Λειτουργικά Συστήματα

Ενότητα 13: Ασφάλεια

Δρ. Μηνάς Δασυγένης
mdasyg@ieee.org
Εργαστήριο Ψηφιακών Συστημάτων και Αρχιτεκτονικής Υπολογιστών
http://arch.icte.uowm.gr/mdasyg

Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ψηφιακά Μαθήματα στο Πανεπιστήμιο Δυτικής Μακεδονίας**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ασφάλεια ΛΣ

- Η προστασία του Λειτουργικού Συστήματος θεωρείται κρίσιμη για την ασφαλή λειτουργία του υπολογιστικού συστήματος καθώς το ΛΣ είναι αυτό που μπορεί να διασφαλίσει:
  - Ασφάλεια των ίδιων των υπηρεσιών που παρέχει.
  - Απομόνωση απειλών που προέρχονται από υψηλότερα επίπεδα, ώστε να μην επηρεαστούν οι υπόλοιπες υπηρεσίες και εφαρμογές ή τα χαμηλότερα επίπεδα.
  - Καταστολή των απειλών που προέρχονται από τα χαμηλότερα επίπεδα, ώστε να διασφαλίζεται η διαθεσιμότητα του συστήματος.

Προστασία αντικειμένων ΛΣ

- Το Λειτουργικό Σύστημα ενός Υπολογιστικού Συστήματος που υποστηρίζει πολλούς διαφορετικούς χρήστες, εκτελεί ένα ευρύ φάσμα εφαρμογών και είναι συνδεδεμένο στο δίκτυο, έχει αυξημένες απαιτήσεις ασφάλειας των αντικειμένων του:
  - Δεδομένα που βρίσκονται είτε στην πρωτεύουσα μνήμη (RAM) είτε σε δευτερεύουσα (σκληροί δίσκοι και αποσπώμενοι δίσκοι).
  - Εκτελέσιμα προγράμματα και διεργασίες εφαρμογών.
  - Συσκευές εισόδου-εξόδου και δικτύου.
  - Διεργασίες και δεδομένα του ίδιου του ΛΣ.

Έννοιες που συνδέονται με την ασφάλεια

- Ευχρηστία - Φιλικότητα (usability).
- Βέλτιστη Αποδοτικότητα (efficiency).
- Ακεραιότητα (integrity).
- Εμπιστευτικότητα (confidentiality).
- Αυθεντικότητα (authenticity). Κάθε χρήστης ή συσκευή αναγνωρίζεται μοναδικά για τις διεργασίες που εκτελεί και τα δεδομένα που χρησιμοποιεί.
- Διαθεσιμότητα (availability).
- Ευκινησία (capacity)- Τα μέτρα προστασίας δεν θα πρέπει να θέτουν άσκοπους περιορισμούς στις ενέργειες των χρηστών.
- Ανιχνευσιμότητα (detectability) των αιτίων μιας πιθανής προσβολής του συστήματος.

Ευπάθειες και απειλές

- Οι κίνδυνοι που υπάρχουν σε ένα λειτουργικό σύστημα είναι η απώλεια, καταστροφή, διαγραφή, τροποποίηση ή διάδοση των δεδομένων χωρίς την απαιτούμενη δικαιοδοσία.
- Συνήθως οι κίνδυνοι αυτοί προέρχονται από:
  - Αστοχία του ίδιου του συστήματος.
  - Κακή χρήση.
  - Συνειδητές κακόβουλες ενέργειες με ενδεχόμενα κίνητρα.
  - Τη περιέργεια.
  - Το οικονομικό όφελος.
  - Πρόκληση.
  - Κατασκοπεία.
  - Και διάφορα άλλα.....

Ενδεικτικές ευπάθειες (1/3)

- Αποκάλυψη συνθηματικών.
- Αναβάθμιση δικαιωμάτων.
- Μη εξουσιοδοτημένη εκτέλεση λογισμικού με στόχο την κατασπατάληση των πόρων ή την παρακολούθηση του συστήματος.
- Άρνηση παροχής υπηρεσίας.
- Κακόβουλο λογισμικό – ενέργειες (τροποποίηση δεδομένων, διαγραφή αρχείων, φυσικός βανδαλισμός κ.λ.π.).
- Συμπτωματικές ασυνέπειες και λάθη (προγραμματιστικές ατέλειες και αμέλεια του διαχειριστή να παρακολουθεί τα patches).

Ενδεικτικές ευπάθειες (2/3)

- Εκμετάλλευση καταπακτών (Προγραμματιστική διάταξη που έχει ως στόχο την παράκαμψη ενός μηχανισμού ασφάλειας).
- Ο ανθρώπινος παράγοντας:
  - Κακόβουλες ενέργειες.
  - Αμέλεια – Άγνοια.
  - Παραπλάνηση.
  - Εκβιασμός.
  - Δωροδοκία.

Ενδεικτικές ευπάθειες (3/3)

Στόχος	Απειλή
Εμπιστευτικότητα δεδομένων	Έκθεση δεδομένων
Ακεραιότητα δεδομένων	Παραποίηση δεδομένων
Διαθεσιμότητα συστήματος	Άρνηση υπηρεσιών
Αποκλεισμός εξωτερικών υπηρεσιών	Σύστημα ελεγχόμενο από ιούς

Εισβολείς

Κοινές κατηγορίες:

- Περιστασιακές υποκλοπές από μη τεχνικούς χρήστες.
- Υποκλοπή από εσωτερικό εχθρό.
- Αποφασιστικές προσπάθειες με στόχο τα λεφτά.
- Εμπορική ή στρατιωτική κατασκοπεία.

Μηχανισμοί ασφάλειας ΛΣ

- Η προστασία ενός ΠΣ γίνεται στα πλαίσια κάποιας πολιτικής ασφάλειας (security policy), η οποία ορίζει ποιες είναι οι βασικές απαιτήσεις ασφάλειας και υλοποιείται με βάση ορισμένους μηχανισμούς ασφάλειας.
- Οι βασικές απαιτήσεις ασφάλειας (μαζί με τους μηχανισμούς ασφάλειας που αξιοποιούνται για τη κάλυψη των) παρατίθενται στη συνέχεια.

Τυχαία καταστροφή δεδομένων

Κοινές αιτίες τυχαίας απώλειας δεδομένων:

- **Φυσικές καταστροφές**: πυρκαγιές, πλημμύρες, σεισμοί, πόλεμοι, εξεγέρσεις, ή αρουραίοι που ροκανίζουν τα αντίγραφα ασφαλείας.
- **Σφάλματα υλικού ή λογισμικού**: δυσλειτουργίες CPU, δυσανάγνωστοι δίσκοι ή ταινίες, λάθη των τηλεπικοινωνιών, σφάλματα προγραμμάτων.
- **Ανθρώπινα λάθη**: λανθασμένη καταχώρηση δεδομένων, λάθος τοποθετημένη δισκέτα ή CD-ROM, λάθος εκτέλεση προγράμματος, ελλιπής δίσκος ή ταινία, ή κάποιο άλλο λάθος.

Αυθεντικοποίηση (1/6)

- Αυθεντικοποίηση.
- Βασίζεται σε:
  - Κάτι που γνωρίζει ο χρήστης (smt the user knows).
  - Κάτι που κατέχει ο χρήστης (smt the user has).
  - Σε βιομετρικά χαρακτηριστικά (smt the user is).
  - Σε τοποθεσία (γεωγραφική ή δικτυακή).
- Οι συνηθέστεροι μηχανισμοί ασφάλειας για την ικανοποίηση της απαίτησης αυθεντικοποίησης είναι:
  - Συνθηματικά.
  - Βιομετρικές μέθοδοι.
  - Αγνωστικά πρωτόκολλα.
  - Μηχανισμοί Δημόσιου κλειδιού.

Αυθεντικοποίηση (2/6)

- Συνθηματικά (πλεονεκτήματα):
  - Ο μηχανισμός είναι απλός και έχει πολύ χαμηλό κόστος εφαρμογής.
  - Δεν απαιτείται εξειδικευμένη εκπαίδευση των χρηστών.
  - Παρέχει ικανοποιητικό βαθμό προστασίας σε περιβάλλοντα χαμηλής ευπάθειας.
  - Όλα τα ΛΣ έχουν εγγενώς ενσωματωμένους τέτοιους μηχανισμούς.

Αυθεντικοποίηση (3/6)

- Συνθηματικά (μειονεκτήματα):
  - Μεταφέρονται εύκολα από χρήστη σε χρήστη.
  - Δεν είναι κατάλληλα για απομακρυσμένη δικτυακή αυθεντικοποίηση, εκτός αν έχει διασφαλισθεί η εμπιστευτικότητα τους με άλλο μηχανισμό κατά τη μετάδοσή τους.
  - Δεν θεωρούνται επαρκή όταν απαιτείται υψηλό επίπεδο προστασίας, εκτός εάν συνδυαστούν με άλλες ισχυρότερες τεχνικές.

Διαρροή πληροφορίας με την αυθεντικοποίηση με κωδικό

LOGIN: mitch
PASSWORD: FooBar!-7
SUCCESSFUL LOGIN

(a)

LOGIN: carol
INVALID LOGIN NAME
LOGIN:

(b)

LOGIN: carol
PASSWORD: Idunno
INVALID LOGIN
LOGIN:

(c)

(a) A successful login.
(b) Login rejected after name is entered.
(c) Login rejected after name and password are typed.

Brute forcing για σύνδεση με κωδικό

LBL> telnet elxsi
ELXSI AT LBL
LOGIN: root
PASSWORD: root
INCORRECT PASSWORD, TRY AGAIN
LOGIN: guest
PASSWORD: guest
INCORRECT PASSWORD, TRY AGAIN
LOGIN: uucp
PASSWORD: uucp
WELCOME TO THE ELXSI COMPUTER AT LBL

How a cracker broke into a U.S. Department of Energy computer at LBL.

Αυθεντικοποίηση (4/6)

- Βιομετρικές μέθοδοι: Στηρίζονται στη μοναδικότητα ορισμένων φυσικών χαρακτηριστικών είτε του ανθρώπινου σώματος, είτε της ανθρώπινης συμπεριφοράς:
  - Ισχυρή αυθεντικοποίηση.
  - Μονοσήμαντη αντιστοίχηση του χρήστη σε φυσική οντότητα.
  - Μη μεταφερσιμότητα ηλεκτρονικής ταυτότητας σε τρίτη οντότητα:
  - Μεγάλο κόστος εφαρμογής.
  - Πολυπλοκότητα αλγορίθμων αναγνώρισης.
  - Υψηλό ποσοστό σφάλματος σε κάποιες περιπτώσεις.

Αυθεντικοποίηση (5/6)

- Αγνωστικά πρωτόκολλα:
  - Με τη χρήση αγνωστικών πρωτοκόλλων είναι δυνατή η αμφίδρομη αυθεντικοποίηση δύο λογικών υποκειμένων με χρήση συνθηματικού, το οποίο όμως δεν είναι απαραίτητο να μεταδοθεί. Βασίζονται στην αξιοποίηση μονόδρομων συναρτήσεων (one-way functions). Αντί του συνθηματικού μεταδίδονται πληροφορίες που αποσκοπούν να αποδείξουν ότι το υπό αυθεντικοποίηση λογικό υποκείμενο γνωρίζει το συνθηματικό {chalenge-response}.

Αυθεντικοποίηση ερώτησης - απόκρισης

Οι ερωτήσεις θα πρέπει να επιλεγούν έτσι ώστε ο χρήστης να μη χρειάζεται να τις γράψει κάπου.

Παραδείγματα:

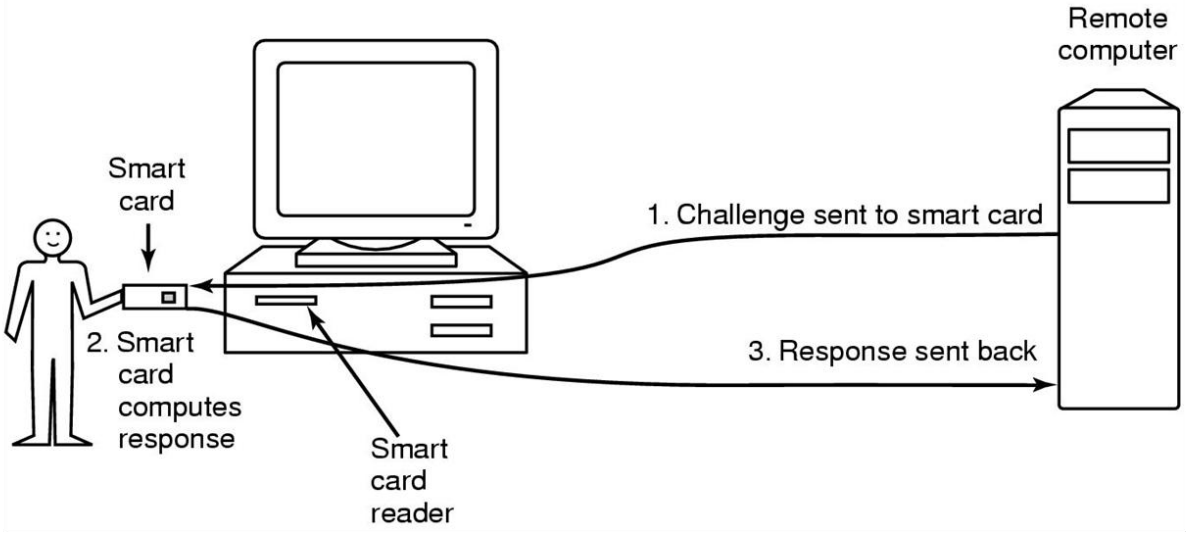
- Ποια είναι η αδερφή της Κικής ;
- Σε ποια οδό βρίσκεται το δημοτικό σχολείο που πήγες;
- Τι δίδασκε ο κύριος Παπαδόπουλος;

Αυθεντικοποίηση (6/6)

Μηχανισμοί Δημόσιου κλειδιού:

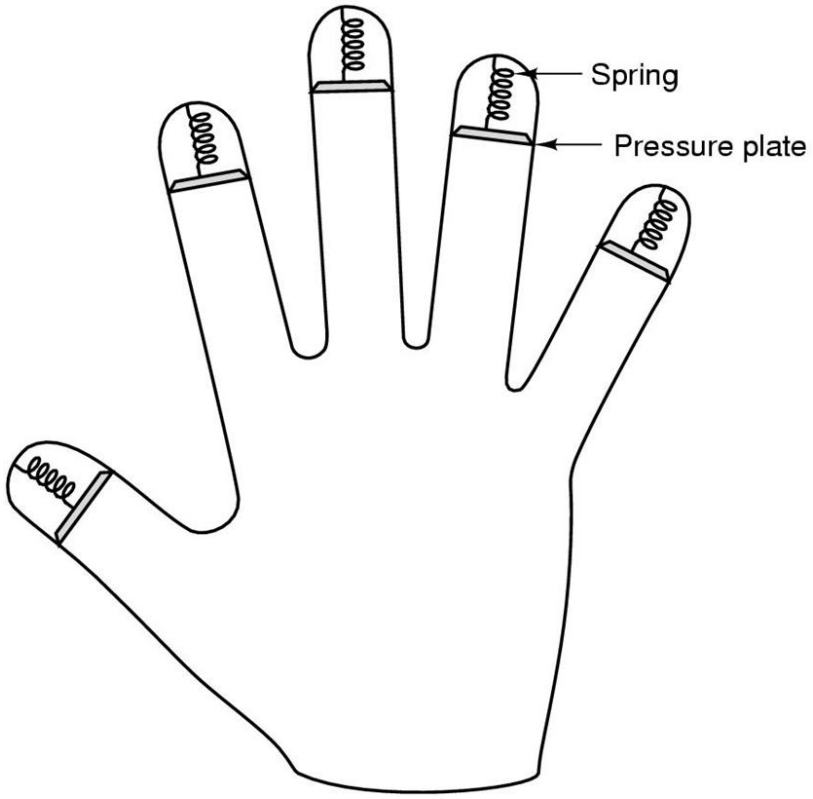
- Δεν απαιτείται μετάδοση μυστικών δεδομένων σε καμία φάση της διαδικασίας αυθεντικοποίησης και συνεπώς δεν απαιτείται εμπιστευτικότητα στην επικοινωνία.
- Τα ζεύγη κλειδιών είναι καθολικά μοναδικά και έτσι συνδέονται μονοσήμαντα με μία μόνο φυσική οντότητα.
- Ενσωματώνεται ήδη στα σύγχρονα ΛΣ.
  - Τα κλειδιά δεν απομνημονεύονται. Συνεπώς τα ιδιωτικά κλειδιά θα πρέπει να αποθηκεύονται σε πολύ καλά προστατευμένα ηλεκτρονικά μέσα.
  - Απαιτείται η ύπαρξη Υποδομής Δημόσιου Κλειδιού για τη διαχείριση των κλειδιών και τη σύνδεσή τους με τις φυσικές οντότητες.

Αυθεντικοποίηση με χρήση φυσικού μέσου



Χρήση μιας έξυπνης κάρτας για αυθεντικοποίηση.

Αυθεντικοποίηση με χρήση βιομετρικών στοιχείων



Συσκευής μέτρησης μήκους δαχτύλων.

Πλαστή είσοδος

(a) (b)

a) Σωστή οθόνη σύνδεσης,
b) Πλαστή οθόνη σύνδεσης.

Έλεγχος προσπέλασης

- Έλεγχος προσπέλασης: Ολοκληρώνεται σε τρία βασικά βήματα:
  - Ταυτοποίηση (Identification): Το υποκείμενο αναφέρει τη ταυτότητα του.
  - Αυθεντικοποίηση (Authentication): Το υποκείμενο επιβεβαιώνει ότι είναι αυτό που ισχυρίσθηκε και το σύστημα ελέγχει.
  - Εξουσιοδότηση (Authorization): Το υποκείμενο αποκτά τα δικαιώματα και το σύστημα ελέγχει.
- Τους μηχανισμούς ασφάλειας .....τους ξέρετε !!!
  - Λίστες ή πίνακες ελέγχου προσπέλασης.
  - Λίστες Δυνατοτήτων.
  - Ρολο-κεντρικές μέθοδοι κ.λ.π.

Εκμετάλλευση σφαλμάτων κώδικα

Βήματα για να εκμεταλλευτείτε ένα σφάλμα:

- Τρέξτε μια σάρωση θυρών για να βρείτε μηχανήματα που δέχονται συνδέσεις telnet.
- Προσπαθήστε να συνδεθείτε μαντεύοντας το όνομα χρήστη και τον κωδικό.
- Μόλις συνδεθείτε, εκτελέστε το εσφαλμένο πρόγραμμα με είσοδο που προκαλεί το σφάλμα.
- Αν το εσφαλμένο πρόγραμμα είναι SETUID, δημιουργήστε ένα κέλυφος SETUID.
- Τρέξτε ένα πρόγραμμα ζόμπι που ακούει σε μια θύρα IP για cmds.
- Φροντίστε ώστε το πρόγραμμα ζόμπι να τρέχει με κάθε εκκίνηση του συστήματος.

Επιθέσεις έγχυσης κώδικα

```
int main(int argc, char *argv[])
{
  char src[100], dst[100], cmd[205] = "cp ";          /* declare 3 strings */
  printf("Please enter name of source file: ");       /* ask for source file */
  gets(src);                                          /* get input from the keyboard */
  strcat(cmd, src);                                   /* concatenate src after cp */
  strcat(cmd, " ");                                   /* add a space to the end of cmd */
  printf("Please enter name of destination file: ");  /* ask for output file name */
  gets(dst);                                          /* get input from the keyboard */
  strcat(cmd, dst);                                   /* complete the commands string */
  system(cmd);                                        /* execute the cp command */
}
```

Προσοχή src[100],dst[100].

Κακόβουλο λογισμικό

- Μπορεί να χρησιμοποιηθεί για εκβιασμό.
- Παράδειγμα: Το λογισμικό κρυπτογραφεί τα αρχεία στο δίσκο του θύματος, στη συνέχεια, εμφανίζει το μήνυμα.

Greetings from General Encryption
To purchase a decryption key for your hard disk, please send $100 in small
unmarked bills to Box 2154, Panama City, Panama.
Thank you. We appreciate your business.

Διαθεσιμότητα ΛΣ (1/3)

- Ένα ΛΣ για να διασφαλίσει τη διαθεσιμότητα του συστήματος στο οποίο εκτελείται πρέπει να διαχειρίζεται αποτελεσματικά όλους τους πόρους, όπως η κύρια και δευτερεύουσα μνήμη, ο κεντρικός επεξεργαστής, το δίκτυο, οι συσκευές εισόδου/εξόδου και οι περιφερειακές συσκευές.
- Πολλές φορές η διασφάλιση της διαθεσιμότητας των πόρων ενός συστήματος έρχεται σε αντίφαση με τις διαδικασίες προστασίας του. Οι περιορισμοί που τίθενται από τους μηχανισμούς ασφάλειας του ΛΣ θα πρέπει να είναι οι ελάχιστοι δυνατοί, έτσι ώστε να εξασφαλίζεται μία ισορροπία μεταξύ της επιδιωκόμενης λειτουργικότητας ενός συστήματος και της ασφάλειάς του.

Διαθεσιμότητα ΛΣ (2/3)

Αρχή διαχωρισμού:

– Διαχωρισμός των συστατικών του ΛΣ (π.χ. χρήστες, δεδομένα, σύστημα, διεργασίες) ώστε ενδεχόμενη κατάρρευση ενός συστατικού να μην επηρεάσει τα υπόλοιπα.

– Πυρήνας ασφάλειας ΛΣ (security kernel): Απομόνωση των διεργασιών του ίδιου του ΛΣ.

Κατανεμημένα (distributed) συστήματα:

– Κατανομή διαφορετικών λειτουργιών σε διαφορετικά αυτόνομα συστήματα.

Συγκροτήματα συστημάτων (clusters):

– Πολλαπλά «αντίγραφα συστήματος» σε ταυτόχρονη λειτουργία.

Διαθεσιμότητα ΛΣ (3/3)

- Διαχείριση μνήμης:
  - –Μηχανισμοί δέσμευσης-αποδέσμευσης της μνήμης που χρησιμοποιείται από διεργασίες.
  - – Μηχανισμοί καθαρισμού «σκουπιδιών».
  - – Αποφυγή ‘διαρροής’ μνήμης.
  - –Αποφυγή αποκάλυψης εμπιστευτικών δεδομένων που παραμένουν στη μνήμη και μετά την αποδέσμευσή της.
  - – Μηχανισμοί Ιδεατής μνήμης (virtual memory) και swapping: Άρση περιορισμών μεγέθους φυσικής μνήμης. Κάθε διεργασία έχει το δικό της χώρο.
- Χρονισμός μονάδας επεξεργασίας:
  - – Χρονο-καταμερισμός διεργασιών (time-slicing).
  - – Χρήση διακοπών (interrupts) για τη λειτουργία των συσκευών εισόδου/εξόδου.

Ακεραιότητα λογισμικού και δεδομένων (1/3)

Απαιτούνται μηχανισμοί για την προστασία της ακεραιότητας:

- Της κύριας Μνήμης του Υπολογιστικού Συστήματος:
  - –Της δευτερεύουσας Μνήμης του Υπολογιστικού Συστήματος.
  - –Των εκτελέσιμων προγραμμάτων και των υπόλοιπων δεδομένων.
- Οι συνηθέστερες τεχνικές που υιοθετούνται είναι:
  - – Μέθοδοι Φραγμών.
  - – Μέθοδοι Καταχωρητών.
  - – Σελιδοποίηση.
  - – Σύνολα Ελέγχου και Συνόψεις Αρχείων.
  - – Μηχανισμοί Ανοχής Σφαλμάτων σε Συστήματα Δίσκων.

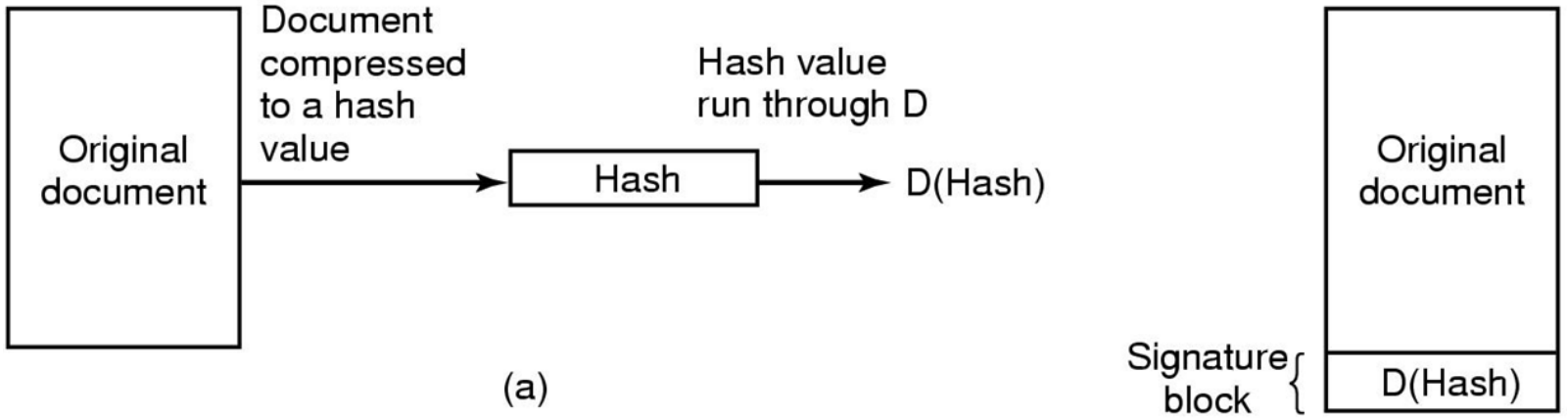
Ακεραιότητα λογισμικού και δεδομένων (2/3)

- Μέθοδος φραγμών:
  - Αφορά περιβάλλοντα single-user.
  - Στατική απομόνωση δεδομένων ΛΣ από αυτά των εφαρμογών.
- Μέθοδος καταχωρητών:
  - Δυναμικός καθορισμός περιοχών μνήμης σε πολυχρηστικά περιβάλλοντα.
  - Ο Καταχωρητής βάσης (base register) υποδεικνύει τη διεύθυνση μνήμης από όπου ξεκινά η δέσμευση για μια διεργασία.
  - Το Βεληνεκές (offset) είναι το εύρος της δέσμευσης μνήμης.

Ακεραιότητα λογισμικού και δεδομένων (3/3)

- Σελιδοποίηση:
  - Η διαθέσιμη μνήμη χωρίζεται σε ίσα τμήματα (σελίδες) με μέγεθος ίσο με δύναμη του 2 (π.χ. 64 KBytes).
  - Δέσμευση, Ανάγνωση και Εγγραφή γίνεται ανά σελίδα.
  - Αύξηση αποτελεσματικότητας και αξιοπιστίας.
  - Πιθανή αύξηση κατανάλωσης μνήμης.
- Ακεραιότητα αρχείων:
  - Σύνολο Ελέγχου (CheckSum) – Πιθανά αναξιόπιστο.
  - Σύνοψη αρχείου (Hash) – Βέβαιο συμπέρασμα.

Ψηφιακές υπογραφές (hash)



(a) Υπολογίζοντας ένα μπλοκ υπογραφής
(b) Τι δέχεται ο παραλήπτης.

Ανοχή σφαλμάτων σε αποθηκευτικά συστήματα (1/2)

- RAID (Redundant Arrays of Inexpensive Disks):
  - Πλεονασμός δεδομένων (redundancy).
- RAID-5:
  - Ν δίσκοι, χωρητικότητας Χ.
  - Διαθέσιμη χωρητικότητα (N-1)*X.
  - Για κάθε bit των N-1 δίσκων παράγονται τα δεδομένα ανοχής (parity bits) και αποθηκεύονται στο Ν-στό (τυχαίο) δίσκο.

Ανοχή σφαλμάτων σε αποθηκευτικά συστήματα (2/2)

– Parity = B1 XOR B2 XOR…XOR Bn-1.

– Ανάκτηση δεδομένων: Αν καταστραφεί ένα bit του δίσκου Κ, τότε:

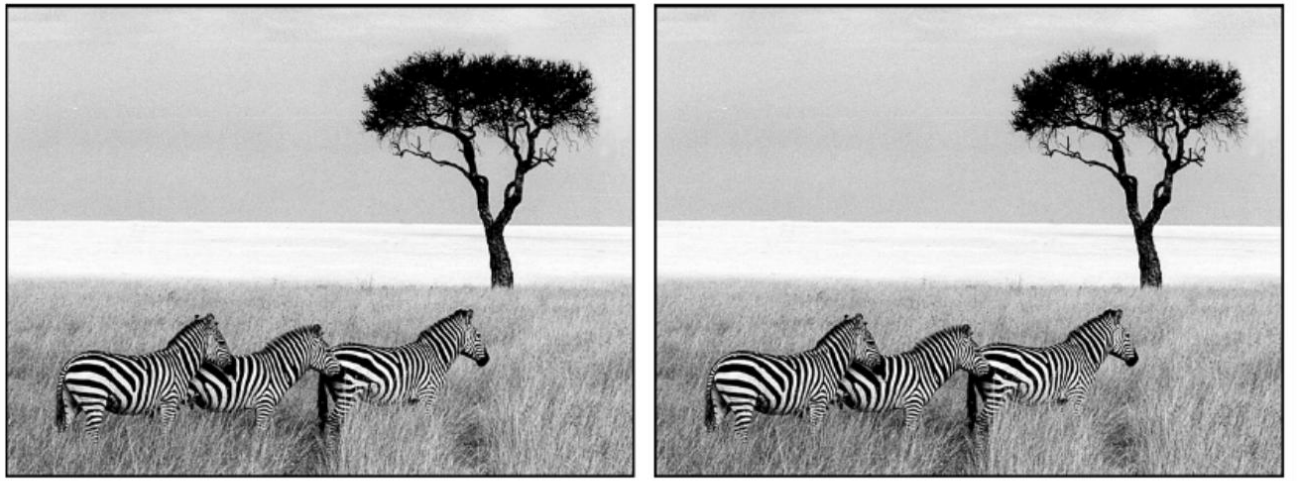
– Bk = B1 XOR B2 XOR … Bk-1 XOR Bk+1 XOR … Bn-1 XOR Parity.

- Συστήματα αρχείων (π.χ. zfs).

Καταγραφή και παρακολούθηση συμβάντων (audit)

- Με βάση την προέλευση:
  - Συμβάντα συστήματος.
  - Συμβάντα εφαρμογών.
  - Συμβάντα ασφάλειας.
- Με βάση την κρισιμότητα:
  - Πληροφοριακά συμβάντα.
  - Προειδοποιήσεις.
  - Κρίσιμα σφάλματα.
- Επιπλέον μηχανισμοί συναγερμού και ειδοποιήσεων (alert & notification).

Συγκεκαλυμμένα κανάλια



(a) (b)

(a) Τρεις ζέβρες και ένα δέντρο.
(b) Τρεις ζέβρες, ένα δέντρο και ένα πλήρες κείμενο από πέντε θεατρικά έργα του William Shakespeare, (download S-tools).

Πρόσθετοι προληπτικοί μηχανισμοί

- Εμπιστευτικότητα:
  - Αξιοποιούν μηχανισμούς υβριδικής κρυπτογραφίας.
  - Επιτρέπουν στο διαχειριστή την ανάκτηση κλειδιών αν πληρούνται κάποιες προϋποθέσεις.
- Περιοδικές προσθήκες και επιδιορθώσεις (patches & fixes).
- Ασφαλής απομακρυσμένη πρόσβαση:
  - Εικονικό Ιδιωτικό Δίκτυο (VPN).
  - ασφαλής δίοδος (tunneling, π.χ. PPTP).
  - ασφαλές κέλυφος (secure shell – SSH).

Πρόσθετοι κατασταλτικοί μηχανισμοί

- Ανάχωμα ασφαλείας (firewalls).
- Προστασία από κακόβουλο λογισμικό (malicious software).
- Σύστημα ανίχνευσης εισβολών (Intrusion Detection System - IDS).
- Παρακολουθούν την «ύποπτη» συμπεριφορά του συστήματος όπως:
  - Χρήση Διαχειριστικών Λογαριασμών από απομακρυσμένες τοποθεσίες:
  - Έντονη Δικτυακή κίνηση από την ίδια τοποθεσία.
  - Έντονη Δικτυακή κίνηση που προέρχεται ταυτόχρονα από διαφορετικές τοποθεσίες με προορισμό νια συγκεκριμένη υπηρεσία του συστήματος.
  - Σάρωση των διαθέσιμων θυρών επικοινωνίας κ.λ.π.

Διαμόρφωση πολιτικών (1/3)

- Παράμετροι λογαριασμών χρηστών:
  - Περίοδος ισχύος τους, κανόνες για τα συνθηματικά.
- Παράμετροι αυθεντικοποίησης:
  - Επιτρεπόμενοι μηχανισμοί, ομαδοποίηση χρηστών, κανόνες για διαχειριστές, χρήστες και επισκέπτες.
- Ρυθμίσεις παρακολούθησης:
  - Τύποι συμβάντων που καταγράφονται, διαχείριση ημερολογίων.
- Παράμετροι λογισμικού:
  - Επιτρεπόμενο λογισμικό που μπορεί να εγκατασταθεί, απαίτηση υπογραφής κατασκευαστή, αυτόματες ενημερώσεις.

Διαμόρφωση πολιτικών (2/3)

- Εξουσιοδότηση στο σύστημα αρχείων:
  - Εξ’ ορισμού βασικές ρυθμίσεις δικαιωμάτων.
- Διαχείριση Επικοινωνίας:
  - Αποκλεισμός διαδικτυακών πρωτοκόλλων, καθορισμός επιτρεπόμενων και απαγορευμένων διευθύνσεων, απαίτηση ασφαλούς απομακρυσμένης σύνδεσης.
- Διαχείριση Συστήματος:
  - Δικαιώματα και υποχρεώσεις διαχειριστών.
  - Ομαδοποίηση των επιτρεπόμενων ενεργειών συστήματος.
  - Περιοδικές ενημερώσεις και επιδιορθώσεις συστήματος.

Διαμόρφωση πολιτικών (3/3)

Επιπλέον ρυθμίσεις ασφάλειας, π.χ.:

- Κανόνες και περιοδικότητα εφεδρικών αντιγράφων.
- Σύνδεση χρηστών με έξυπνες κάρτες.
- Υποδομή δημόσιου κλειδιού.
- Πρωτόκολλο Ipsec.

Είδη ιών

- Ιοί συντροφιάς.
- Εκτελέσιμοι ιοί.
- Παρασιτικοί ιοί.
- Ιοί που κατοικούν στη μνήμη.
- Ιοί τομέα εκκίνησης.
- Ιοί συσκευών οδήγησης.
- Μακρο- ιοί.
- Ιοί πηγαίου κώδικα.

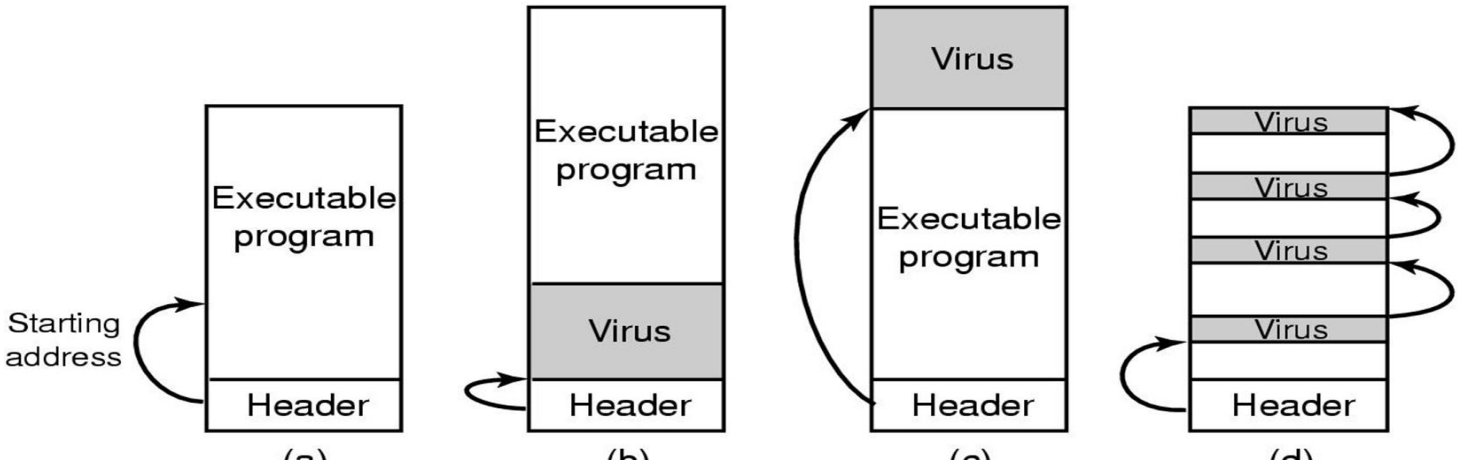
Εκτελέσιμοι ιοί (1/2)

```
#include <sys/types.h>                  /* standard POSIX headers */
#include <sys/stat.h>
#include <dirent.h>
#include <fcntl.h>
#include <unistd.h>
struct stat sbuf;                       /* for lstat call to see if file is sym link */

search(char *dir_name)
{                                       /* recursively search for executables */
        DIR *dirp;                      /* pointer to an open directory stream */
        struct dirent *dp;              /* pointer to a directory entry */

        dirp = opendir(dir_name);       /* open this directory */
        if (dirp == NULL) return;       /* dir could not be opened; forget it */
```

Εκτελέσιμοι ιοί (2/2)

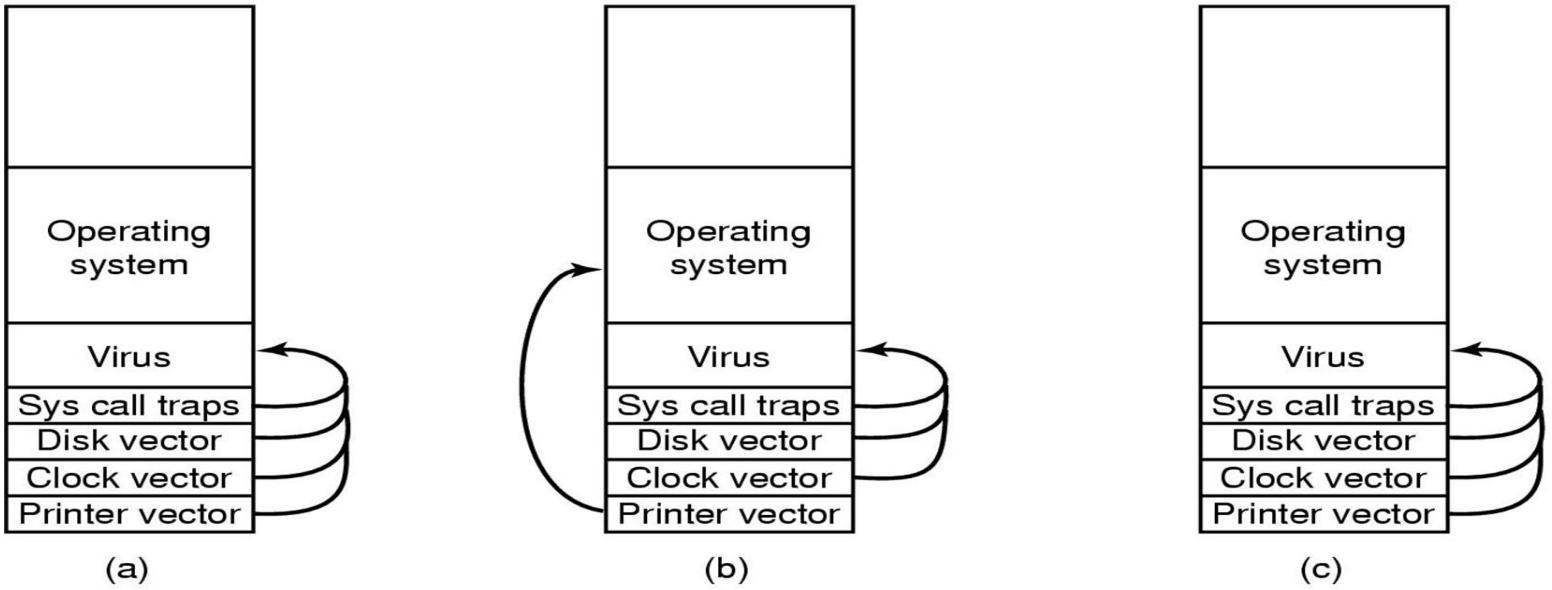
```
    while (TRUE) {
        dp = readdir(dirp);                          /* read next directory entry */
        if (dp == NULL) {                            /* NULL means we are done */
        chdir ("..");                                /* go back to parent directory */
        break;                                       /* exit loop */
    }
    if (dp->d_name[0] == '.') continue;              /* skip the . and .. directories */
    lstat(dp->d_name, &sbuf);                        /* is entry a symbolic link? */
    if (S_ISLNK(sbuf.st_mode)) continue;             /* skip symbolic links */
    if (chdir(dp->d_name) == 0) {                    /* if chdir succeeds, it must be a dir */
        search(".");                                 /* yes, enter and search it */
    } else {                                                 /* no (file), infect it */
        if (access(dp->d_name,X_OK) == 0) /* if executable, infect it */
            infect(dp->d_name);
    }
    closedir(dirp);                                  /* dir processed; close and return */
}
```

Παρασιτικοί ιοί



Ένα εκτελέσιμο πρόγραμμα με έναν ιό στην αρχή του προγράμματος.
(c) Με έναν ιό στο τέλος.
(d) Με έναν ιό διασκορπισμένο στον ελεύθερο χώρο του προγράμματος.

Ιοί εκκίνησης τομέα



a) Μετά την καταγραφή των σημάτων διακοπής και παγίδων από τον ιό.

b) Αφού το ΛΣ έχει πάρει ξανά το διάνυσμα διακοπής του εκτυπωτή.

c) Μετά την παρατήρηση του ιού ότι έχει χάσει το διάνυσμα διακοπής του εκτυπωτή και το καταγραφεί ξανά.

Κατασκοπευτικό λογισμικό (1/2)

Περιγραφή:

- Εγκαθίστανται κρυφά στον υπολογιστή εν αγνοία του χρήστη.
- Τρέχουν στο παρασκήνιο κάνοντας ενέργειες πίσω από την πλάτη του χρήστη.

Κατασκοπευτικό λογισμικό (2/2)

Χαρακτηριστικά:

- Κρύβεται, το θύμα δε μπορεί να το εντοπίσει εύκολα.
- Συλλέγει δεδομένα σχετικά με τον χρήστη.
- Στέλνει τις πληροφορίες που συλλέγει στον συγγραφέα του προγράμματος.
- Προσπαθεί να επιβιώσει ακόμα και στις βίαιες προσπάθειες διαγραφής του.

Πως διαδίδονται τα κατασκοπευτικά λογισμικά

Πιθανοί τρόποι:

- Όπως τα κακόβουλα λογισμικά ή με δούρειους ίππους.
- Από downloads και επισκέψεις σε μολυσμένα site:
  - Ιστοσελίδες προσπαθούν να τρέξουν ένα αρχείο .exe.
  - Ανυποψίαστοι χρήστες εγκαθιστούν μολυσμένα toolbar.
  - Εγκαθίστανται κακόβουλοι έλεγχοι ActiveX.

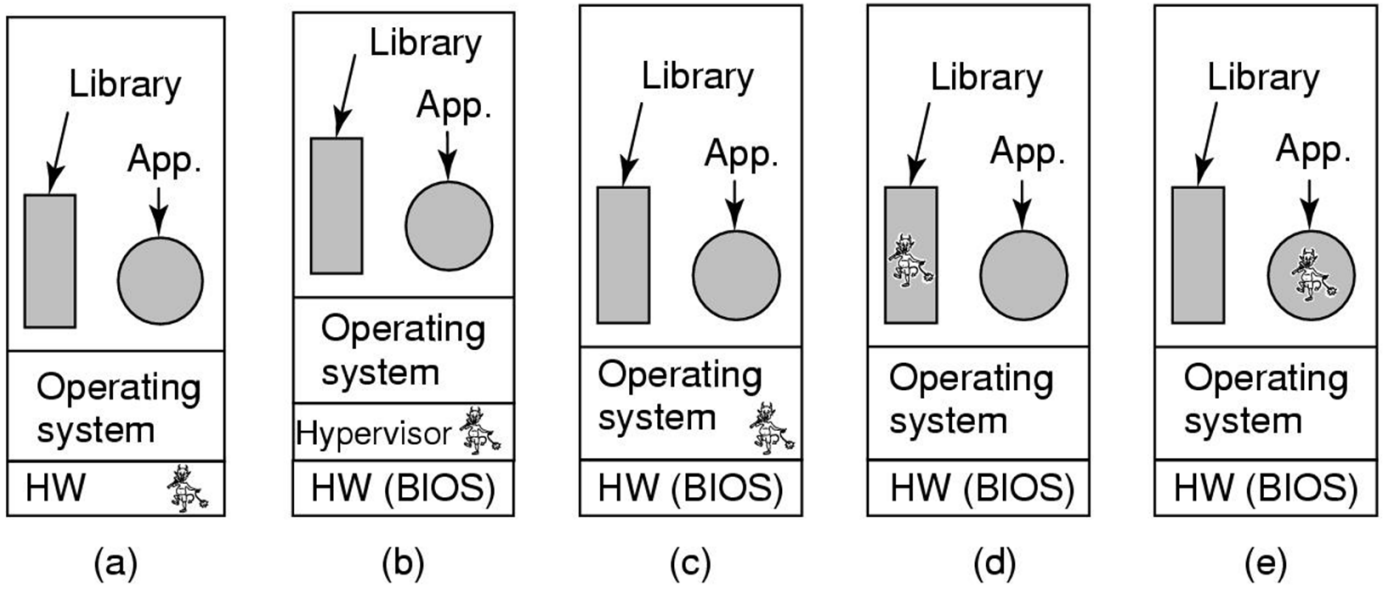
Δράσεις κατασκοπευτικού λογισμικού

- Αλλαγή της αρχικής σελίδας του φυλλομετρητή.
- Τροποποίηση της λίστας των αποθηκευμένων σελίδων.
- Πρόσθεση νέων toolbars στον φυλλομετρητή.
- Αλλαγή του προ επιλεγμένου προγράμματος αναπαραγωγής πολυμέσων.
- Αλλαγή της προ επιλεγμένης μηχανής αναζήτησης.
- Πρόσθεση νέων εικονιδίων στην επιφάνεια εργασίας των Windows.
- Αντικατάσταση των διαφημιστικών σε ιστοσελίδες με τα δικά του διαφημιστικά.
- Τοποθέτηση διαφημιστικών στα παράθυρα διαλόγου των Windows.
- Εκτέλεση μιας συνεχούς και ασταμάτητης ροής διαφημίσεων pop-up.

Τύποι Rootkits (1/2)

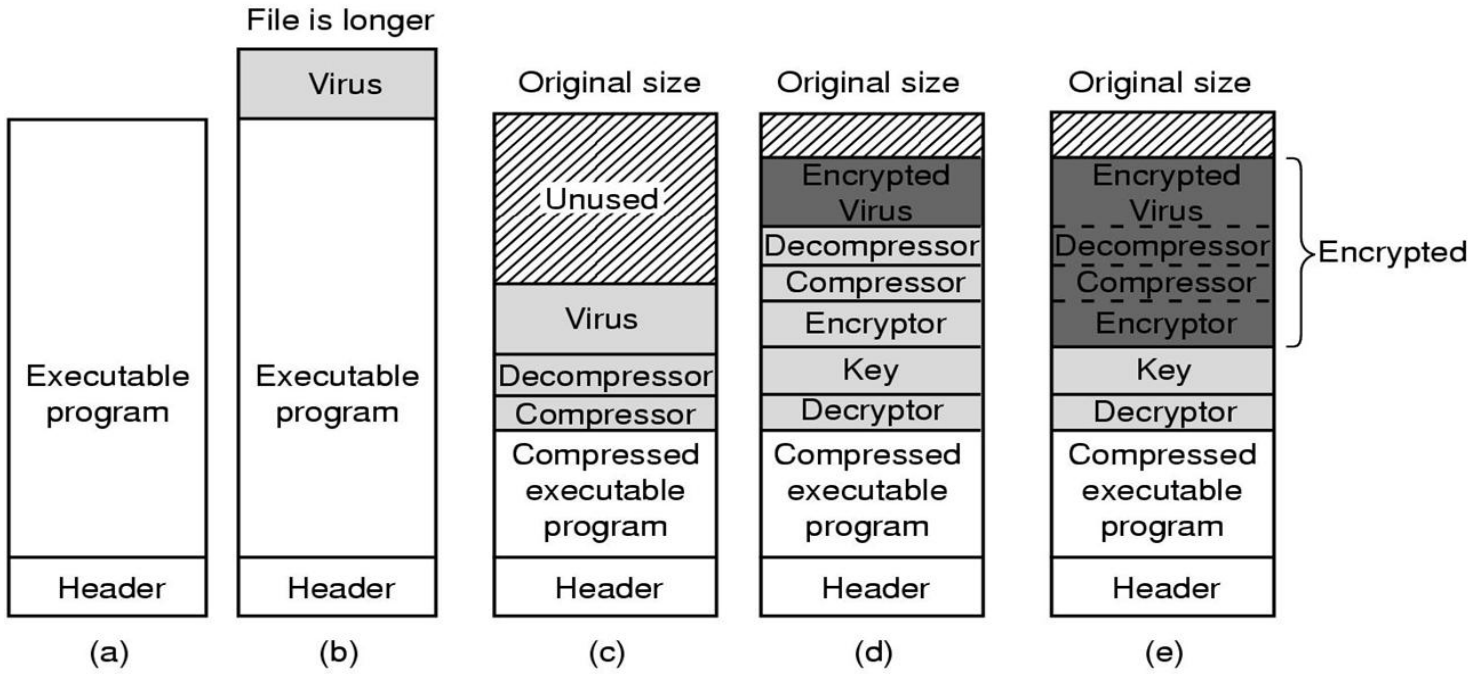
- Firmware rootkits.
- Hypervisor rootkits.
- Rootkits πυρήνα.
- Rootkits βιβλιοθήκης.
- Rootkits εφαρμογής.

Τύποι Rootkits (2/2)



Πέντε μέρη στα οποία μπορεί να κρυφτεί ένα rootkit.

Σαρωτές ιών (1/2)



Ένα πρόγραμμα.
Ένα μολυσμένο πρόγραμμα.
Ένα συμπιεσμένο μολυσμένο πρόγραμμα.
Ένας κρυπτογραφημένος ιός.
Ένας συμπιεσμένος ιός με κρυπτογραφημένο συμπιεσμένο κώδικα.

Σαρωτές ιών (2/2)

```
MOV A,R1
ADD B,R1
ADD C,R1
SUB #4,R1
MOV R1,X
```
(a)

```
MOV A,R1
NOP
ADD B,R1
NOP
ADD C,R1
NOP
SUB #4,R1
NOP
MOV R1,X
```
(b)

```
MOV A,R1
ADD #0,R1
ADD B,R1
OR R1,R1
ADD C,R1
SHL #0,R1
SUB #4,R1
JMP .+1
MOV R1,X
```
(c)

```
MOV A,R1
OR R1,R1
ADD B,R1
MOV R1,R5
ADD C,R1
SHL R1,0
SUB #4,R1
ADD R5,R5
MOV R1,X
MOV R5,Y
```
(d)

```
MOV A,R1
TST R1
ADD C,R1
MOV R1,R5
ADD B,R1
CMP R2,R5
SUB #4,R1
JMP .+1
MOV R1,X
MOV R5,Y
```
(e)

Παραδείγματα πολυμορφικών ιών (και τα 5 έχουν το ίδιο τελικό αποτέλεσμα).

Προϋποθέσεις για τη Σχεδίαση Ασφαλών ΛΣ (1/2)

- **Πολιτική ασφάλειας** (security policy): Είναι απαραίτητη η ύπαρξη μία δέσμης βασικών αρχών, εκφρασμένων με σαφήνεια, η οποία να περιλαμβάνει τους στόχους του σχεδιαστή του ΛΣ.
- **Ταυτοποίηση** (identification): Κάθε αντικείμενο του συστήματος θα πρέπει να μπορεί να αναγνωρισθεί μονοσήμαντα.
- **Σήμανση** (marking): Κάθε αντικείμενο του συστήματος πρέπει να συνοδεύεται από μία ένδειξη του βαθμού εμπιστευτικότητας του και άλλων χαρακτηριστικών ασφάλειας.

Προϋποθέσεις για τη Σχεδίαση Ασφαλών ΛΣ (2/2)

- **Ελεγξιμότητα** (accountability): Το ΛΣ θα πρέπει να καταγράφει όλες τις ενέργειες που αφορούν ή μπορούν να επηρεάσουν την ασφάλειά του.
- **Διαβεβαίωση** (assurance): Το υπολογιστικό σύστημα πρέπει να παρέχει τεχνικές ρύθμισης για την υλοποίηση της πολιτικής ασφάλειας, οι οποίες να μπορούν να εκτιμηθούν ως προς την αποτελεσματικότητά τους.
- **Ακεραιότητα προστασίας** (protection integrity): Οι τεχνικές εξασφάλισης του λειτουργικού συστήματος πρέπει να προστατεύονται από κάθε ανεπιθύμητη μετατροπή.

Μεθοδολογία σχεδίασης Ασφάλειας ΛΣ (1/2)

- **Αρχή της ελάχιστης από κοινού χρήσης**:
  Ελαχιστοποίηση των αντικειμένων που χρησιμοποιούνται από κοινού από πολλούς χρήστες, τα οποία δυνητικά μπορούν να αποτελέσουν μέσα για διαρροή διαβαθμισμένων δεδομένων.
- **Αρχή των ελάχιστων προνομίων**:

  Κάθε χρήστης πρέπει να διατηρεί τα ελάχιστα προνόμια, ώστε να ελαχιστοποιούνται οι πιθανές αρνητικές συνέπειες από μία ενέργειά του, διατηρώντας ταυτόχρονα την απαιτούμενη λειτουργικότητα στο σύστημα.

Μεθοδολογία σχεδίασης Ασφάλειας ΛΣ (2/2)

- **Αρχή του ανοικτού σχεδιασμού**: Η ισχύς των μηχανισμών ασφάλειας δεν πρέπει να στηρίζεται στην άγνοια των χρηστών σχετικά με τις τεχνικές ασφάλειας που χρησιμοποιούνται, αλλά στην αποτελεσματική τους σχεδίαση.
- **Διαχωρισμός προνομίων**: Η πρόσβαση στα αντικείμενα του συστήματος πρέπει να βασίζεται στα διακεκριμένα προνόμια που πρέπει να διαθέτει κάθε χρήστης και τα οποία τον διαφοροποιούν από τους άλλους χρήστες.
- **Αρχή της εξ ορισμού άρνησης προσπέλασης**: Κάθε χρήστης πρέπει εξορισμού να μη διαθέτει δυνατότητα πρόσβασης σε ένα αντικείμενο, εκτός αν καθορισθεί διαφορετικά από τον διαχειριστή.

Πιστοποίηση Ασφάλειας ΛΣ (1/3)

- ITSEC (Information Technology Security Evaluation Criteria):
  - –Ελεγκτικότητα (accountability).
  - –Στην ταυτοποίηση και αυθεντικοποίηση χρηστών (identification & authentication).
  - – Στην παρακολούθηση (audit).
  - – Στην επαναχρησιμοποίηση αντικειμένων (object reuse).
  - – Στον έλεγχο προσπέλασης (access control).
  - – Στην ακρίβεια (accuracy) και στην αξιοπιστία (reliability of service).

Πιστοποίηση Ασφάλειας ΛΣ (2/3)

- TCSEC (Trusted Computer Systems Evaluation Criteria) αλλιώς γνωστό ως «orange book» σύμφωνα με το οποίο τα ΛΣ κατατάσσονται σε κλάσεις ανάλογα με τα χαρακτηριστικά ασφάλειας που διαθέτουν:
  - Κλάση D: παροχή στοιχειώδους ή καμιάς ασφάλειας.
  - Κλάση C: Τα ΛΣ αυτής της κλάσης παρέχουν «διακριτική» προστασία στους χρήστες και τα αντικείμενά τους. Διαιρείται στις υποκλάσεις C1 και C2.
  - Κλάση B: Σε αυτή την κλάση τα ΛΣ επιβάλλουν αυστηρό έλεγχο πρόσβασης στα αντικείμενά τους, περιέχουν διαδικασίες καταγραφής και παρακολούθησης, μοναδική αναγνώριση των αντικειμένων και διαιρείται και αυτή σε υποκλάσεις B1, B2, B3.
  - Κλάση A: Εδώ εντάσσονται τα ΛΣ που διαθέτουν επιπλέον μηχανισμούς ασφάλειας και για τα οποία μπορεί να αποδειχθεί με αυστηρό τρόπο ότι είναι ασφαλή.

Πιστοποίηση Ασφάλειας ΛΣ (3/3)

ΛΣ	Κλάση ITSEC	Κλάση TCSEC
Novell Trusted Netware 4	E2 F-C2	C2
Trusted Solaris 8	E3 F-B1	B1
Solaris 8	E3 F-C2	C2 (υπό αξιολόγηση για B1)
Windows 2000	E3 F-C2	C2
IBM CMW for AIX	E3 F-B1	B1

Common Criteria Certificate Microsoft Corporation

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Microsoft Corporation

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Microsoft Windows Server 2003 SP2 including R2, Standard, Enterprise, Datacenter, x64, and Itanium Editions; Windows XP Professional SP2 and x64 SP2; Windows XP Embedded SP2 (for specific TOE software, updates, patches, and hotfixes see Section 1 of Security Target)
Evaluation Platform: Unisys RASCAL ES7000 (x64); Dell OptiplexGX620; Dell PowerEdgeSC1420; Dell PowerEdge1800; Dell PowerEdge2850; HP ProLiantDL385; HP rx1620 Bundle Solution Server; HP xw9300 Workstation; IBM eServer326m; Gemplus GemPC Twin USB Smart Card Reader

CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-VID10184-2008
Assurance Level: EAL 4 Augmented ALC_FLR.3
Date Issued: 07 February 2008
Protection Profile Identifier: Controlled Access Protection Profile, V1.d, October 8, 1999

Original Signed By
Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By
Information Assurance Director
National Security Agency

Common Criteria Certificate Windows 7 and Windows 2008 R2

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Windows 7 and Windows Server 2008 R2

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: Microsoft Windows 7 and Windows Server 2008 R2; Windows 7 Enterprise Edition; Windows 7 Ultimate Edition; Windows Server 2008 R2 Standard Edition, Windows Server 2008 R2 Enterprise Edition, Windows Server 2008 R2 Datacenter Edition, Windows Server 2008 R2 Itanium Edition

Evaluation Platform: As specified in Section 1.1 of the *Microsoft Windows 7 and Microsoft Windows Server 2008 R2 Security Target, Version 1.0*

CCTL: Science Applications International Corporation

Validation Report Number: CCEVS-VR-VID10390-2010

Date Issued: 24 March 2011

Assurance Level: EAL 4 Augmented ALC_FLR.3

Protection Profile Identifier: U.S. Government Protection Profile General-Purpose Operating Systems in a Networked Environment, Version 1.0, 30 August 2010

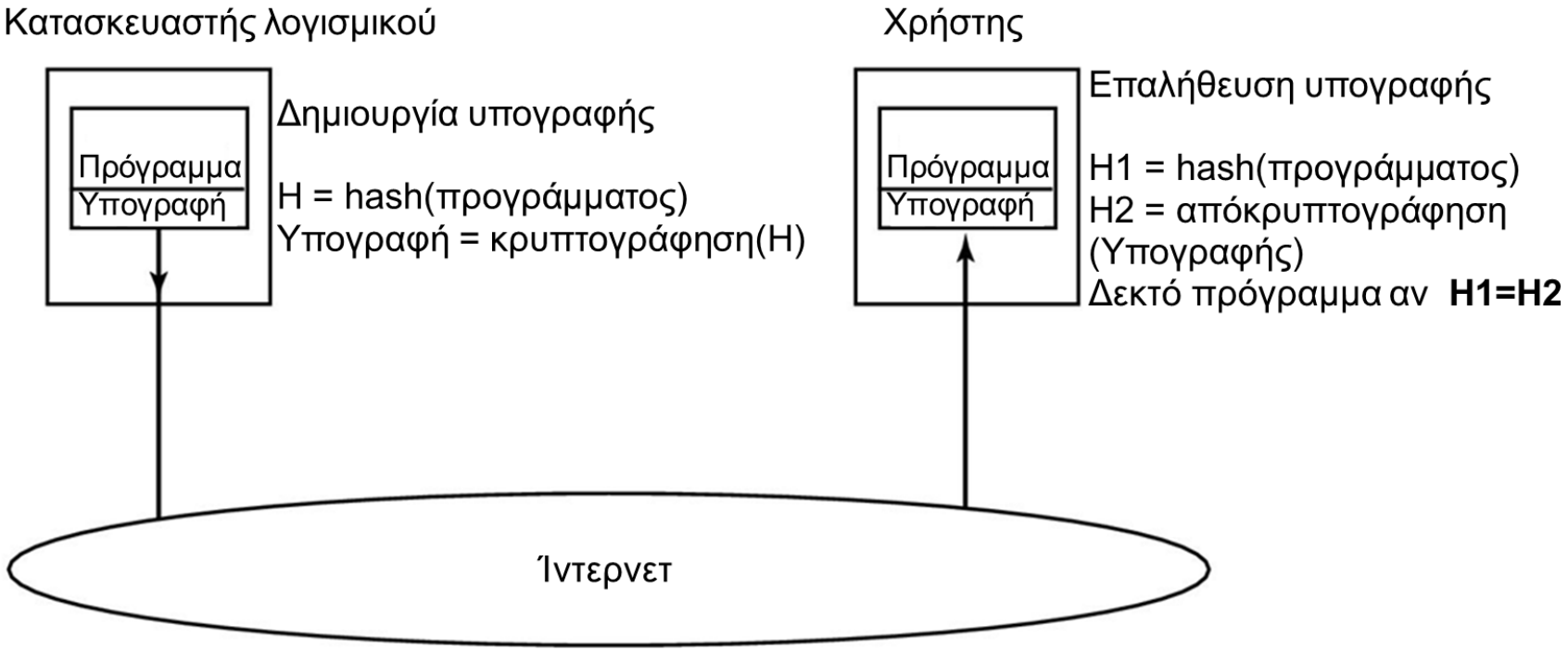
Original Signed By

Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By

Information Assurance Director
National Security Agency

Υπογραφή κώδικα (1/2)



Υπογραφή κώδικα (2/2)

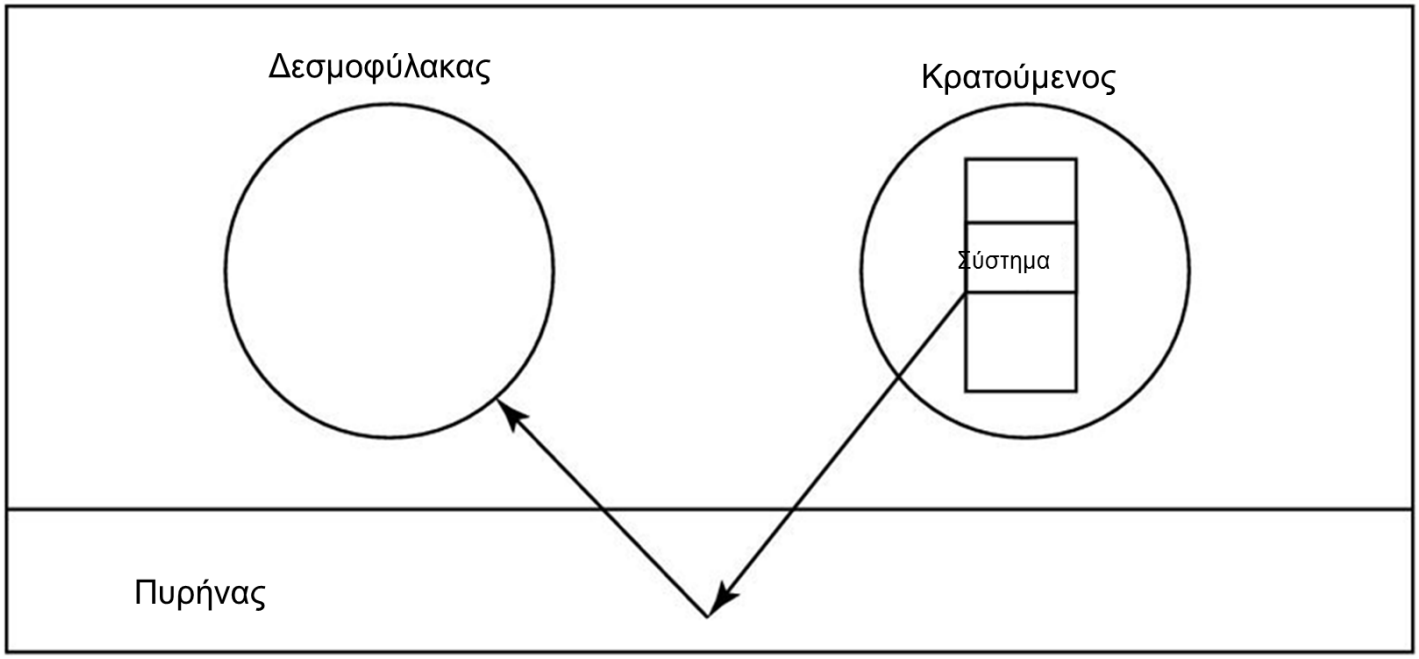
- Ο συγγραφέας τοποθετεί στο site του την ψηφιακή υπογραφή (hash) του αρχείου που διανείμει:

```
bigb5# more /usr/ports/sysutils/zeitgeist/distinfo
SHA256 (zeitgeist-0.8.2.tar.gz) = 6155611ee182f642c
SIZE (zeitgeist-0.8.2.tar.gz) = 358781
```

- Όταν κατεβάσουμε το αρχείο από το διαδίκτυο, επιβεβαιώνουμε την ψηφιακή υπογραφή:

```
bigb5# sha256 zeitgeist-0.8.2.tar.gz
SHA256 (zeitgeist-0.8.2.tar.gz) = 615561
```

Φυλακή



Η λειτουργία μιας φυλακής.

FreeBSD Jail

```
bigb5# ps axuwww | grep 'J'
root        3372  0.0  0.0  5992   572  ??  IsJ  22May12   0:00.71 /usr/sbin/syslogd -s
610         3503  0.0  0.4 163936 15368  ??  IJ   22May12  56:30.71 /usr/local/bin/freeswitch -nc -u freeswitch -g freeswitch
root        3560  0.0  0.0  6920   572  ??  IsJ  22May12   0:01.24 /usr/sbin/cron -s
root       85687  0.0  0.0  8060  1392   1  S+   11:09PM   0:00.00 grep J
bigb5#
bigb5# jls
   JID  IP Address      Hostname                      Path
     1  192.168.55.101  pbx                           /home/j/pbx
bigb5# jexec 1 ps axuw
USER         PID %CPU %MEM   VSZ   RSS  TT  STAT STARTED      TIME COMMAND
root        3372  0.0  0.0  5992   572  ??  SsJ  22May12   0:00.71 /usr/sbin/syslogd -s
freeswitch  3503  0.0  0.4 163936 15276  ??  IJ   22May12  56:30.25 /usr/local/bin/freeswitch -nc -u freeswitch -g freeswitch
root        3560  0.0  0.0  6920   572  ??  SsJ  22May12   0:01.24 /usr/sbin/cron -s
root       85666  0.0  0.0  6984  1308   1  R+J  11:08PM   0:00.00 ps axuw
bigb5#
bigb5# jexec 1 csh
pbx# ps axuw
USER         PID %CPU %MEM   VSZ   RSS  TT  STAT STARTED      TIME COMMAND
root        3372  0.0  0.0  5992   572  ??  SsJ  22May12   0:00.71 /usr/sbin/syslogd -s
freeswitch  3503  0.0  0.4 163936 15372  ??  IJ   22May12  56:30.89 /usr/local/bin/freeswitch -nc -u freeswitch -g freeswitch
root        3560  0.0  0.0  6920   572  ??  SsJ  22May12   0:01.24 /usr/sbin/cron -s
root       86455  0.0  0.1  9256  2612   1  SJ   11:10PM   0:00.01 csh
root       86459  0.0  0.0  6984  1308   1  R+J  11:10PM   0:00.00 ps axuw
pbx#
```

```
JAIL(8)                 FreeBSD System Manager's Manual                 JAIL(8)

NAME
     jail — create or modify a system jail

SYNOPSIS
     jail [-dhi] [-J jid_file] [-l -u username | -U username] [-c | -m]
          [parameter=value ...]
     jail [-hi] [-n jailname] [-J jid_file] [-s securelevel]
          [-l -u username | -U username] [path hostname [ip[,...]] command ...]
     jail [-r jail]

DESCRIPTION
     The jail utility creates a new jail or modifies an existing jail, option-
     ally imprisoning the current process (and future descendants) inside it.

     The options are as follows:
```

Για περισσότερες πληροφορίες υπάρχει το μάθημα "Ασφάλεια Υπολογιστών και Δικτύων", σε ανώτερο εξάμηνο.

Τέλος Ενότητας