ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε
ΜΕΤΑΠΤΙΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ

Ασφάλεια

ΛΙΑΓΚΟΥ ΒΑΣΙΛΙΚΗ
ΔΙΑΛΕΞΗ-ΙΙ

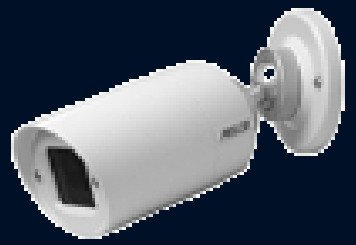
Syllabus

1. Έλεγχος Λογικής & Φυσικής Πρόσβασης
2. Αυθεντικοποίηση Οντότητας – Γενικές Έννοιες
3. Αυθεντικοποίηση Χρήστη με κωδικούς ασφάλειας (passwords)
4. Αυθεντικοποίηση με Κωδικούς Μιας Χρήσης (one-time passwords) & Αυθεντικοποίηση 2 παραγόντων
5. Αυθεντικοποίηση Οντότητας με Πρόκληση-Απάντηση
6. Επιθέσεις Πλαστοπροσωπίας (Phishing, Man-in-the-Middle attacks)

Μηχανισμοί Ασφάλειας - 1η Θεώρηση

Πρόληψη

Φυσική ασφάλεια, access control, replication, Firewalls, Κρυπτογράφηση, Ψηφ. Υπογραφή, Προγράμματα antivirus, Ασφαλής Προγραμματισμός, Πολιτική κωδικών ασφάλειας,…



Ανίχνευση

Συστήματα Ανίχνευσης Εισβολών (IDS), Αρχεία καταγραφής, penetration testing,…

Απόκριση

Back-up, Digital forensics, malware removal, hot sites,…

Κατηγορία Ελέγχου`	Πρόληψη	Ανίχνευση	Αντιμετώπιση
Φυσικής πρόσβασης (παραδείγματα)			
Φράχτες	X		X
Προσωπικό Ασφαλείας	X	X	X
Έξυπνες Κάρτες (smartcards), Βιομετρία	X		
Διαχειριστικός (παραδείγματα)			
Πολιτικές Ασφάλειας	X	X	X
Έλεγχος και Εποπτεία	X	X	
Εκπαίδευση υπαλλήλων	X	X	X
Λογικής Πρόσβασης (παραδείγματα)			
Λίστες Ελέγχου Πρόσβασης (ACLs), MAC, RBAC,…	X		
Passwords, CAPTCHAs	X		
Λογισμικό Antivirus, Anti-spam, Anti-Spyware,..	X	X	X
Κρυπτογράφηση Δεδομένων και Επικοινωνιών	X	X	
Firewalls (Packet Filters, Application Gateways)	X	X	
Συστήματα Ανίχνευσης & Αποτροπής Εισβολών (IDS/IPS)	X	X	X

http://www.cs.uwf.edu/~rdavid/CEN4540/sec3.ppt

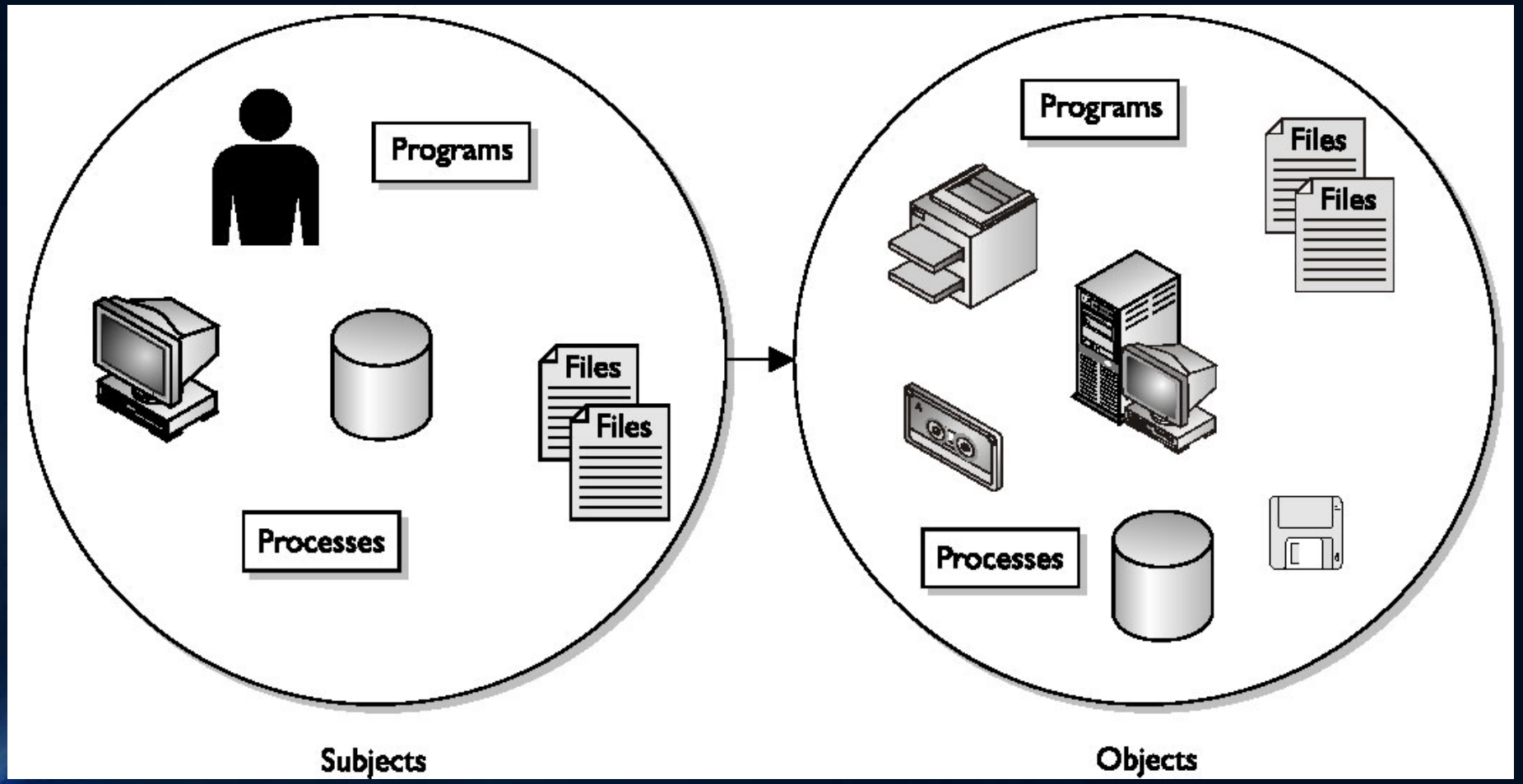
Μηχανισμοί Ασφάλειας - 2η Θεώρηση*

NIST 800-100 I.S. Handbook: A Guide for Managers

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 11-1: Security Control Class, Family, and Identifier

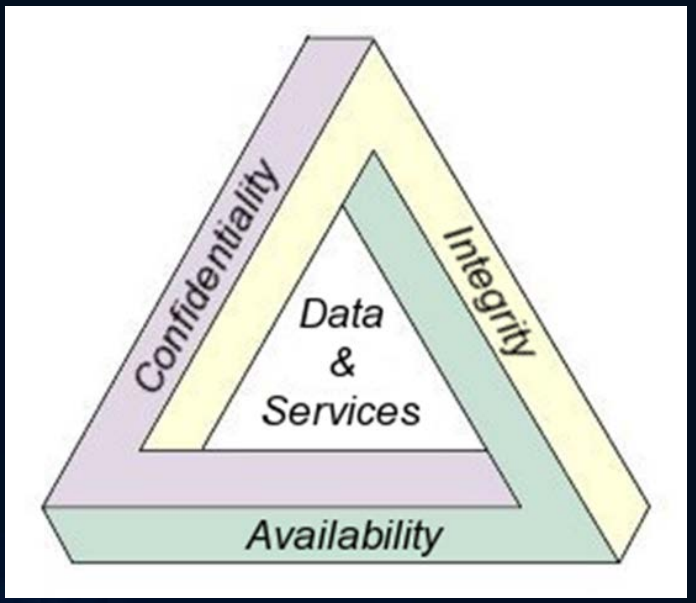
1. Έλεγχος Πρόσβασης – Γενικά



Έλεγχος Πρόσβασης – Γενικά

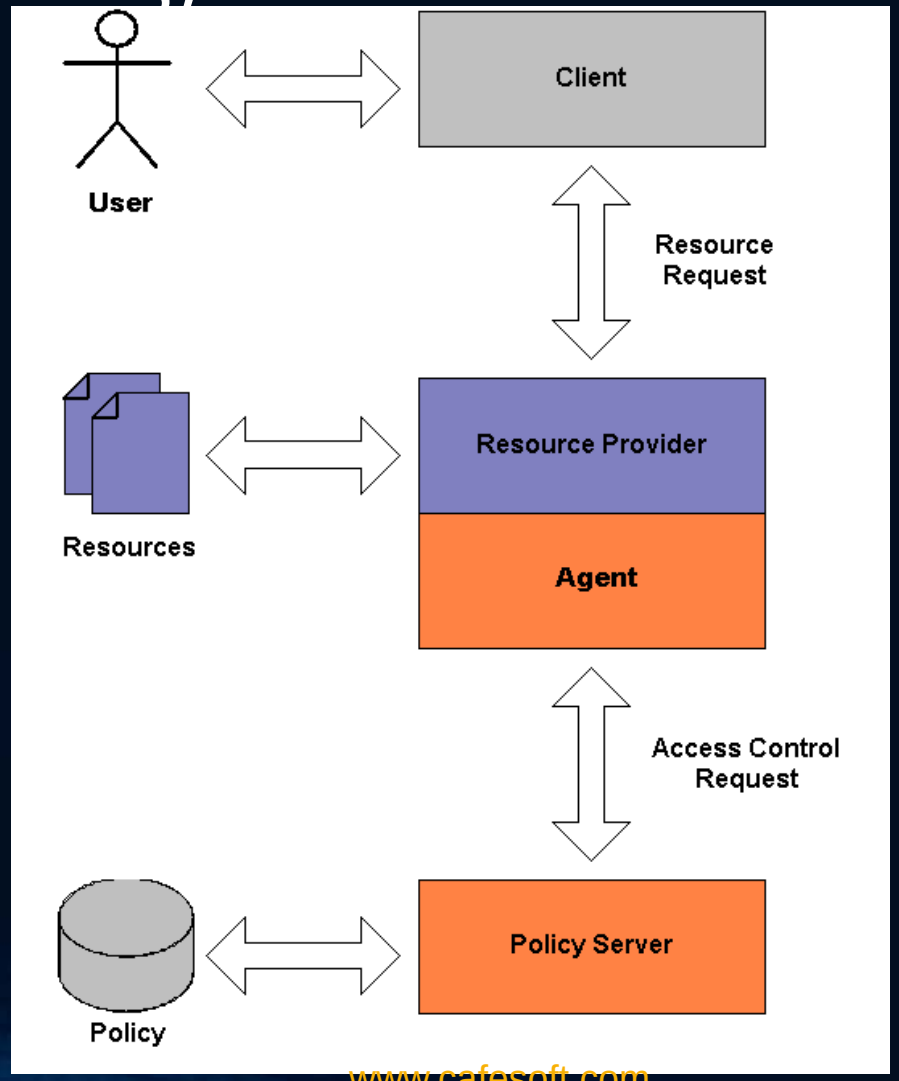
- Πρόσβαση
  - Ροή της πληροφορίας μεταξύ υποκειμένου και αντικειμένου
- Υποκείμενο
  - Μια οντότητα που αιτείται πρόσβαση σε αντικείμενο (ή σε δεδομένα στο αντικείμενο)
- Αντικείμενο
  - Μια (παθητική) οντότητα που περιέχει πληροφορία

- Έλεγχος Πρόσβασης – Γιατί;
  - Εμπιστευτικότητα
  - Διαθεσιμότητα
  - Ακεραιότητα



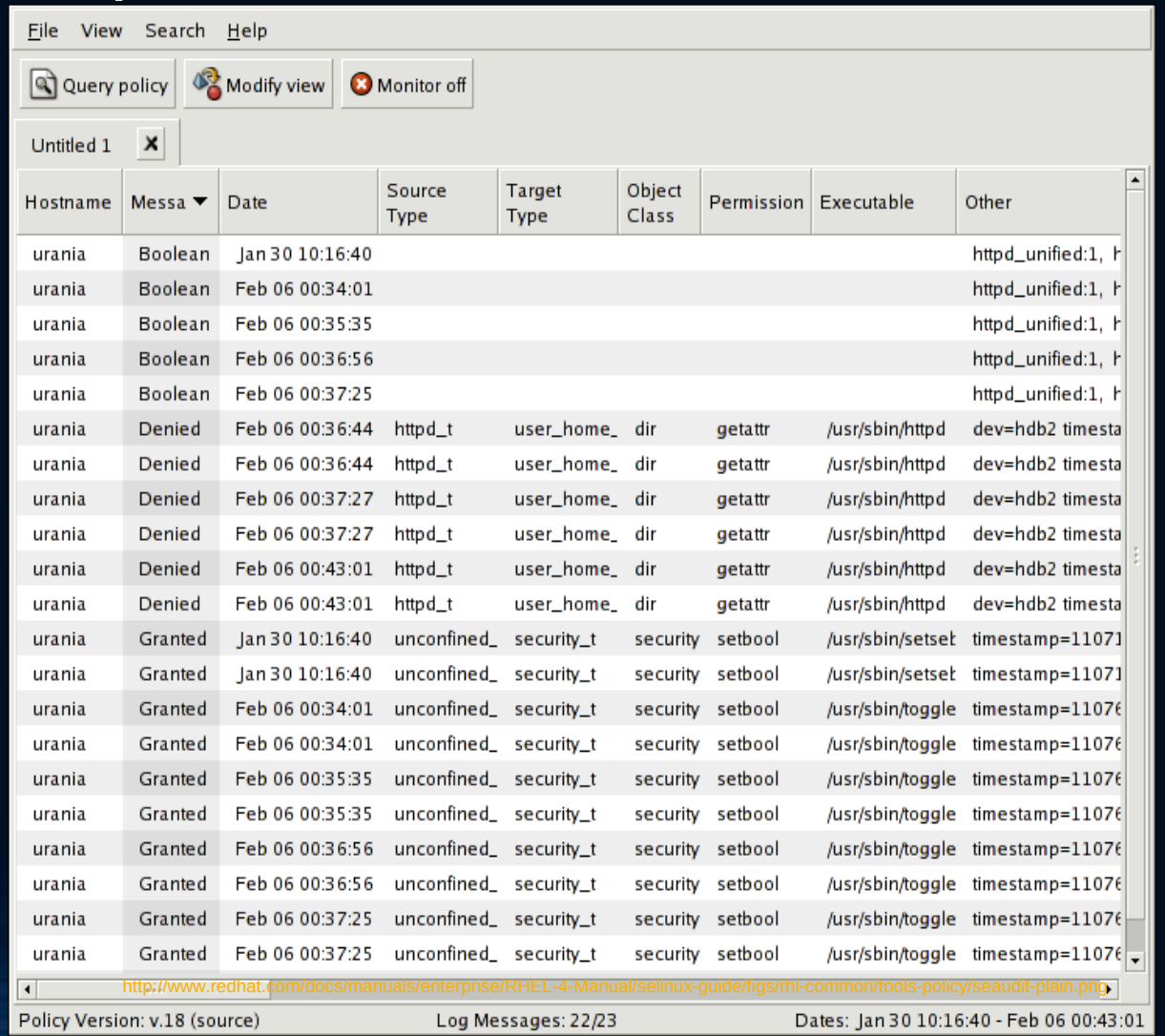
Έλεγχος Πρόσβασης – Πώς;

1. Το υποκείμενο A αποδεικνύει την ταυτότητα του, υποβάλλοντας τα διαπιστευτήρια του (credentials)
   - Τεχνικές και Τεχνολογίες Αυθεντικοποίησης Οντότητας
2. Έλεγχος δικαιωμάτων πρόσβασης που έχει ο A στο αντικείμενο B
   - Εξουσιοδότηση (Authorization)



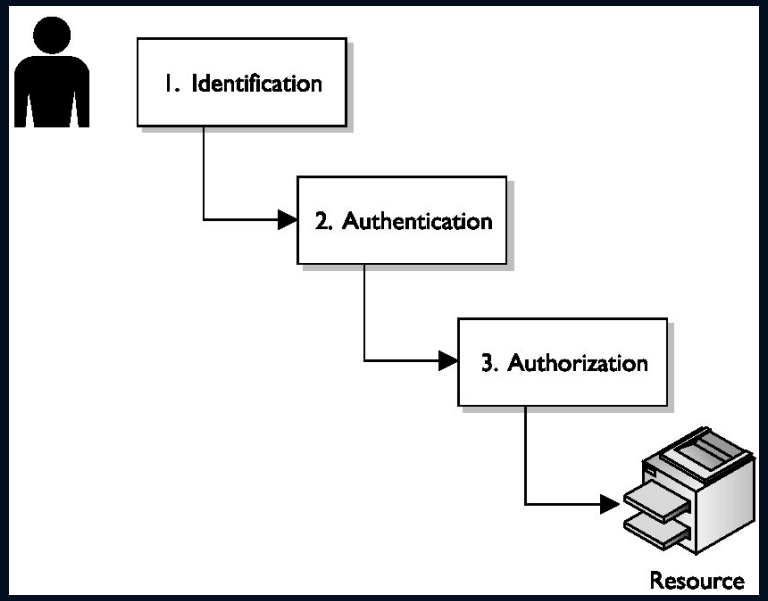
Έλεγχος Πρόσβασης – Πώς;

3. Για όση ώρα αποκτά πρόσβαση στο αντικεί-μενο, οι ενέργειες του χρήστη καταγράφονται
   - Καταγραφή και παρακολούθηση (Logging & Monitoring)



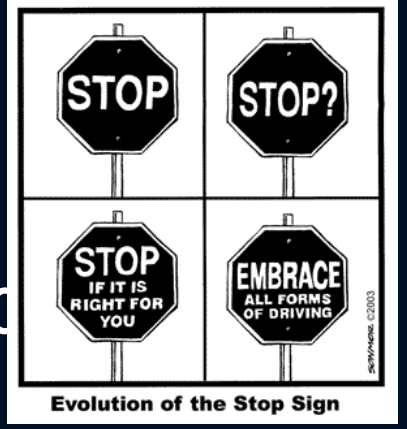
Έλεγχος (Λογικής) Πρόσβασης – Πού

Τα εργαλεία λογισμικού για την ταυτοποίηση, εξουσιοδότηση και καταγραφή, μπορεί να αποτελούν τμήμα του Λειτουργικού Συστήματος, των εφαρμογών λογισμικού, των Βάσεων Δεδομένων κλπ



Logical Access Control

Έλεγχος Φυσικής & λογικής Πρόσβα

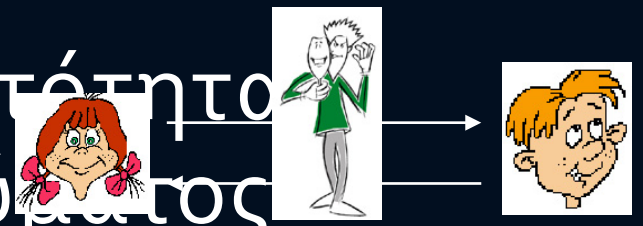


Evolution of the Stop Sign

1. Έλεγχος φυσικής πρόσβασης
   - Φυσική ασφάλεια, συστήματα συναγερμού,
   - Κάρτες πρόσβασης, biometrics,
2. Έλεγχος λογικής πρόσβασης
   - Αυθεντικοποίηση οντότητας & αυθεντικοποίηση μηνύματος
     - π.χ. Passwords, PINs, CAPTCHAs, challenge response …
     - Ψηφιακές υπογραφές, MAC (Message authentication codes),…
   - Εξουσιοδότηση (Authorization)
     - π.χ. Λίστες Ελέγχου Πρόσβασης (ACLs)
     - Έλεγχος ροής (MAC, DAC, RBAC, Chinese Wall, BMA, Inference control…)
     - Firewalls, Antivirus software,…
   - Καταγραφή και παρακολούθηση (Logging & Monitoring)
     - IDS (Intrusion detection systems)

Κατηγορία Ελέγχου`	Πρόληψη	Ανίχνευση	Αντιμετώπιση
Φυσικής πρόσβασης (παραδείγματα)			
Φράχτες	X		X
Προσωπικό Ασφαλείας	X	X	X
Έξυπνες Κάρτες (smartcards), Βιομετρία	X		
Διαχειριστικός (παραδείγματα)			
Πολιτικές Ασφάλειας	X	X	X
Έλεγχος και Εποπτεία	X	X	
Εκπαίδευση υπαλλήλων	X	X	X
Λογικής Πρόσβασης (παραδείγματα)			
Λίστες Ελέγχου Πρόσβασης (ACLs), MAC, RBAC,…	X		
Passwords, CAPTCHAs	X		
Λογισμικό Antivirus, Anti-spam, Anti-Spyware,..	X	X	X
Κρυπτογράφηση Δεδομένων και Επικοινωνιών	X		
Firewalls (Packet Filters, Application Gateways)	X	X	
Συστήματα Ανίχνευσης & Αποτροπής Εισβολών (IDS/IPS)	X	X	X

2. Αυθεντικοποίηση Οντότητα Αυθεντικοποίηση Μηνύματος



Σενάριο Α: Η Alice και ο Bob είναι online και επικοινωνούν σε πραγματικό χρόνο

- **<u>Αυθεντικοποίηση Οντότητας</u>** (Entity Authentication)
  - Αναφέρεται και ως Ταυτοποίηση (Identification)
- Η επικοινωνία μπορεί να είναι διπλής κατεύθυνσης
  - Ταυτοποίηση της Alice από Bob
  - Ταυτοποίηση του Bob από Alice
- Παραδείγματα
  - Τεχνικές Κωδικών Password
  - Πρωτόκολλα Πρόκλησης Απάντησης (Challenge-Response)

Σενάριο Β: Η Alice δημιουργεί ένα μήνυμα το οποίο κάποια στιγμή στο μέλλον παραλαμβάνει ο Bob

- **<u>Αυθεντικοποίηση Προέλευσης Μηνύματος</u>** (Data Origin Auth.)
  - Αναφέρεται και ως αυθεντικοποίηση μηνύματος (message authentication)
- Η επικοινωνία μπορεί να είναι μονής ή διπλής κατεύθυνσης
  - π.χ. Α e-mails Β
- Παραδείγματα
  - Ψηφιακές Υπογραφές
  - Συναρτήσεις MAC

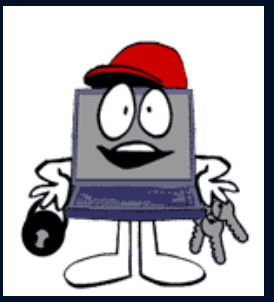
Επιπλέον προσφέρουν και Ακεραιότητα!

Πιστοποίηση Οντότητας - Ταυτοποίηση

Mao, W. Modern Cryptography: Theory and Practice. Prentice Hall, 2003

1. User <--> User
2. User <--> Process/Host
3. Process/Host <--> Process/Host

Αυθεντικοποίηση Οντότητας - Ταυτοποίηση



- Ταυτοποίηση:
  1. Ανθρώπου από Άνθρωπο
  2. Ανθρώπου από Πρόγραμμα/διάταξη
  3. Προγράμματος/Διάταξης από Πρόγραμμα/Διάταξη

- Οι δύο πρώτες κατηγορίες παρουσιάζουν προβλήματα διαχείρισης ☺

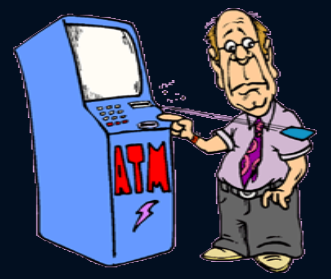
Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αυθεντικοποίηση Οντότητας

- Οι τεχνικές ταυτοποίησης προσφέρουν πειστήρια π.χ. στην Alice σχετικά με:
  1. Την ταυτότητα του Bob
  2. Το γεγονός ότι ο Bob ήταν ενεργός (active) τη στιγμή που δημιουργήθηκαν και αποκτήθηκαν τα πειστήρια

Παράδειγμα Α: Ο Bob τηλεφωνεί στην Alice - **Αμοιβαία Αυθεντικοποίηση** (mutual authentication)

Παράδειγμα Β: Ο Bob εισάγει την κάρτα του και στέλνει το PIN του μέσω του ATM. **Μονομερής αυθεντικοποίηση** (unilateral authentication)



http://www.grinningplanet.com/2004/03-30/atm-banking-copyright1.gif

http://www.callrecordingsolutions.com/images/converstioncartoon.gif

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αυθεντικοποίηση Μηνύματος

- Οι τεχνικές αυθεντικοποίησης μηνύματος προσφέρουν πειστήρια π.χ. στην Alice για :
  - Την ταυτότητα του υποκειμένου που δημιούργησε το μήνυμα που έλαβε.
  - Το γεγονός ότι το υποκείμενο ήταν ενεργός (active) τη στιγμή που δημιουργήθηκε το μήνυμα
- Τα δύο υποκείμενα, μπορεί να μην είναι ενεργά (online) την ίδια χρονική στιγμή

Παράδειγμα Γ: Ο Bob στέλνει ένα e-mail στην Alice. Το μήνυμα αποθηκεύεται στον server αλληλογραφίας της Alice. Κάποια στιγμή, η Alice συνδέεται στο δίκτυο και παραλαμβάνει το mail

http://www.geocities.com/Rainforestwind/ninarchives_emailhumor.gif

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Υπηρεσίες Αυθεντικοποίησης και Ακεραιότητας

Συχνά στη βιβλιογραφία, η Αυθεντικοποίηση Μηνύματος συνδέεται άρρηκτα με την έννοια της Ακεραιότητας. !!!

- π.χ. Εάν το μήνυμα τροποποιηθεί κατά τη μετάδοση του, τότε δεν το έγραψε ο Bob !

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001

Αυθεντικοποίηση Οντότητας

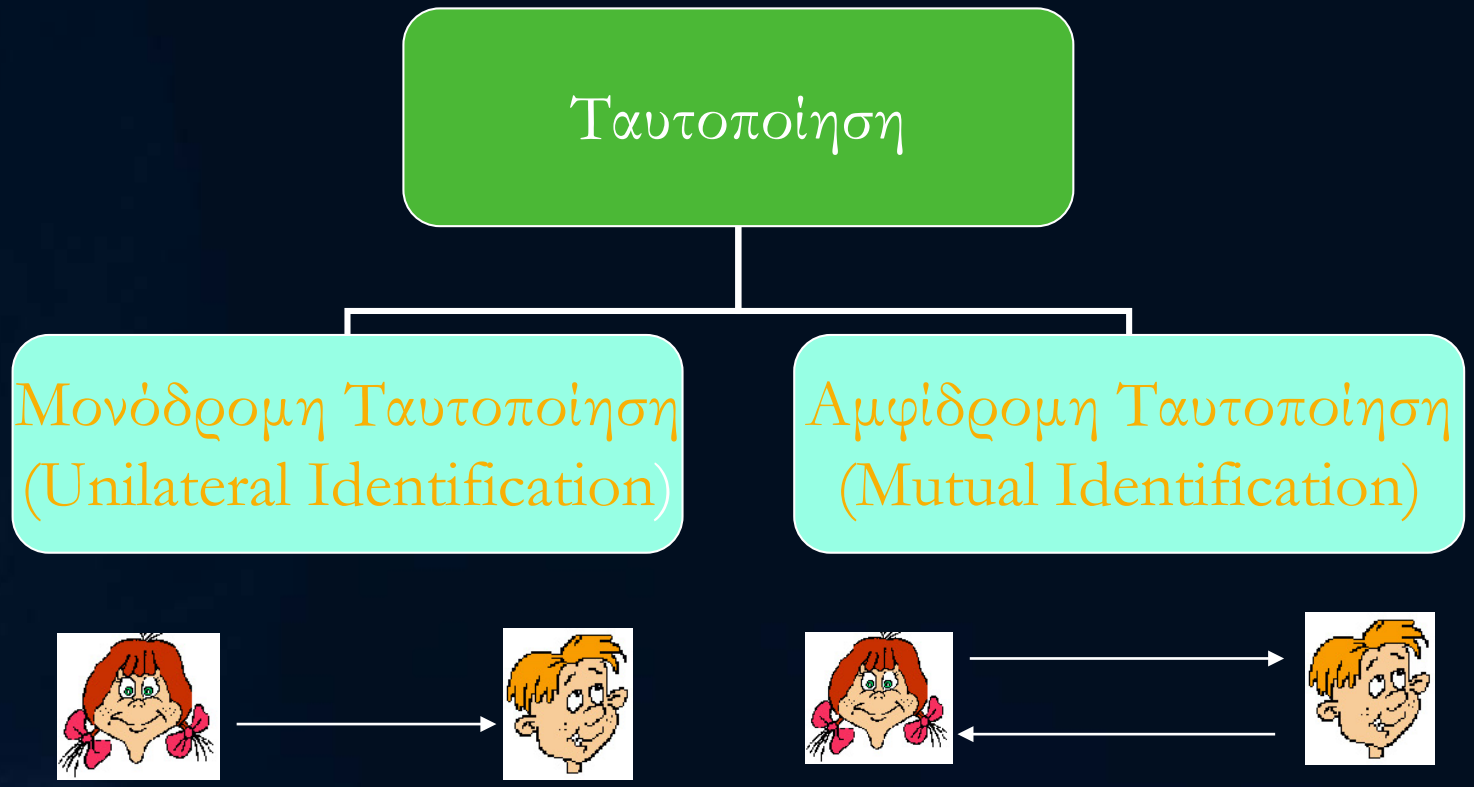
Μια οντότητα Α βεβαιώνεται (μέσω απόκτησης πειστηρίων) για την ταυτότητα Β μιας άλλης οντότητας, καθώς επίσης και για το γεγονός ότι ο Β συμμετέχει (είναι δηλαδή ενεργός) στο πρωτόκολλο τη στιγμή που αυτό διενεργείται

Στόχοι Αυθεντικοποίησης

1. **Περατότητα**: Αν οι Α και Β συμπεριφέρονται τίμια, ο Α αποδέχεται πάντοτε την ταυτότητα του Β ως αυθεντική
2. **Μη Μεταφερσιμότητα**: Ο Α δε μπορεί να χρησιμοποιήσει όσα «βλέπει» & να πλαστοπροσωπήσει τον Β σε κάποιον τρίτο
3. **Ασφάλεια από Πλαστοπροσωπία**: Είναι «δύσκολο» για κάποια τρίτη οντότητα C, να πείσει τον Α ότι είναι ο χρήστης Β !!

Πρωτόκολλα Ταυτοποίησης

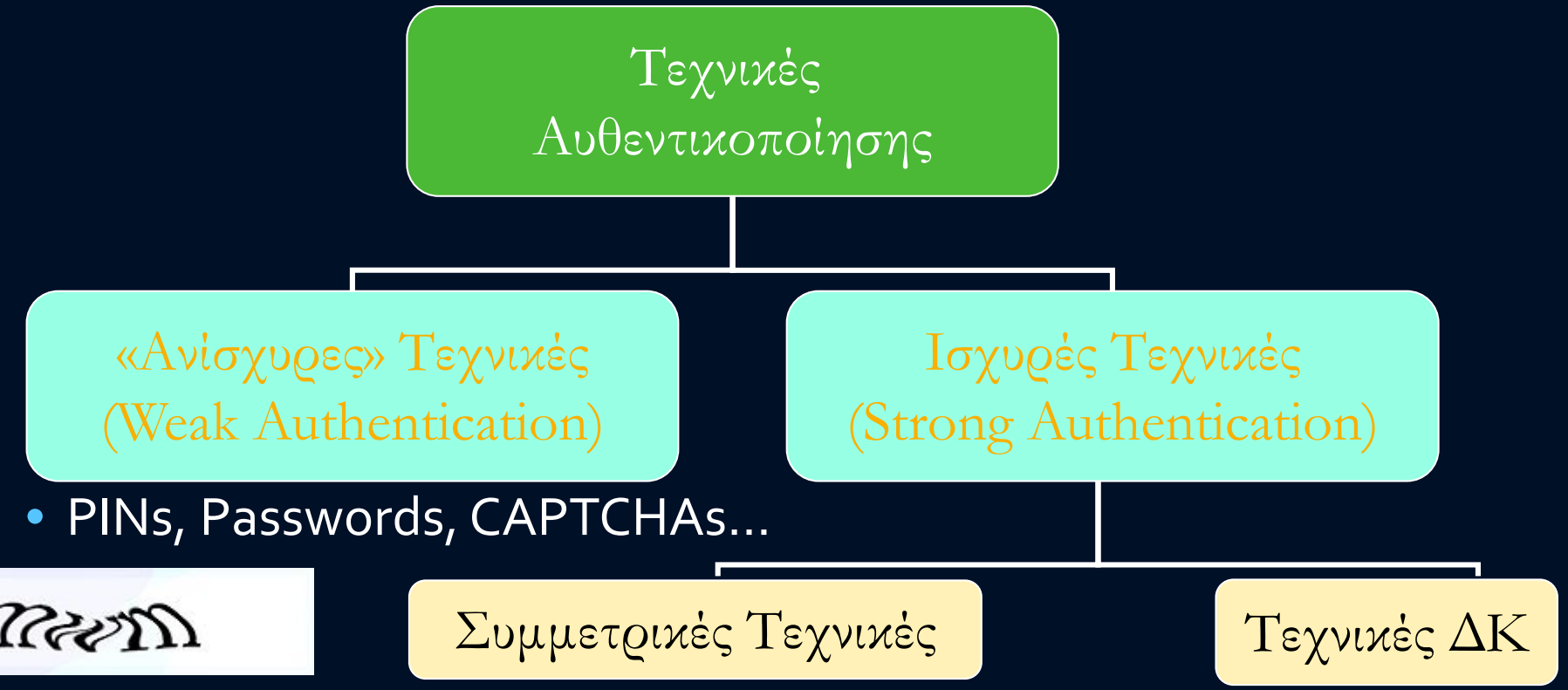
Κατηγοριοποιήσεις



- Ο Bob ταυτοποιεί την Alice (ή το αντίστροφο)
- Ο Bob ταυτοποιεί την Alice ΚΑΙ η Alice ταυτοποιεί τον Bob

Πρωτόκολλα Ταυτοποίησης

Κατηγοριοποιήσεις



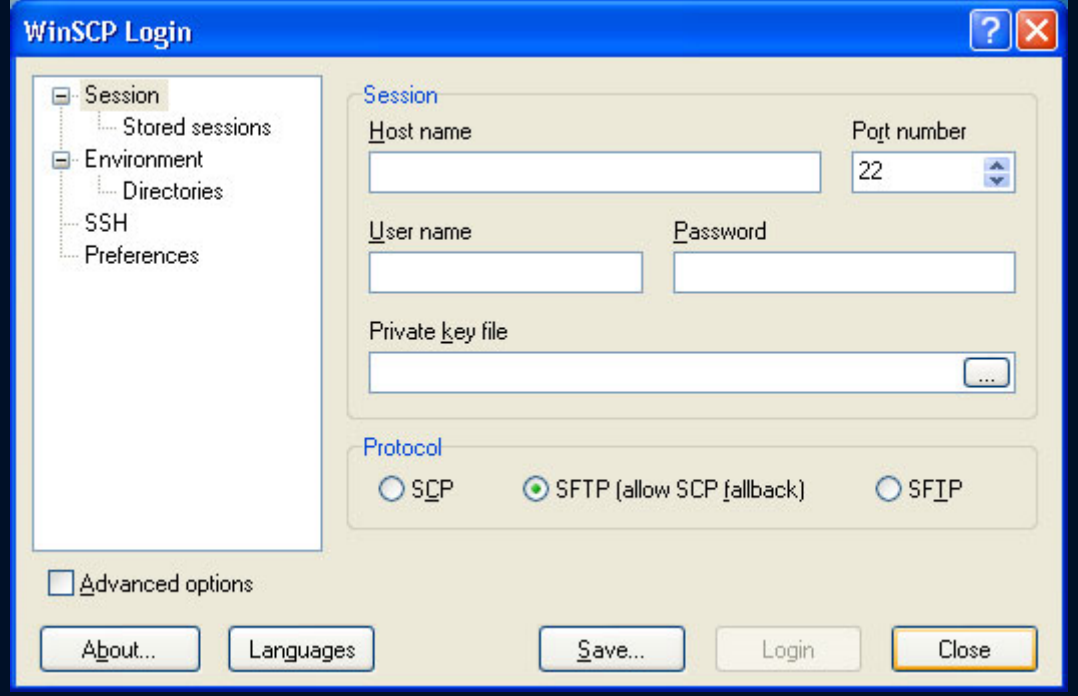
- PINs, Passwords, CAPTCHAs…

- Πρωτόκολλα Πρόκλησης – Απάντησης
- Αποδείξεις μηδενικής γνώσης
- …

Ταυτοποίηση χρηστών

(Human_User to Process/Host)

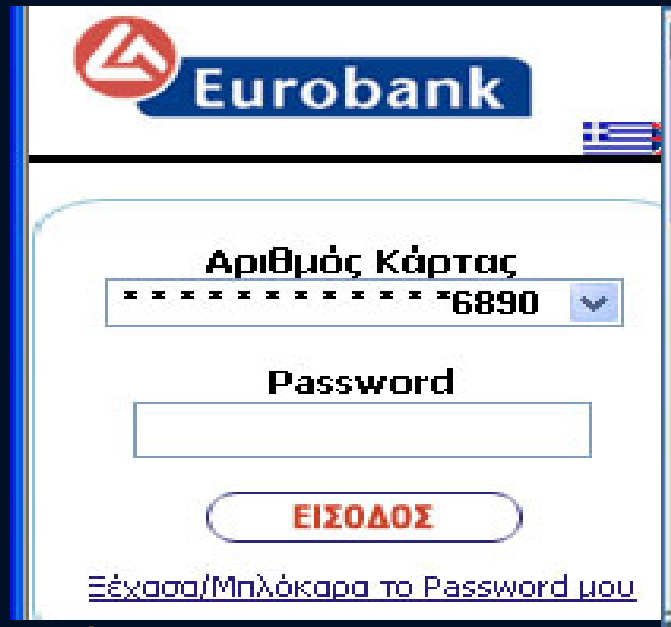
- Η αυθεντικοποίηση χρήστη μπορεί να γίνει με τρεις τρόπους.
  1. Γνώση μιας πληροφορίας (“Something You Know”)
  - Passwords, PIN, κρυπτ/κό κλειδί, προσωπικές πληροφορίες,…
  2. Φυσική κατοχή ενός αντικειμένου (“Something You Have”)
  - PDA, USB flash, κάρτα (π.χ. smart card)
  3. Φυσικά χαρακτηριστικά (“Something /Who You Are”)
  - Βιολογικά ή Συμπεριφοράς: Ίριδα, δαχτ. αποτυπώματα, βάδισμα,…
  4. Τοποθεσία (“Where you are”)
  - Σύνδεση από συγκεκριμένο υπολογιστή, IP δίκτυο,…
  5. Πολλαπλών παραγόντων (multiple factor authentication)
  - Δύο ή περισσότεροι τρόποι ταυτόχρονα (στην ίδια σύνοδο)



Ασφαλής σύνδεση σε απομακρυσμένο Η/Υ

Συναλλαγές σε ATM με τη χρήση κωδικού PIN

PIN σε κινητό



Σύνδεση στο web banking

log-in σε περιβάλλον Windows

Passwords Found in One's Head

Here are some of the passwords that one of the authors currently holds:

Worthless: internal recruiting Web pages, *New York Times* online, private Web area, yahoo.com, realtor.com

Slightly important: acm.org, usenix.org, buy.com, quicken.com, inciid.org, Ibaby.com, amazon.com, barnseandnoble.com, Marriott rewards, continental.com frequent flier account, EZPass PIN, e-toys, ticketmaster, Web interface to voice mail, combination lock on backyard fence, publisher royalties online access, hushmail.com e-mail account

Quite secure: employee services Web site, child care reimbursement program, Unix account login, former university account login, NT domain account login, online phone bill, home voice mail access code, work voice mail access code, cell phone voice mail access code, quicken password for each *linked site*, domain name registration account, drivers license online registration, dial-in password, OTP-based password, keyless access code for car

Top security: garage (2 doors + temporary nanny code), burglar alarm (regular code, master code, nanny's code, and a distress code), bank Web login, online broker, PCAnywhere password for remote control and file transfer, quicken PIN vault, 401k account online access and phone access, stock options account, dial-in password, online access to IRA from previous job, paypal account

A total of 53 passwords.

Firewalls and Internet Security, 2nd Edition. Bellovin et al, 2003

3. Κωδικοί Πρόσβασης (Συνθηματικά)

- Ζητήματα με τους κωδικούς πρόσβασης (Anderson, 2008)
  1. Εγγενής αντίφαση:
  - Θέλουμε κωδικούς «τυχαίους» και «μνημοτεχνικούς» ☺
  2. Εξ' ορισμού συμμετρική τεχνική ταυτοποίησης
  - Ο εκδότης-διαχειριστής γνωρίζει (;) τον κωδικό
  - Πώς επιτυγχάνεται η μη αποποίηση ευθύνης (non-repudiaton);
  3. Διαχείριση κωδικών πρόσβασης
  - Πώς δημιουργούνται / μεταφέρονται οι καινούριοι κωδικοί
  - Πώς θυμάται ο χρήστης τους κωδικούς του;
  - Πώς & πόσο συχνά ανανεώνει τους κωδικούς του;
  - Σε ποιες και πόσες εφαρμογές τους χρησιμοποιεί;
  - …

Περίπτωση: «εύκολα» passwords που όμως δεν χρησιμοποιούνται συχνά, ξεχνιούνται !

Κωδικοί Πρόσβασης (Συνθηματικά) Από τη σκοπιά του χρήστη

- Υπάρχουν τρεις βασικές «έγνοιες» (Anderson, 2008)
  1. Θα αποκαλύψει ο χρήστης τον κωδικό σε κάποιον τρίτο;
     - Κατά λάθος, επίτηδες, ή ως αποτέλεσμα παραπλάνησης;
  2. Θα εισάγει ο χρήστης το σωστό κωδικό με μεγάλη πιθανότητα;
     - Σχετικό: θα εισάγει ο χρήστης το σωστό ζεύγος (user name / password);
  3. Θα θυμάται ο χρήστης τον κωδικό;
     - Αν ναι, μήπως είναι πολύ εύκολο; → ευπάθεια
     - Αν όχι, ο χρήστης θα το σημειώσει κάπου; → ευπάθεια

Η εντροπία ως μέτρο της αντοχής του κωδικού πρόσβασης

- Στους Η/Υ μετρούμε την αντοχή του password με βάση την εντροπία της πληροφορίας., με βάση τον αριθμό των bits
- Αντί να μετράμε τις απόπειρες πρόβλεψης που απαιτούνται μετράμε τον λογάριθμο με βάση-2 ενός δεδομένου αριθμού που αντιπροσωπεύει τον αριθμό των "bits εντροπίας» σε έναν κωδικό πρόσβασης.

Πόσο δυνατοί είναι οι κωδικοί που διαλέγουμε;

Passwords & Εντροπία (1/2)

n	26 lower-case letters	36 lower-case letters and digits	62 alpha-numeric characters	95 printable characters	all 128 ASCII characters
1	30 msec.	40 msec.	80 msec.	120 msec.	160 msec.
2	800 msec.	2 sec.	5 sec.	11 sec.	20 sec.
3	22 sec.	58 sec.	5 min.	17 min.	44 min.
4	10 min.	35 min.	5 hrs.	28 hrs.	93 hrs.
5	4 hrs.	21 hrs.	318 hrs.	112 days	500 days
6	107 hrs.	760 hrs.	2.2 yrs.	29 yrs.	174 yrs.

(Morris and Thompson, 1979)

Mixed Alpha and Numerals	0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz					
Password		Class of Attack				
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	3,844	Instant	Instant	Instant	Instant	Instant	Instant
3	238,328	23 Secs	< 3 Secs	Instant	Instant	Instant	Instant
4	15 Million	24½ Mins	2½ Mins	15 Secs	< 2 Secs	Instant	Instant
5	916 Million	1 Day	2½ Hours	15¼ Mins	1½ Mins	9 Secs	Instant
6	57 Billion	66 Days	6½ Days	16 Hours	1½ Hours	9½ Mins	56 Secs
7	3.5 Trillion	11 Years	1 Year	41 Days	4 Days	10 Hours	58 Mins
8	218 Trillion	692 Years	69¼ Years	7 Years	253 Days	25¼ Days	60½ Hours

Password Recovery Speeds, 2009 *

Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC, 2001 *

Πόσο δυνατοί είναι οι κωδικοί που διαλέγουμε;

Passwords & Εντροπία (2/2)

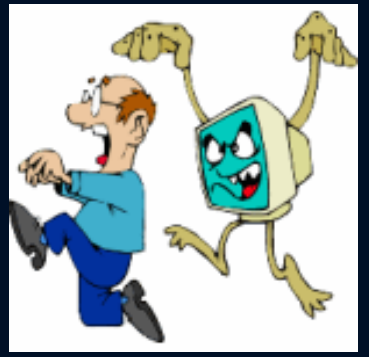
$\rightarrow c$ $\downarrow n$	26 (lowercase)	36 (lowercase alphanumeric)	62 (mixed case alphanumeric)	95 (keyboard characters)
5	23.5	25.9	29.8	32.9
6	28.2	31.0	35.7	39.4
7	32.9	36.2	41.7	46.0
8	37.6	41.4	47.6	52.6
9	42.3	46.5	53.6	59.1
10	47.0	51.7	59.5	65.7

Table 10.1: *Bitsize of password space for various character combinations. The number of n-character passwords, given c choices per character, is c^n. The table gives the base-2 logarithm of this number of possible passwords.*

… Ας μην βιαζόμαστε όμως: Η εντροπία είναι μέγιστη, όταν όλοι οι χαρακτήρες είναι ισοπίθανοι (=τυχαίοι). Σε διαφορετική περίπτωση, η ασφάλεια είναι μικρότερη. π.χ. Rate(English, lower case) = 1.5 bits/character (Shannon, 1957)

(..also see here, pp. 101-105, 413-414)

Κωδικοί Πρόσβασης (Συνθηματικά) Από τη σκοπιά του επιτιθέμενου



(Anderson, 2008)

1. Επίθεση σε έναν (συγκεκριμένο) λογαριασμό
   - Ποιο είναι το PIN για το λογαριασμό τραπέζης του χρήστη Α;
2. Επίθεση σε οποιοδήποτε λογαριασμό του συστήματος
   - Θέλω να συνδεθώ στο σύστημα ως οποιοσδήποτε χρήστης
3. Επίθεση σε οποιοδήποτε λογαριασμό οποιουδήποτε συστήματος
   - Θέλω να συνδεθώ σε οποιοδήποτε σύστημα ως οποιοσδήποτε χρήστης
4. Επίθεση άρνησης εξυπηρέτησης (DOS)
   - Θέλω να εμποδίσω το νόμιμο χρήστη να εισέλθει στο σύστημα