Ασφάλεια Πληροφοριακών Συστημάτων

«Έλεγχος Προσπέλασης και Ιδιωτικότητα»

Τμήμα Πληροφορικής

Λέκτορας Π.Κοτζανικολάου
Επ. Καθ. Δ. Πολέμη
pkotzani@unipi.gr , dpolemi@unipi.gr,

4η θεματική ενότητα

4. Έλεγχος προσπέλασης και προστασία ιδιωτικότητας

- **Αναγνώριση ταυτότητας - αυθεντικοποίηση**
- Μοντέλα ελέγχου πρόσβασης
- Τεχνικές προστασίας και διαχείρισης ιδιωτικότητας

Βασικοί όροι

- Ταυτοποίηση (Identification)
  - Η διαδικασία κατά την οποία ένα *υποκείμενο* παρέχει σε ένα σύστημα πληροφορίες ώστε να συσχετιστεί με μία αναγνωρίσιμη από το σύστημα οντότητα
    - (π.χ. Username)
- Αυθεντικοποίηση (Authentication)
  - Η διαδικασία κατά την οποία ένα υποκείμενο παρέχει σε ένα σύστημα πληροφορίες ώστε να αποδείξει ότι πράγματι είναι η οντότητα που ανέφερε κατά τη διαδικασία ταυτοποίησης για να αποκτήσει πρόσβαση σε ένα ή περισσότερα *αντικείμενα* του Π.Σ.
    - (π.χ. Password)
- Εξουσιοδότηση (Authorization)
  - Η διαδικασία κατά την οποία ένα ήδη αυθεντικοποιημένο υποκείμενο λαμβάνει συγκεκριμένα δικαιώματα πρόσβασης σε ένα ή περισσότερα αντικείμενα του Π.Σ.
    - (π.χ. Access Control List)
- Υποκείμενο του Π.Σ. (subject)
  - Χρήστης, διεργασία, δικτυακός κόμβος κτλ
- Αντικείμενο του Π.Σ. (object)
  - Υπολογιστής, αρχείο, φάκελος, μνήμη, εκτυπωτής κτλ.

Μέθοδοι αυθεντικοποίησης

1. Πληροφορία που γνωρίζω
   - Συνθηματικό (password, passphrase, PIN)
   - κρυπτογραφικό κλειδί
2. Πληροφορία που κατέχω
   - Κάρτα αναγνώρισης (Proximity / RFID)
   - Έξυπνη κάρτα
   - Ψηφιακό πιστοποιητικό
3. Πληροφορία που είμαι
   - Βιομετρικό χαρακτηριστικού (biometrics), π.χ.
     - Σχήμα προσώπου
     - Ίριδα ματιού
     - Δακτυλικό αποτύπωμα
     - Φωνή
     - Αναγνώριση τεχνικού χαρακτηριστικού του υλικού

1. Συνθηματικό (Password)

- Απλό στη χρήση
- Χαμηλό κόστος εφαρμογής
- Για την επιλογή των συνθηματικών πρέπει να ακολουθούνται *κανόνες πολυπλοκότητας*
  - Μήκος (>8 χαρακτήρες)
  - Χρήση κεφαλαίων – πεζών, αριθμών, συμβόλων
  - Να μην χρησιμοποιούνται κανονικές λέξεις που βρίσκονται σε λεξικό (ευάλωτο σε dictionary attack)
  - Αποφυγή λέξης που συνδέεται με το χρήστη (όνομα, διεύθυνση, τηλέφωνο κτλ)
  - Να έχει εύκολη απομνημόνευση (μόνο για τον κάτοχο)

Προβλήματα ασφάλειας συνθηματικών

- Αποκάλυψη κατά τη χρήση (*Trojans, οπτική επαφή* κτλ)
- Υποκλοπή κατά τη μεταφορά (*sniffers*)
- Υποκλοπή αποθηκευμένων password στο server (*server-side attacks*)
- Λανθασμένη επιλογή συνθηματικών (με μικρή πολυπλοκότητα)
- Χρήση για μεγάλο χρονικό διάστημα
- Ταυτόχρονη χρήση σε πολλά συστήματα / εφαρμογές
- Άλλες επιθέσεις:
  - Επιθέσεις λεξικού (*dictionary attack*)
  - Εξαντλητική επίθεση (*Brute-force attack*)

Μέτρα προστασίας συνθηματικών

- Μη αποκάλυψη σε κανένα τρίτο
- Τακτική αλλαγή
- Αλλαγή συνθηματικού αμέσως μετά από υποψία αποκάλυψης
- Επιλογή συνθηματικών με μεγάλη πολυπλοκότητα
- Αποθήκευση μόνο σε κρυπτογραφημένη (ή hashed) μορφή
- Αποφυγή αποστολής μέσω μη ασφαλών μέσων (π.χ. Email, απλό http κτλ)
- Προσοχή κατά την πληκτρολόγηση

Παραδείγματα «κακών» συνθηματικών

- “james8" - Based on the user’s name, it is too short also
- “samatha" - The name of the user’s girlfriend; easy to guess
- “harpo" - The user’s name (Oprah) backwards
- “superstitious" - Listed in a dictionary
- " sUperStiTIous " - Just adding random capitalization does not make it safe
- “kadhal - Listed in a Tamil foreign language dictionary
- “obiwan" - Listed in word lists
- “spicer" - Listed in a geological dictionary
- "qwertyuiop" - Listed in word lists

Παραδείγματα «καλών» συνθηματικών

The "Mary Had A Little Lamb" Formula

Consider a phrase: "*Mary had a little lamb. The lamb had white fleece.*"

Consider the first letter of each word, i.e.: MHALLTLHWF

Every second letter of the abbreviation can be put in the lower case, i.e. MhAlLtLhWf

Replace "A" with "@" and "L" with "!". Thus, a new alphanumeric password with more than eight characters will be formed

New Password: **Mh@l!t!hWf**

Διαγραφή αποθηκευμένων συνθηματικών

1. Start → run → cmd
   - ***rundll32.exe keymgr.dll,KRShowKeyMgr***
   - Εμφανίζονται τα αποθηκευμένα συνθηματικά
2. Select → *κάποια εγγραφή* → Properties
   - Εμφανίζεται υπάρχουσα πληροφορία
3. Select → *κάποια εγγραφή* → Select Remove
   - Διαγραφή

Password crackers

- Λογισμικό το οποίο μπορεί
  - να αποκρυπτογραφήσει αποθηκευμένα συνθηματικά ή
  - να απενεργοποιήσει εντελώς την αυθεντικοποίηση.
- Brute force ή dictionary attack
- Ο στόχος του επιτιθέμενου είναι συνήθως να αποκτήσει root/admin password
- Π.χ για να αλλάξει δικαιώματα αρχείων, να εγκαταστήσει «Δούρειους Ίππους» για μελλοντική πρόσβαση κτλ
- Μπορεί όμως να ξεκινήσει με ένα password απλού χρήστη και στη συνέχεια να προσπαθήσει να κάνει *αύξηση των δικαιωμάτων του* (*privilege escalation*)

Μέθοδος cracking

- Σπάσιμο αρχείου συνθηματικών σε πολλά μικρότερα αρχεία
- Δοκιμή αποκρυπτογράφησης κάθε τμήματος χωριστά
- Για κάθε πιθανή αποκρυπτογράφηση, δοκιμή επανακρυπτογράφησης (hashing) και σύγκριση με το κρυπτογραφημένο αρχείο
- Όσα συνθηματικά «έσπασαν» συγκεντρώνονται σε ένα αρχείο

Εργαλεία cracking

- Cain & Abel
- John the Ripper
- LC4
- Hydra
- RAR
- …
- Automated Random Password Generator
- Rainbow Tables Genratator

Εργαλεία Προστασίας

- Password Administrator
  - Password account manager
  - Κρυπτογραφεί τα password σε βάση
- Password Safe
  - Άλλος ένας password manager (TwoFish κρυπτογράφηση)
- My Password Manager
- webPassword
  - Προστασία ιστοσελίδων με password
  - Χρησιμοποιεί ισχυρή κρυπτογραφία
- Easy Web Password
  - Προστασία ιστοσελίδων με password

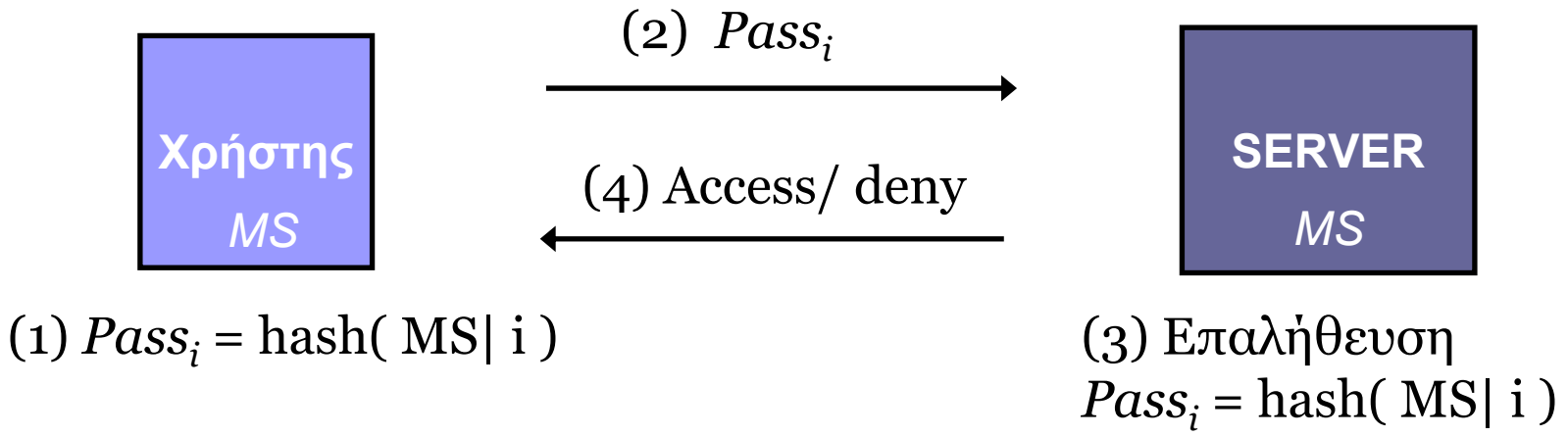
Προστασία συνθηματικών στο UNIX

Bobbie, 4238, e(Dog, 4238)
Tony, 2918, e(6%%TaeFF, 2918)
Laura, 6902, e(Shakespeare, 6902)
Mark, 1694, e(XaB#Bwcz, 1694)
Deborah, 1092, e(LordByron,1092)

Χρήση «αλατιού» (salt) για την αντιμετώπιση επιθέσεων προ-υπολογισμού κρυπτογραφημένων συνθηματικών (precomputation of encrypted passwords).

2. Συνθηματικό μίας χρήσης (One-time password)

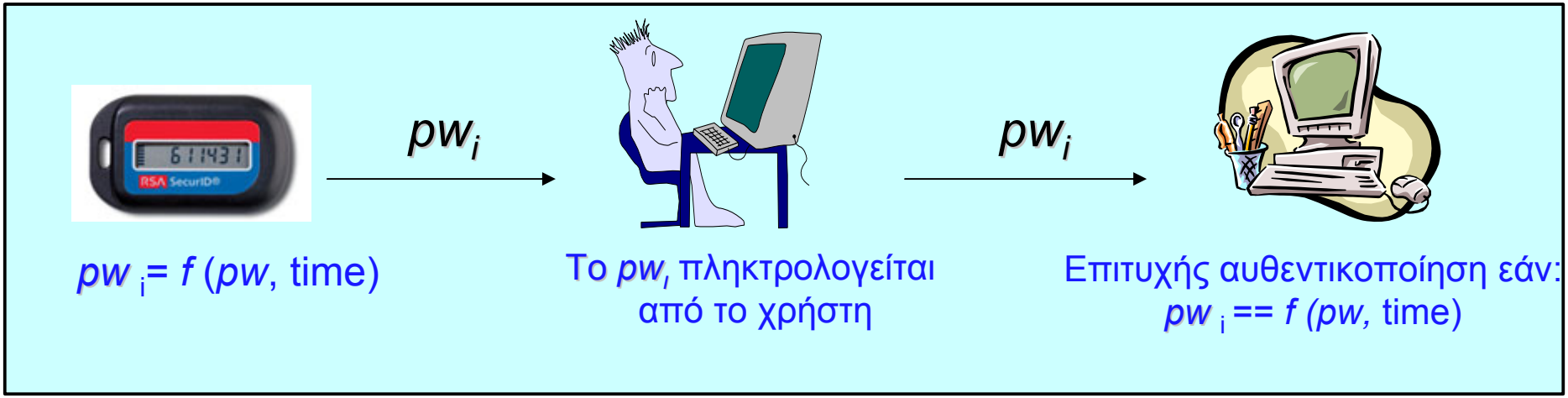
- Ο χρήστης και ο εξυπηρετητής μοιράζονται ένα Master Secret (MS)
- Σε κάθε πρόσβαση, το Master Secret χρησιμοποιείται ώστε να δημιουργηθεί ένα συνθηματικό μίας χρήσης, μαζί με κάποια άλλη πληροφορία



2. Συνθηματικό μίας χρήσης

Παράδειγμα: Χρήση συσκευής με συγχρονισμό

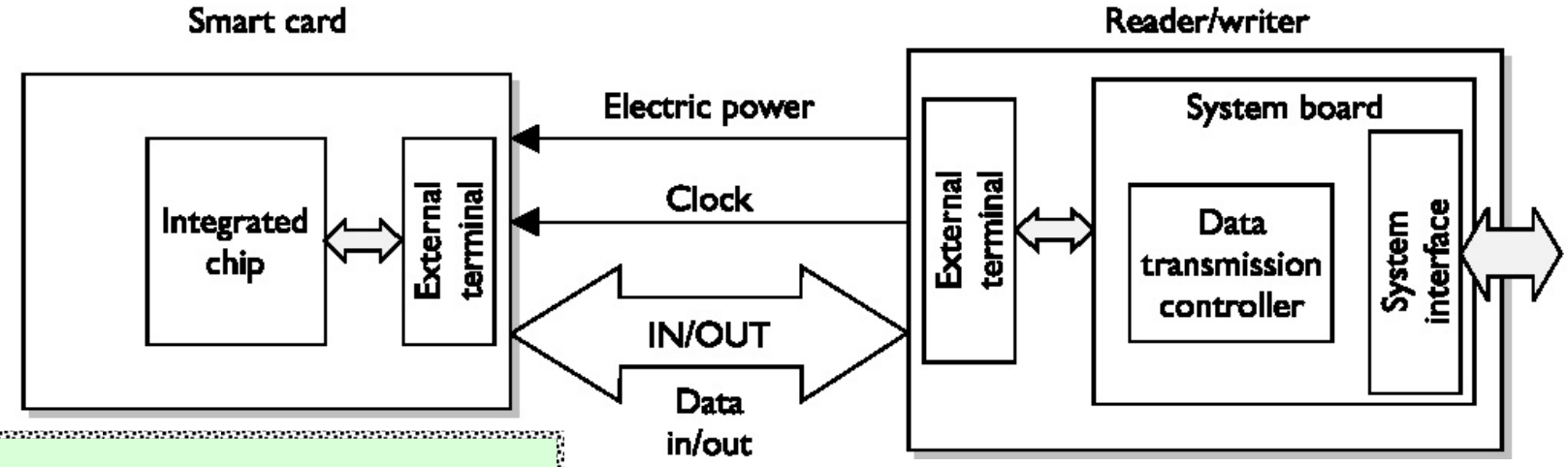
- Χρήση συσκευής (security token) με ενσωματωμένο master-password (*pw*) και *ρολόι*.
- Ο χρήστης χρησιμοποιεί το token με το ενσωματωμένο *pw*
- Το *pw* + *η ώρα περνά από μία hash συνάρτηση*
- Ο server υπολογίζει ανεξάρτητα το ίδιο
- Παράδειγμα: RSA SecureID
  - Πλεονεκτήματα: Πολύ ασφαλέστερο από απλό password
  - Μειονεκτήματα: Συγχρονισμός



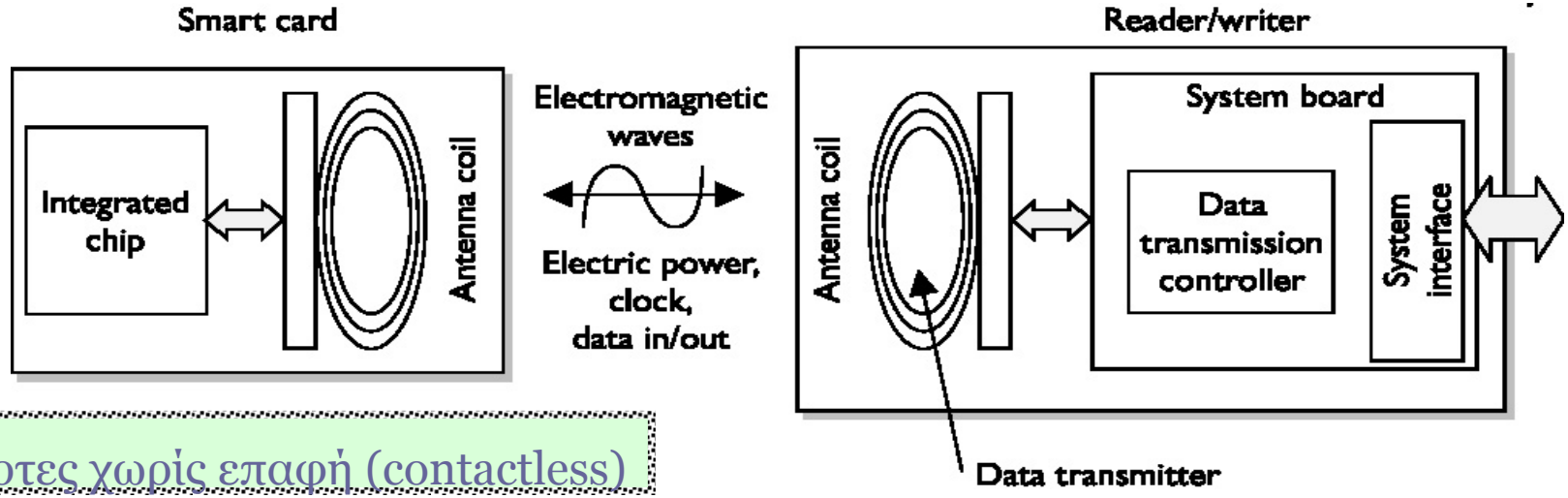
2. Συνθηματικό μίας χρήσης

Παράδειγμα: Πρόκληση/απάντηση (challenge/response)

3. Έξυπνες Κάρτες (Smartcards)



Κάρτες με επαφή (contact)



Κάρτες χωρίς επαφή (contactless)

4. Βιομετρικά χαρακτηριστικά

- Συλλογή κάποιου *«μοναδικού» βιομετρικού χαρακτηριστικού*
  - Δακτυλικό αποτύπωμα,
  - Ίριδα, αμφιβληστροειδής ματιού,
  - Χροιά φωνής,
  - Σχήμα προσώπου κτλ
- Δημιουργία *«αποτυπώματος» (fingerprint)* και αποθήκευση σε μία βάση
- Σε κάθε προσπάθεια αυθεντικοποίησης ενός χρήστη:
  - Δημιουργείται και πάλι σε πραγματικό χρόνο το αποτύπωμα του χρήστη,
  - Ελέγχεται με το αποθηκευμένο αποτύπωμα.

Προβλήματα βιομετρικών χαρακτηριστικών

- *Ιδιωτικότητα χρηστών*: Συλλογή προσωπικών δεδομένων για μεγάλο αριθμό χρηστών
  - Πιθανώς χωρίς τη συγκατάθεσή τους
- *False Acceptance Rate*
  - Υπάρχει πιθανότητα να αυθεντικοποιηθεί (να γίνει αποδεκτή η πρόσβαση) από λάθος χρήστη.
- *False Rejection Rate*
  - Υπάρχει πιθανότητα να μην αυθεντικοποιηθεί (να μην γίνει αποδεκτή η πρόσβαση) από τον πραγματικό χρήστη.

Συστήματα Ενιαίας Πρόσβασης (Single Sign On)

- Οι χρήστες διαχειρίζονται πολλά διαφορετικά password για διαφορετικές εφαρμογές
- Ανάγκη απομνημόνευσης πολλών συνθηματικών
- Χρήση ίδιου συνθηματικού σε διαφορετικές εφαρμογές
- Τα *Single Sign-On (SSO)* συστήματα διαχειρίζονται όλα τα συνθηματικά που ανήκουν σε ένα χρήστη
- Προστατεύουν τα συνθηματικά με κρυπτογράφηση
- Απαιτείται προσοχή για την ασφάλεια του SSO συστήματος

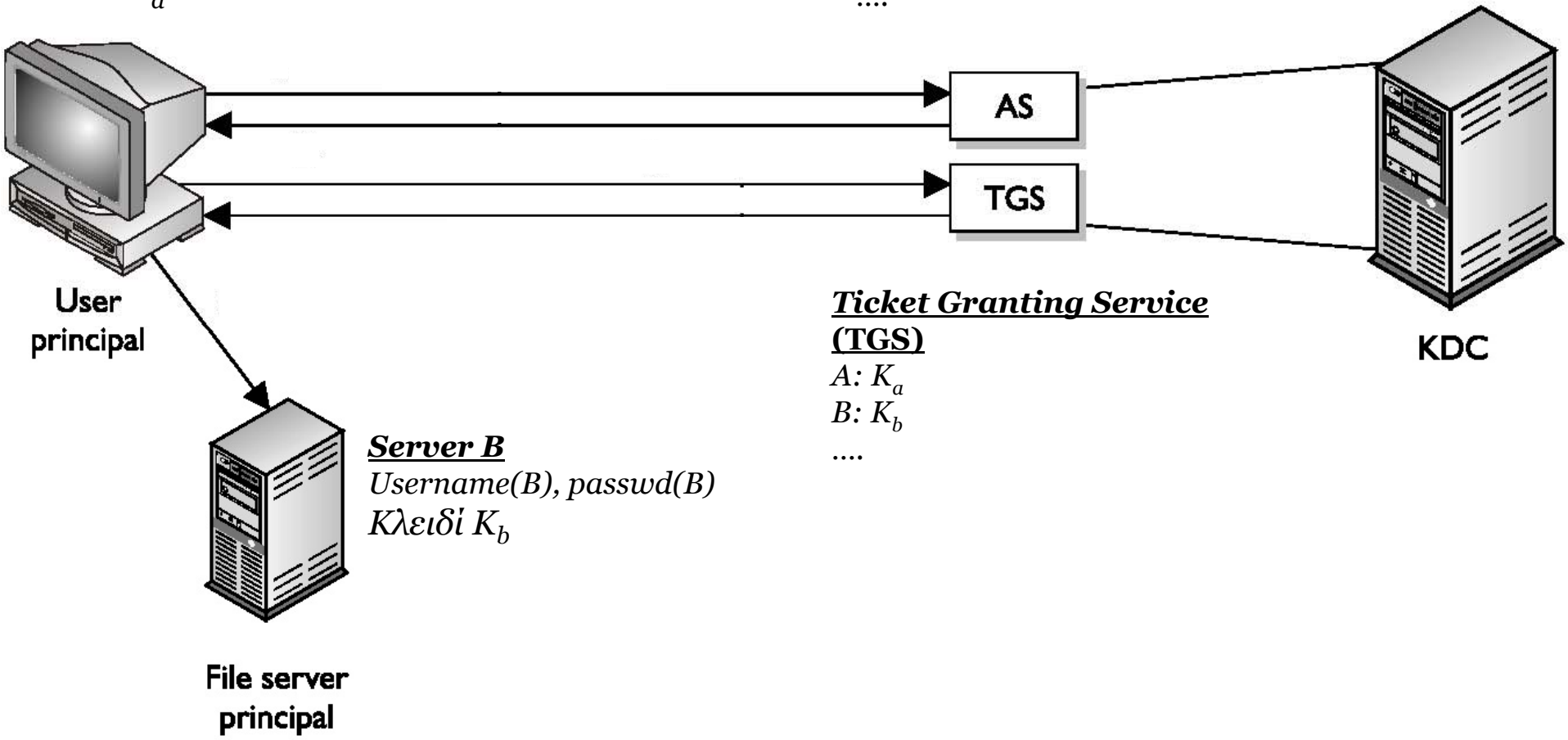
Σύστημα Kerberos

- Βασίζεται σε *Κέντρο Διανομής Κλειδιών –ΚΔΚ (Key Distribution Center – KDC)* και συμμετρική κρυπτογράφηση
- Προσφέρει υπηρεσίες αυθεντικοποίησης, κρυπτογράφησης και ελέγχου πρόσβασης
- Βασική λειτουργία:
  - Κάθε υποκείμενο (π.χ. χρήστης) ή αντικείμενο (π.χ. server) του Π.Σ. αυθεντικοποιείται στην υπηρεσία Authentication Service (AS) του Kerberos.
  - Εάν ο χρήστης Α θέλει να μιλήσει στον server (ή χρήστη) Β, επικοινωνεί με την υπηρεσία Ticket Granting Service (TGS) του Kerberos.
  - Η TGS ελέγχει τα δικαιώματα πρόσβασης του χρήστη Α στον server Β και εκδίδει ένα εισιτήριο με ένα κοινό κλειδί επικοινωνίας για τους Α και Β (K_{ab})

Σύστημα Kerberos

Χρήστης Α
username(A), passwd(A)
Κλειδί K_a

***Authentication Server* (AS)**
A: username, passwd
B: username, passwd
....



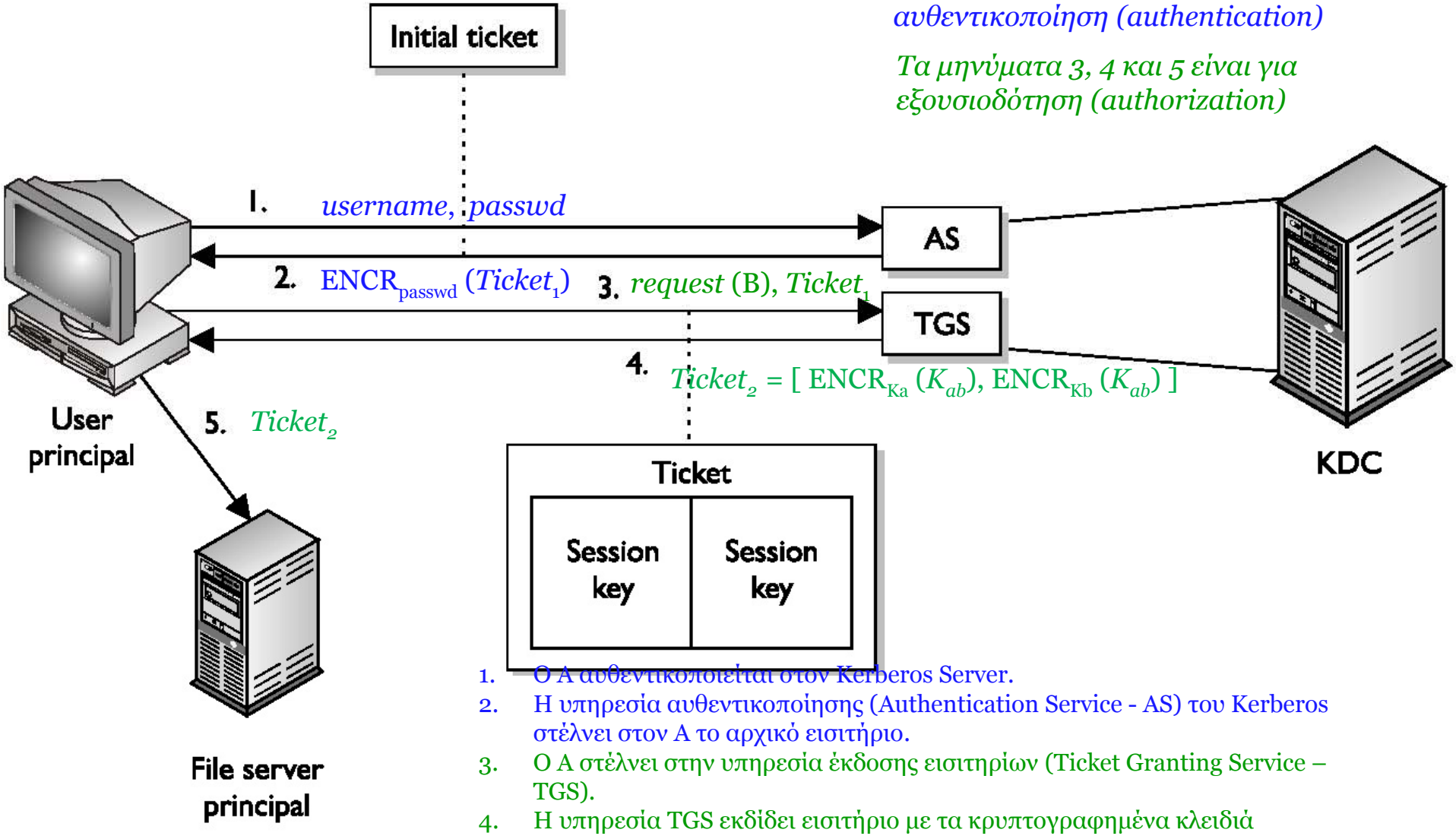
***Ticket Granting Service* (TGS)**
A: K_a
B: K_b
....

Server B
Username(B), passwd(B)
Κλειδί K_b

Σύστημα Kerberos

Τα μηνύματα 1 και 2 είναι για αυθεντικοποίηση (authentication)

Τα μηνύματα 3, 4 και 5 είναι για εξουσιοδότηση (authorization)



1. Ο Α αυθεντικοποιείται στον Kerberos Server.
2. Η υπηρεσία αυθεντικοποίησης (Authentication Service - AS) του Kerberos στέλνει στον Α το αρχικό εισιτήριο.
3. Ο Α στέλνει στην υπηρεσία έκδοσης εισιτηρίων (Ticket Granting Service – TGS).
4. Η υπηρεσία TGS εκδίδει εισιτήριο με τα κρυπτογραφημένα κλειδιά πρόσβασης.
5. Ο Α εξάγει το κλειδί K_{ab} και στέλνει στο Β τιψκετ για να εξάγει και αυτός το K_{ab}

4η θεματική ενότητα

4. Έλεγχος προσπέλασης και προστασία ιδιωτικότητας

- Αναγνώριση ταυτότητας - αυθεντικοποίηση
- **Μοντέλα ελέγχου πρόσβασης**
- Τεχνικές προστασίας και διαχείρισης ιδιωτικότητας

Εξουσιοδότηση (Authorization)

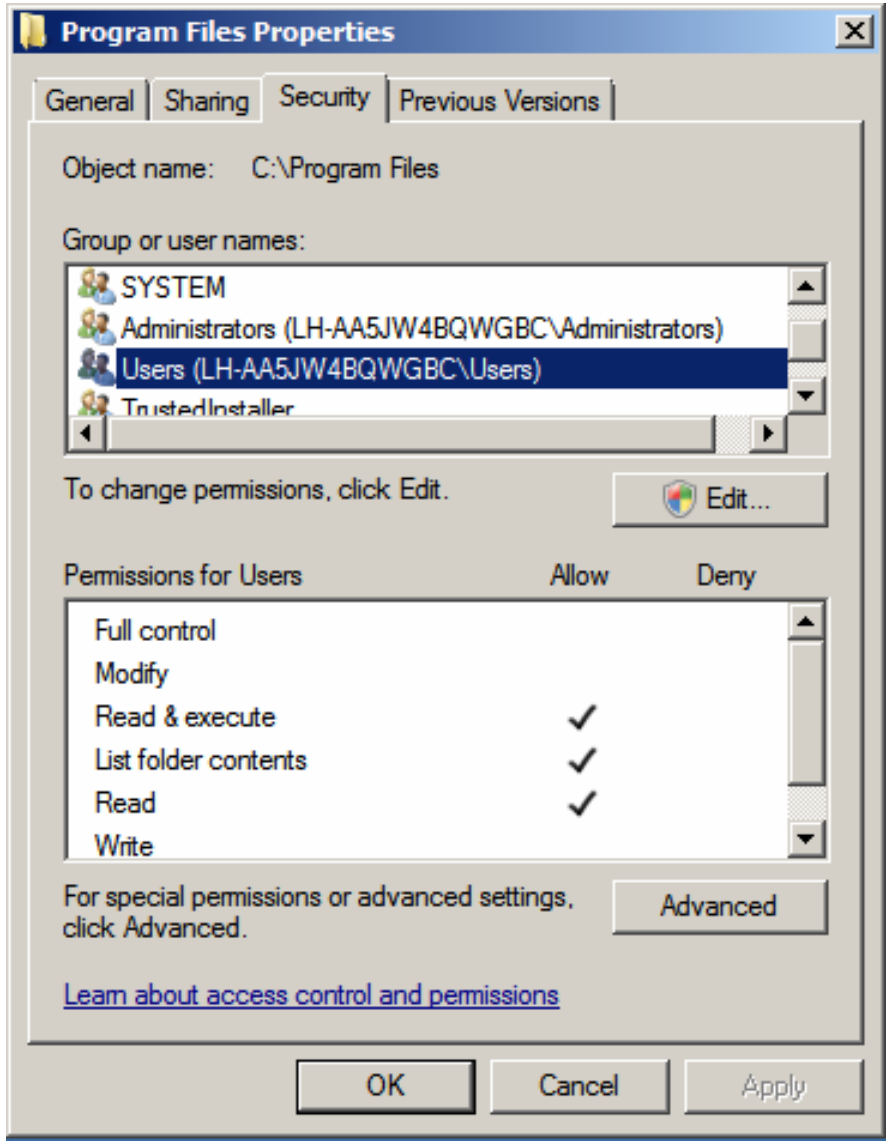
1. Κριτήρια Πρόσβασης (Access Criteria)
2. Δικαιώματα Πρόσβασης (Access Permissions)

Έλεγχος Πρόσβασης
Μοντέλα Ελέγχου Πρόσβασης

1. Διακριτός Έλεγχος Πρόσβασης (Discretionary Access Control – DAC)
2. Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control – MAC)
3. Έλεγχος Πρόσβασης Βασισμένος σε Ρόλους (Role Based Access Control – RBAC)

Έλεγχος Πρόσβασης
Μοντέλα DAC

- Ο χρήστης είναι ο ιδιοκτήτης των αντικειμένων (αρχείων) που δημιουργεί.
- Ο ιδιοκτήτης επιτρέπει ή απαγορεύει την πρόσβαση στο αντικείμενο, βάσει της ταυτότητας κάθε υποκειμένου:
  1. Όνομα του υποκειμένου
  2. Ομάδα στην οποία ανήκει
- Οι εφαρμογές και οι διεργασίες εκτελούνται με τα δικαιώματα του χρήστη



http://www.developer.com/img/2007/09/Basics1.png

Έλεγχος Πρόσβασης
Μοντέλα MAC

- Κάθε υποκείμενο ανήκει σε μία *κατηγορία ασφάλειας (security class)*.
- Κάθε αντικείμενο έχει μία *ετικέτα ασφάλειας (security label)*.
- Για να έχει πρόσβαση ένα υποκείμενο (χρήστης) σε ένα αντικείμενο (π.χ. αρχείο) πρέπει να έχει *το ίδιο ή μεγαλύτερο επίπεδο ασφάλειας* από την ετικέτα του αντικειμένου.
- Στηρίζεται στην αρχή *της αναγκαίας γνώσης* (Need to know principle) και στην αρχή των *ελάχιστων προνομίων* (least privilage principle).

Έλεγχος Πρόσβασης
Μοντέλα MAC

Ετικέτες ασφάλειας (Security labels)

Επίπεδο Ασφάλειας (Security Level)	Υποκείμενο (Subject)	Αντικείμενο (Object)
Top Secret	George	Personnel files
Secret	Joan	E-mail
Confidential	Henry	Application logs
Unclassified	Mark	System manuals

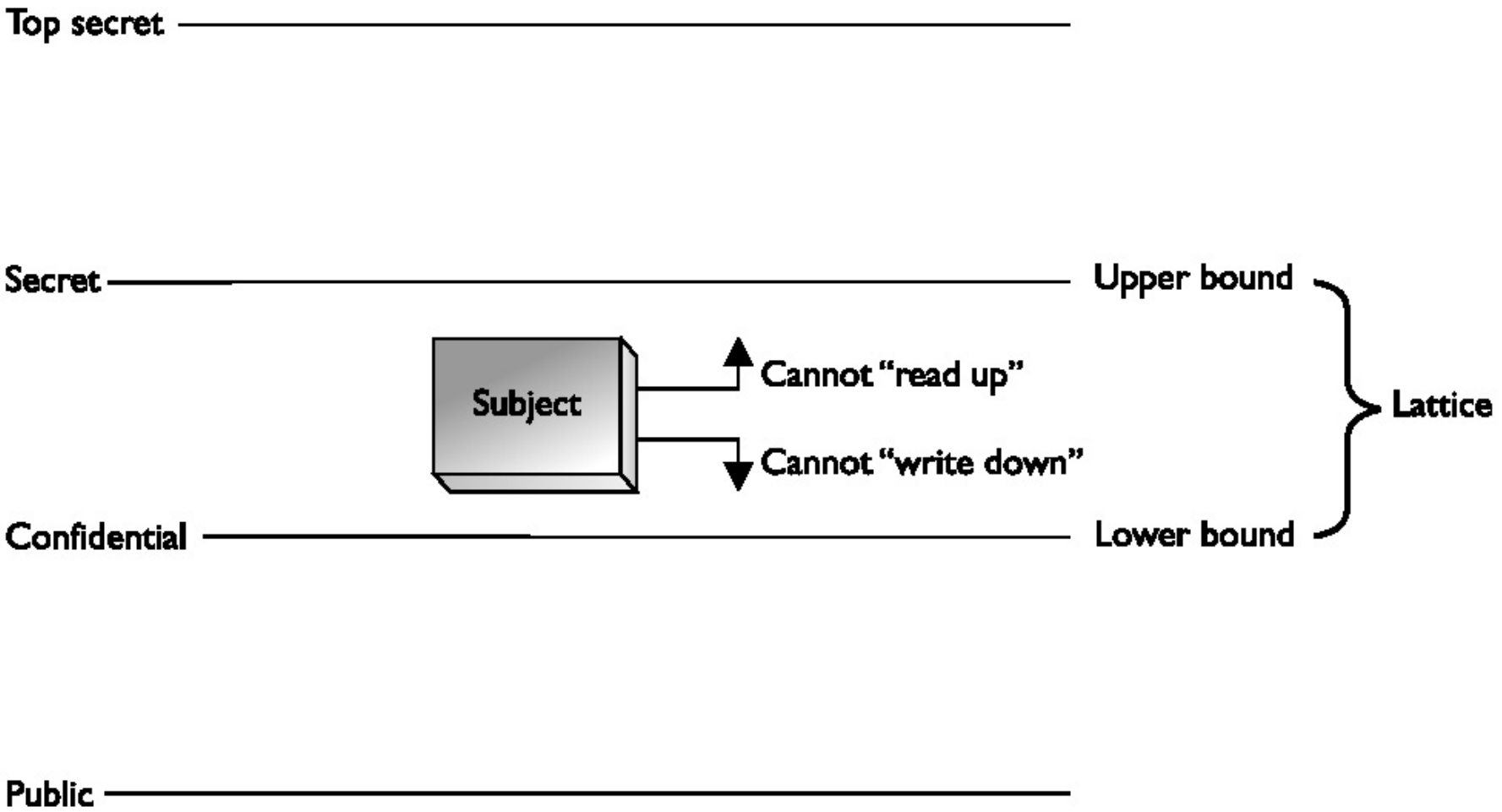
- Ο George μπορεί να διαβάσει όλα τα αρχεία/έγγραφα
- Η Joan δεν μπορεί να διαβάσει τα αρχεία προσωπικού
- Ο Henry μπορεί να διαβάσει μόνον τα logs & manuals
- ...

Μοντέλα MAC

(Α) Το μοντέλο Bell-LaPadula (1/3)

- Προσανατολισμένο στην εμπιστευτικότητα.
- Κανόνες του μοντέλου Bell-La Padula:
  - ***Η απλή ιδιότητα της ασφάλειας***: Μία διεργασία που εκτελείται στο επίπεδο ασφάλειας *k* μπορεί να διαβάσει αντικείμενα που βρίσκονται σε επίπεδο χαμηλότερο ή ίσο του *k* (no read up).
  - **Η ιδιότητα *** : Μία διεργασία που εκτελείται στο επίπεδο ασφάλειας *k* μπορεί να γράψει αντικείμενα στο ίδιο ή σε υψηλότερο επίπεδο (no write down).

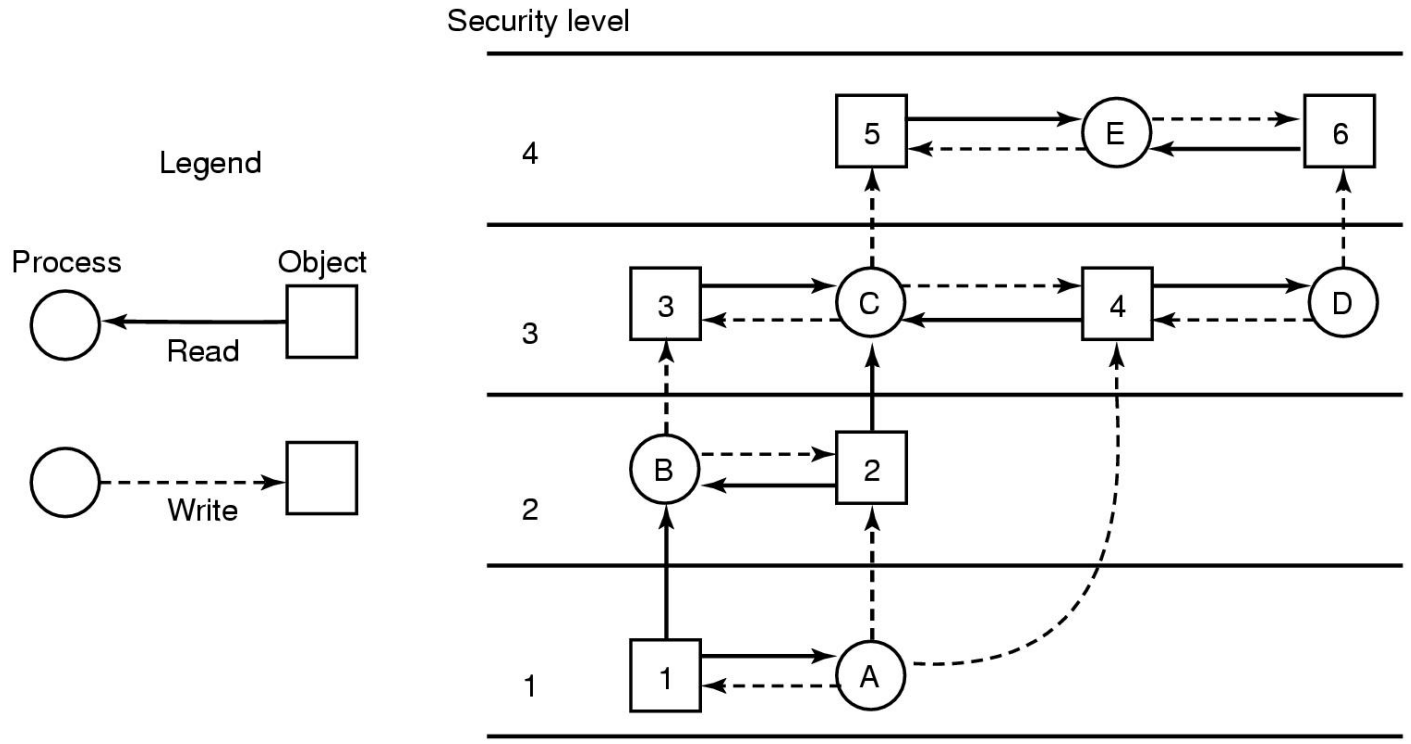
Μοντέλα MAC
(Α) Το μοντέλο Bell-LaPadula (2/3)



Μοντέλο Bell-LaPadula (Εμπιστευτικότητα)

Μοντέλα MAC

(A) Το μοντέλο Bell-LaPadula (3/3)



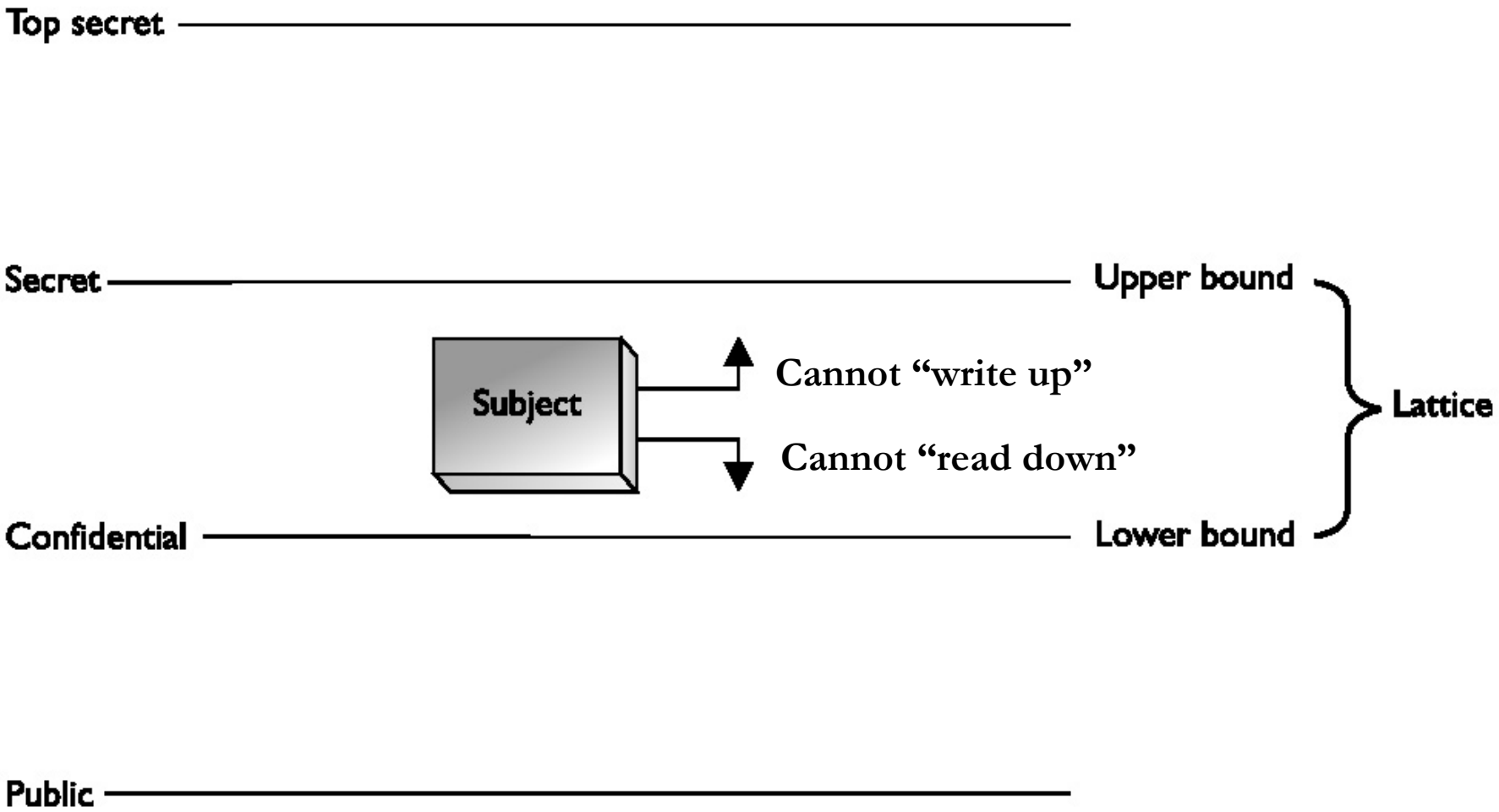
Το μοντέλο ασφάλειας Bell-La Padula με πολλά επίπεδα

Μοντέλα MAC

(Β) Το μοντέλο Biba (1/2)

- Προσανατολισμένο στην ακεραιότητα.
- Κανόνες του μοντέλου Biba :
  - ***Η απλή ιδιότητα της ακεραιότητας***: Μία διεργασία που εκτελείται στο επίπεδο ασφάλειας *k* μπορεί να γράψει αντικείμενα που βρίσκονται σε επίπεδο χαμηλότερο ή ίσο του *k* (no write up).
  - ***Ή ιδιότητα ακεραιότητας*** *: Μία διεργασία που εκτελείται σε επίπεδο ασφάλειας *k* μπορεί να διαβάσει αντικείμενα που βρίσκοται σε επίπεδο ίσο ή μεγαλύτερο του *k* (no read down).

Μοντέλα MAC
(Β) Το μοντέλο Biba (2/2)



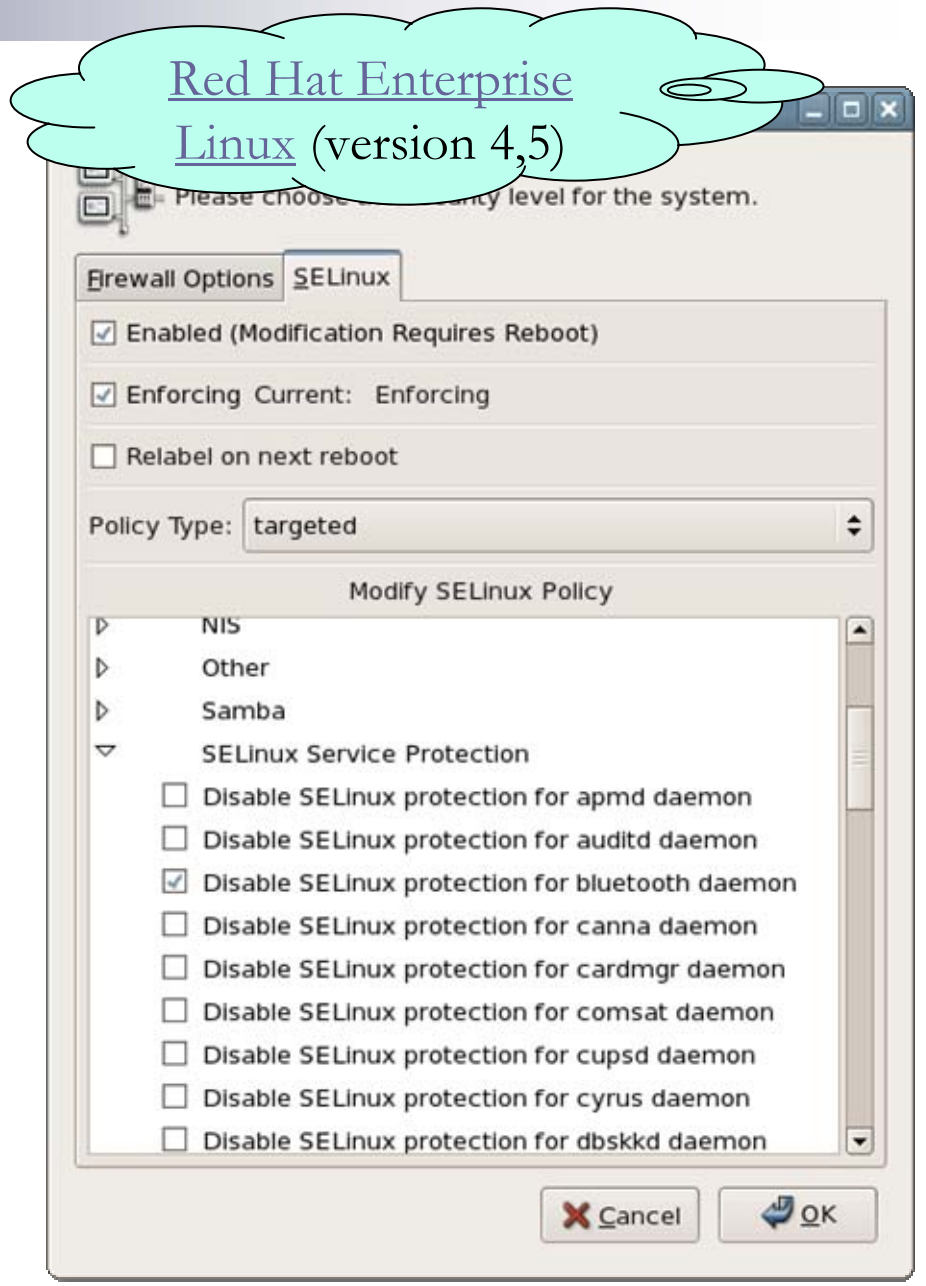
Μοντέλο Biba (Ακεραιότητα)

Χαρακτηριστικά παραδείγματα εφαρμογής των μοντέλων Bell-Labadula και Biba

- Bell-Lapadula
  - Σε υψηλό επίπεδο (High): ένα αρχείο καταγραφής (Log file)
    - *Μπορούν να γράψουν σε αυτό όλες οι διεργασίες συστήματος.*
  - Σε χαμηλό επίπεδο (Low): μία διεργασία συστήματος (System Process)
    - *Δεν μπορεί να αλλοιωθεί από διεργασίες χρηστών.*
- Biba
  - Σε υψηλό επίπεδο (High): Αρχεία συστήματος (System Files)
    - *Δεν μπορεί να αλλοιωθεί από διεργασίες χρηστών.*
  - Σε χαμηλό επίπεδο (Low): Αντίγραφο ασφαλείας (System backup)
    - *Μπορούν να γράψουν σε αυτό όλοι.*

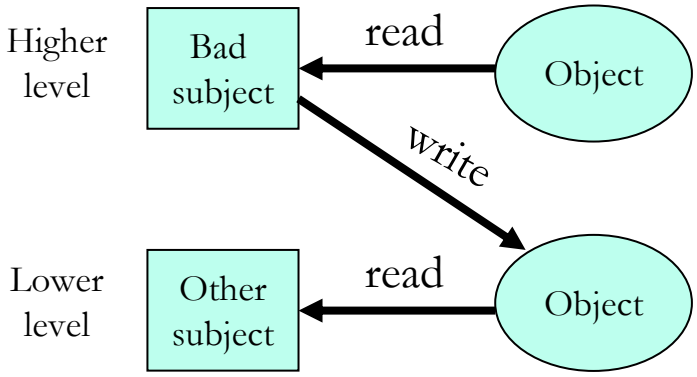
Έλεγχος Πρόσβασης
Biba - Επεκτάσεις

- Αρχή "Low Water Mark"
  - Περίπτωση: LOMAC, 2000
- Το σύστημα υποστηρίζει δύο επίπεδα ασφάλειας
  - High Integrity (π.χ. System files)
  - Low Integrity (π.χ. Network)
- Όταν ένα πρόγραμμα επιπέδου High δέχεται input από το δίκτυο, αυτομάτως υποβιβάζεται στο επίπεδο Low



Έλεγχος Πρόσβασης
Ροές πληροφορίας

- Μοντέλα MAC
  - θέτουν το πλαίσιο για την ανάπτυξη πολιτικών για την ασφαλή ροή πληροφορίας μεταξύ οντοτήτων με διαφορετικά επίπεδα εμπιστοσύνης



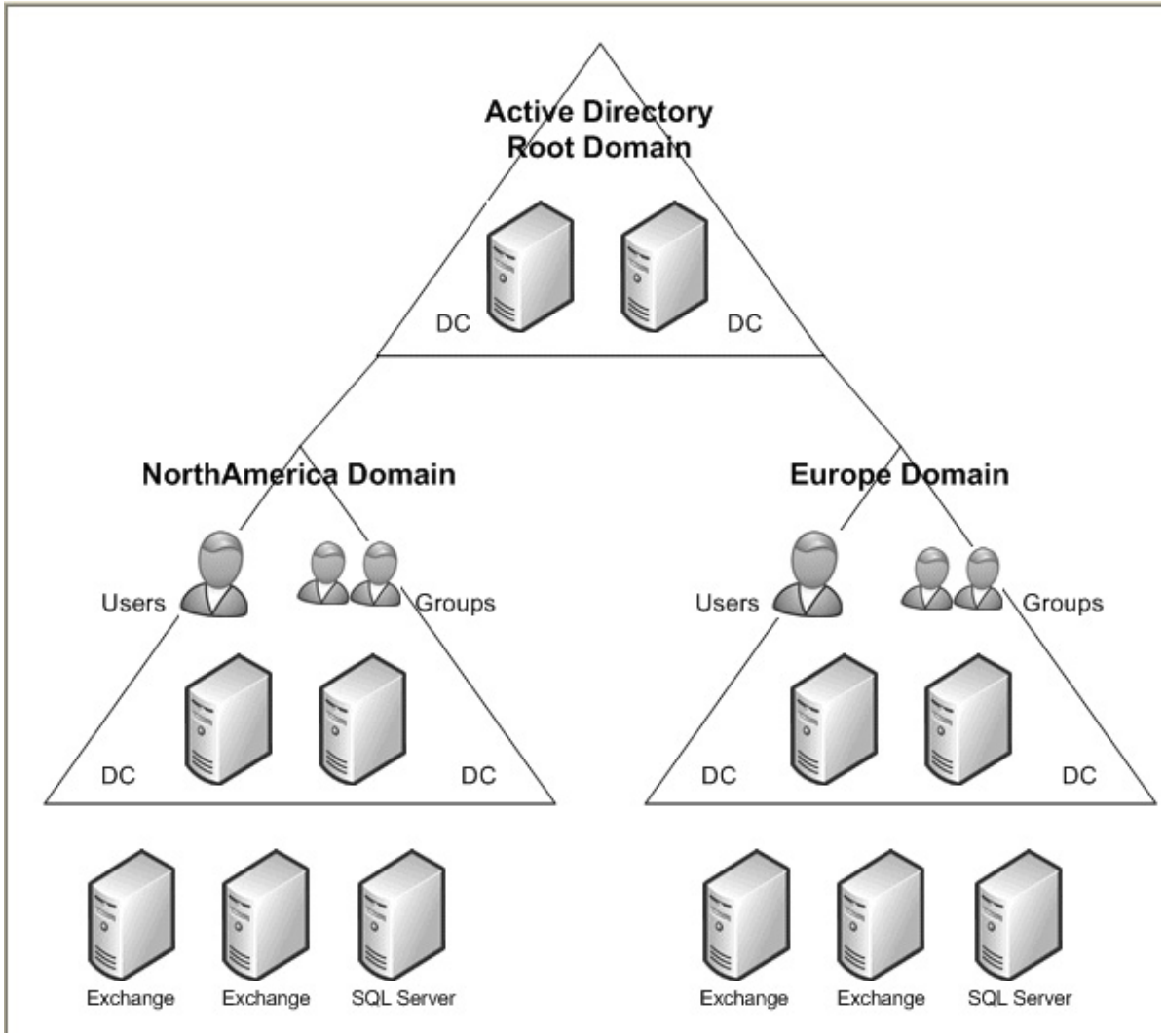
- Ροή πληροφορίας σε ένα σύστημα υπάρχει όταν υποκείμενα αποκτούν πρόσβαση σε αντικείμενα
  - π.χ. Χρήστες προς αρχεία
  - Διεργασίες προς μνήμη
  - Μνήμη προς μνήμη
  - Καταχωρητής προς καταχωρητή
  - ...
- Το μοντέλο Bell-LaPadula δίνει έμφαση στην εμπιστευτικότητα, ενώ το Biba στην Ακεραιότητα

Έλεγχος Πρόσβασης
Μοντέλα RBAC

- Η έννοια του ρόλου
  - *Ρόλος (role)*: Αρμοδιοτήτες & δικαιώματα
  - Δικαιώματα πρόσβασης (access privileges): Τα δικαιώματα εκχωρούνται σε ρόλους
    - Ένας χρήστης μπορεί να λάβει ένα ρόλο για κάποιο χρονικό διάστημα
    - Για το διάστημα αυτό λαμβάνει τα δικαιώματα του ρόλου του
  - Ιδανική στρατηγική για μεγάλες επιχειρήσεις, με προσωπικό που αλλάζει (απολύσεις, μεταθέσεις, αλλαγή ρόλων)
  - Αν ο Διαχειριστής Χ παραιτηθεί, τότε ο αντικαταστάτης του Υ, μπορεί να αντιστοιχηθεί στο ρόλο «Διαχειριστής»
    - Στο μοντέλο DAC ίσως θα έπρεπε να αλλάξουν οι λίστες πρόσβασης στα αντικείμενα)

Τομείς Ασφάλειας (Security Domains)

- Μεγάλα συστήματα, συχνά οργανώνονται ιεραρχικά:
  1. Δένδρο
     - Πολλοί Τομείς, με το ίδιο namespace
  1. Δάσος (Forrest)
     - Πολλά δένδρα, με διαφορετικά namespaces



http://technet.microsoft.com/

Τεχνικές ελέγχου πρόσβασης

- Πίνακες Ελέγχου Πρόσβασης (Access Control Matrix)
- Δυνατότητες (Capabilities)
- Λίστες Ελέγχου Πρόσβασης (Access Control Lists)
- Κατάλογος (Directory)
- Δακτύλιοι

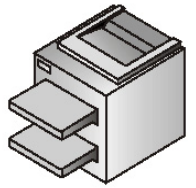
Πίνακας Ελέγχου Πρόσβασης (Access Control Matrix)

User	File1	File2	File3
Diane	Read and execute	Read, write, and execute	No access
Katie	Read and execute	Read	No access
Chrissy	Read, write, and execute	Read and execute	Read
John	Read and execute	No access	Read and write

- Οι πίνακες αυτοί συνήθως είναι αραιοί και χάνουν σε απόδοση για μεγάλο αριθμό χρηστών.
- Για μεγαλύτερη ευελιξία, ο καθορισμός των δικαιωμάτων πρόσβασης μπορεί να είναι προσανατολισμένος:
  - Στα υποκείμενα (**Λίστα Δυνατοτήτων**)
  - Στα αντικείμενα (**Λίστα Ελέγχου Πρόσβασης**)

Λίστα ελέγχου πρόσβασης
Access Control List (1/2)

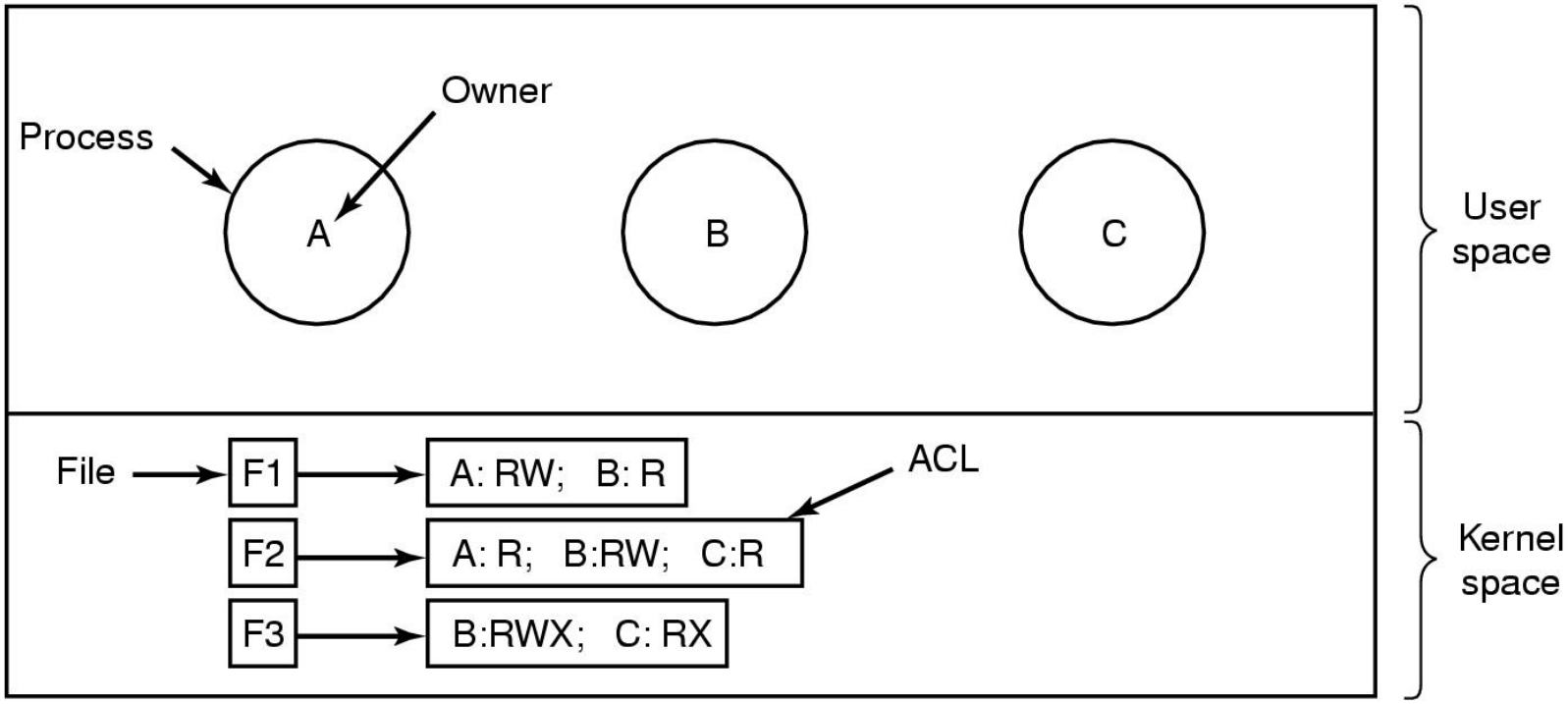
- Αποτελεί θεώρηση ενός Πίνακα Ελέγχου Πρόσβασης **ανά στήλες**
- Για κάθε αντικείμενο υπάρχει μία λίστα όλων των υποκειμένων και τα δικαιώματά τους σε αυτό.
- Δικαιώματα read-r, write-w, execute-x
- Λύνονται τα προβλήματα του ευρετηρίου
- Δύσκολη η αναίρεση των δικαιωμάτων ενός υποκειμένου
  - *Απαιτείται αναζήτηση σε όλες τις λίστες των αντικειμένων*



Access Control List

Tom Harris—Print
Joni Swenson—Full control
Maynard Harris—No access
Evelyn Seaton—Print
Iqqi Hammond—Full control
David Arnold—Print

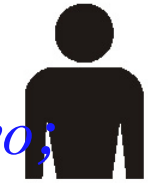
Λίστα ελέγχου πρόσβασης
Access Control List (2/2)



Χρήση ACL για τον έλεγχο πρόσβασης σε αρχεία.

Δυνατότητες (Capabilities) (1/4)

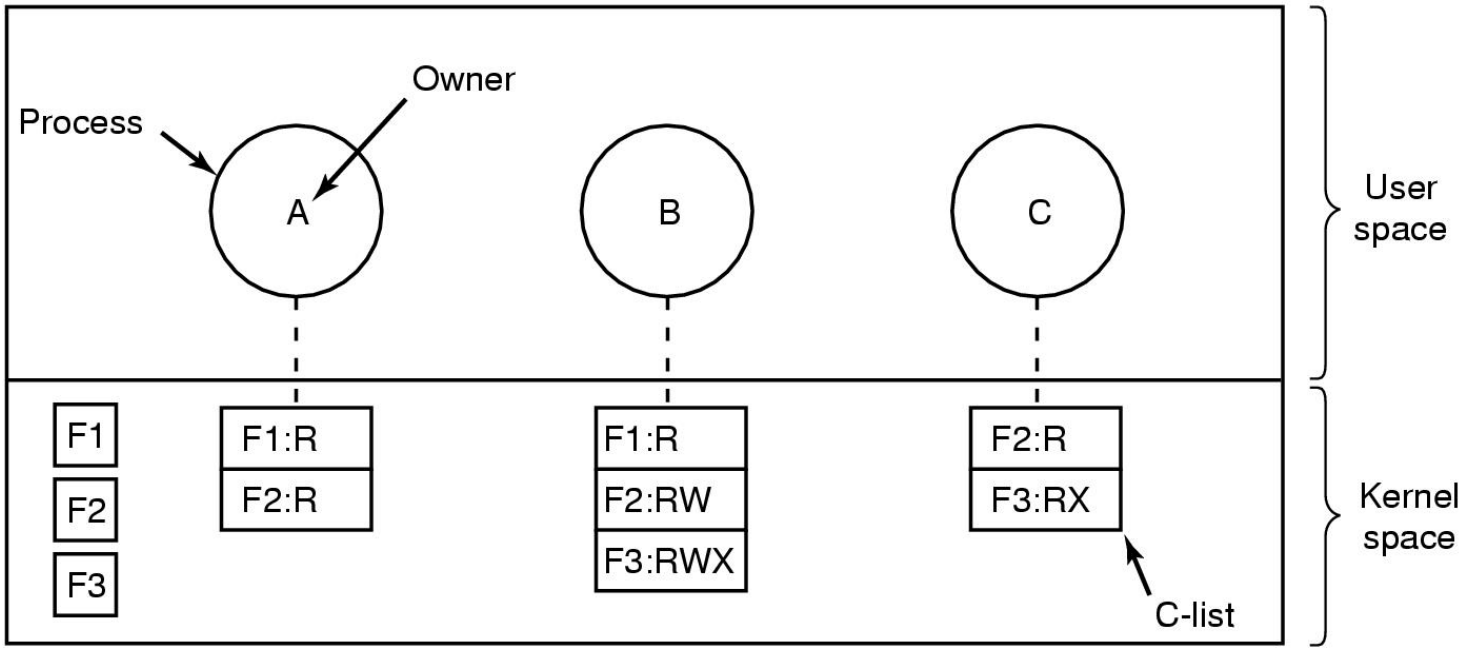
- Ουσιαστικά αποτελεί θεώρηση ενός Πίνακα Ελέγχου Πρόσβασης **ανά γραμμές**
- Ποια δικαιώματα έχει ένα υποκείμενο επάνω σε ποια αντικείμενα;
- Υπάρχει το δικαίωμα μεταβίβασης της δυνατότητας
- Προβλήματα
  - *Ποια υποκείμενα έχουν πρόσβαση σε ένα αντικείμενο;*
  - *Πως ανακαλείται η δυνατότητα;*



Capability Table

Plotter—Print
Printer1—Print
Printer2—No access
Accountng.xls—Full control
Accounting.doc—Read, write
Payroll.xls—No access
Clipart—Full control

Δυνατότητες (Capabilities) (2/4)



Κάθε διεργασία έχει μία λίστα δυνατοτήτων (capacity list).

Δυνατότητες (Capabilities) (3/4)

Server	Object	Rights	f(Objects,Rights,Check)

Κρυπτογραφική προστασία των δυνατοτήτων.

Δυνατότητες (Capabilities) (4/4)

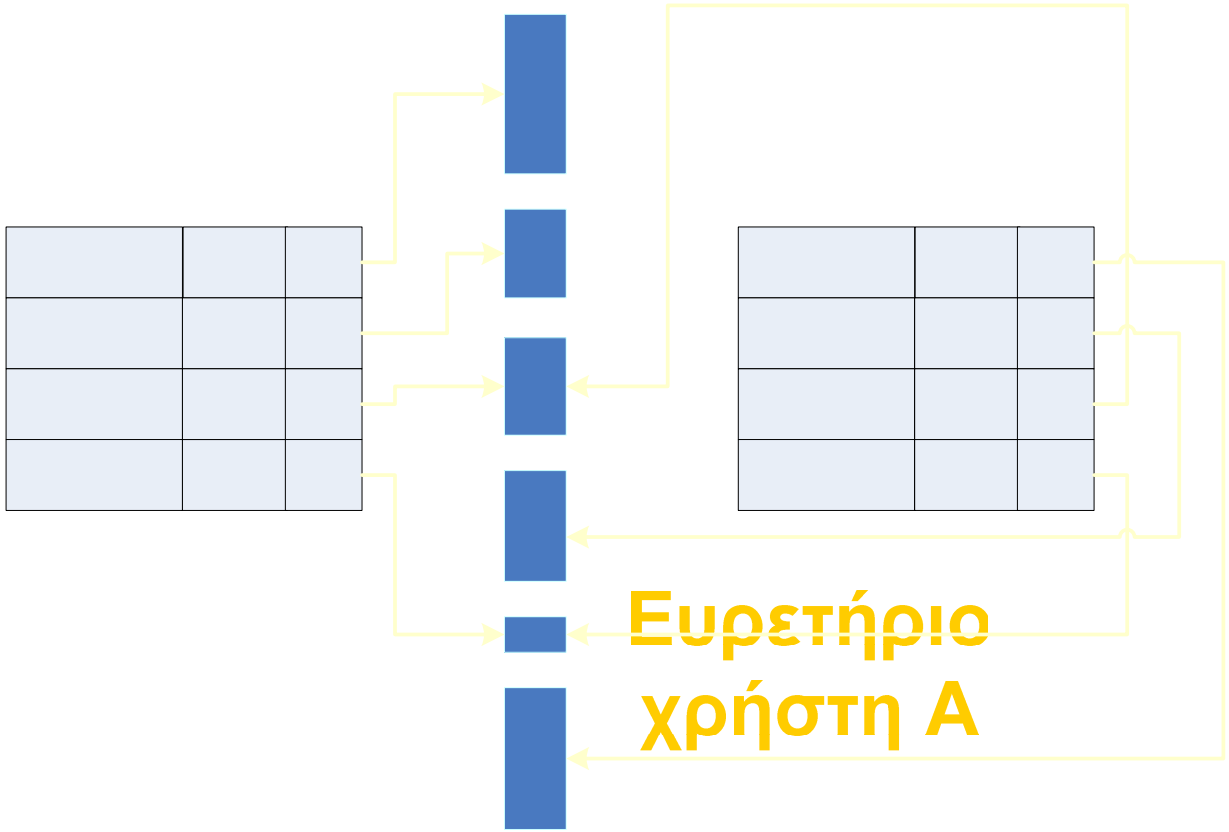
Παραδείγματα δυνατοτήτων:

- Copy capability: create a new capability for the same object.
- Copy object: create a duplicate object with a new capability.
- Remove capability: delete an entry from the C-list; object unaffected.
- Destroy object: permanently remove an object and a capability.

Κατάλογος (Directory) (1/2)

- Κάθε αντικείμενο έχει ένα μοναδικό ιδιοκτήτη, ο οποίος καθορίζει τα δικαιώματα προσπέλασης.
- Κάθε υποκείμενο έχει ένα κατάλογο (λίστα) όλων των αντικειμένων για τα οποία έχει κάποιο δικαίωμα προσπέλασης.
- Στα δικαιώματα read -r, write -w, execute -x προστίθεται και το **owner -o.**
- Προβλήματα:
  - *Μέγεθος λιστών υποκειμένων*
  - *Χρόνος πολλαπλής αναζήτησης*
  - *Η χρήση ψευδωνύμων δημιουργεί πρόβλημα*

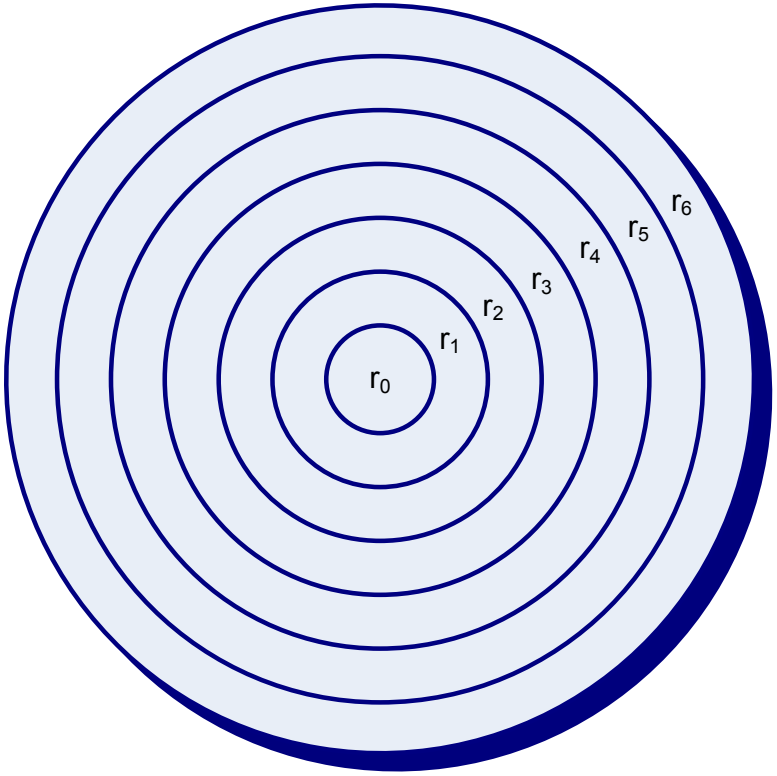
Κατάλογος (Directory)



Test.c	ORW
Test.exe	OX
Refs.doc	ORW

Δακτύλιοι (Protection rings)

- Κάθε υποκείμενο και αντικείμενο συ-σχετίζεται με ένα δακτύλιο r_n, ανάλογα με τη σημασία του.
- Ο δακτύλιος r_o παρέχει το μεγαλύτερο βαθμό προστασίας (πχ. με αυτόν σχετίζεται ο πυρήνας του λειτουργικού συστήματος).
- Ένα υποκείμενο του δακτυλίου r_i έχει πρόσβαση σε ένα αντικείμενο του δακτυλίου r_j, *αν και μόνο αν* $i \leq j$.



4η θεματική ενότητα

4. Έλεγχος προσπέλασης και προστασία ιδιωτικότητας
   - Αναγνώριση ταυτότητας - αυθεντικοποίηση
   - Μοντέλα ελέγχου πρόσβασης
   - **Τεχνικές προστασίας και διαχείρισης ιδιωτικότητας**

Έλεγχος Πρόσβασης και Ιδιωτικότητα

- Ο έλεγχος πρόσβασης και η προστασία της ιδιωτικότητας (user privacy) είναι ορθογώνια προβλήματα.
  - Ο έλεγχος πρόσβασης απαιτεί την αναγνώριση του χρήστη
- Ζητήματα Ιδιωτικότητας
  - Προστασία Ανωνυμίας
  - Προστασία από σύνδεση διαφορετικών προσβάσεων

Τεχνικές Ιδιωτικότητας

- Ανώνυμη Πρόσβαση
  - Proxy Server
  - Ανώνυμα δικαιώματα πρόσβασης (anonymous credentials)
  - Ψευδώνυμα (pseudonyms)
- Προστασία από σύνδεση (ανώνυμων) προσβάσεων
  - Ψευδώνυμα μίας χρήσης

Βιβλιογραφία

1. Tanenbaum, Modern Operating Systems 3 e, (c) 2008 Prentice-Hall, Inc. All rights reserved. 0-13-6006639
2. Κάτσικας Σ., "Πολιτικές και Φορμαλιστικά Μοντέλα Ασφάλειας", στο Ασφάλεια Πληροφοριακών Συστημάτων, Κάτσικας Σ., Γκρίτζαλης Δ., Γκρίτζαλης Σ. (επ. επ.), σελ.145-172, Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004.
3. Σ. Κάτσικας Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις Νέων Τεχνολογιών, 2003.
4. Bishop M., Computer Security: Art and Science, Addison-Wesley, USA 2003.
5. Gollmann D., Computer Security, J. Wiley, United Kingdom 1999.
6. Pfleeger C., Security in Computing, Prentice-Hall (2nd ed.), USA 2001.
7. Polemi D., Biometric Techniques: Review and Evaluation, European Commission, ETS Programme, April 1997.
8. Zviran M., Haga W., A comparison of password techniques for multilevel authentication mechanisms, Naval Postgraduate School, USA, June 1990.