ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΙΙ (Θ)

Ενότητα 5: ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΙΙ

- Νικολαΐδης Αθανάσιος
- Διδάκτορας Ανάπτυξης Τεχνικών Προστασίας Πληροφορίας Εικόνας
- ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΤΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

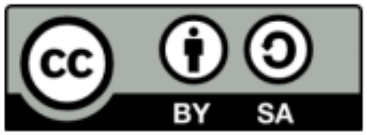
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

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 Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής 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.

Ενότητα 5

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ Ι

Νικολαΐδης Αθανάσιος
Διδάκτορας Ανάπτυξης Τεχνικών Προστασίας Πληροφορίας Εικόνας

Περιεχόμενα ενότητας

1. Ευρυζωνική Πρόσβαση ΜΕΤΑΛΛΟΥΡΓΙΚΕΣ
2. Ασύρματη Ευρυζωνική Πρόσβαση
3. Ευρυζωνικά Ασύρματα Δίκτυα
4. Ανάπτυξη της Ευρυζωνικότητας
5. Τεχνικές Προκλήσεις Ευρυζωνική Πρόσβαση
6. Τεχνικές Προκλήσεις- Ασύρματο ραδιοκυματικό κανάλι
7. Τεχνικές Προκλήσεις- Παρεμπόδιση λόγω μεγάλων εμποδίων – Διακύμανση περιβάλλουσας
8. Τεχνικές Προκλήσεις- Διασυμβολική Παρεμβολή
9. Τεχνικές Προκλήσεις-Διασπορά συχνότητας λόγω κίνησης
10. Τεχνικές Προκλήσεις- Παρεμβολή

Σκοποί ενότητας

Το πρόβλημα της ασφάλειας

- Προστασία είναι ο μηχανισμός για έλεγχο πρόσβασης προγραμμάτων, διεργασιών ή χρηστών στους πόρους ενός Η/Υ.

- Αυτό δουλεύει όσο οι χρήστες συμμορφώνονται με τις καθορισμένες πολιτικές χρήσης και διαμοιρασμού πόρων.

Το πρόβλημα της ασφάλειας

- Η ασφάλεια πρέπει να λαμβάνει υπόψη το εξωτερικό περιβάλλον του συστήματος και να το προστατεύει από:
  - Μη εξουσιοδοτημένη πρόσβαση.
  - Κακόβουλη τροποποίηση ή καταστροφή.
  - Τυχαία εισαγωγή ασυνέπειας.
  - Άρνηση υπηρεσίας.
- Ευκολότερο να προστατεύσει από τυχαία παρά από κακόβουλη κατάχρηση.

Το πρόβλημα της ασφάλειας

- Απόλυτη προστασία από κακόβουλη χρήση δεν είναι δυνατή.
- Στόχος της ασφάλειας είναι να κάνει το κόστος για τον δράστη αρκετά υψηλό ώστε να αποτρέψει προσπάθειες για μη εξουσιοδοτημένη πρόσβαση.
- Τα μέτρα ασφαλείας στη φυσική τοποθεσία όπως και η διαλογή των χρηστών είναι κρίσιμα.
- Ασφαλείς γραμμές επικοινωνίας χρειάζονται για να προστατεύσουν από υποκλοπή δεδομένων και διακοπή υπηρεσιών.
- Ασχολούμαστε με την ασφάλεια στο επίπεδο του Λ.Σ.

Ταυτοποίηση

- Η ταυτότητα του χρήστη συνήθως αποδεικνύεται μέσω *κωδικών πρόσβασης*
  - Μπορεί να συσχετίζεται με ένα αγαθό ή με διάφορα δικαιώματα πρόσβασης σε ένα αγαθό (ανάγνωση, εγγραφή, εκτέλεση)
- Οι κωδικοί πρέπει να κρατούνται μυστικοί.
  - Συχνή αλλαγή κωδικών (ηλικίωση).
  - Χρήση μη «μαντέψιμων» κωδικών (μεγαλύτεροι, κεφαλαία/πεζά)
  - Αποφυγή surfers και sniffers
  - Καταγραφή όλων των προσπαθειών πρόσβασης.
- Οι κωδικοί μπορεί επίσης να είναι κρυπτογραφημένοι ή να επιτρέπεται να χρησιμοποιηθούν μόνο μια φορά.
- Βιομετρικά στοιχεία.

Προγραμματιστικές απειλές

- ***Δούρειος Ίππος***
  - Ελεύθερο πρόγραμμα διαθέσιμο σε ανυποψίαστο χρήστη.
  - Τοποθέτηση αλλαγμένης έκδοσης προγράμματος εφαρμογής στον υπολογιστή του θύματος
  - Εξαπάτηση του χρήστη ώστε να εκτελέσει κάτι που δεν θα έπρεπε
- ***Πίσω πόρτα***
  - Συγκεκριμένο αναγνωριστικό χρήστη ή κωδικός που παρακάμπτει τις κανονικές διαδικασίες ασφάλειας.
  - Μπορεί να περιλαμβάνεται σε ένα μεταγλωττιστή. Όλοι οι αντικείμενοι κώδικες θα έχουν την πίσω πόρτα. Δύσκολο να ανιχνευθούν.

Προγραμματιστικές απειλές

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v) break;
}
execute_shell(name);
```

(a)

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v || strcmp(name, "zzzzz") == 0) break;
}
execute_shell(name);
```

(b)

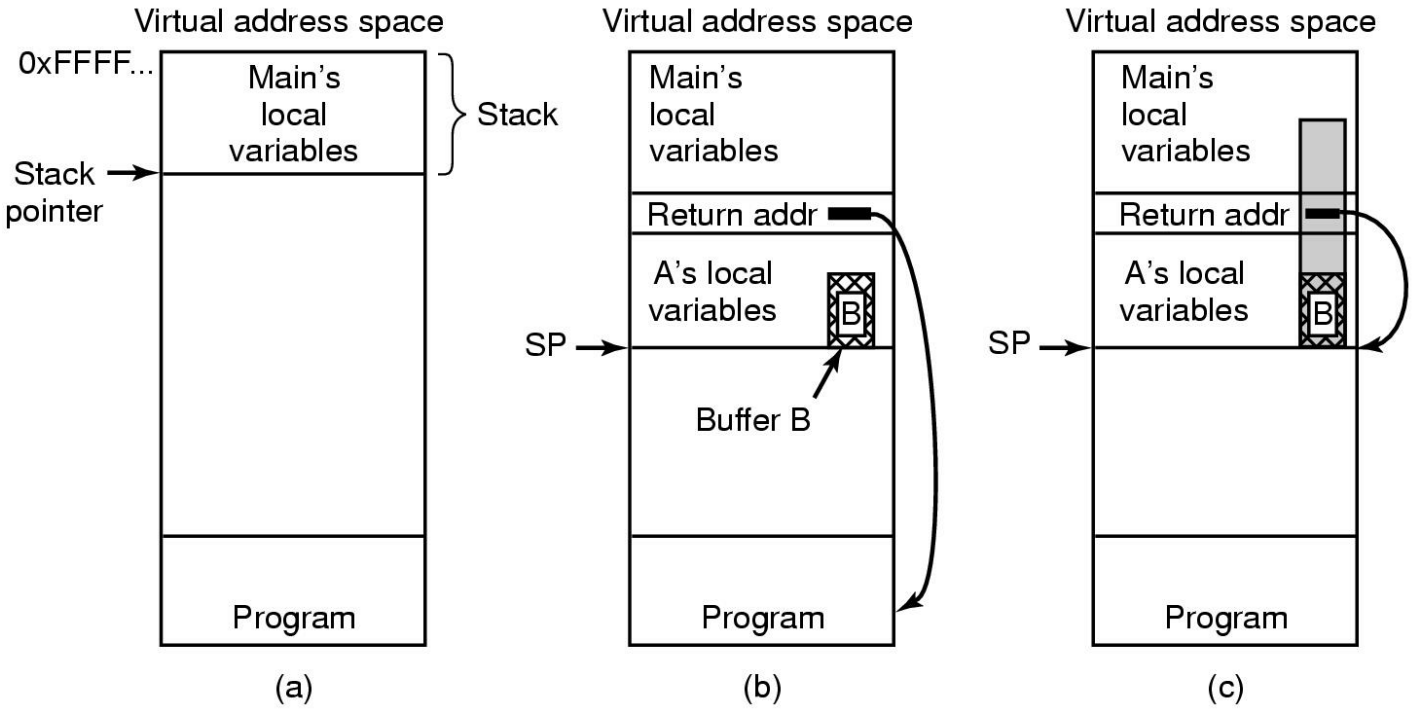
(a) Κανονικός κώδικας προτροπής εισόδου.
(b) Κώδικας με πίσω πόρτα.

Προγραμματιστικές απειλές

- ***Υπερχείλιση στοίβας και απομονωτή***
  - Εκμεταλλεύεται ένα σφάλμα σε πρόγραμμα (υπερχείλιση της στοίβας ή του απομονωτή μνήμης) για να επιτύχει κλιμάκωση δικαιωμάτων.
  - Ο εισβολέας στέλνει περισσότερα δεδομένα από όσα περιμένει το πρόγραμμα μέχρι να τα γράψει στη στοίβα
    - Επικαλύπτει την τρέχουσα διεύθυνση επιστροφής με τη διεύθυνση του κώδικα υπερχείλισης και εκτελεί τον κώδικα
    - Παράδειγμα: φόρμα ιστοσελίδας περιμένει ένα όνομα χρήστη, ο εισβολέας προσθέτει στο τέλος επιπλέον χαρακτήρες για να υπερχειλίσει τον απομονωτή, στέλνει τη διεύθυνση επιστροφής για να φορτωθεί στη στοίβα και τον κώδικα προς εκτέλεση. Όταν επιστρέφει η ρουτίνα ανάγνωσης του απομονωτή, τρέχει ο κώδικας του εισβολέα.
    - Ο επεξεργαστής SPARC της Sun και το Solaris έχουν ένα χαρακτηριστικό που απαγορεύει την εκτέλεση κώδικα σε ένα τμήμα στοίβας της μνήμης.

Προγραμματιστικές απειλές

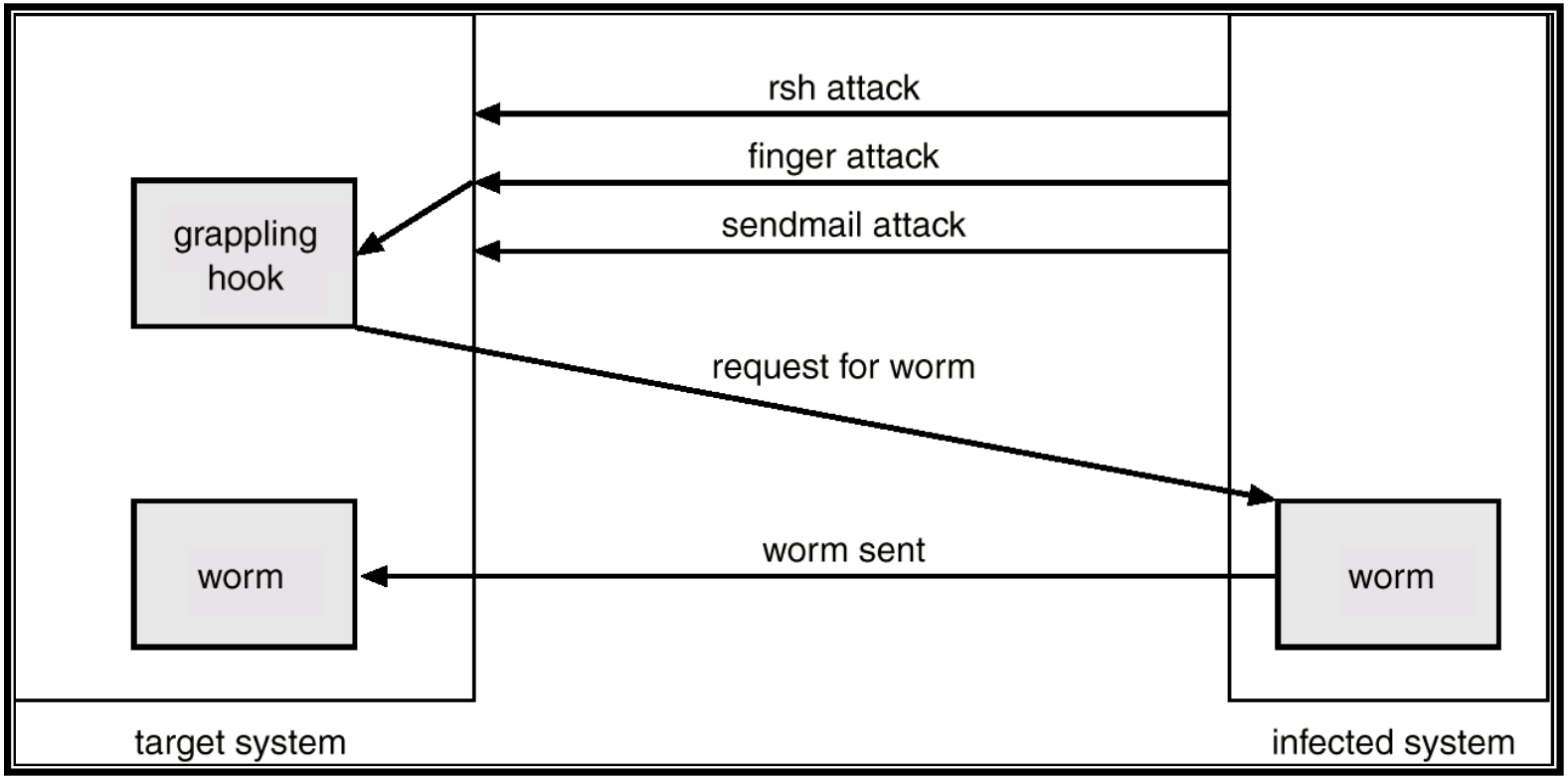
- ***Υπερχείλιση στοίβας και απομονωτή***



Απειλές συστήματος

- Τα Λ.Σ. παρέχουν ένα μέσο ώστε μια διεργασία να «γεννά» άλλες διεργασίες. Αυτό μπορεί να οδηγήσει σε κατάχρηση των αγαθών του Λ.Σ. και των αρχείων χρηστών.
- ***Σκουλήκια*** – χρησιμοποιούν μηχανισμούς αναπαραγωγής. Τελείως ανεξάρτητα προγράμματα.
- Σκουλήκι διαδικτύου
  - Εκμεταλλεύτηκε δικτυακά χαρακτηριστικά του UNIX (απομακρυσμένη πρόσβαση) και σφάλματα στα προγράμματα finger και sendmail.
  - Το πρόγραμμα «γάντζος αρπαγής» φόρτωνε το κυρίως πρόγραμμα του σκουληκιού.

Το σκουλήκι διαδικτύου του Morris



Απειλές συστήματος

- ***Ιοί*** – τμήμα κώδικα ενσωματωμένο σε νόμιμο πρόγραμμα.
  - Κυρίως αφορούν μικροϋπολογιστές. Οι πολυχρηστικοί υπολογιστές δεν είναι επιρρεπείς γιατί τα εκτελέσιμα προστατεύονται από γράψιμο από το Λ.Σ.
  - Εξαπλώνονται κατεβάζοντας μολυσμένα προγράμματα από το διαδίκτυο ή ανταλλάσσοντας φορητά μέσα αποθήκευσης. Επίσης, με μακροεντολές σε αρχεία του MS Office.
  - Καλύτερη προστασία: ασφαλής χρήση υπολογιστή (μορφή RTF, σφραγισμένο λογισμικό, όχι άνοιγμα επισυνάψεων e-mail που περιέχουν εκτελέσιμο κώδικα).

- ***Άρνηση υπηρεσίας***
  - Υπερφόρτωση υπολογιστή-στόχου αποτρέποντάς τον να κάνει ουσιαστική δουλειά.
    - Αρχικοποίηση συνδέσεων TCP/IP χωρίς να ολοκληρώνονται.

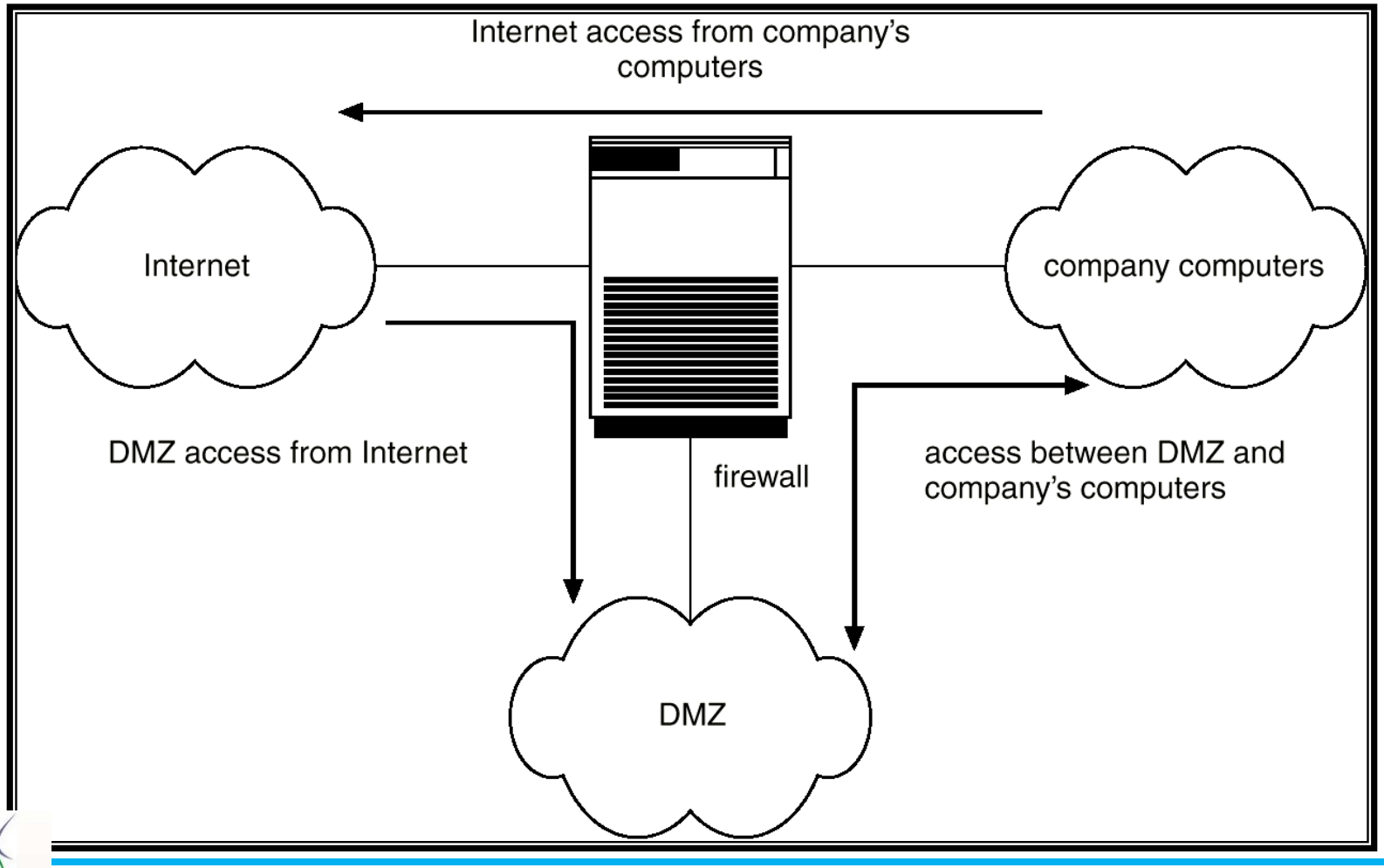
Παρακολούθηση απειλών

- Έλεγξε για ύποπτη δραστηριότητα – π.χ. πολλές αποτυχημένες προσπάθειες για εισαγωγή κωδικού.
- Καταγραφή ελέγχου – καταγράφει ώρα, χρήστη και τύπο προσβάσεων σε ένα αντικείμενο. Χρήσιμο για ανάνηψη από παραβίαση.
- Σάρωσε το σύστημα περιοδικά για οπές ασφάλειας (όποτε υπάρχει χαμηλή χρήση ΚΜΕ).
- Έλεγξε για:
  - Μικρούς ή εύκολους να μαντέψεις κωδικούς
  - Μη εξουσιοδοτημένα προγράμματα με set-uid.
  - Μη εξουσιοδοτημένα προγράμματα σε καταλόγους συστήματος
  - Διεργασίες που τρέχουν περισσότερο από το αναμενόμενο
  - Μη κατάλληλη προστασία καταλόγων
  - Μη κατάλληλη προστασία σε αρχεία δεδομένων συστήματος
  - Επικίνδυνες εγγραφές στο μονοπάτι αναζήτησης προγράμματος (δούρειος ίππος)
  - Αλλαγές σε προγράμματα συστήματος: παρακολούθηση τιμών αθροισμάτων ελέγχου

Τείχος προστασίας

- Είναι υπολογιστής ή δρομολογητής που τοποθετείται ανάμεσα σε έμπιστους και μη έμπιστους κόμβους.
- Περιορίζει την δικτυακή πρόσβαση ανάμεσα σε αυτά τα δύο πεδία ασφαλείας.
  - Περιορίζει τις συνδέσεις βάσει της διεύθυνσης πηγής ή προορισμού ή της κατεύθυνσης της σύνδεσης
- Αποστρατικοποιημένη ζώνη (DMZ): είναι ένα ημιασφαλές και ημιέμπιστο δίκτυο.

Ασφάλεια δικτύου με διαχωρισμό πεδίων μέσω τείχους προστασίας



Ανίχνευση εισβολής

- Ανίχνευσε τις προσπάθειες εισβολής στον Η/Υ
  - Ανίχνευση βάσει υπογραφής: καθορισμένα πρότυπα δικτυακής κίνησης
    - Πολλαπλές αποτυχημένες προσπάθειες εισόδου σε λογαριασμό
    - Ανιχνεύει βάσει γνωστών υπογραφών
  - Ανίχνευση βάσει ανωμαλίας
    - Ασυνήθιστη ώρα εισόδου χρήστη
    - Πιθανή χρήση υπερχείλισης απομονωτή
    - Δυσκολία – ανιχνεύει νέες επιθέσεις αλλά πώς αποφασίζεις τι είναι «κανονικό»;
- Μέθοδοι ανίχνευσης:
  - Επεξεργασία διαδρομών ελέγχου – αντιστοίχισε συμβάντα σχετικά με ασφάλεια με υπογραφές επιθέσεων ή ανάλυσέ τα ως προς ανώμαλη συμπεριφορά
  - Εργαλείο tripwire για έλεγχο ακεραιότητας συστήματος αρχείων
    - Λογισμικό για UNIX που ελέγχει αν έχουν αλλάξει συγκεκριμένα αρχεία ή κατάλογοι
    - Παρακολούθηση κλήσεων συστήματος – για να ανιχνευθεί αν μια διεργασία εκτρέπεται από την αναμενόμενη συμπεριφορά
      - Μπορεί να χρησιμοποιηθεί για ανίχνευση εκμετάλλευσης υπερχείλισης απομονωτή

Πίνακας που προκύπτει από ακολουθίες κλήσεων συστήματος

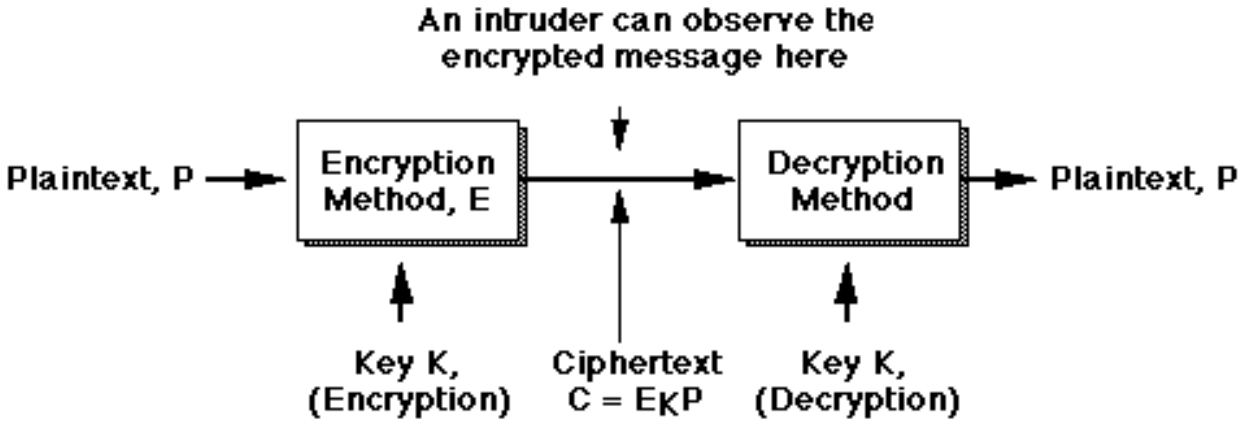
system call	distance = 1	distance = 2	distance = 3
open	read getrlimit	mmap	mmap close
read	mmap	mmap	open
mmap	mmap open close	open getrlimit	getrlimit mmap
getrlimit	mmap	close	
close			

- Η ακολουθία [open, read, mmap, open, open, getrlimit, mmap, close] μπορεί να είναι εισβολή

Κρυπτογραφία

- Εξάλειψε την ανάγκη να εμπιστευτείς το δίκτυο (θεωρείται ανέφικτο να υπάρξει έμπιστο δίκτυο)
- Ένα μήνυμα για κρυπτογράφηση (***απλό κείμενο***) μετασχηματίζεται με χρήση μιας συνάρτησης (ή αλγόριθμου) παραμετροποιημένης από ένα ***κλειδί***. Παραδοσιακά, το ίδιο κλειδί χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση.
- Η ασφάλεια του ***κρυπτοκείμενου*** εξαρτάται από:
  - Τη φύση της μεθόδου κρυπτογράφησης
  - Τη μυστικότητα του κλειδιού και το μέγεθός του
- Επιτρέπει στον παραλήπτη του μηνύματος να επαληθεύσει ότι δημιουργήθηκε από έναν Η/Υ που κατέχει συγκεκριμένο κλειδί.
- Ένας αποστολέας μπορεί να μεταδώσει ένα μήνυμα έτσι ώστε μόνο ένας υπολογιστής με συγκεκριμένο κλειδί μπορεί να το αποκωδικοποιήσει

Κρυπτογραφία



Κρυπτογραφία

- Ιδιότητες καλής τεχνικής:
  - Απλότητα χρήσης από εξουσιοδοτημένους χρήστες
  - Δε βασιζόμαστε στη μυστικότητα του αλγορίθμου αλλά του κλειδιού
  - Δύσκολο για εισβολέα να καθορίσει το κλειδί.
- DES (Data Encryption Standard): αντικαθιστά χαρακτήρες και τους αναδιατάσσει βάσει ενός κλειδιού που παρέχεται στους εξουσιοδοτημένους χρήστες με ασφαλή μηχανισμό.
- Πρόβλημα διανομής κλειδιού.
- Η κρυπτογραφία δημόσιου κλειδιού βασίζεται στο ότι κάθε χρήστης έχει δυο κλειδιά:
  - Δημόσιο κλειδί – δημοσιοποιημένο κλειδί για κρυπτογράφηση δεδομένων.
  - Ιδιωτικό κλειδί – γνωστό μόνο σε συγκεκριμένο χρήστη για αποκρυπτογράφηση δεδομένων.

Κρυπτογραφία

- Το κλειδί κρυπτογράφησης πρέπει να μπορεί να δημοσιοποιηθεί χωρίς να είναι εύκολο να υποτεθεί το κλειδί αποκρυπτογράφησης.
  - Εύκολα ελέγχεται αν ένας αριθμός είναι πρώτος αλλά δύσκολα βρίσκονται οι πρώτοι παράγοντες
- Η κρυπτογραφία δημόσιου κλειδιού είναι πολύ πιο αργή από αυτή απλού κλειδιού (και είναι δύσκολο να ελεγχθεί η γνησιότητα δημόσιων κλειδιών, παλιών κλειδιών, επικίνδυνων κλειδιών κλπ.).

Κρυπτογραφία

- Κάθε μέλος που εμπλέκεται δημιουργεί ένα ζεύγος κλειδιών.
- Κάθε μέρος δημοσιοποιεί το δημόσιο κλειδί του. Αυτό γνωστοποιείται σε όλους τους πιθανούς εταίρους επικοινωνίας.
- Κάθε μέρος ασφαλίζει το ιδιωτικό του κλειδί, το οποίο πρέπει να παραμείνει μυστικό.
- Υποθέτοντας ότι ο Α θέλει να στείλει ένα μήνυμα στον Β, ο Α κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί του Β.
- Ο Β μπορεί να αποκρυπτογραφήσει το μήνυμα χρησιμοποιώντας το ιδιωτικό του κλειδί. Αφού κανείς άλλος δεν ξέρει το ιδιωτικό κλειδί του Β, αυτό είναι απολύτως ασφαλές – κανείς άλλος δε μπορεί να το αποκρυπτογραφήσει.

Τέλος Ενότητας