Cryptography and Network Security Chapter 21

Fifth Edition

by William Stallings

Chapter 21 – Malicious Software

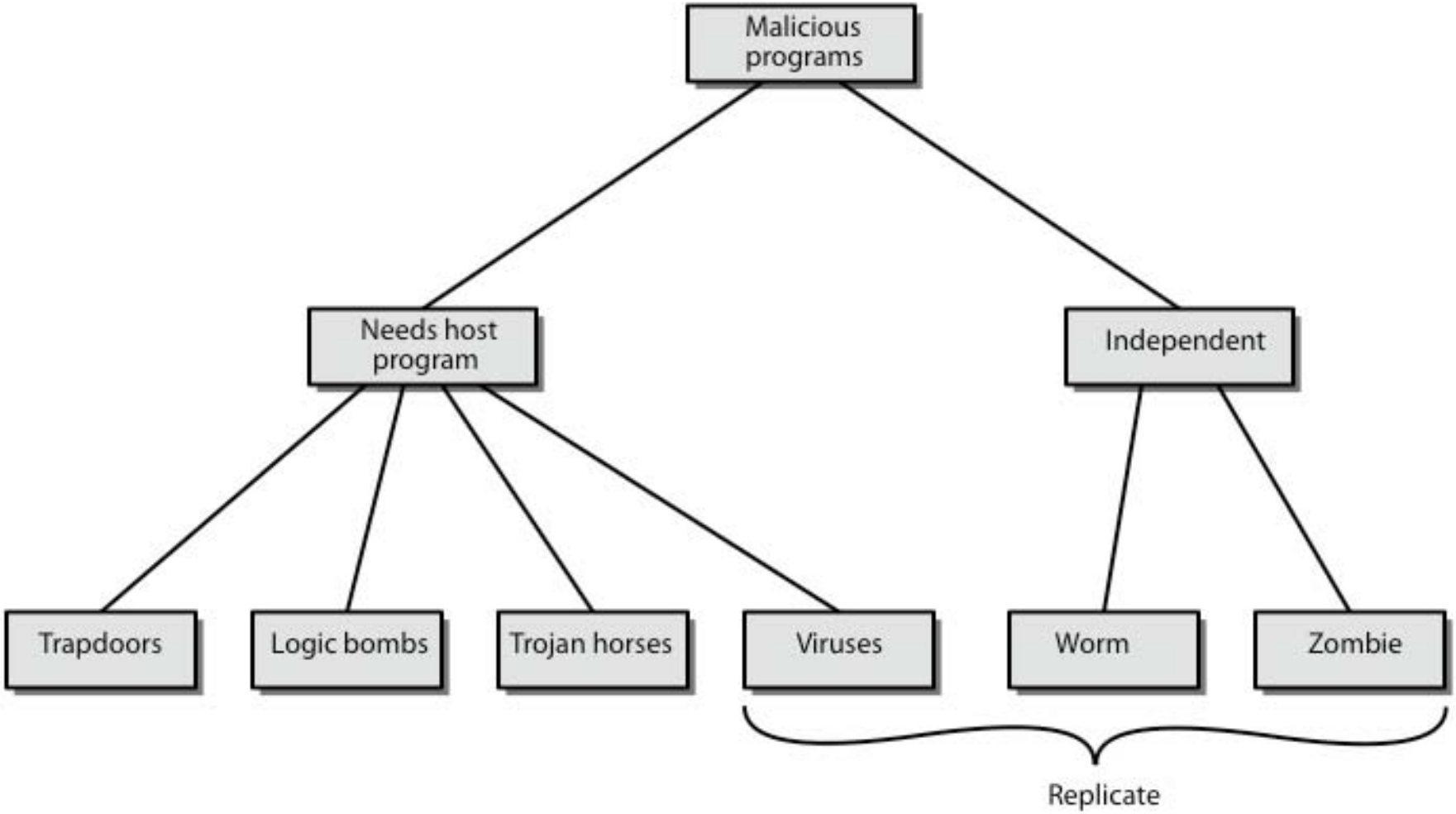
What is the concept of defense: The parrying of a blow. What is its characteristic feature: Awaiting the blow.

—*On War*, Carl Von Clausewitz

Ιοι και άλλο κακοβουλο Λογισμικο

- Οι ιοι των υπολογιστων εχουν γνωρισει αρκετη δημοσιοτητα τα τελευταια χρονια
- Είναι ενα μονο μελος της οικογενειας του κακοβουλου λογισμικου
- Τα αποτελεσματα τους είναι συνηθως εμφανη και γι'αυτο εχουν ισως μεγαλυτερη δημοσιοτητα απ'οση τους αξιζει
- Αποτελουν ωστοσο ενα υπαρκτο προβλημα

Κακοβουλο Λογισμικο



Κερκοπορτα (Backdoor ή Trapdoor)

- Μυστικο σημειο εισοδου σε ένα προγραμμα
- Επιτρεπει σε αυτους που το γνωριζουν να αποκτουν προσβαση παρακαμπτοντας τη συνηθη διαδικασια ασφαλειας
- Χρησιμοποιουνται συχνα από αυτους που αναπτυσσουν το λογισμικο
- Είναι όμως μια απειλη όταν παραμενουν στα προγραμματα κανονικης παραγωγης γιατι μπορει να τα εκμεταλλευτουν οι επιτιθεμενοι
- Ειναι πολυ δυσκολο να εντοπιστουν και να μπλοκαριστουν απο τα λειτουργικα συστηματα
- Απαιτουν καλη αναπτυξη και ενημερωση λογισμικου

Λογική Βομβα (Logic Bomb)

- Ενας από του παλιοτερους τυπους κακοβουλου λογισμικου
- Κωδικας ενσωματωμενος σε κανονικο προγραμμα
- Ενεργοποιειται οταν πληρουνται συγκεκριμενες συνθηκες
  - Π.χ. παρουσια ή απουσια καποιου αρχειου
  - Συγκεκριμενη ημερομηνια
  - Συγκεκριμενος χρηστης
- Οταν ενεργοποιουνται συνηθως κανουν ζημια στο συστημα
  - Τροποποιουν/Διαγραφουν αρχεια/δισκους, σταματουν το μηχανημα, κλπ

Δουρειος Ιππος

- Προγραμμα με κρυμμενες παρενεργειες
- Συνηθως είναι υπερβολικα εκλυστικο
  - Π.χ. game, s/w upgrade, etc
- Οταν τρεχει εκτελει καποιες προσθετες λειτουργιες
  - Επιτρεπει στον επιτιθεμενο να αποκτησει εμμεσα προσβαση που αμεσα δεν θα ειχε
- Συχνα χρησιμοποιειται για να διαδωσει έναν ιο ή ένα σκουληκι ή για να εγκαταστησει μια κερκοπορτα
- Η απλα για να καταστρεψει δεδομενα

Ζομπι

- Προγραμμα που αναλαμβανει κρυφα τον ελεγχο ενος αλλου υπολογιστη που είναι συνδεδεμενος στο Internet
- Στη συνεχεια χρησιμοποιει τον υπολογιστη για να εξαπολυσει επιθεσεις των οποιων η πραγματικη προελευση θα ειναι δυσκολο να εντοπιστει
- Χρησιμοποιουνται συνηθως σε επιθεσεις DoS

Κινητος Κωδικας

- Προγραμμα/script/macro που τρεχει χωρις αλλαγη:
  - σε ετερογενη συλλογη απο πλατφορμες
  - σε μια ετερογενη συλλογη (Windows)
- Μεταδιδεται απο το μακρυνο συστημα οταν εκτελειται στο τοπικο συστημα
- Συχνα για να μολυνει το συστημα με ιο, σκουληκι ή Δουρειο ιππο
- Ή για να εκτελεσει δικες του επιβλαβεις εμεργειες
  - Μη εξουσιοδοτημενη προσβαση, root compromise

Κακοβουλο Λογισμικο Πολλαπλης Απειλης

- Το κακοβουλο λογισμικο μπορει να λειτουργει με πολλους τροπους
- Ο πολυμερης ιος (multipartite virus) μολυνει με πολλαπλους τροπους
  - Π.χ. πολλαπλους τυπους αρχειων
- Η μεικτη επιθεση (blended attack) χρησιμοποιει πολλαπλες μεθοδους για μολυνση ή μεταδοση
  - Για να μεχιστοποιησει την ταχυτητα και τη σοβαροτητα της μολυνσης
  - Μπορει να περιλαμβανει πολλαπλους τυπους κακοβουλου λογισμικου
  - π.χ. το Nimda εχει κωδικα worm, virus, mobile code
  - Μπορει επισης να χρησιμοποιει Instant Messages & P2P

Ιοι

- Κομματια software που μολυνουν προγραμματα
  - Τα τροποποιουν και ενσωματωνουν σε αυτά ένα αντιγραφο του ιου
  - Ετσι εκτελειται μυστικα ο κωδικας του ιου, όταν τρεχει το προγραμμα που εχει μολυνθει
- Είναι ειδικα για συγκεκριμενα λειτουργικα συστηματα και hardware
  - Εκμεταλλευονται τις λεπτομερειες τους και τις αδυναμιες τους
- Ενας τυπικος ιος περναει από τις εξης φασεις:
  - Σε υπνωση (dormant)
  - Διαδοση (propagation)
  - Ενεργοποιηση (triggering)
  - Εκτελεση (execution)

Δομη του Ιου

- Συνιστωσες:
  - Μηχανισμος μολυνσης – επιτρεπει την αναπαραγωγη
  - Ενεργοποιηση – γεγονος που κανει το φορτιο (payload) του ιου να ενεργοποιηθει
  - Φορτιο – αυτό που κανει ο ιος. Κακοβουλο ή καλοηθες
- Προτασσομενος (prepended) / postpended / ενσωματωμενος
- Όταν το μολυσμενο προγραμμα καλειται, εκτελει τον κωδικα του ιου, και στη συνεχεια τον κανονικο κωδικα του προγραμματος
- Μπορουμε ειτε να εμποδισουμε την αρχικη μολυνση (δυσκολο)
- Ή τη διαδοση (με ελεγχο προσβασης)

Δομη του Ιου

```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
          then goto loop
          else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

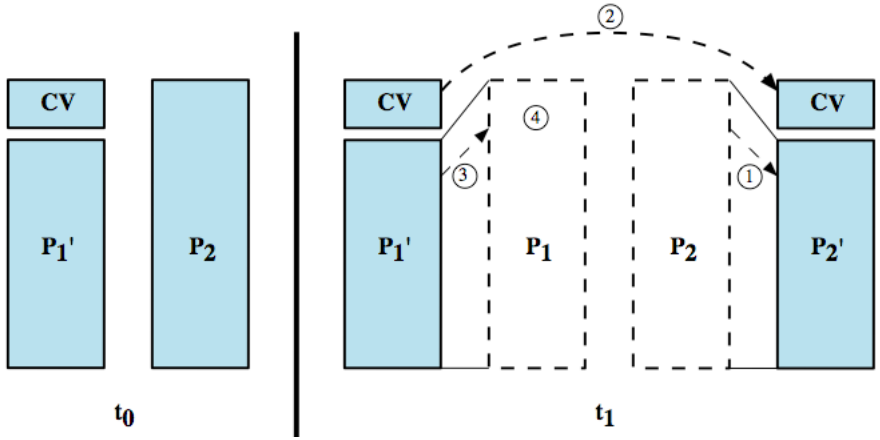
Ιος συμπιεσης

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
          {loop:
               file := get-random-executable-file;
          if (first-line-of-file = 01234567) then goto loop;
        (1)    compress file;
        (2)    prepend CV to file;
        }

main:   main-program :=
          {if ask-permission then infect-executable;
        (3)    uncompress rest-of-file;
        (4)    run uncompressed file;}
        }
```



Καταταξη Ιου

- Ιος τομεα εκκινησης (boot sector)
- Μολυντης αρχειων (file infector)
- Ιος Μακροεντολων (macro virus)
- Κρυπτογραφημενος ιος (encrypted virus)
- Αορατος ιος (stealth virus)
- Πολυμορφικος ιος (polymorphic virus)
- Μεταμορφικος ιος (metamorphic virus)

Ιος Μακροεντολων (Macro Virus)

- Οι ιοι αυτης της κατηγοριας εγιναν πολυ διαδεδομενοι στα μεσα του 1990s επειδη ειναι
  - Ανεξαρτητοι από πλατφορμα
  - Μολυνουν κειμενα (documents)
  - Διαδιδονται ευκολα
- Εκμεταλλευεται τις δυνατοτητες του Office να τρεχει μακροεντολες
  - Εκτελεσιμο προγραμμα, ενσωματωμενο στα αρχεια doc του Office
  - Συχνα είναι γραμμενο σε μια μορφη Basic
- Πιο προσφατες εκδοσεις περιλαμβανουν προστασια
- Αναγνωριζονται από πολλα αντι-ιικα προγραμματα

Ιοι E-Mail

- Εχουν αναπτυχθει πιο προσφατα
- Π.χ. ο ιος «Melissa»
  - Εκμεταλλευεται ενα MS Word macro σε επισυναπτομενο στο e-mail αρχειο doc
  - Αν το attachment ανοιχτει, το macro ενεργοποιειται
  - Στελνει email σε ολους τους χρηστες που περιεχει η address list
  - Και κανει τοπικη ζημια
- Στη συνεχεια εμφανιστηκαν versions που ενεργοποιουνται και μονο με την αναγνωση του email
- Ετσι διαδιδεται πολυ γρηγοροτερα

Αντιμετρα για τους Ιους

- Προληψη – ιδανικη λυση αλλα δυσκολη
- Το πιο ρεαλιστικο είναι να επιδιωξουμε:
  - Ανιχνευση (detection)
  - Προσδιορισμο (identification)
  - Απομακρυνση (removal)
- Αν ανιχνευτει αλλα δεν μπορουμε να τον προσδιορισουμε ή να τον απομακρυνουμε, τοτε ειμαστε υποχρεωμενοι να διαγραψουμε και να αντικαταστησουμε το μολυσμενο προγραμμα

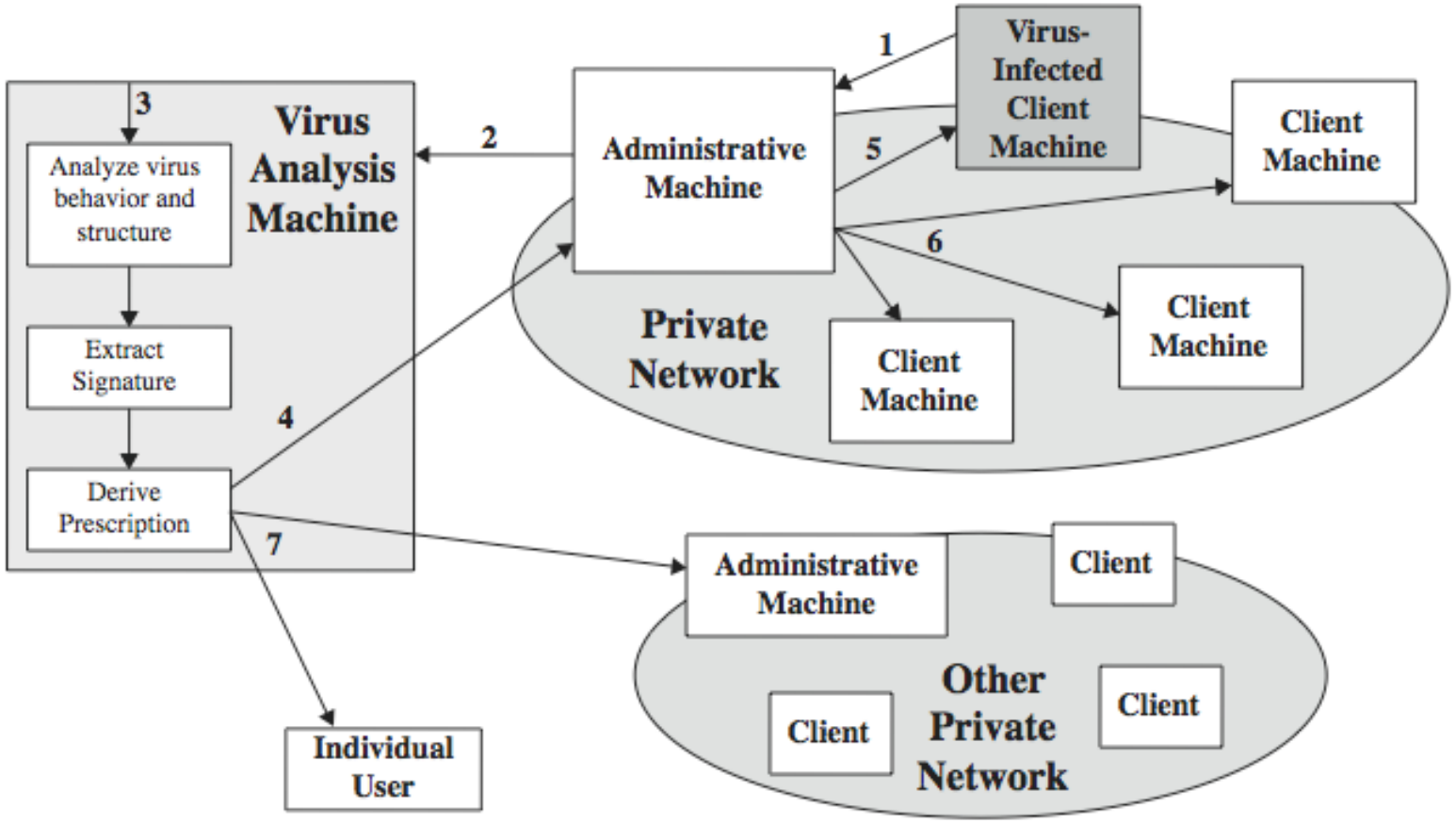
Η εξελιξη των Αντι-ιικων

- Η τεχνολογιες τοσο των ιων, οσο και των αντι-ιικων εχει εξελιχθει
- Οι πρωτοι ιοι ηταν απλοι στον κωδικα, ηταν ευκολα ανιχνευσιμοι, και ηταν ευκολο να διαγραφουν
- Οσο γινονται πιο συνθετοι, τοσο πιο συνθετα πρεπει να είναι και τα αντιμετρα για την αντιμετωπιση τους
- Γενιες αντιμετρων:
  - πρωτη - signature scanners
  - δευτερη - heuristics
  - τριτη - identify actions
  - τεταρτη - combination packages

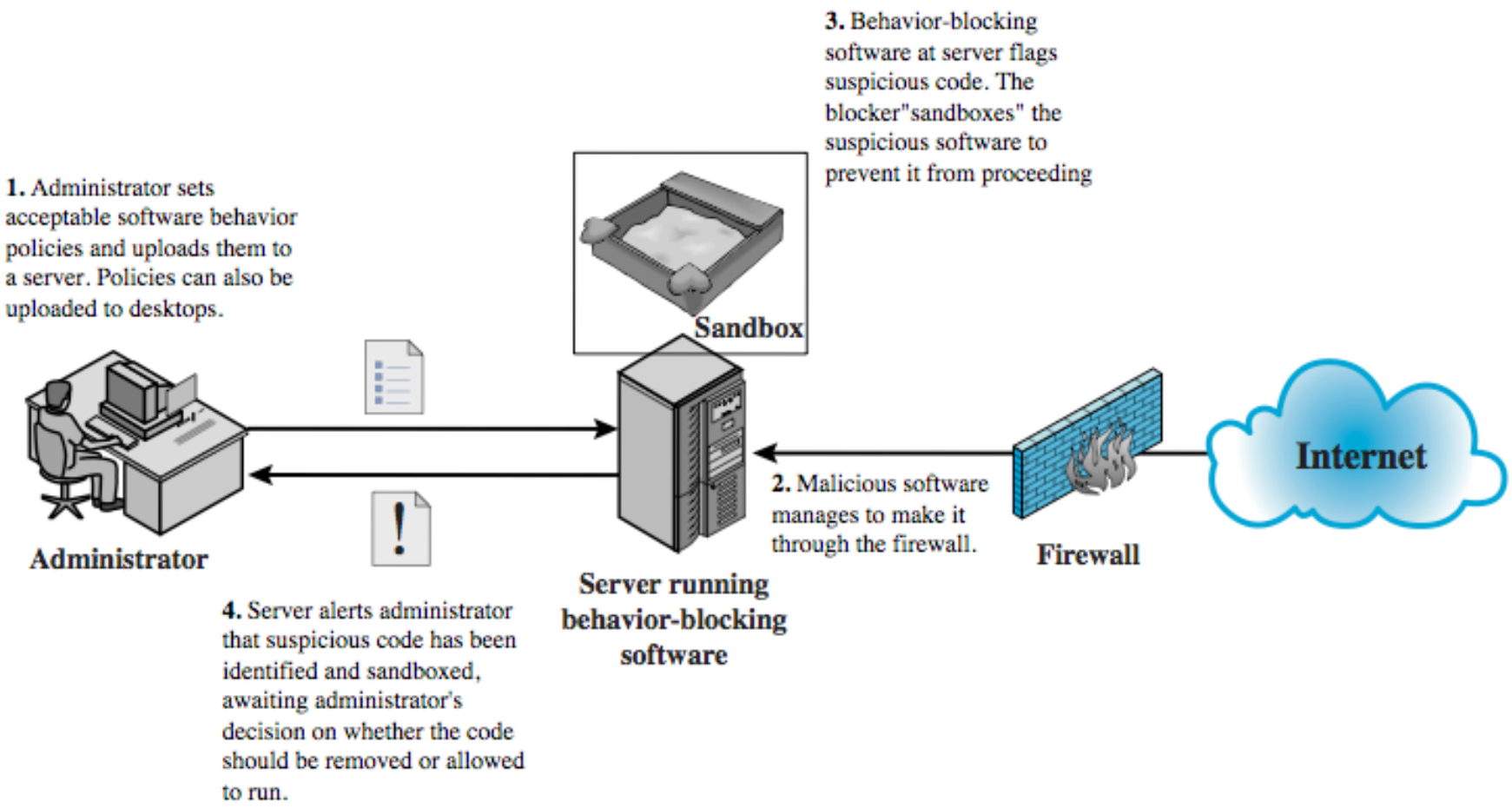
Γενικη Αποκρυπτογραφηση (Generic Decryption, GD)

- Τρεχει εκτελεσιμα αρχεια μεσω του GD scanner:
  - **CPU emulator** μεταφραζει (interpret) εντολες
  - **Σαρωτης ιων** που ελεγχει για υπογραφες γνωστων ιων
  - **Τμημα ελεγχου emulation** για τον ελεγχο της διαδικασιας
- Αφηνει τον ιο να αποκρυπτογραφηθει στον interpreter
- Περιοδικα σκανναρει για υπογραφες ιων
- Το προβλημα ειναι οτι παιρνει χρονο για interpretation και σκαναρισμα
  - Υπαρχει tradeoff αναμεσα στην πιθανοτητα ανιχνευσης και στη χρονικη καθυστερηση

Digital Immune System



Behavior-Blocking Software



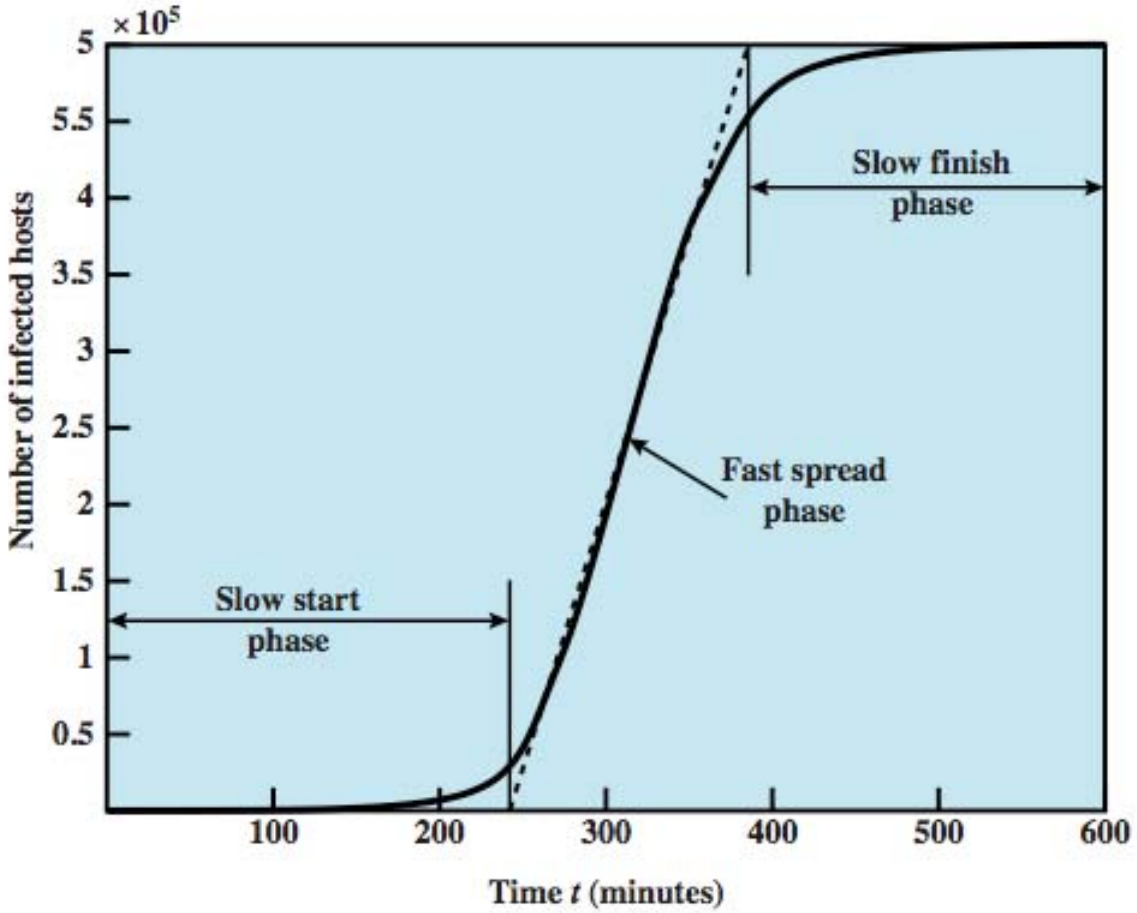
Σκουληκια (Worms)

- Αναπαραγομενο προγραμμα που αναπαραγεται μεσω του δικτυου
  - Χρησιμοποιωντας email, remote exec, remote login
- Περναει από φασεις όπως ο ιος:
  - Υπνωσης, διαδοσης, ενεργοποιησης, εκτελεσης
  - Φαση διαδοσης (propagation phase): αναζητει αλλα συστηματα, συνδεεται σε αυτά, αντιγραφει τον εαυτο του σε αυτά και και τρεχει
- Μπορει να μεταμφιεστει σε διεργασια του συστηματος

Morris Worm

- Ένα από τα καλυτερα γνωστα σκουληκια
- Δημιουργηθηκε από τον Robert Morris το 1988
- Διενεργει διαφορες επιθεσεις σε συστηματα UNIX
  - «Σπαζει» το password file και χρησιμοποιει login/password για να μπει σε αλλα συστηματα
  - Εκμεταλλευεται ένα bug στο πρωτοκολλο finger
  - Επισης, ένα bug στο sendmail
- Αν επιτυχει, εχει remote shell access
  - Στελνει προγραμμα bootstrap για να κοπιαρει το worm

Μοντελο διαδοσης Worm



Προσφατες Επιθεσεις Σκουληκιων

- Code Red
  - July 2001 exploiting MS IIS bug
  - probes random IP address, does DDoS attack
- Code Red II variant includes backdoor
- SQL Slammer
  - early 2003, attacks MS SQL Server
- Mydoom
  - mass-mailing e-mail worm that appeared in 2004
  - installed remote access backdoor in infected systems
- Warezov οικογενεις σκουληκιων
  - scan for e-mail addresses, send in attachment

Τεχνολογια Σκουληκιων (Worm Technology)

- Πολυπλατφορμικα (multiplatform)
- Πολλαπλης εκμεταλλευσης (multi-exploit)
- Πολυ γρηγορη εξαπλωση (ultrafast spreading)
- Πολυμορφικα (Polymorphic)
- Μεταμορφικα (Metamorphic)
- Οχηματα μεταφορας (transport vehicles)
- Εκμεταλλευση την «ημερα μηδεν» (zero-day exploit)

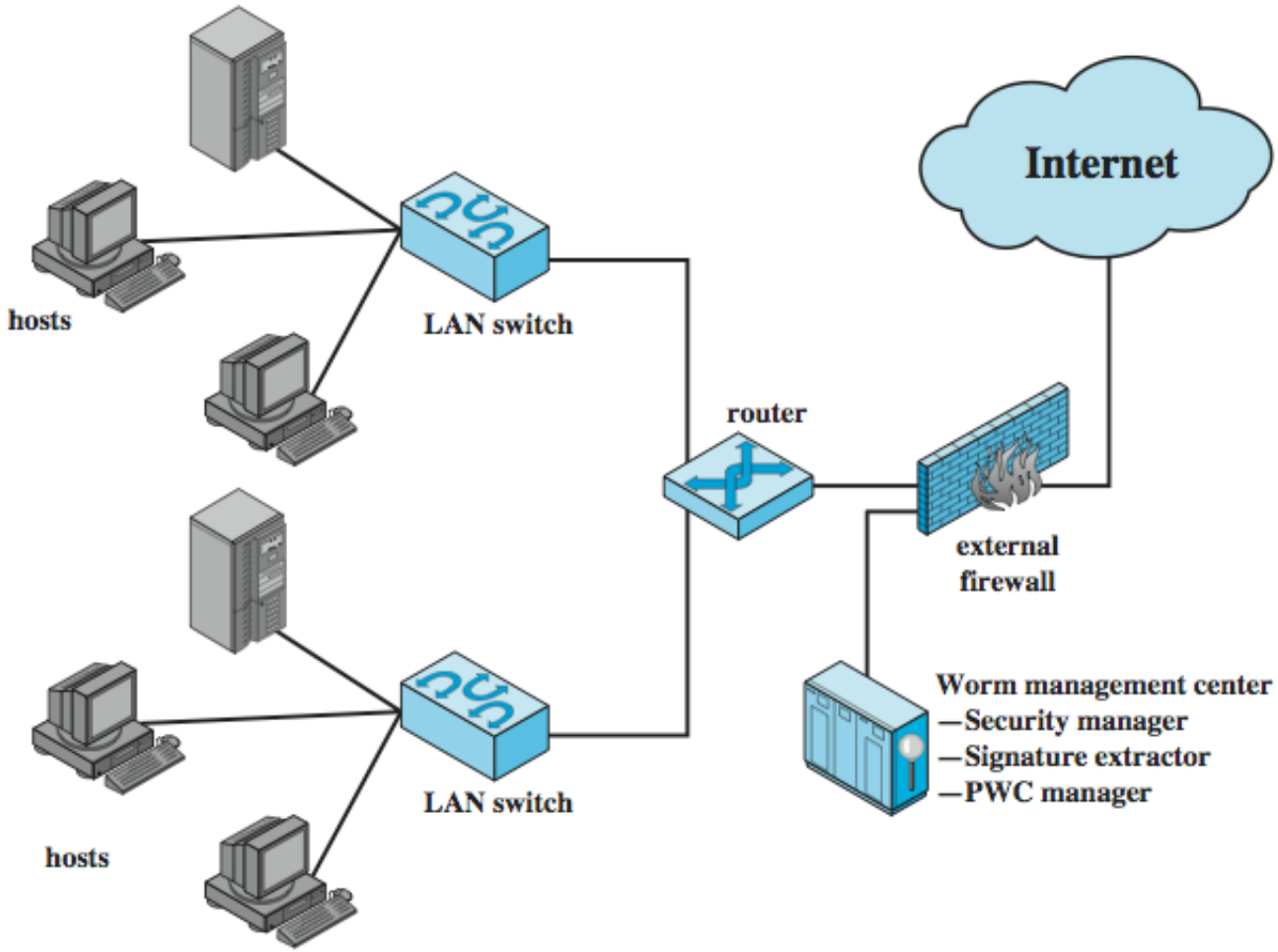
Σκουληκια Κινητων Τηλεφωνων

- Πρωτοεμφανιστηκαν σε κινητα τηλεφωνα το 2004
  - Στοχευουν σε smartphone που μπορουν να εγκαθιστουν s/w
- Επικοινωνουν μεσω Bluetooth ή MMS
- Απενεργοποιουν το τηλεφωνο, διαγραφουν δεδομενα στο τηλεφωνο, η στελνουν premium-priced messages
- Το CommWarrior, δημιουργηθηκε το 2005
  - Αναπαραγεται μεσω Bluetooth σε κοντινα τηλεφωνα
  - Και μεσω MMS χρησιμοποιωντας αριθμους που βρισκει στο ευρετηριο

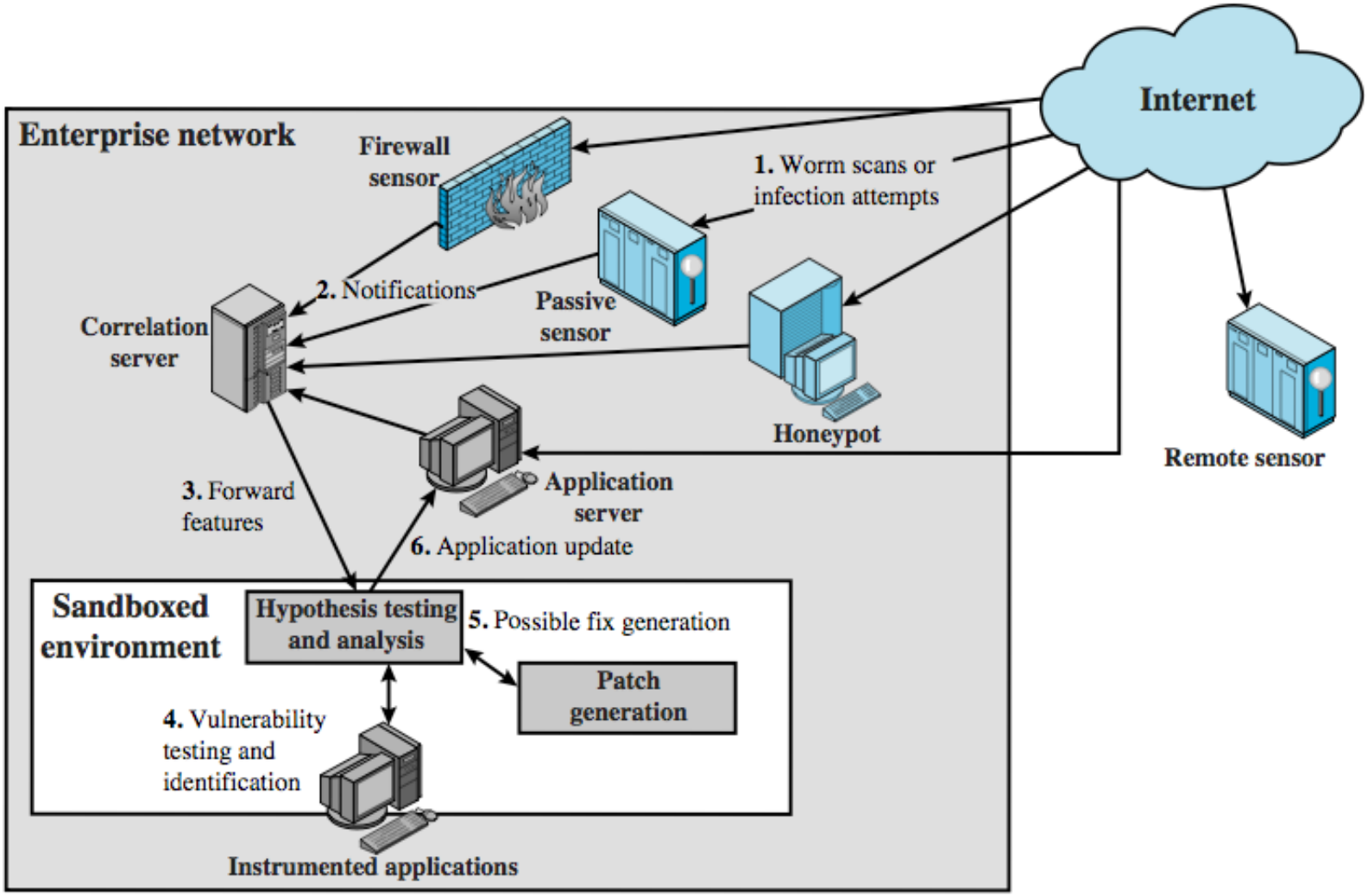
Αντιμετρα κατά των Σκουληκιων

- Υπαρχει επικαλυψη με τις τεχνικες κατά των ιων
- Μπορει να ανιχνευτουν από A/V
- Τα σκουληκια επισης προκαλουν σημαντικη δραστηριοτητα στο δικτυο
- Οι προσεγγισεις αμυνας κατα των σκουληκιων περιλαμβανουν:
  - signature-based worm scan filtering
  - filter-based worm containment
  - payload-classification-based worm containment
  - threshold random walk scan detection
  - rate limiting and rate halting

Proactive Worm Containment



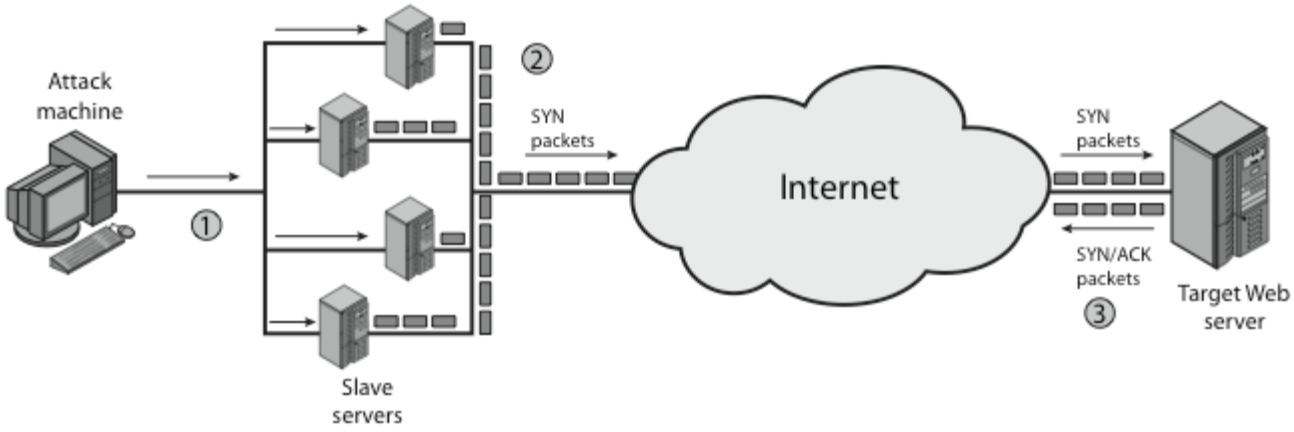
Network Based Worm Defense



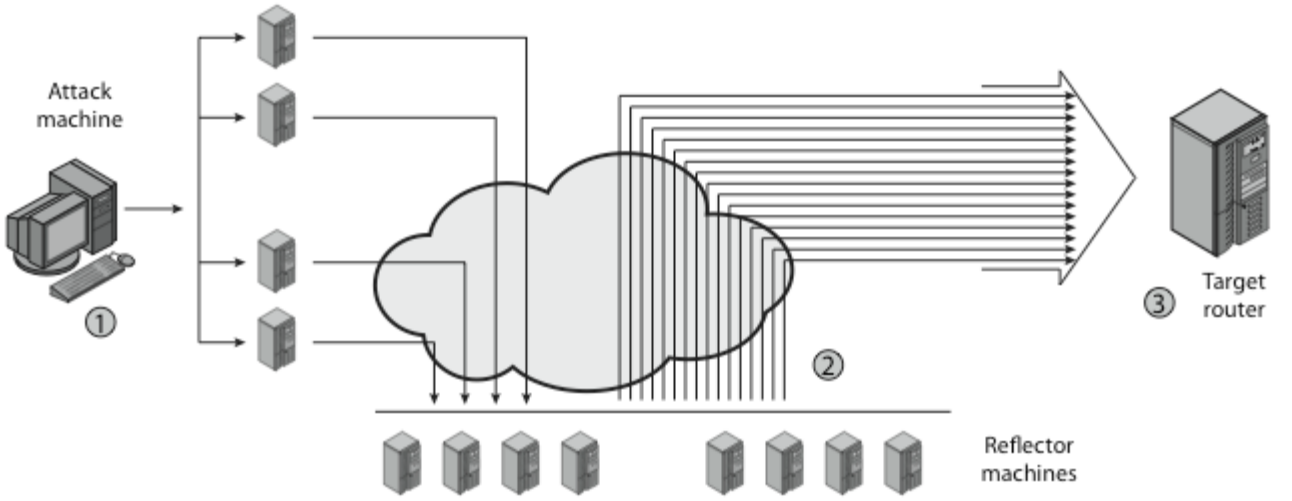
Κατανεμημενη Επιθεση Αρνησης Υπηρεσιας (DDoS)

- Η Κατανεμημενη Επιθεση Αρνησης Υπηρεσιας (DDoS) αποτελει μια σημαντικη απειλη για την ασφαλεια
- Καθιστα τα δικτυωμενα συστηματα μη διαθεσιμα
- Κατακλυζοντας τα με αχρηστο traffic
- Χρησιμοποιει μεγαλους αριθμους υπολογιστων-ζομπι
- Οι επιθεσεις αυτές γινονται ολοενα και πιο εξελιγμενες και οι τεχνολογιες αμυνας απεναντι τους δυσκολευονται να ανταποκριθουν

Distributed Denial of Service Attacks (DDoS)

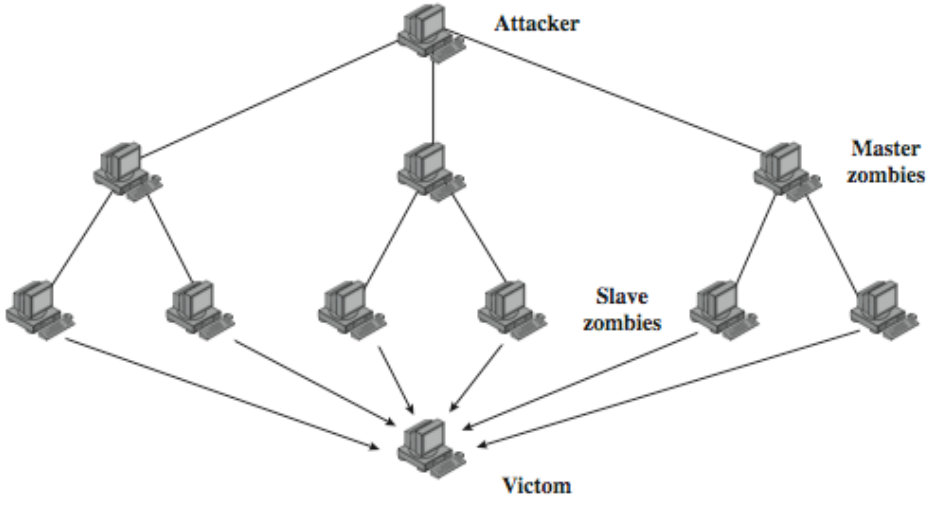


(a) Distributed SYN flood attack

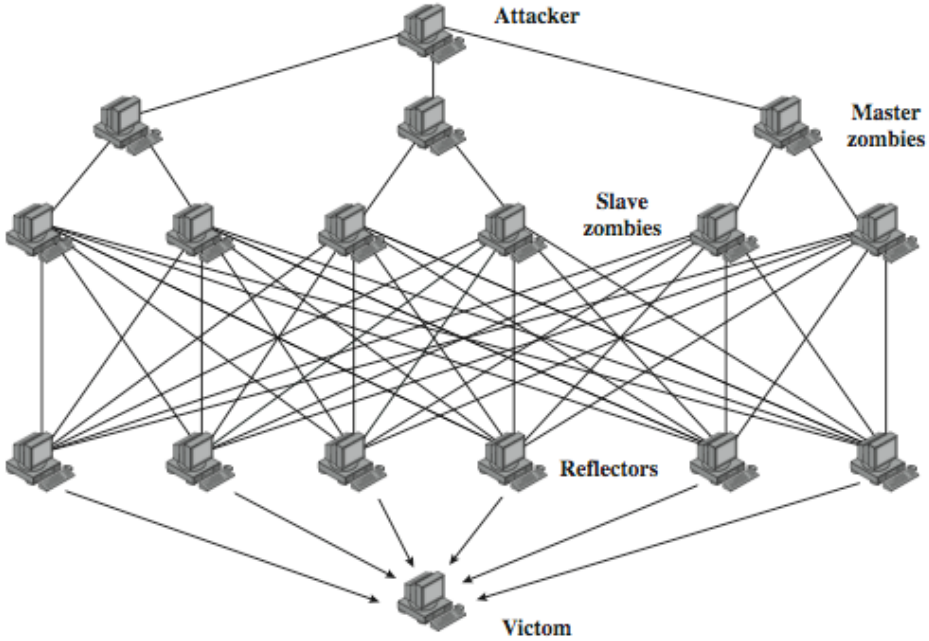


(a) Distributed ICMP attack

DDoS Flood Types



(a) Direct DDoS Attack



(b) Reflector DDoS Attack

Κατασκευη ενός Δικτυου Επιθεσης (Constructing an Attack Network)

- Πρεπει να μολυνθει ενας μεγαλος αριθμος υπολογιστων-ζομπι
- Απαιτουνται:

1. Λογισμικο για την υλοποιηση της επιθεσης DDoS
2. Να ειναι τρωτος ενας μεγαλος αριθμος συστηματων
3. Μια στρατηγικη σαρωσης που να βρισκει τα τρωτα συστηματα
   - τυχαια, τοπολογικη, τοπικου υποδικτυου, κλπ

Αντιμετρα για την επιθεση DDoS

- Τρεις ευρειες γραμμες αμυνας:
  1. Αποτροπη και προληψη της επιθεσης (πριν την επιθεση)
  2. Ανιχνευση και φιλτραρισμα (κατα τη διαρκεια της επιθεσης)
  3. Προς τα πισω ανιχνευση και προσδιορισμος της πηγης της επιθεσης (μετα την επιθεση)
- Υπαρχει μια τεραστια γκαμα δυνατοτητων επιθεσης
- Πρεπει συνεπως να εξελιχθουν και τα αντιστοιχα αντιμετρα

Περιληψη

- Εξετασαμε:
  - Διαφορα κακοβουλα προγραμματα
  - Κερκοπορτες, λογικες βομβες, δουρειοι ιπποι, ζομπι
  - Ιοι
  - Σκουληκια
  - Κατανεμημενες επιθεσεις αρνησης υπηρεσιας