Chapter 9

Intruders and Viruses

Henric Johnson

Blekinge Institute of Technology, Sweden

http://www.its.bth.se/staff/hjo/

henric.johnson@bth.se

Outline

- Intruders
  - Intrusion Techniques
  - Password Protection
  - Password Selection Strategies
  - Intrusion Detection
- Viruses and Related Threats
  - Malicious Programs
  - The Nature of Viruses
  - Antivirus Approaches
  - Advanced Antivirus Techniques
- Recommended Reading and WEB Sites

Intruders

- Three classes of intruders (hackers or crackers):
  - Masquerader
  - Misfeasor
  - Clandestine user

Intrusion Techniques

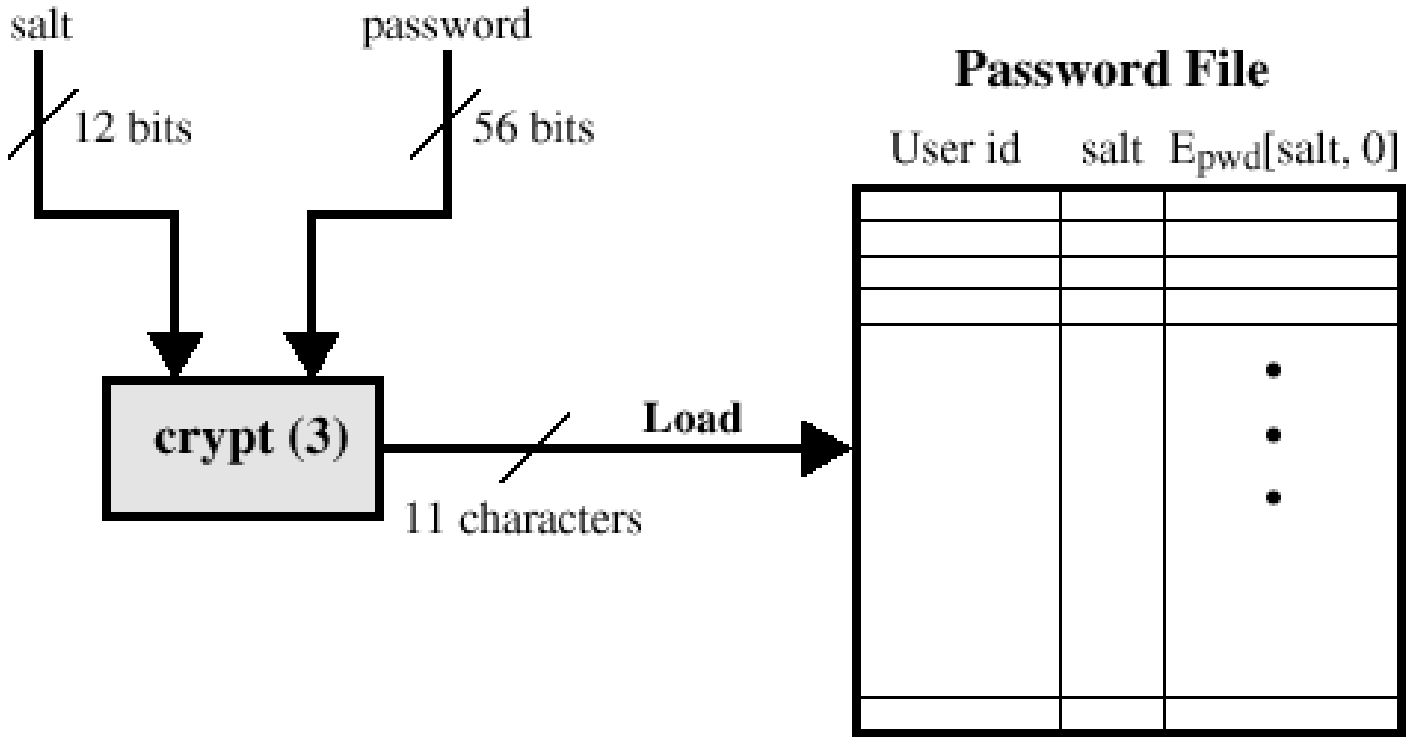
- System maintain a file that associates a password with each authorized user.
- Password file can be protected with:
  - One-way encryption
  - Access Control

Intrusion Techniques

- Techniques for guessing passwords:
  - Try default passwords.
  - Try all short words, 1 to 3 characters long.
  - Try all the words in an electronic dictionary(60,000).
  - Collect information about the user's hobbies, family names, birthday, etc.
  - Try user's phone number, social security number, street address, etc.
  - Try all license plate numbers (MUP103).
  - Use a Trojan horse
  - Tap the line between a remote user and the host system.

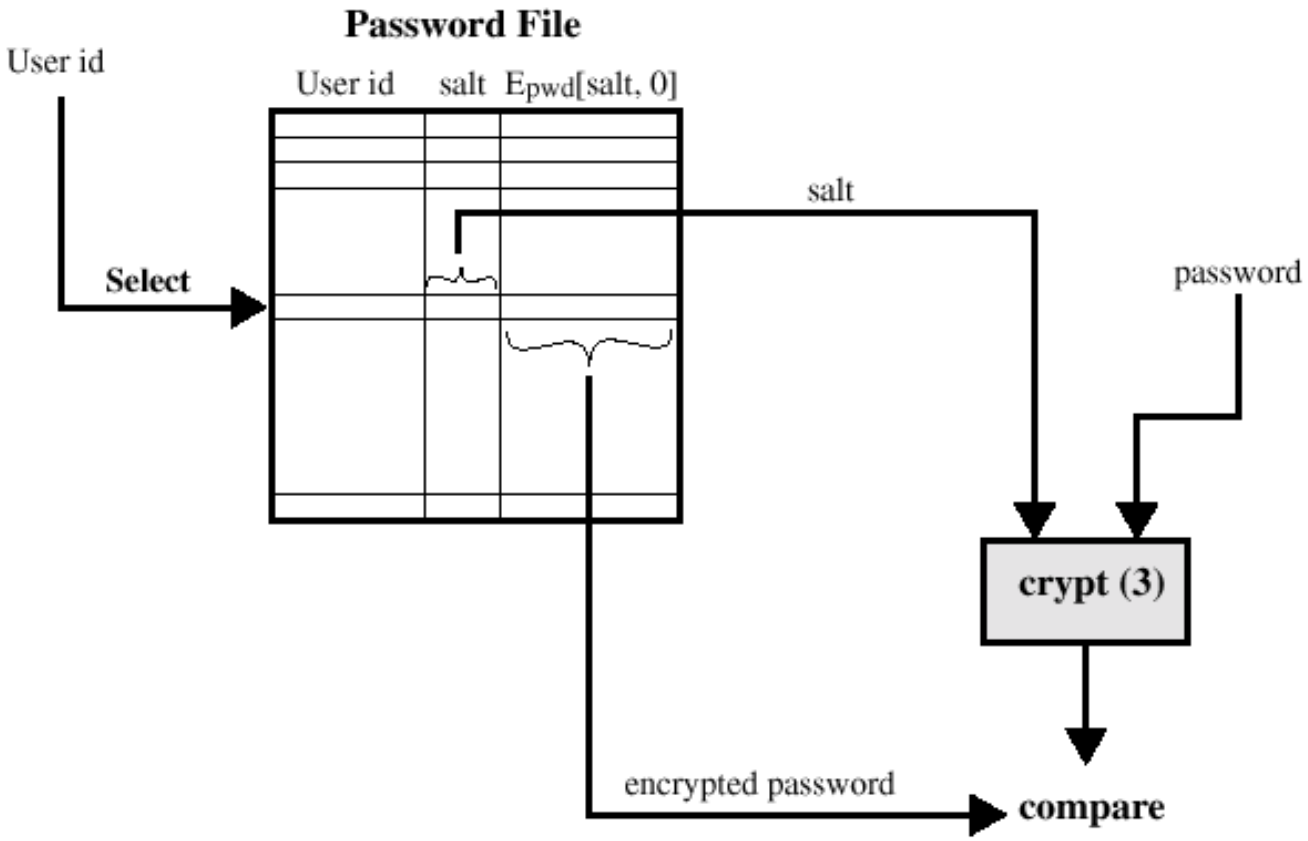
Prevention: Enforce good password selection (Ij4Gf4Se%f#)

UNIX Password Scheme



Loading a new password

UNIX Password Scheme



Verifying a password file

Storing UNIX Passwords

- UNIX passwords were kept in in a publicly readable file, etc/passwords.
- Now they are kept in a "shadow" directory and only visible by "root".

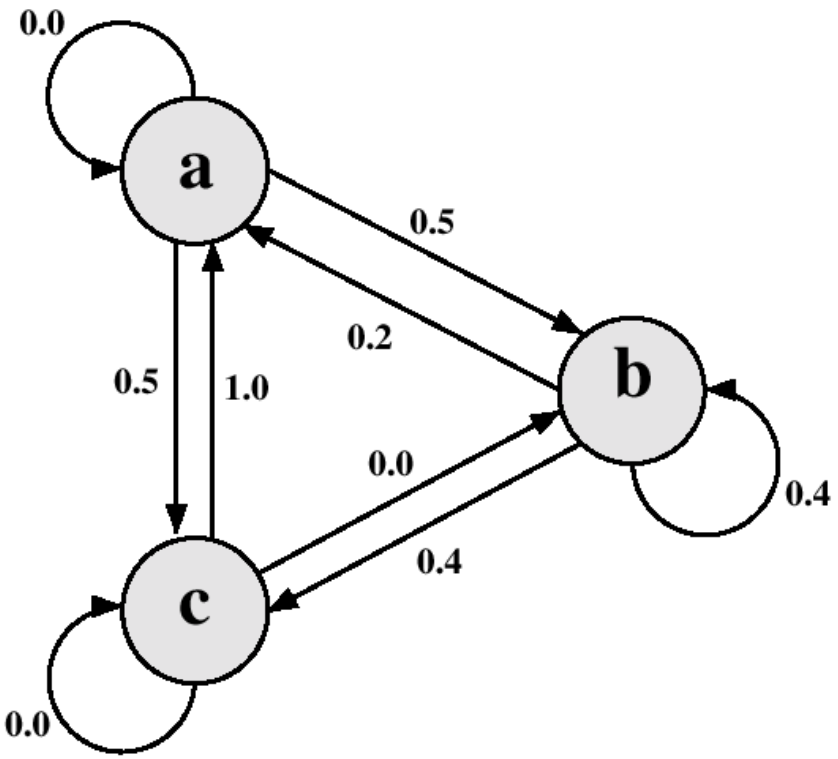
"Salt"

- The salt serves three purposes:
  - Prevents duplicate passwords.
  - Effectively increases the length of the password.
  - Prevents the use of hardware implementations of DES

Password Selecting Strategies

- User ducation
- Computer-generated passwords
- Reactive password checking
- Proactive password checking

Markov Model



M = {3, {a, b, c} , T, 1 } where

$$T = \begin{bmatrix} 0.0 & 0.5 & 0.5 \\ 0.2 & 0.4 & 0.4 \\ 1.0 & 0.0 & 0.0 \end{bmatrix}$$

e.g., string probably from this language: abbcacaba

e.g., string probably not from this language: aacccbaaa

Transition Matrix

1. Determine the frequency matrix f, where f(*i*,*j*,*k*) is the number of occurrences of the trigram consisting of the *i*th, *j*th and *k*th character.
2. For each bigram *ij*, calculate f(*i*,*j*,∞) as the total number of trigrams beginning with *ij*.
3. Compute the entries of T as follows:

$$T(i,j,k) = \frac{f(i,j,k)}{f(i,j,\infty)}$$

Spafford (Bloom Filter)

$$H_i(X_i) = y \quad 1 \le i \le k; \quad 1 \le j \le D; \quad 0 \le y \le N-1$$

where

$$X_i = jth\, word\ in\ password\ dictionary$$

$$D = number\, of\ word\ in\ password\ dictionary$$

The following procedure is then applied to the dictionary:

1. A hash table of N bits is definied, with all bits initially set to 0.
2. For each password, its *k* hash values are calculated, and the responding bits in the hash table are set to 1

Spafford (Bloom Filter)

- Design the hash scheme to minimize false positive.
- Probability of false positive:

$$P \approx (1 - e^{-kD/N})^k = (1 - e^{-k/R})^k$$

$$or, equivalently,$$

$$R \approx \frac{-k}{\ln(1 - P^{1/k})}$$

$$where$$

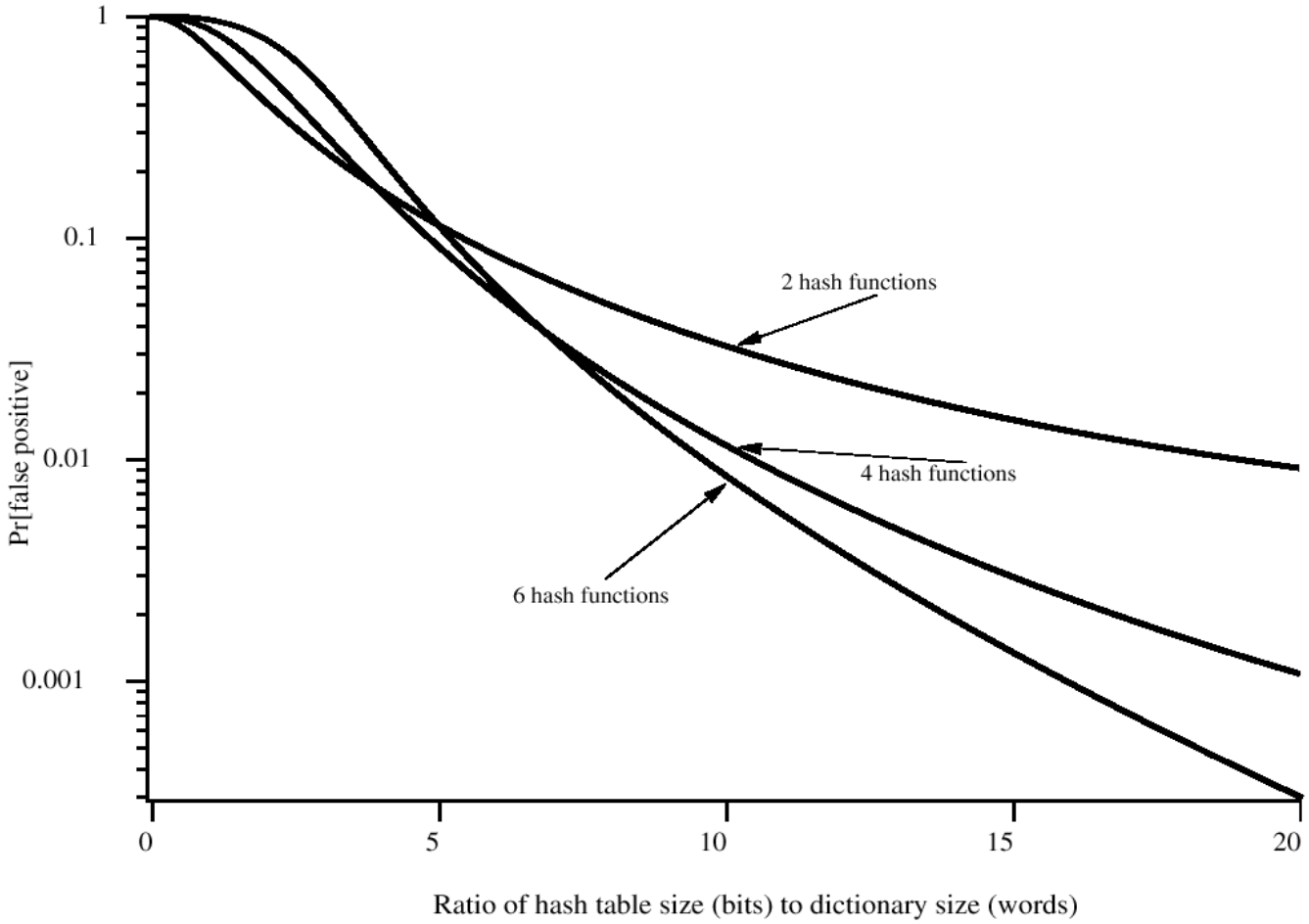
$$k = number\ of\ hash\ function$$

$$N = number\ of\ bits\ in\ hash\ table$$

$$D = number\ of\ words\ in\ dictionary$$

$$R = N / D, ratio\ of\ hash\ table\ size\ (bits)\ to\ dictionary\ size\ (words)$$

Performance of Bloom Filter



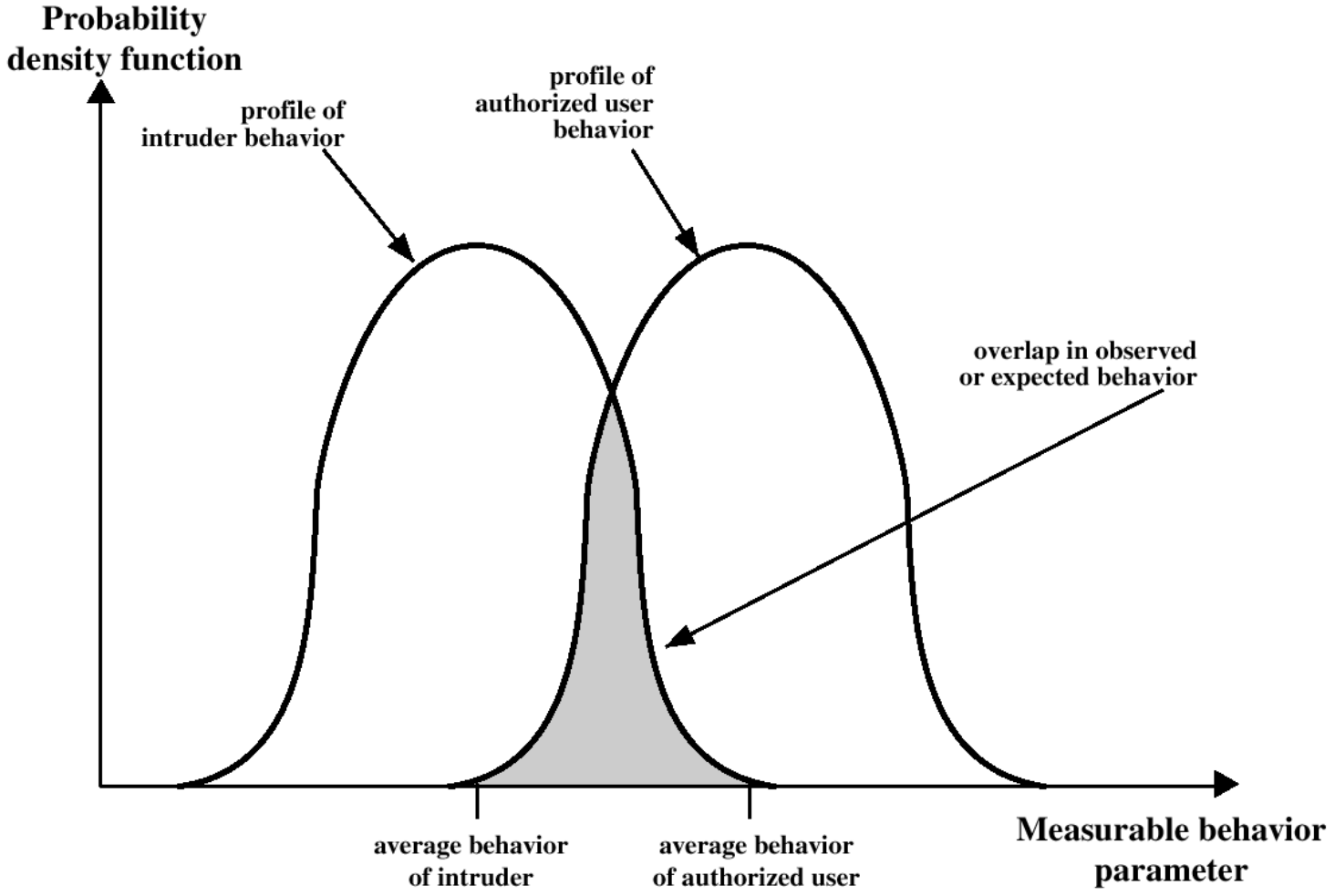
The Stages of a Network Intrusion

1. Scan the network to:
   - locate which IP addresses are in use,
   - what operating system is in use,
   - what TCP or UDP ports are "open" (being listened to by Servers).
2. Run "Exploit" scripts against open ports
3. Get access to Shell program which is "suid" (has "root" privileges).
4. Download from Hacker Web site special versions of systems files that will let Cracker have free access in the future without his cpu time or disk storage space being noticed by auditing programs.
5. Use IRC (Internet Relay Chat) to invite friends to the feast.

Intusion Detection

- The intruder can be identified and ejected from the system.
- An effective intrusion detection can prevent intrusions.
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Profiles of Behavior of Intruders and Authorized Users



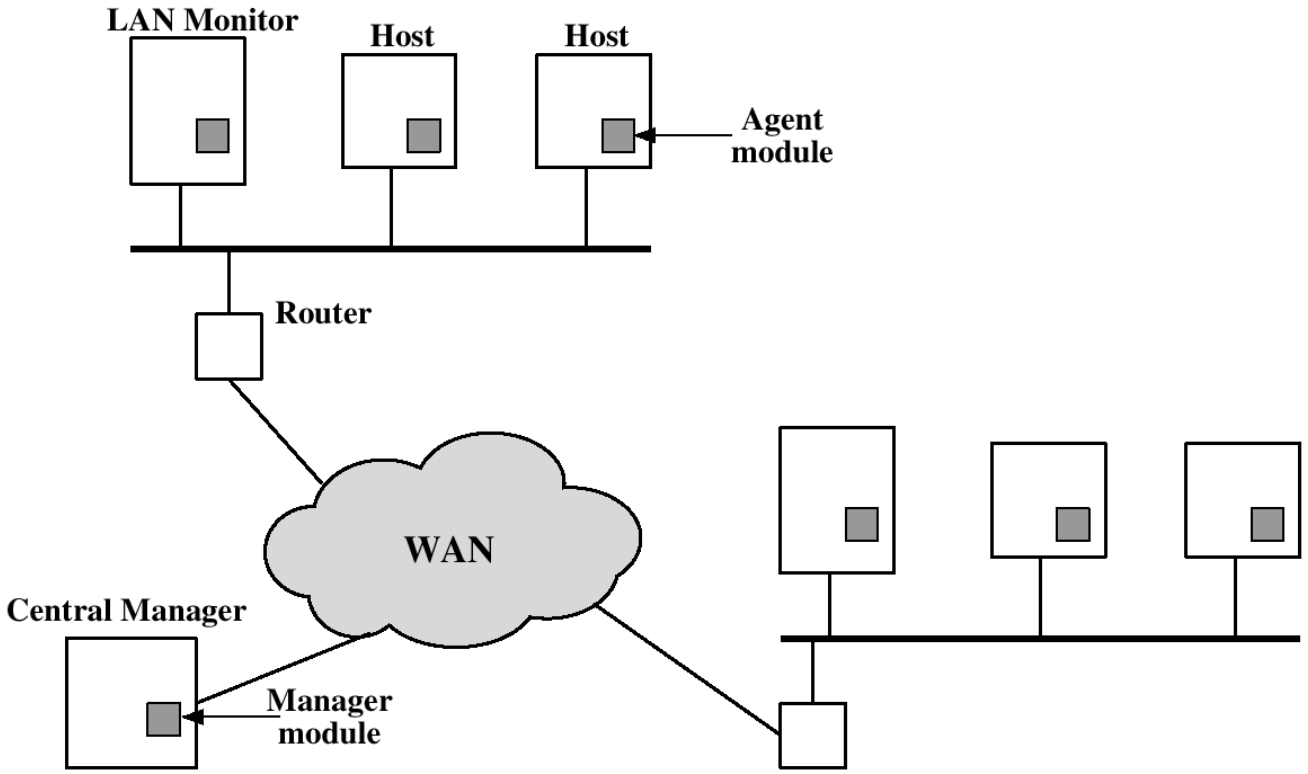
Intrusion Detection

- Statistical anomaly detection
  - Treshold detection
  - Profile based
- Rule based detection
  - Anomaly detection
  - Penetration identidication

Measures used for Intrusion Detection

- Login frequency by day and time.
- Frequency of login at different locations.
- Time since last login.
- Password failures at login.
- Execution frequency.
- Execution denials.
- Read, write, create, delete frequency.
- Failure count for read, write, create and delete.

Distributed Intrusion Detection



Developed at University of California at Davis

Distributed Intrusion Detection

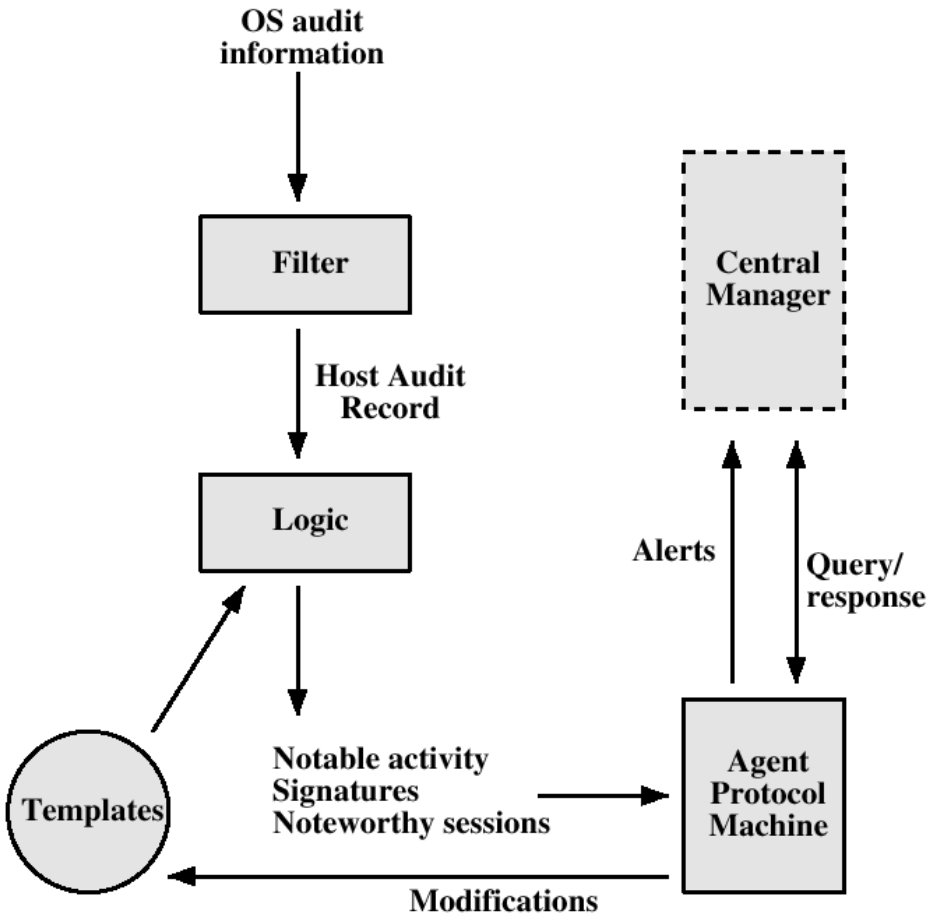


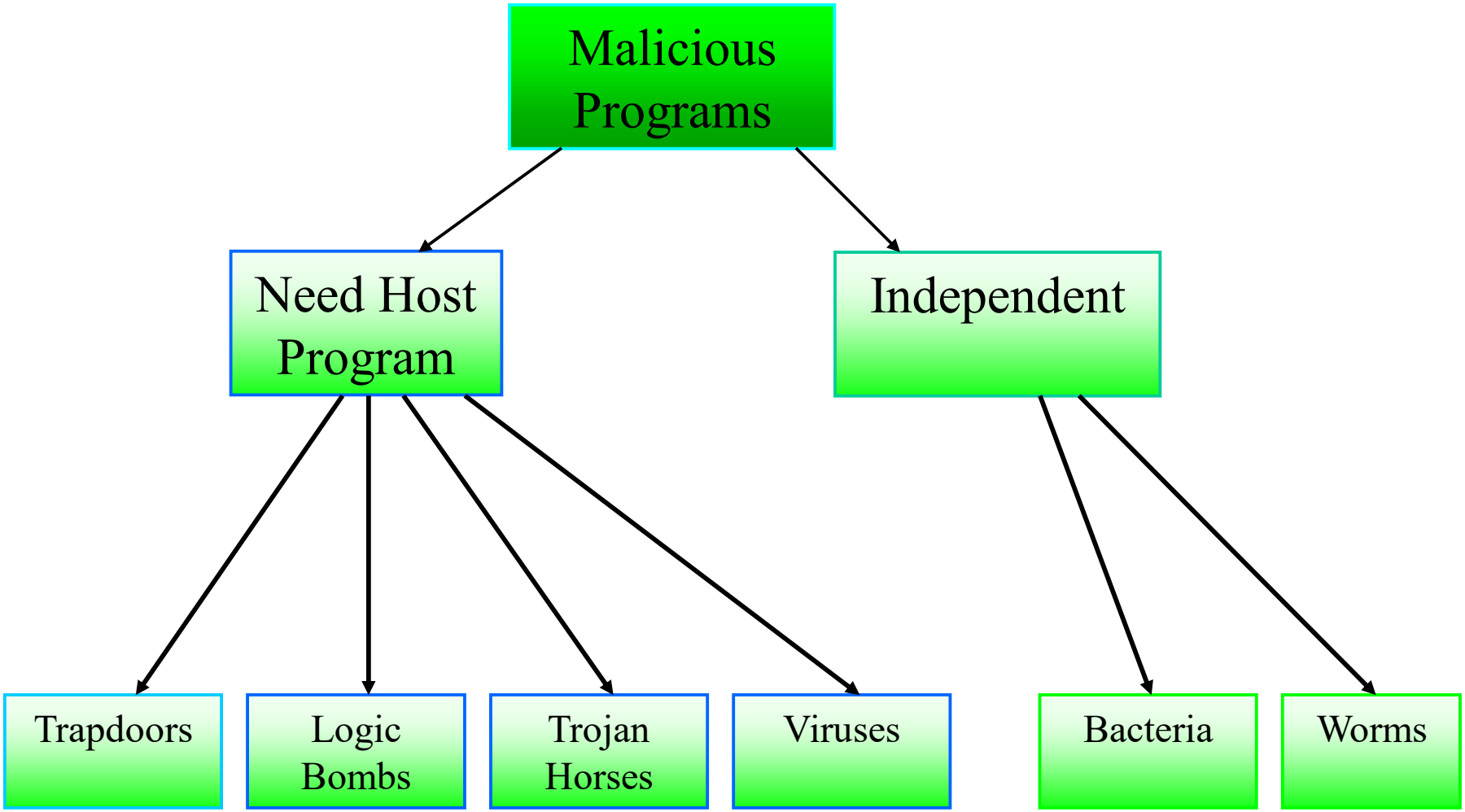
Figure 9.6 Agent Architecture

Viruses and "Malicious Programs"

- Computer "Viruses" and related programs have the ability to replicate themselves on an ever increasing number of computers. They originally spread by people sharing floppy disks. Now they spread primarily over the Internet (a "Worm").

- Other "Malicious Programs" may be installed by hand on a single machine. They may also be built into widely distributed commercial software packages. These are very hard to detect before the payload activates (Trojan Horses, Trap Doors, and Logic Bombs).

Taxanomy of Malicious Programs



Definitions

- Virus - code that copies itself into other programs.
- A "Bacteria" replicates until it fills all disk space, or CPU cycles.
- Payload - harmful things the malicious program does, after it has had time to spread.
- Worm - a program that replicates itself across the network (usually riding on email messages or attached documents (e.g., macro viruses).

Definitions

- Trojan Horse - instructions in an otherwise good program that cause bad things to happen (sending your data or password to an attacker over the net).
- Logic Bomb - malicious code that activates on an event (e.g., date).
- Trap Door (or Back Door) - undocumented entry point written into code for debugging that can allow unwanted users.
- Easter Egg - extraneous code that does something "cool." A way for programmers to show that they control the product.

Virus Phases

- **Dormant phase** - the virus is idle
- **Propagation phase** - the virus places an identical copy of itself into other programs
- **Triggering phase** – the virus is activated to perform the function for which it was intended
- **Execution phase** – the function is performed

Virus Protection

Have a well-known virus protection program, configured to scan disks and downloads automatically for known viruses.

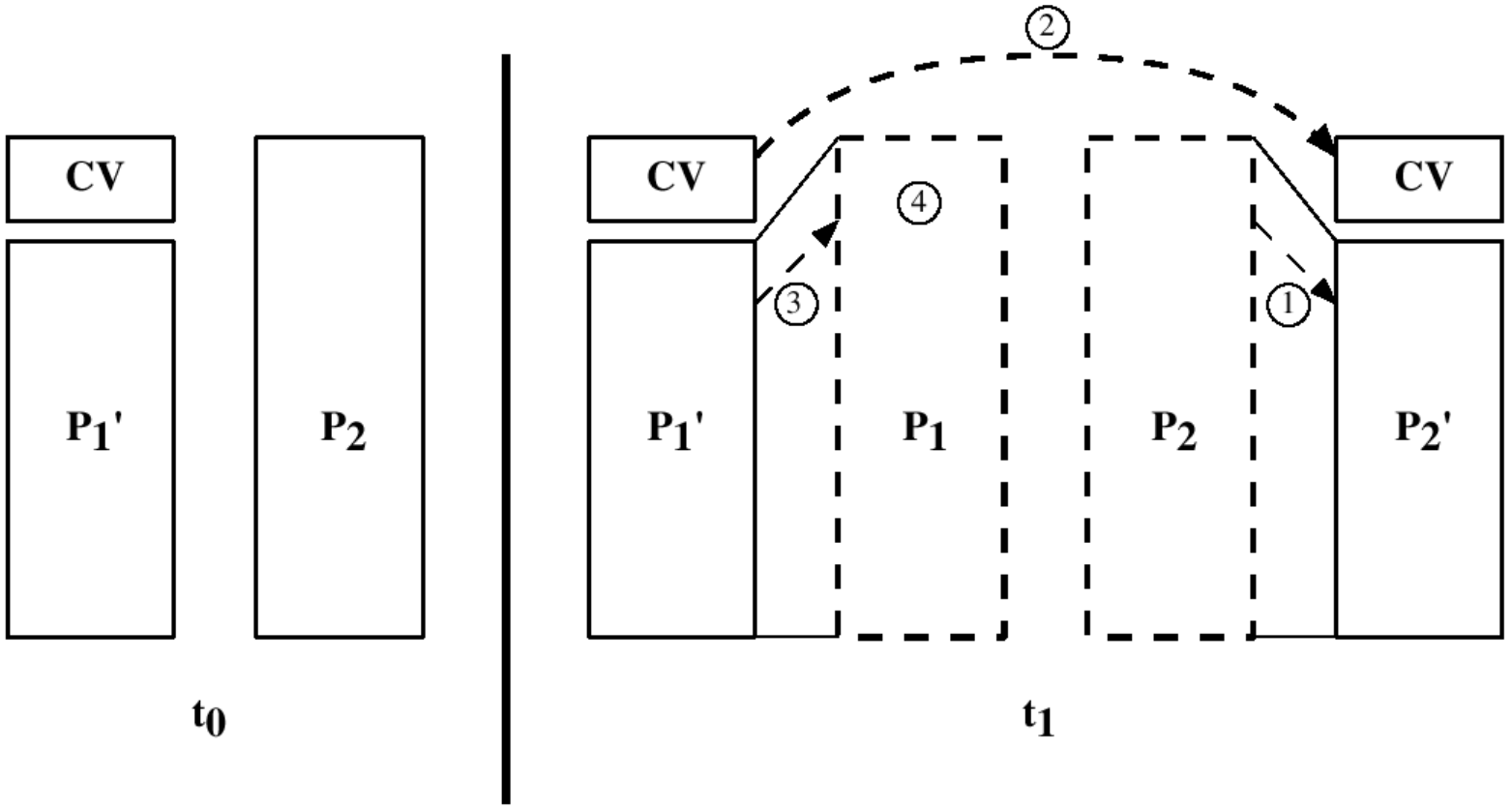
Do not execute programs (or "macro's") from unknown sources (e.g., PS files, Hypercard files, MS Office documents,

Avoid the most common operating systems and email programs, if possible.

Virus Structure

```
        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:

}
```

A Compression Virus



Types of Viruses

- **Parasitic Virus** - attaches itself to executable files as part of their code. Runs whenever the host program runs.
- **Memory-resident Virus** - Lodges in main memory as part of the residual operating system.
- **Boot Sector Virus** - infects the boot sector of a disk, and spreads when the operating system boots up (original DOS viruses).
- **Stealth Virus** - explicitly designed to hide from Virus Scanning programs.
- **Polymorphic Virus** - mutates with every new host to prevent signature detection.

Macro Viruses

- Microsoft Office applications allow "macros" to be part of the document. The macro could run whenever the document is opened, or when a certain command is selected (Save File).
- Platform independent.
- Infect documents, delete files, generate email and edit letters.

Antivirus Approaches

1st Generation, Scanners: searched files for any of a library of known virus "signatures." Checked executable files for length changes.

2nd Generation, Heuristic Scanners: looks for more general signs than specific signatures (code segments common to many viruses). Checked files for checksum or hash changes.

3rd Generation, Activity Traps: stay resident in memory and look for certain patterns of software behavior (e.g., scanning files).

4th Generation, Full Featured: combine the best of the techniques above.

Advanced Antivirus Techniques

- Generic Decryption (GD)
  - CPU Emulator
  - Virus Signature Scanner
  - Emulation Control Module
- For how long should a GD scanner run each interpretation?

Advanced Antivirus Techniques

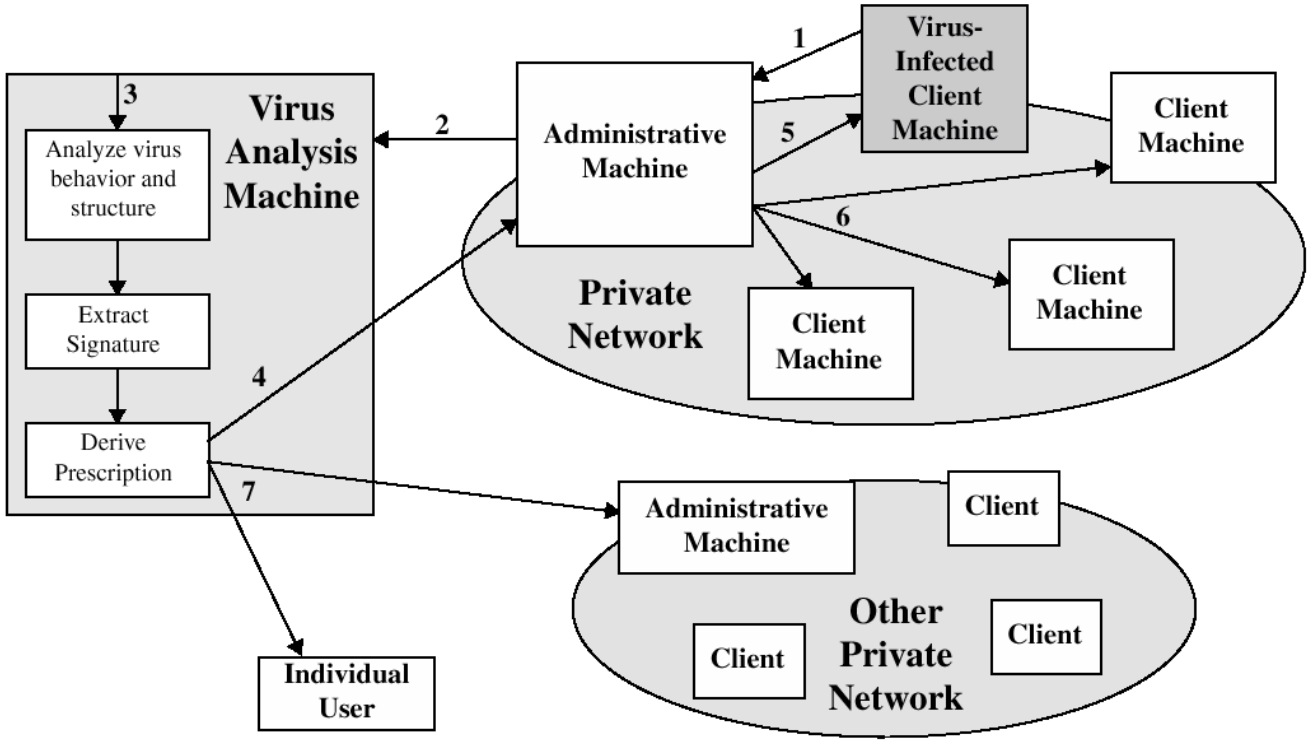


Figure 9.11 Digital Immune System

Recommended Reading and WEB Sites

- Denning, P. *Computers Under Attack: Intruders, Worms, and Viruses.* Addison-Wesley, 1990
- CERT Coordination Center (WEB Site)
- AntiVirus Online (IBM's site)