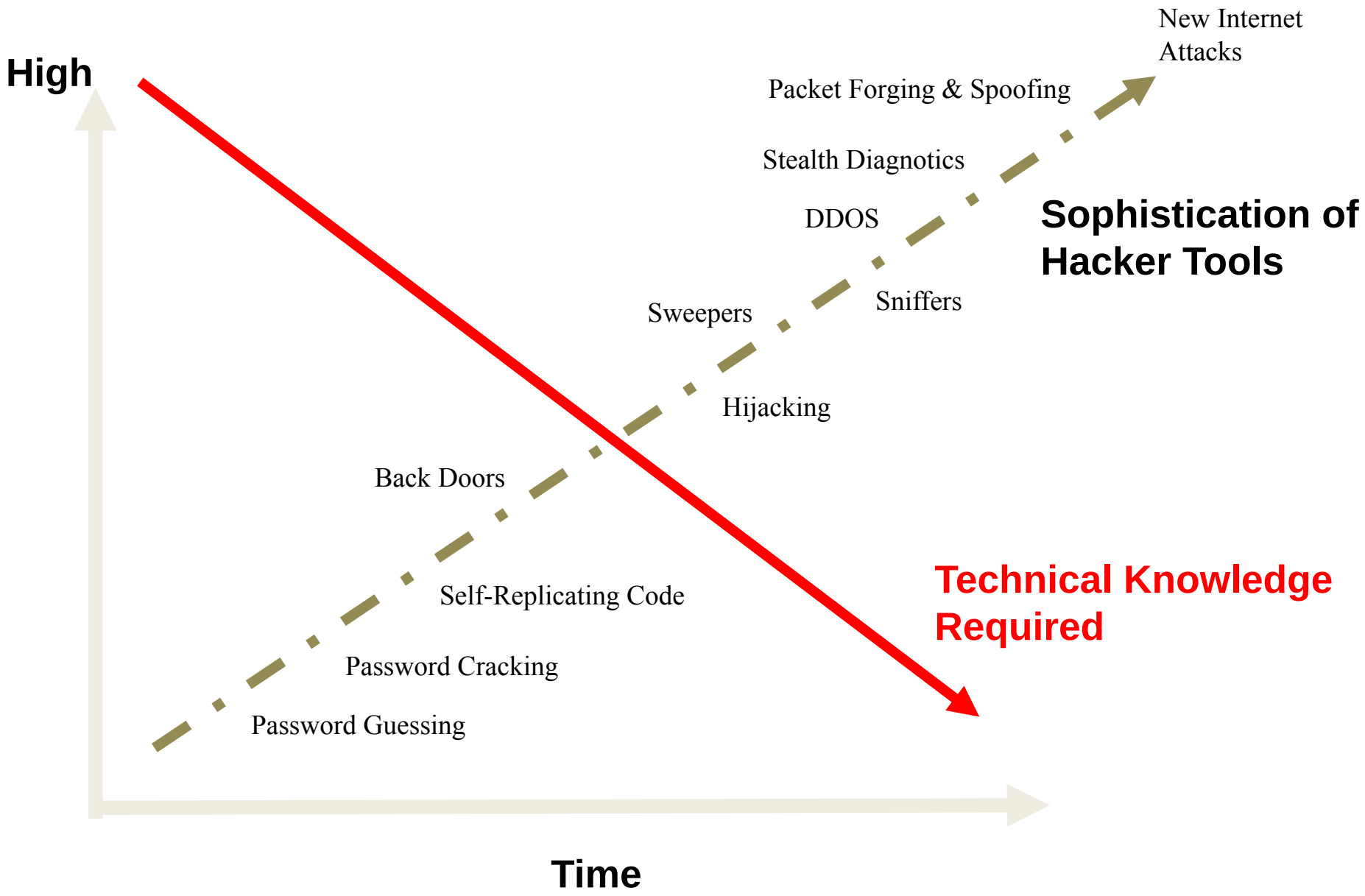
Τύποι επιτιθέμενων

- Τύποι επιτιθέμενων (κατηγοριοποίηση Ι)
  - Ερασιτέχνες
    - Ευκαιριακοί (π.χ. βρίσκω ένα συνθηματικό και το χρησιμοποιώ)
    - Ερασιτέχνες (π.χ. Script kiddies)
  - Hackers (καλόβουλοι)
  - Crackers (κακόβουλοι)
  - Καριερίστες
  - Επαγγελματίες κατάσκοποι, ακτιβιστές



- Τύποι επιτιθέμενων (κατηγοριοποίηση ΙΙ)
  - Recreational hackers / Institutional hackers
  - Organized criminals / Industrial spies / Terrorists
  - National intelligence gatherers / Info warriors

- Το hacking ως διαμαρτυρία. *Hactivism ("the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends"), Electro-Hippies, DDOS attacks on government agencies, SPAM attacks as "retaliation".*



[Barbara Edicott-Popovsky and Deborah Frincke, CSSE592/492, U. Washington]

Μέθοδοι άμυνας

- Πέντε βασικές προσεγγίσεις:
  - Prevent attack
    - Εμπόδισε την επίθεση / διόρθωσε την αδυναμία
  - Deter attack
    - Δυσκόλεψε την επίθεση (δυστυχώς, όχι αδύνατη)
  - Deflect attack
    - Κάνε κάποιο άλλο στόχο ελκυστικότερο
  - Detect attack
    - Κατά τη διάρκεια ή μετά
  - Recover from attack

"Is that the firewood we ordered or are we under siege?"

Μηχανισμοί Ελέγχου

Μεσαιωνικά κάστρα

- Τοποθεσία με φυσικά εμπόδια
- Τάφρος
- Κινητή γέφυρα
- Ισχυρή τοιχοποιία
  - Πολεμίστρες
- Ισχυρή πύλη εισόδου
  - Πύργος
- Φρουροί / Συνθηματικά
- Θυλακωτό σύστημα τειχών

Π.Σ. σήμερα

- Κρυπτογραφία
- Έλεγχοι S/W
- Έλεγχοι H/W
- Πολιτικές και διαδικασίες
- Φυσικοί έλεγχοι

Μηχανισμοί Ελέγχου

- Υπολογιστικά συστήματα:
  - Περίμετρος – ορίζει το “μέσα/έξω”
  - Αποτροπή – εκφόβιση του επιτιθέμενου
  - Πρόληψη – Αποθάρρυνση του επιτιθέμενου
  - Ομοιώματα (π.χ. honeypot) – η επίθεση επικεντρώνεται σε κάποιο ομοίωμα στόχου σε άγνοια του επιτιθέμενου

→ Πολυεπίπεδη αμυντική τακτική

Κρυπτογραφία

- **Βασικό εργαλείο ελέγχου!**
- Αρχικό κείμενο (Cleartext) → Κρυπτογράφημα (ciphertext)
- Παροχή προστασίας στις συνιστώσες της CIA:
  - Εμπιστευτικότητα: απόκρυψη (masking) πληροφοριών
  - Ακεραιότητα: προστασία από αλλαγές στα δεδομένα
    - Π.χ. άθροισμα ελέγχου (checksum)
  - Διαθεσιμότητα: με χρήση κρυπτογραφικών πρωτοκόλλων

"Kumor's responsible for all the computer passwords, so the boss had him encrypted."

Έλεγχοι σε επίπεδο S/W

- Λογισμικό / εφαρμογές:
  - OS and network controls
    - Π.χ. OS: sandbox* / virtual machine (software implementation of a machine)
    - Logs/firewalls, OS/Network virus scans, recorders
  - Independent control programs
    - Π.χ. password checker, virus scanner, Intrusion Detection System (IDS)
  - Internal program controls (τμήμα εφαρμογής)
    - Π.χ. read/write controls in DBMSs
  - Development controls
    - Π.χ. πρότυπα ποιότητας που ακολουθούν οι κατασκευαστές λογισμικού
      - Testing

"NOW TRY ANOTHER BLOODY VIRUS SCAN!!"

*A ***sandbox*** *is a* security mechanism for separating running programs. It is often *used to execute untested code, or untrusted programs from unverified third-parties, suppliers and untrusted users*

Έλεγχοι σε επίπεδο S/W

- Ζητήματα χρηστικότητας (για Software Controls)
  - Πόσο διαφανή είναι στο χρήστη και πόσο επηρεάζουν την εργασία του;
    - Π.χ. ζητούν νέο συνθηματικό πολύ συχνά

"It's very user-friendly, once it gets to know you."

Έλεγχοι σε επίπεδο H/W

- h/w για την παροχή υψηλότερου επιπέδου ασφάλειας …
  - Κλειδιαριές και καλώδια (notebooks)
  - Έξυπνες κάρτες, dongles, hardware keys, ...
  - …

Πολιτικές και διαδικασίες ασφάλειας

- Πολιτική (policy) vs. Διαδικασία (procedure)
  - Policy: τι ακριβώς επιτρέπεται/απαγορεύεται
  - Procedure: το *πώς επιβάλω την πολιτική*

- Κάθε πολιτική πρέπει να λαμβάνει υπόψη:
  - Σε συμφωνία με τις ισχύουσες νομικές και ηθικές νόρμες
  - Πιθανότητα υλοποίησης

    Άβολη: συνθηματικό 200 χαρακτήρων, πολύ συχνή αλλαγή συνθηματικών

    (ενδέχεται να είναι) πετυχημένη: αντικατάσταση συνθηματικών με βιομετρικά συστήματα
  - Περιοδικοί έλεγχοι / αναθεώρηση
    - Οι άνθρωποι, τα συστήματα και οι στόχοι τους αλλάζουν με το χρόνο

"Good news! I've created a new policy that's both arbitrary *and* inconsistent."

Αποτελεσματικότητα ελέγχων

- Γνώση για το πρόβλημα (Awareness)
  - Οι άνθρωποι πρέπει να πειστούν για την αναγκαιότητα των ελέγχων
- Πιθανότητα χρήσης
  - Άμεση σχέση με την πολυπλοκότητα
- Επικαλυπτόμενοι μηχανισμοί
  - 1 έλεγχος για κάθε αδυναμία
    - Layered defense: το επόμενο επίπεδο αποκαθιστά μια αποτυχία σε ένα προηγούμενο
- Περιοδικοί επανέλεγχοι
  - Συνήθως, ένας έλεγχος ατονεί με την πάροδο του χρόνου
  - Ανάγκη αντικατάστασης αναποτελεσματικών πρακτικών με καλύτερες

"Don't worry Honey there isn't anyone for miles!"

Επιστροφή στο CIAAAN: Τεχνικές εφαρμογής ελέγχων αυθεντικοποίησης

- **Τύπος Ι**: Κάτι που το λογικό υποκείμενο γνωρίζει *(πχ. ένα συνθηματικό ή ένα PIN)*
- **Τύπος ΙΙ**: Κάτι που το λογικό υποκείμενο κατέχει *(μαγνητική συσκευή αναγνώρισης π.χ. έξυπνη κάρτα ή ψηφιακό πιστοποιητικό)*
- **Τύπος ΙΙΙ**: Κάτι που χαρακτηρίζει το λογικό υποκείμενο με βάση μονοσήμαντα βιομετρικά χαρακτηριστικά του *(συστήματα βιομετρικής τεχνολογίας, π.χ. εφαρμογές δακτυλικών αποτυπωμάτων, αναγνώριση φωνής και ίριδας ματιού)*
- **Τύπος ΙV**: Κάτι που προσδιορίζει την τοποθεσία που βρίσκεται το λογικό υποκείμενο *(π.χ. διεύθυνση IP).*

Σχήματα αυθεντικοποίησης προστατευόμενων πόρων

Προστατευόμενος πόρος	**Κάτι που γνωρίζεις**	**Κάτι που έχεις**	**Κάτι που είσαι**	**Γεωγραφική θέση**
Πλατφόρμα, Host	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα	Βιομετρικό σύστημα (δακτυλικό αποτύπωμα, γεωμετρία χεριού, αναγνώριση προσώπου0	Αναγνωριστικό υπολογιστή ή IP διεύθυνση
Σύστημα Διαχείρισης Δικτύου (σύστημα αρχείων και εκτυπώσεων)	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα - Ψηφιακό πιστοποιητικό	Βιομετρικό σύστημα (δακτυλικό αποτύπωμα, γεωμετρία χεριού, αναγνώριση προσώπου0	Έλεγχος χρονικής στιγμής ή θέση του Η/Υ από τον οποίο γίνεται η πρόσβαση
Υπηρεσία Δικτύου (Web, FTP, Telnet)	Όνομα χρήστη/ συνθηματικό	Ιδιωτικό κλειδί - Έξυπνη κάρτα		Διεύθυνση IP
Σύστημα Διαχείρισης Βάσεων Δεδομένων	Όνομα χρήστη/ συνθηματικό			Διεύθυνση IP

Πλεονεκτήματα και μειονεκτήματα

- **Τύπος Ι: Κάτι που γνωρίζει**

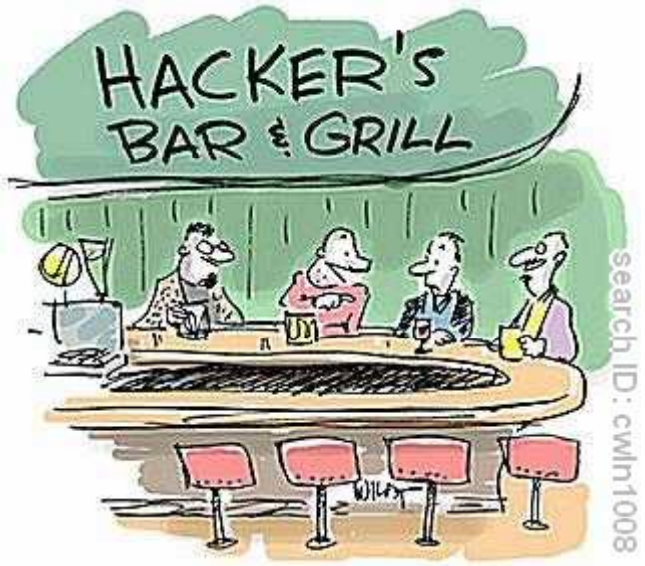
- Μειονεκτήματα:

1. Τα τεκμήρια αυθεντικοποίησης μπορούν εύκολα να αντιγραφούν
2. Συνήθως είναι εύκολο να τα μαντέψει κανείς, χωρίς ιδιαίτερες τεχνικές γνώσεις
3. Συνήθως μπορούν να αποκαλυφθούν με αυτοματοποιημένες μεθόδους

- Πλεονεκτήματα:

1. Εύκολη υλοποίηση και εφαρμογή
2. Τροποποιούνται εύκολα
3. Δε χάνονται ή κλέβονται
4. Αν και είναι απλά στη χρήση τους, στην περίπτωση που είναι ένας μοναδικός συνδυασμός αριθμών και γραμμάτων, δεν αποκαλύπτονται εύκολα

Περίπου 40% των συνθηματικών που επιλέγουν οι χρήστες μαντεύεται εύκολα από προγράμματα. 3.8% των συνθηματικών είναι μία μοναδική λέξη που υπάρχει σε λεξικό και 12% μια λέξη και ένα τελικό ψηφίο. Τα 2/3 αυτών των ψηφίων ήταν 1.



Πλεονεκτήματα και μειονεκτήματα

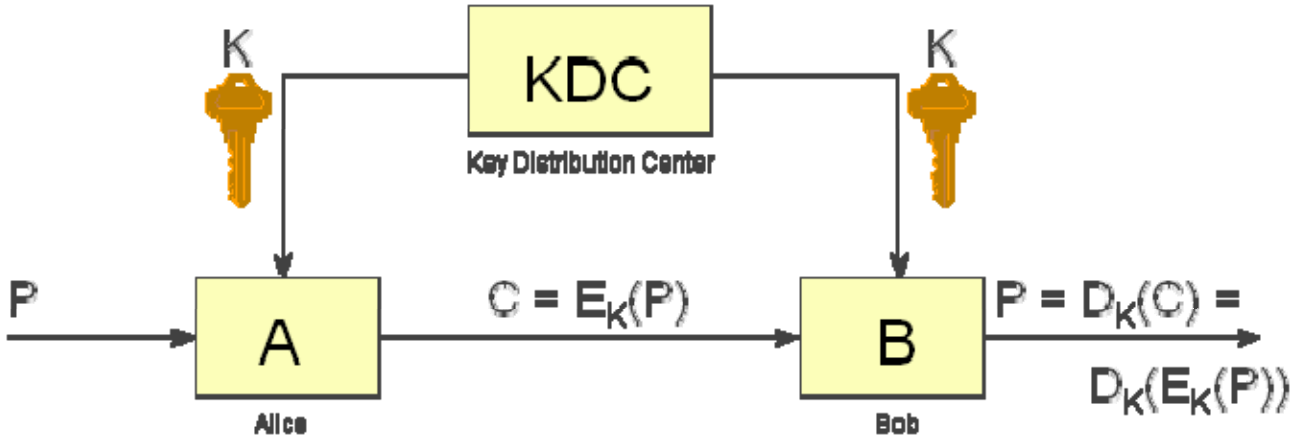
- **Τύπος ΙΙ: Κάτι που κατέχει**
  - Μειονεκτήματα:
    1. Υψηλό κόστος
    2. Μπορούν να χαθούν ή να κλαπούν
  - Πλεονεκτήματα:
    1. Δεν αντιγράφονται εύκολα καθώς κατασκευάζονται από ειδικά υλικά τα οποία δεν είναι ευρέως διαθέσιμα

- **Τύπος ΙΙΙ: Κάτι που το χαρακτηρίζει**
  - Μειονεκτήματα:
    1. Δυσκολίες στην κατασκευή αξιόπιστων συσκευών αναγνώρισης με χαμηλό κόστος
    2. Δεν είναι αλάνθαστα
  - Πλεονεκτήματα:
    1. Παρέχουν μεγαλύτερη ασφάλεια από τον Τύπο Ι και Τύπο ΙΙ.

Συμμετρική και Ασύμμετρη Κρυπτογραφία

- Συμμετρική (Κλασική) Κρυπτογραφία
  - Το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και για την αποκρυπτογράφηση δεδομένων
  - Τα συναλλασσόμενα μέρη πρέπει να συμφωνήσουν εκ των προτέρων για το κλειδί που θα χρησιμοποιηθεί
  - Η προστασία και διανομή του κλειδιού αποτελεί κρίσιμο πρόβλημα
- Ασύμμετρη (Δημόσιου Κλειδιού) Κρυπτογραφία
  - Χρησιμοποιούνται δύο διαφορετικά κλειδιά, ένα ιδιωτικό και ένα δημόσιο, τα οποία σχετίζονται μεταξύ τους με μονόδρομες συναρτήσεις (one-way functions)
  - Τα δεδομένα που κρυπτογραφούνται με το ένα κλειδί, αποκρυπτογραφούνται αποκλειστικά με το άλλο
  - Μόνο μία φυσική οντότητα γνωρίζει το ιδιωτικό κλειδί, ενώ το δημόσιο κλειδί είναι εύκολα διαθέσιμο στο κοινό

Συμμετρική Κρυπτογραφία

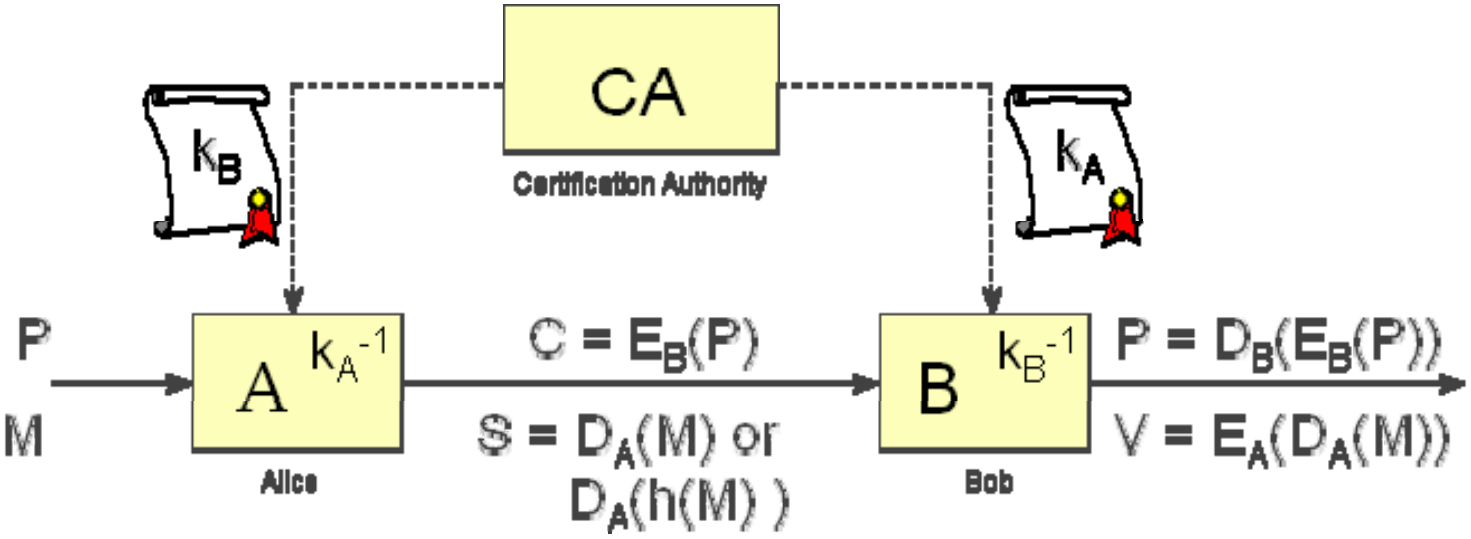


Γνωστοί Συμμετρικοί αλγόριθμοι:

- DES, Triple-DES
- Blowfish, SAFER, CAST
- RC2, RC4 (ARCFOUR), RC5, RC6

"The new locks are more secure,
but carrying the keys sure are a hassle."

Κρυπτογραφία Δημόσιου Κλειδιού



Γνωστοί αλγόριθμοι Δημόσιου Κλειδιού

- RSA
- Diffie-Hellman Key Exchange
- ElGamal, Digital Signature Standard (DSS)

Υβριδική Κρυπτογραφία

- Η ασύμμετρη κρυπτογραφία είναι μη αποτελεσματική για την κρυπτογράφηση μεγάλου όγκου δεδομένων, αντίθετα από τη συμμετρική
- Συνηθισμένη χρήση της ασύμμετρης κρυπτογραφίας είναι η αποστολή ενός συμμετρικού κρυπτογραφικού κλειδιού μέσω ενός ανασφαλούς διαύλου
- Ένα «Κέντρο Διανομής Κλειδιών» (Key Distribution Center) διανέμει με ασφάλεια στα συναλλασσόμενα μέρη ένα συμμετρικό κλειδί, κρυπτογραφημένο με τα δημόσια κλειδιά των εμπλεκομένων
- Οι συναλλασσόμενοι αποκρυπτογραφούν το κλειδί αυτό και ξεκινούν εμπιστευτικές συνόδους μεταξύ τους, χρησιμοποιώντας συμμετρικούς αλγόριθμους
- Ο συνδυασμός των δύο τεχνολογιών ονομάζεται Υβριδική Κρυπτογραφία με Ψηφιακό Φάκελο (digital envelope)

Προβλήματα της Κρυπτογραφίας Δημόσιου Κλειδιού

- Πώς επαληθεύεται η ταυτότητα του κατόχου ενός ζεύγους κλειδιών;
- Πώς διασφαλίζεται η μυστικότητα και η ακεραιότητα των κλειδιών κατά τη δημιουργία και τη χρήση τους;
- Πώς διανέμονται στο κοινό τα δημόσια κλειδιά, έτσι ώστε να διασφαλίζεται η αντιστοίχησή τους με μία φυσική οντότητα;
- Πώς ολοκληρώνεται ο κύκλος ζωής τους, όταν αυτό κριθεί αναγκαίο;
- Διαφαίνεται η ανάγκη ύπαρξης μίας «Έμπιστης Τρίτης Οντότητας» που διαχειρίζεται «Ψηφιακά Πιστοποιητικά».

"You'll have to wait until I find my keys."

Ηλεκτρονική Υπογραφή

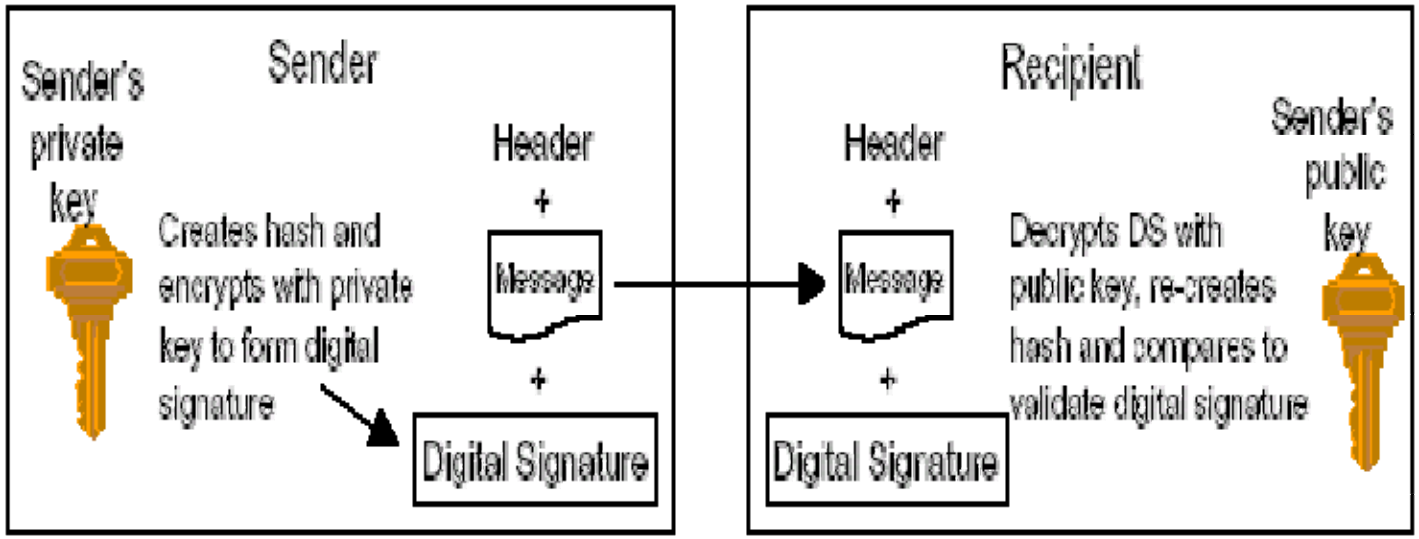
- Η Ηλεκτρονική Υπογραφή (electronic signature) είναι δεδομένα συνημμένα ή συσχετισμένα με ένα ηλεκτρονικό κείμενο, τα οποία χρησιμεύουν στην επαλήθευση της αυθεντικότητάς του

- Χαρακτηριστικά:
  - Είναι μονοσήμαντα συνδεδεμένη με τον υπογράφοντα
  - Παρέχει τη δυνατότητα αναγνώρισης του υπογράφοντα
  - Δημιουργείται με μέσα που βρίσκονται στον αποκλειστικό έλεγχο του υπογράφοντα
  - Είναι μονοσήμαντα συνδεδεμένη με το σχετικό κείμενο, με τρόπο ώστε να διασφαλίζεται η ακεραιότητά του

Συναρτήσεις Σύνοψης (Hash functions)

- Δέχονται ως είσοδο δεδομένα μεταβλητού μεγέθους και επιστρέφουν μία σειρά bits σταθερού μήκους
- Το αποτέλεσμα ονομάζεται «Σύνοψη» ή «Ίχνος» ή «Αποτύπωμα» του αρχικού κειμένου
- Οι συναρτήσεις είναι μονόδρομες και συνεπώς η ανάκτηση του αρχικού κειμένου από τη σύνοψη είναι πρακτικά ανέφικτη
- Η σύνοψη χαρακτηρίζει μοναδικά το αρχικό κείμενο, δηλαδή είναι πρακτικά ανέφικτο να βρεθούν δύο αρχικά κείμενα με την ίδια σύνοψη
- Γνωστές συναρτήσεις σύνοψης: RIPEMD-160, MD2, MD5, SHA-256, BSAH, Square-Mod (σύνηθες μήκος σύνοψης: 128-160 bits)

Δημιουργία και Επαλήθευση Ψηφιακής Υπογραφής



Later, Don Diego de Vega would modify his mark to a simple letter z.

Νομικό πλαίσιο

- Διεθνής αναγνώριση των ψηφιακών υπογραφών ως ισότιμες με τις ιδιόχειρες
- Η Ευρωπαϊκή οδηγία EC/93/1999 για τις ηλεκτρονικές υπογραφές έχει ήδη υιοθετηθεί από όλα τα κράτη-μέλη
- Στην Ελλάδα υιοθετήθηκε με το Π.Δ. 150/2001
- Η ΕΕΤΤ με την απόφαση 248/71 (ΦΕΚ 603/Β'/16-5-2002) ρυθμίζει τη διαπίστευση των παρόχων υπηρεσιών πιστοποίησης και την έκδοση «αναγνωρισμένων πιστοποιητικών»

Ψηφιακό Πιστοποιητικό

- Ψηφιακό Πιστοποιητικό είναι μία ψηφιακά υπογεγραμμένη δομή δεδομένων, η οποία αντιστοιχίζει μία ή περισσότερες ιδιότητες μιας φυσικής οντότητας στο δημόσιο κλειδί που της ανήκει

- Το πιστοποιητικό είναι υπογεγραμμένο από μία Τρίτη Οντότητα, η οποία είναι Έμπιστη και Αναγνωρισμένη να δρα ως «Πάροχος Υπηρεσιών Πιστοποίησης» (Trusted Third Party – TTP & Certification Services Provider – CSP)

- Διασφαλίζει με τεχνικά, αλλά και νομικά, μέσα ότι ένα δημόσιο κλειδί ανήκει σε μία και μόνο συγκεκριμένη οντότητα και συνεπώς ότι η οντότητα αυτή είναι ο νόμιμος κάτοχος του αντίστοιχου ιδιωτικού κλειδιού

Περιεχόμενα ενός πιστοποιητικού

Ένα ψηφιακό πιστοποιητικό περιέχει τις παρακάτω βασικές ομάδες πεδίων:

- *Αναγνωριστικά πιστοποιητικού:* Τύπος - Πρότυπο, Έκδοση, Σειριακός αριθμός, Αλγόριθμος υπογραφής
- *Περίοδος Ισχύος:* Από – Έως
- *Πληροφορίες Εκδότη:* Διακριτικό όνομα, Σημείο πρόσβασης, Αναγνωριστικό κλειδιού
- *Υποκείμενο:* Πλήρες Διακριτικό Όνομα του κατόχου του πιστοποιητικού
- *Δημόσιο κλειδί* που αντιστοιχεί στο υποκείμενο
- *Επεκτάσεις:* Επιτρεπόμενες χρήσεις, Σημείο διανομής πληροφοριών κατάστασης, άλλα εξειδικευμένα ανά εφαρμογή πεδία
- *Κρίσιμες επεκτάσεις:* Όπως οι προηγούμενες, αλλά χαρακτηρισμένες ως «απαράβατες».
- *Υπογραφή Εκδότη* σε όλη τη δομή
- *Σύνοψη* πιστοποιητικού ως κλειδί αναφοράς

Δείγμα πιστοποιητικού X.509 v3 σε μορφή κειμένου

Certificate:
Data:
Version: 3 (0x0)
Serial Number: 2003532 (0x0)
Signature Algorithm: md5withRSAEncryption
Issuer: C=GR, L=Athens, O=University of the Aegean, OU=Certification Authority, CN=ca.aegean.gr, Email=ca@aegean.gr
Validity
Not Before: Nov 14 17:15:25 2003 GMT
Not After : Dec 14 17:15:25 2003 GMT
Subject: C=GR, L=Hermoupolis, O= University of the Aegean, OU=Syros, CN=www.aegean.gr, Email=webmaster@aegean.gr

Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Modulus:
00:9a:92:25:ed:a4:77:69:23:d4:53:05:2b:1f:3a:
55:32:bb:26:de:0a:48:d8:fc:c8:c0:c8:77:f6:5d:
61:fd:1b:33:23:4f:f4:a8:2d:96:44:c9:5f:c2:6e:
45:6a:9a:21:a3:28:d3:27:a6:72:19:45:1e:9c:80:
a5:94:ac:8a:67
Exponent: 65537 (0x10001)
Key Usage: Digital Signature, Key Encipherment, Client Authentication
Signature Algorithm: md5withRSAEncryption

7c:8e:7b:58:b9:0e:28:4c:90:ab:20:83:61:9e:ab:7
8:2b:a4:

54:39:80:7b:b9:d9:49:b3:b2:2a:fe:8a:52:f4:c2:8
9:0e:5c:

7b:92:f8:cb:77:3f:56:22:9d:96:8b:b9:05:c4:18:0
1:bc:40:
ee:bc:0e:fe:fc:f8:9b:9d:70:e3

Γενική Κατηγοριοποίηση

- *Προσωπικό πιστοποιητικό ή Πιστοποιητικό Ταυτότητας* (Personal or Identity certificate): Το υποκείμενο είναι φυσικό πρόσωπο
- *Πιστοποιητικό Συσκευής ή Εξυπηρετητή* (Server or Device certificate): Π.χ. Δρομολογητής ή Web server
- *Πιστοποιητικό Ρόλου* (Role-based certificate): Το υποκείμενο δεν είναι φυσικό πρόσωπο και ο κάτοχος του ιδιωτικού κλειδιού μπορεί να αλλάζει
- *Πιστοποιητικό Οργανισμού* (Organisational certificate): Π.χ. "Microsoft Corp" για την υπογραφή λογισμικού
- *Πιστοποιητικό Ιδιοτήτων* (Attribute certificate): Χωρίς κλειδί. Αποδίδει ρόλους και δικαιώματα σε μια φυσική οντότητα
- *Ομαδικό Πιστοποιητικό* (Group certificate): Ταυτοποιεί μία ομάδα και επιβεβαιώνει τη συμμετοχή οντοτήτων σε αυτή
- *Πιστοποιητικό Αντιπροσώπου ή Προσωρινό* (Proxy certificate): Παράγεται από το ίδιο το υποκείμενο, έχει διάρκεια ισχύος λίγων ωρών, π.χ. μηχανισμοί single-sign-on

Ανάκληση Πιστοποιητικών

- Λόγοι ανάκλησης
  - Απώλεια ιδιωτικού κλειδιού
  - Κλοπή ή διαρροή ιδιωτικού κλειδιού
  - Αλλαγή στοιχείων ή ρόλου
  - Παύση λειτουργίας CSP
- Δημοσίευση της Πληροφορίας Κατάστασης Πιστοποιητικών (Certificate Status Information – CSI)
  - Λίστα Ανάκλησης Πιστοποιητικών (CRL – Certificate Revocation List)
  - Online Certification Status Protocol – OCSP (RFC-2560)
  - delta-CRL: Μόνο τα ανακληθέντα πιστοποιητικά που δεν υπήρχαν στην προηγούμενη delta-CRL
  - Πρόσβαση σε online βάσεις δεδομένων (http, ftp, ldap)

Εμπιστοσύνη (trust)

"Μία οντότητα Α θεωρείται ότι εμπιστεύεται μία δεύτερη οντότητα Β όταν η οντότητα Α αποδέχεται ότι η οντότητα Β θα συμπεριφερθεί ακριβώς όπως αναμένεται και απαιτείται".

- Εμπιστοσύνη βασισμένη στο λογισμό: εκτίμηση του βαθμού εξάρτησης από τις άλλες οντότητες, το προσδοκώμενο όφελος και τους ενδεχόμενους κινδύνους
- Εμπιστοσύνη βασισμένη στην πληροφορία: μείωση της αίσθησης αβεβαιότητας και ελαχιστοποίηση των ενδεχόμενων κινδύνων
- Μεταβατική εμπιστοσύνη: «τυφλή» εμπιστοσύνη προς τις οντότητες που υποδεικνύονται
- Εμπιστοσύνη προς το κοινωνικό σύστημα: δεν απαιτείται συνεύρεση ή γνωριμία των εμπλεκόμενων μερών

Αρχές Ασφαλείας

- Η αρχή της ευκολότερης διείσδυσης (Principle of Easiest Penetration)

  Ο επιτιθέμενος αναμένεται να χρησιμοποιήσει οποιοδήποτε μέσο για να διεισδύσει στο σύστημα

  "The attacker will exploit any vulnerability available, not just the ones of which we are aware, much less those for which we have the strongest controls".

- Η αρχή της επαρκούς προστασίας (Principle of Adequate Protection)

  Οι πόροι πρέπει να προστατεύονται στο βαθμό που το δικαιούνται και μόνο για το χρονικό διάστημα που έχουν κάποια αξία

Αρχές Ασφαλείας

- Η αρχή της αποτελεσματικότητας (Principle of Effectiveness)

  Κάθε μηχανισμός ελέγχου πρέπει να χρησιμοποιείται σωστά ώστε να είναι αποτελεσματικός.

  "Efficient, easy to use, and appropriate"

- Η αρχή του ποιο αδύναμου συνδέσμου (Principle of Weakest Link)

  Η ασφάλεια είναι τόσο ισχυρή όσο ο πιο αδύναμη συνιστώσα της

  "Whether it is the power supply that powers the firewall or the operating system under the security application or the human, who plans, implements, and administers controls, a failure of any control can lead to a security failure"

"A hacker broke into our computer and, in an act of random kindness, organized our student files."

Περισσότερες αρχές ασφαλείας

- ***Μην επικοινωνείς με αγνώστους***

  – Πρέπει να είσαι απολύτως βέβαιος (ή τουλάχιστον σχεδόν βέβαιος) για την ταυτότητα μιας συσκευής ή / και ενός χρήστη πριν επικοινωνήσεις μαζί του

  – Όλες οι παραδοσιακές μέθοδοι επικοινωνίας βασίζονται σε κάποιου είδους αναγνώριση της ταυτότητας του συνομιλητή

    - Π.χ., όταν μιλάμε στο τηλέφωνο αναγνωρίζουμε το συνομιλητή από τη φωνή του αλλά και έμμεσα από το περιεχόμενο των πληροφοριών που μεταδίδει

- Δεν αρκεί όμως πάντοτε η επαλήθευση της ταυτότητας του συνομιλητή κάνοντας χρήση κάποιας διαδικασίας αυθεντικοποίησης. Είναι επίσης εξίσου απαραίτητο να γνωρίζουμε ότι κάθε μήνυμα που λαμβάνουμε προέρχεται από τον πραγματικό αποστολέα

- Η απλούστερη μέθοδος για να το επιτύχουμε αυτό είναι να ζητούμε από το συνομιλητή να αποδείξει ότι γνωρίζει ένα μυστικό κλειδί ή συνθηματικό

- Η περαιτέρω ενσωμάτωση του μυστικού κλειδιού σε κάθε μήνυμα που λαμβάνεται ή αποστέλλεται μπορεί (υπό προϋποθέσεις) να εγγυηθεί την αυθεντικότητα των επιμέρους μηνυμάτων.

Περισσότερες αρχές ασφαλείας

- ***Μην αποδέχεσαι τίποτα χωρίς εγγυήσεις***

  – Στο χώρο της ασφάλειας επικοινωνιών ο όρος «εγγύηση» σημαίνει εγγύηση αυθεντικότητας. Δηλ., απόδειξη ότι κάποιο μήνυμα δεν έχει αλλοιωθεί

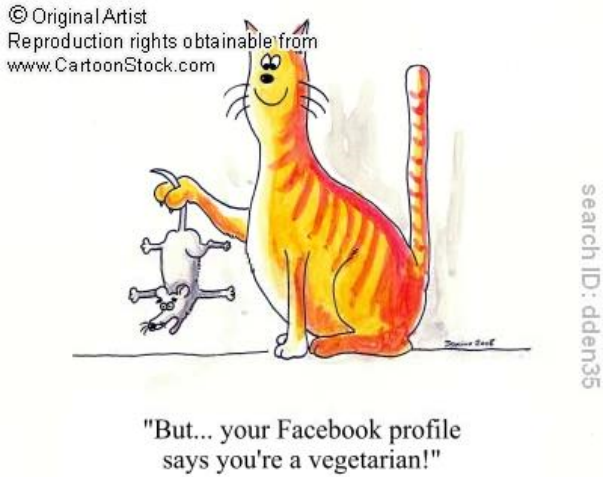
  – Αν και ο συνομιλητής πρέπει να αυθεντικοποιηθεί πριν γίνουν αποδεκτά τα μηνύματά του, δεν είμαστε σε θέση να γνωρίζουμε αν τα μηνύματα που λαμβάνουμε αμέσως μετά τη διαδικασία αυθεντικοποίησης είναι αυτά που αυτός έστειλε ή κατά κάποιο τρόπο αλλοιώθηκαν, καθυστέρησαν ή έχουν αντικατασταθεί εξ ολοκλήρου με κάποια άλλα

  – Για αυτό το λόγο είναι απαραίτητη η προστασία της ακεραιότητας των μηνυμάτων που μεταδίδονται μεταξύ των επικοινωνούντων στοιχείων δικτύου

Περισσότερες αρχές ασφαλείας

- ***Όλοι πρέπει να αντιμετωπίζονται ως εν δυνάμει εχθροί μέχρι αποδείξεως του εναντίου*:**

  – Στο ενσύρματο περιβάλλον του γραφείου μας είμαστε σε θέση - με κάποιο βαθμό βεβαιότητας - να γνωρίζουμε το που συνδεόμαστε με την έννοια ότι τοποθετούμε το καλώδιο δικτύου στην πρίζα του τοίχου που ανήκει στον οργανισμό στον οποίο εργαζόμαστε



- Όμως, σε ένα ασύρματο περιβάλλον, οι σταθμοί των χρηστών είναι κατασκευασμένοι ώστε μόλις ενεργοποιούνται να αναζητούν τα δίκτυα με τα οποία μπορούν να συνδεθούν.

- Έτσι, ο επιτιθέμενος θα μπορούσε να εγκαταστήσει ένα πλαστό AP στο απέναντι κτίριο, το οποίο θα εκπέμπει την ταυτότητα του γνήσιου δικτύου αναμένοντας ότι πολλές συσκευές χρηστών θα εξαπατηθούν και θα συνδεθούν τελικά σε αυτό

Περισσότερες αρχές ασφαλείας

- ***Μην εμπιστεύεσαι κανέναν και τίποτα για μεγάλο διάστημα***

  – Η εγκαθίδρυση σχέσεων εμπιστοσύνης (trust) μεταξύ των επικοινωνούντων μερών είναι πολύ σημαντική

  – Απαραίτητη όμως είναι και η τακτική αναθεώρηση αυτών των σχέσεων εμπιστοσύνης

"As a security precaution we will cancel your cards, close your accounts and pretend we've never seen you."

- Συνήθως, η συσκευή μας επικοινωνεί μόνο με συσκευές άλλων χρηστών με τις οποίες έχει προηγουμένως ανταλλάξει κάποιου είδους τεκμήριο ασφάλειας (security token). Π.χ., ένα μυστικό κλειδί, ένα ψηφιακό πιστοποιητικό, κλπ.

- Παρόλα αυτά, όλα τα τεκμήρια ασφαλείας έχουν συνήθως περιορισμένη διάρκεια ζωής και πρέπει να ανανεώνονται τακτικά

Περισσότερες αρχές ασφαλείας

- ***Πάντοτε να χρησιμοποιείς καλά δοκιμασμένες και αποτελεσματικές λύσεις***
  - Πάγια τακτική στο χώρο της ασφάλειας επικοινωνιών είναι η δυσπιστία για καθετί καινούργιο, όπως μια νέα πολιτική, ένα νέο πρωτόκολλο ή μηχανισμός ασφαλείας
  - Π.χ., ένας νέος αλγόριθμος κρυπτογράφησης θα πρέπει να τεθεί στη δοκιμασία του χρόνου για αρκετά μεγάλο διάστημα προκειμένου να μπορούμε να πούμε με κάποιο ποσοστό βεβαιότητας ότι είναι ασφαλής με τα μέσα που προς το παρόν διαθέτουμε

- Π.χ., οι μηχανισμοί ασφαλείας που χρησιμοποιούνται αποκλειστικά στην περιοχή των ασύρματων και κινητών επικοινωνιών θα πρέπει να αντιμετωπίζονται με σκεπτικισμό – καθότι αρκετά νέοι ακόμα – μέχρις ότου αποδείξουν ότι είναι πραγματικά ασφαλείς

Περισσότερες αρχές ασφαλείας

Πάντοτε να βρίσκεσαι σε επιφυλακή

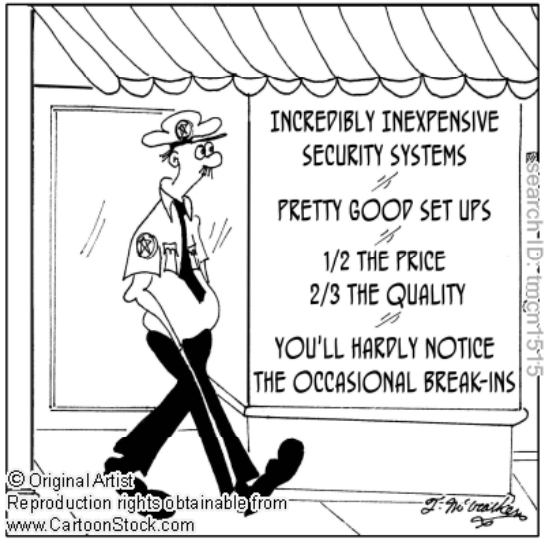
– Όλα τα συστήματα, μη εξαιρουμένων του λογισμικού και του υλικού, κατασκευάζονται κάνοντας κάποιες υποθέσεις συνειδητές ή ασυνείδητες (συμπεριλαμβανομένων και των αναπόφευκτων κατασκευαστικών λαθών)

– Π.χ., οι υπεύθυνοι ανάπτυξης ενός αρθρώματος λογισμικού αναλυτή μηνυμάτων (parser module) για ένα εξυπηρετητή ενδέχεται (ασυνείδητα) να υποθέσουν ότι ο εξυπηρετητής θα δέχεται πάντα σωστά μηνύματα κωδικοποιημένα σύμφωνα με τα ισχύοντα πρότυπα

Burying my bones
was not a safe enough option for me...

- Τι θα συμβεί όμως αν ένας επιτιθέμενος αρχίσει να αποστέλλει μηνύματα που ο αναλυτής του εξυπηρετητή δεν μπορεί να επεξεργαστεί;
- Ένα διαφορετικό παράδειγμα αποτελεί η δημιουργία ενός νέου ή η παράλλαξη ενός υπάρχοντος ιομορφικού λογισμικού, το οποίο τα ήδη εγκατεστημένα αντίμετρα δεν μπορούν να ανιχνεύσουν
- Κανένα προϊόν, μέθοδος, πρωτόκολλο, μηχανισμός ή πολιτική ασφάλειας δεν μπορεί να θεωρηθεί 100% ασφαλής, ακόμα και αν έχει δοκιμαστεί στην πράξη για μεγάλο χρονικό διάστημα

Ερωτήσεις;


INCREDIBLY INEXPENSIVE SECURITY SYSTEMS
PRETTY GOOD SET UPS
1/2 THE PRICE
2/3 THE QUALITY
YOU'LL HARDLY NOTICE THE OCCASIONAL BREAK-INS
© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com