Chap. 10 Malicious Software

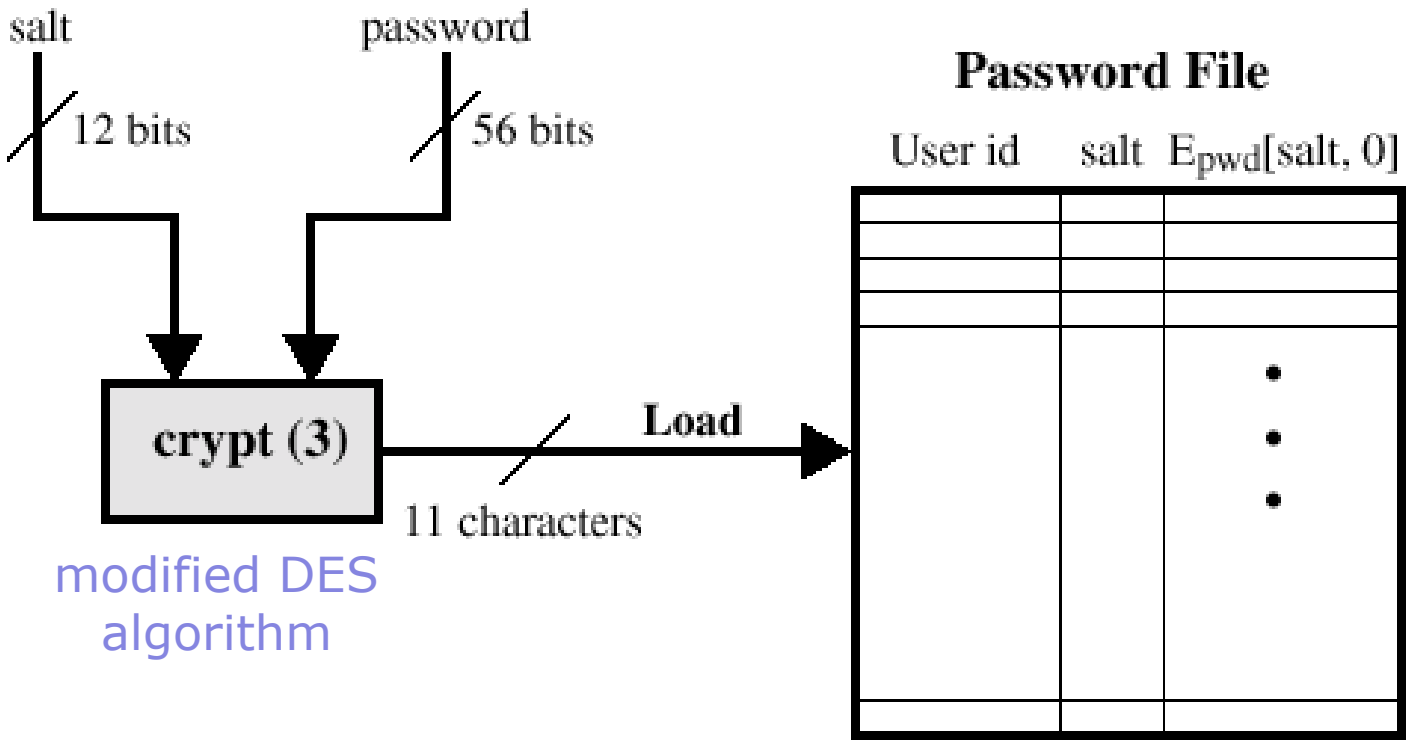
- Viruses
- Malicious Software
- Virus Protection

UNIX Password Scheme

- Techniques for guessing passwords:
  - Try default passwords, all short words, all the words in an electronic dictionary
  - Collect information about the user: hobbies, family names, birthday, phone number, SSN number, street address, license plate numbers, etc.
  - Use a trojan horse
  - Tap the line between a remote user and the server
- Prevention: Enforce good password selection and use encryption

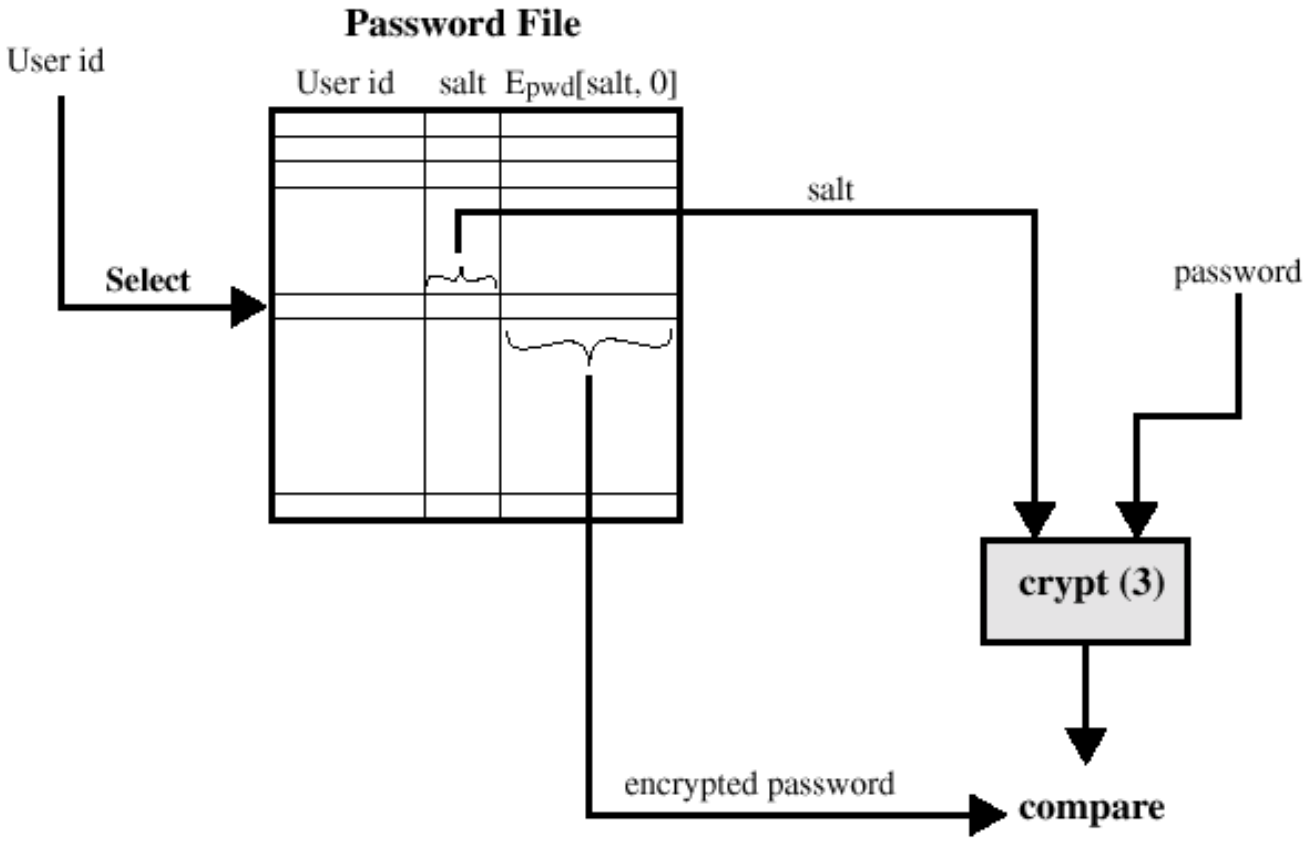
UNIX Password Scheme

- Loading a new password



UNIX Password Scheme

- Verifying a password



UNIX Password Scheme

- Storing UNIX Passwords
  - UNIX passwords were kept in in a publicly readable file, "/etc/password"
  - Now they are kept in a "shadow" directory and only visible by "root": "/etc/shadow"
- Modified DES using salt :
  - Prevents duplicate passwords
  - Effectively increases the length of the password
  - Prevents the use of hardware implementations of DES

Password Selecting Strategies

- User education to select strong passwords
- Computer-generated passwords
- Reactive password checking
  - Periodically checking user's password notifies the user if his password is guessable
- Proactive password checking
  - Check user's password when user selects his password

Malicious Software

- Malicious Programs: computer "Viruses" and related programs
  - they have the ability to replicate themselves on an ever-increasing number of computers
  - they spread thru portable devices or over the Internet
  - 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)

Malicious Software

- Propagation mechanisms
  - include infection of existing executable and interpreted content by viruses that is used subsequently spread to other system
  - Exploit of software vulnerabilities either locally or over a network by worms or drive-by-downloads to allow the malware to replicate
  - Social engineering attacks that convince users to bypass security mechanisms to install trojans or to respond to phishing attacks

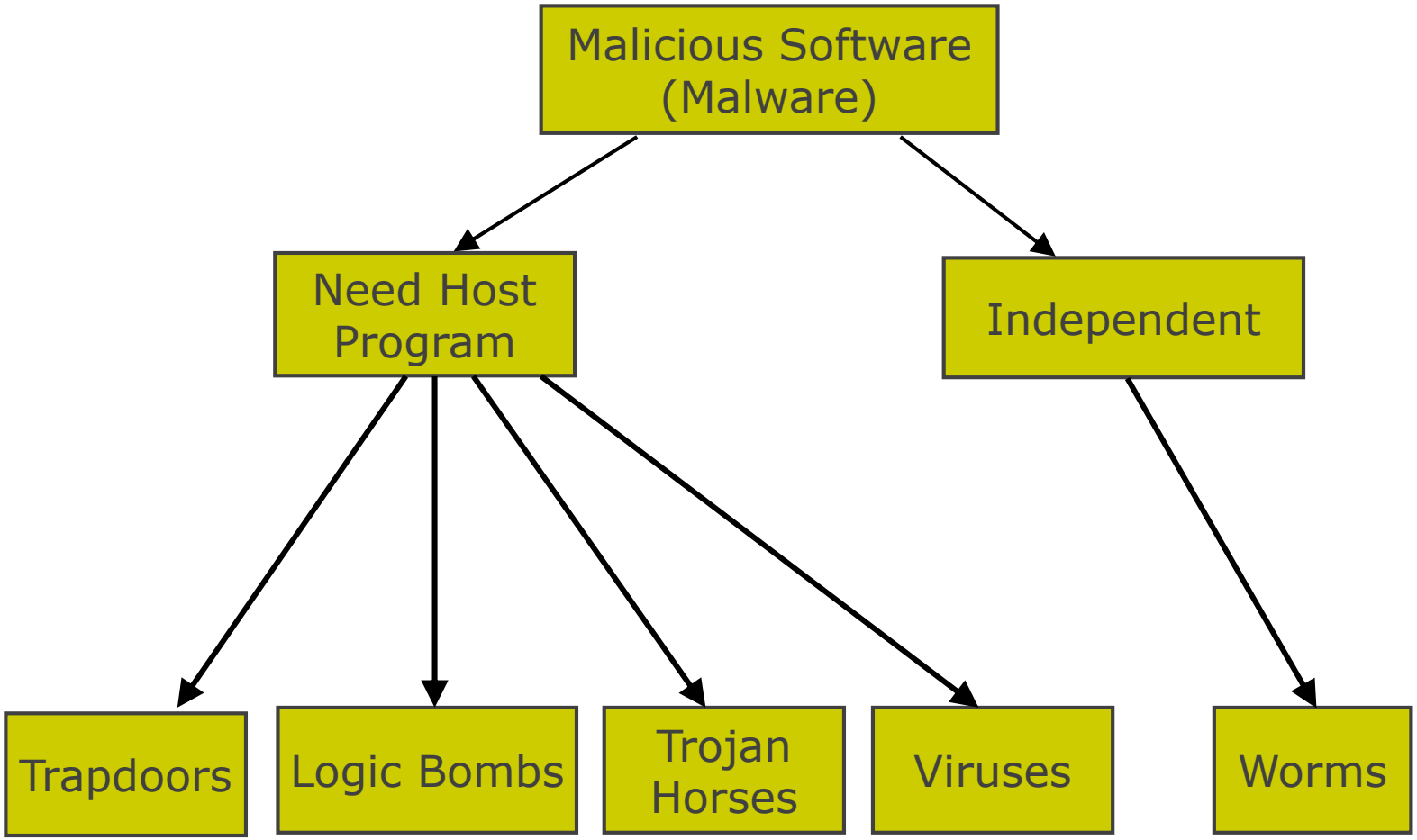
Malicious Software

- Payload actions performed by malware once it reaches a target system
  - Corruption of system or data files
  - Theft of service (C&C) in order to make the system a zombie agent of attack as part of a botnet
  - Theft of information from the system, especially of logins, passwords, or other personal details by keylogging or spyware programs
  - Stealthing where the malware hides its presence on the system from attempts to detect and block it

Malicious Software

- APT(Advanced Persistent Threat) attack
  - an attack with an intelligent, persistent application of a wide variety of intrusion technologies and malware to selected targets, for business or political purpose
  - APT attacks differ from other types of attack by careful target selection, and persistent, often stealthy (zero-day attacks), intrusion efforts over extended periods
  - (e.g.) Aurora, RSA, Stuxnet, Naver/Cyworld 개인정보 유출

Taxanomy of Malicious Software



Malwares

- Virus
  - Embedded in other programs and infect and do some malicious actions
  - cannot run by itself
- Worm
  - a stand-alone program that replicates itself across the network – usually riding on email messages or attached documents (e.g., macro viruses)
- Logic Bomb
  - malicious code that activates on an event (e.g., date)
- Key-loggers
  - Captures keystrokes on a compromised computer

Malwares

- Trojan Horse
  - Embedded in other program and appears to have a useful function but also have a hidden and malicious function (sending your data or password over the net)
  - (e.g.) Spyware, adware
- Trap Door (or Back Door)
  - undocumented entry point written into code for debugging that can allow unwanted access
  - Bypass the normal authentication procedure
- Zombie
  - Program that secretly takes over another Internet-attached computer and uses it to launch attacks to other computers

Malwares

- Spammer
  - program used to send a large volumes of unwanted e-mails
- Rootkit
  - A malicious program that conceals itself or defends itself from being removed by modifying host's OS
  - if infected, OS kernel or firmware must be removed and re-installed
  - (e.g.) Stuxnet worm, Sony rootkit

Vulnerability to Malwares

- Security defects in software
  - Malware exploits security defects in the design or implementation of software (OS, application software, etc.)
  - Needs continuous security check using anti-virus software and patches
  - (e.g.) SW upgrade checking software
- Insecure action or user error
  - Allows booting from an infected device (CD or USB devices) or auto-running a software in an infected device

Vulnerability to Malwares

- Over-privileged users or programs
  - In poorly designed systems, users and programs can be assigned more privileges than they should be
- Use of the same OS
  - When all computers use the same OS, on exploiting one, one worm can exploit them all

Virus Phases

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

Virus Protection

- Use a virus protection program configured to scan disks and downloads automatically for known viruses
- Do not execute programs with "macro" from unknown sources
  - (e.g.) PS files, Hypercard files, MS Office documents
- Avoid the most common operating systems and email programs, if possible

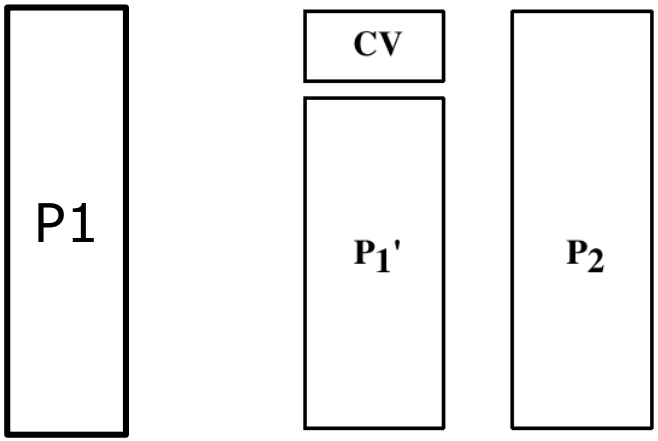
Virus Structure

- Infected program
  - Size is increased

```
        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:

}
```

Compression Virus

- Infection
  - Compress original P1 and prepend CV




```
    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;}
        }
```

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

Types of Viruses

- Virus concealment strategies:
  - Stealth Virus:
    - explicitly designed to hide from Virus Scanner
  - Encrypted virus:
    - Portion of the virus creates a random encryption key and encrypts the remainder of the virus
    - When an infected program is invoked, the virus uses the stored random key to decrypt the virus
    - When the virus replicates, a different random key is selected

Types of Viruses

- Virus concealment strategies:
  - Polymorphic Virus
    - mutates with every new host to prevent signature detection
  - Metamorphic Virus
    - Mutates with every infection
    - Rewrites itself completely at each iteration, increasing the difficulty of detection

Macro Viruses

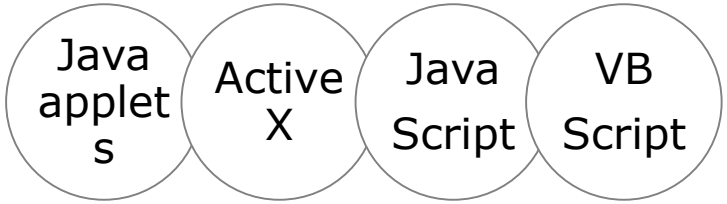
- Macro virus
  - applications like Microsoft Office allow “macros” to be part of the document
  - The macros run whenever the document is opened, or when a certain command is selected (Save File)
  - is platform independent (script code)
  - Macro viruses are easily spread, as the documents they exploit are shared in normal use
  - may infect documents, delete files, generate email and edit letters

Worms

- Worms:
  - a program that actively seeks out machines to infect: on activation, it replicates itself and propagate
  - For propagation, a worm uses some means to access remote systems:
    - Electronic mail or instant messenger facility,
    - Remote execution or login capability,
    - Remote file access or transfer capability, etc.

Mobile codes

- Mobile codes:
  - a script program that can be shipped to a heterogeneous collection of platforms and executed



  - The most common ways of using mobile code for malicious operations on local system:
    - Cross-site scripting (XSS)
    - E-mail attachments
    - Downloads from untrusted sites or of untrusted SW

Drive-by-downloads

- Drive-by-downloads :
  - an attack that downloads automatically a malware w/o the user's consent when a user accesses a web site
  - uses the vulnerabilities of a web browser (plugins: Adobe Flash, Adobe reader, Java & JavaScript, etc.)
  - similar attacks: an attack that downloads a software w/ the user's consent but the software was replaced with a malware by the attacker (downloads of anti-virus SW on a bank site)

SPAM

- SPAM :
  - Unsolicited bulk e-mail which is used mostly to carry a malware
  - Imposes significant costs on both the network and on users who need to filter their legitimate e-mails
  - May be used in a phishing attack
  - Most spam is sent by botnets using compromised Zombie systems

Bots

- Bots:
  - a malware that takes over PC and can be remotely controlled by a master (an attacker)
  - Perform the following actions:
    - Distributed denial-of-service (DDoS) attacks
    - sending SPAMs
    - Sniffing traffic
    - Keylogging
    - Spreading new malware or installing advertisement add-ons

Countermeasures

- Basic countermeasures :
  - ensure all systems are as current as possible, with all patches applied, in order to reduce the number of vulnerabilities that might be exploited on the system
  - set appropriate access controls on the applications and data stored on the system, to reduce the number of files that any user can access, and hence potentially infect or corrupt by executing some malware code
  - countermeasures against social engineering attacks by user education and training

Anti-malware Approaches

- Real-time protection against installation of malware
  - Scans all incoming network data for malware and blocks any threats it can come across
- Detection and removal of malware software installed on a computer
  - Scans all files (registry, OS files, and installed applications, etc.) to check any threats
  - Lists up and remove the malwares found
  - Real-time protection scans files at download time and blocks the activity of malware

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)
  - integrity check: checking files for checksum or hash changes

Antivirus Approaches

- 3rd Generation, Activity Traps
  - stay resident in memory and look for certain patterns of software behavior rather than its structure in an infected program: (e.g.) scanning files on the system
- 4th Generation, Full Featured
  - combine all the best techniques in the above