CS 0111:
INTRODUCTION TO IT SECURITY

LECTURE 06
Access Controls

Access Control

- *Access control is a process to determine "Who does what to what," based on a policy.*
- It is controlling access of who gets in and out of the system and who uses what resources, when, and in what amounts.
- Access control is restricting access to a system or system resources based on something other than the identity of the user.

TERMINOLOGIES

- **Identification**
  - ✓Identification is a process through which one system confirms the identity of another person / entity/ computer system. **(Compare one to many)**
- **Authentication**
  - ✓Authentication is a process to verify the credentials of the principal or the system. **(Compare one to one)**
- **Authorization**
  - ✓It is a process by which the principal is either granted access or disallowed to protected resources. Only the trusted principal can be granted secure access.

ACCESS CONTROL

- Two parts to access control
- **Identification:** Who goes there?

1. **Authentication:** Is that really you?
   - ✓Determine whether access is allowed
   - ✓Authenticate human to machine
   - ✓Authenticate machine to machine
2. **Authorization:** Are you allowed to do that?
   - ✓Once you have access, what can you do?
   - ✓Enforces limits on actions

- Note: Access control often used as synonym for authorization

AUTHENTICATION

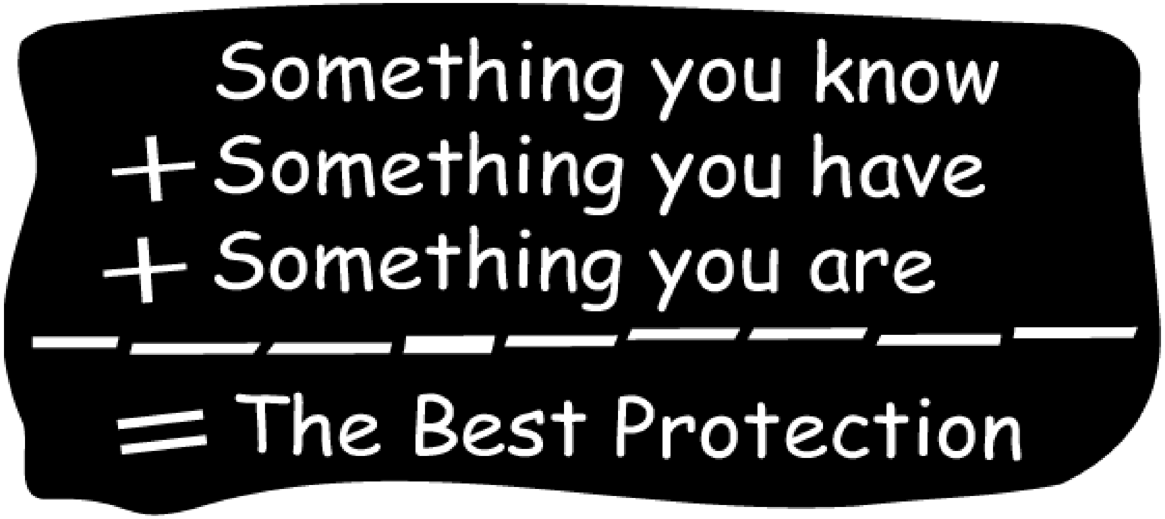
AUTHENTICATION :

Who goes there?

- How to authenticate a human to a machine?
- Can be based on…
  - ✓Something you **know**
  - ✓Something you **have**
  - ✓Something you **are**

AUTHENTICATION

- **3 types of authentication**
- **The Best Protection**



Something you know
+ Something you have
+ Something you are

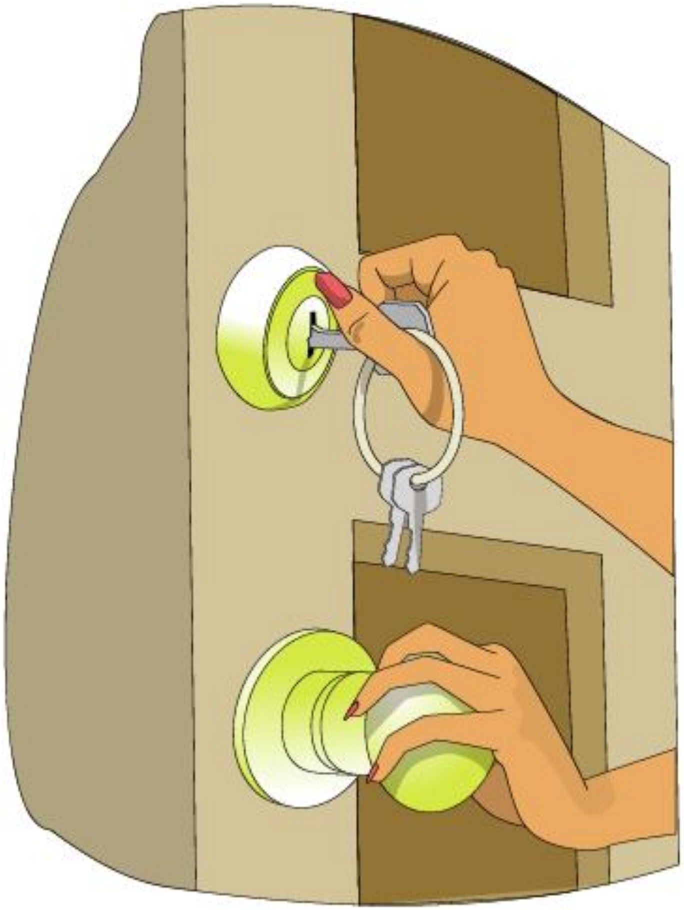
= The Best Protection

Something You Know

- Username
- Password
- PIN
- Passphrase

Something You Have

- Smart cards (NIDA)
  - ✓Multi-function
- Examples
  - ✓National ID card (NIDA)
  - ✓Driver’s license
  - ✓ATM card



Something You Are (Biometrics)

- Face
- Signature
- Fingerprint
- Retina
- Iris
- Palm geometry
- Voice
- DNA

Passwords

- Passwords are the most common authentication method

Something You Know!

Why Passwords?

- Why is “something you know” more popular than “something you have” and “something you are”?
- **Cost**: passwords are free
- **Convenience**: easier for System Administrators to reset password than to issue user a new thumb

Classic password rules

- The best passwords are those that are both easy to remember and hard to crack using a dictionary attack.
- The best way to create passwords that fulfill both criteria is to use two small unrelated words or phonemes, ideally with a special character or number.

Classic password rules

- Good examples would be *hex7goop* or -*typetin*
- **Don’t use:**
  - ✓Common names, DOB, spouse, phone #, etc.
  - ✓Word found in dictionaries
  - ✓Password as a password
  - ✓Systems defaults

AUTHENTICATION

- **Use Strong Passwords**
  - ✓Passwords are like house keys
  - ✓Different key for each lock
  - ✓Brute force attacks
  - ✓Sniffing clear text

AUTHENTICATION

Use Strong Passwords

- **SUPR** tests
  - ✓**<u>S</u>trong** – Password strong (length and content)?
  - ✓**<u>U</u>nique** – Unique and unrelated to other passwords?
  - ✓**<u>P</u>ractical** – Can you remember it?
  - ✓**<u>R</u>ecent** – Have you changed it recently?

PASSWORD MANAGEMENT

- Configure system to use string passwords
- Set password time and lengths limits
- Limit unsuccessful logins
- Enabled auditing
- How policies for password resets and changes

Problems with passwords

- **Insecure** - Given the choice, people will choose easily remembered and hence easily guessed passwords such as names of relatives, phone numbers, birthdays, hobbies, etc.
- **Easily broken** - Programs such as crack, SmartPass, PWDUMP, NTCrack & l0phtcrack can easily decrypt Unix, NetWare & NT passwords.
  - ✓Dictionary attacks are only feasible because users choose easily guessed passwords!

Problems with passwords…

- **Inconvenient** - In an attempt to improve security, organizations often issue users with computer-generated passwords that are difficult, if not impossible to remember
- **Repudiable** - Unlike a written signature, when a transaction is signed with only a password, there is no real proof as to the **identity** of the individual that made the transaction

Other Password Issues

- Users choose bad passwords
- Failure to change default passwords
- Social engineering

Passwords

- The bottom line
- **Password cracking is too easy!**
  - ✓One weak password may break security
  - ✓Users choose bad passwords
  - ✓Social engineering attacks, etc.
- The bad guy has all of the advantages
- Passwords are a **big** security problem

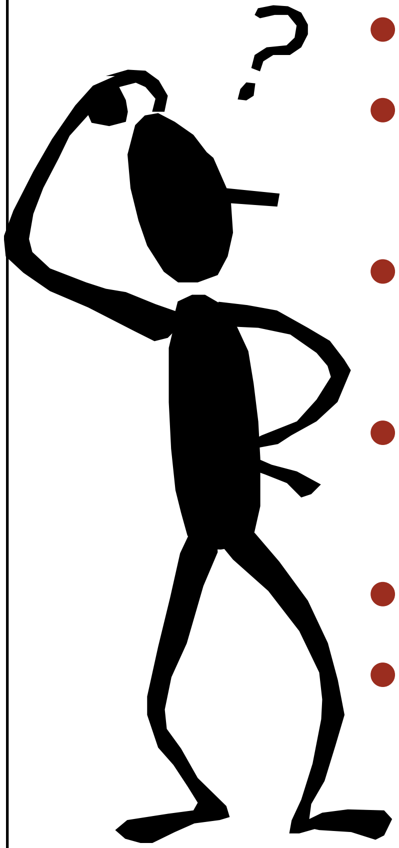
Attacks on Passwords

- **Attacker could…**
  - ✓Target one particular account
  - ✓Target any account on system
  - ✓Target any account on any system
- **Common attack path**
  - ✓Outsider → normal user → administrator
  - ✓May only require **one** weak password!

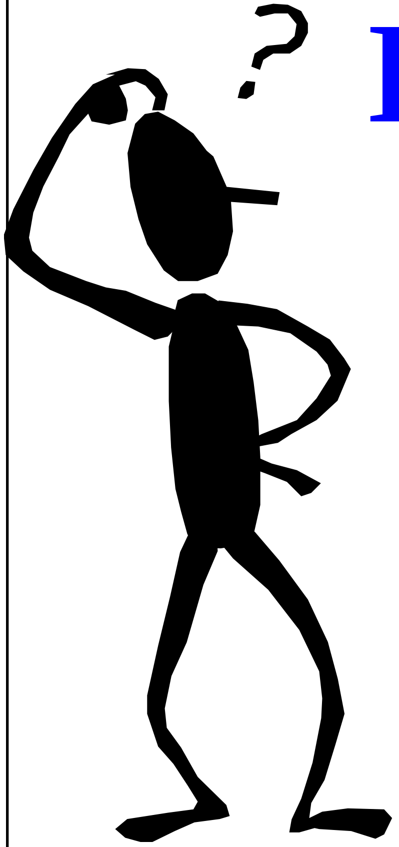
Passwords Attacks

- **Passwords Attacks:**
  - ✓Guessing
  - ✓Dictionary Attacks
  - ✓Brute force attacks
  - ✓Social Engineering

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 (T103 AAA).
- Use a **Trojan horse**



How to avoid Guessable passwords?

How to avoid Guessable passwords?

- Techniques used to avoid guessable passwords.

- Four technique exist:

1. **User education**
2. **Computer-generated passwords**
3. **Reactive password checking**
4. **Proactive password checking**

How to avoid Guessable passwords? (2)

1. **User education:** Users can be told the importance of using hard-to-guess passwords and can be provided with guidelines for selecting strong passwords.
2. **Computer-generated passwords:** Users are provided passwords generated by a computer algorithm.

How to avoid Guessable passwords? (4)

3. **Reactive password checking:** the system periodically runs its own password cracker to find guessable passwords. The system cancels any passwords that are guessed and notifies the user.
4. **Proactive password checking:** a user is allowed to select his or her own password. However, at the time of selection, the system checks to see if the password is allowable and, if not, rejects it.

Password Cracking Tools

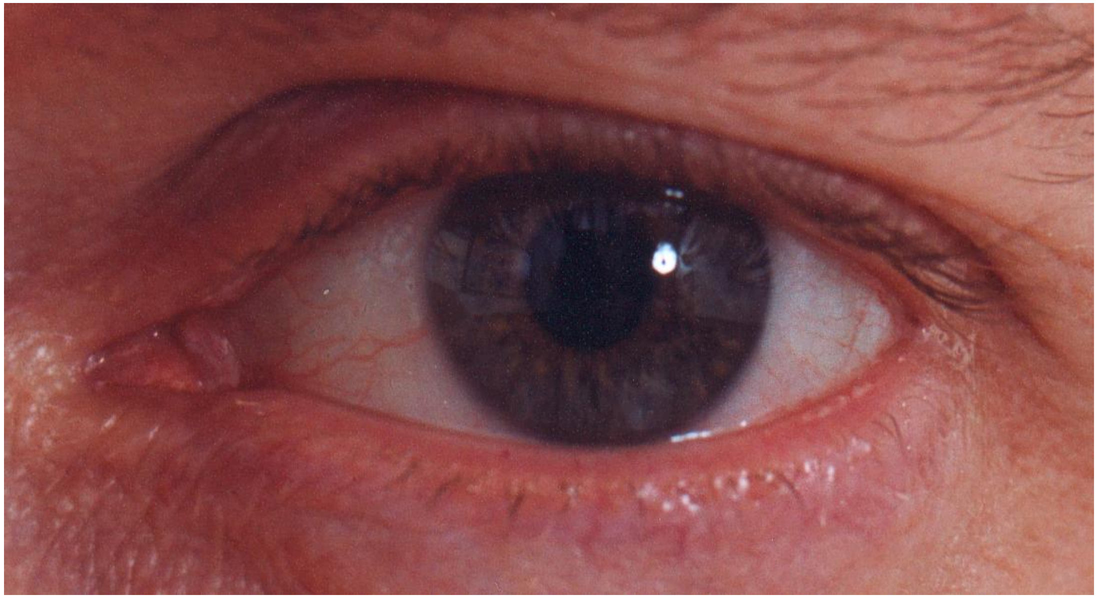
- Popular password cracking tools
  - ✓Password Crackers
  - ✓Password Portal
  - ✓L0phtCrack and LC4 (Windows)
  - ✓John the Ripper (Unix)
- Admins should use these tools to test for weak passwords since attackers will!
- Good article on password cracking
  - ✓Passwords - **Cornerstone** of Computer Security

Password protection

- Two common techniques used to protect a password file
- **One-way encryption:** The system stores only an encrypted form of the user's password. When the user presents a password, the system encrypts that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the encryption function and in which a fixed-length output is produced.
- **Access control:** Access to the password file is limited to one or a very few accounts.

Something You Are

Biometric



Biometrics

- Authenticating a user via human characteristics
- Using measurable physical characteristics of a person to prove their identification
  - ✓Fingerprint
  - ✓Handwritten signature
  - ✓Facial recognition
  - ✓Speech recognition
  - ✓Iris
  - ✓Retina
  - ✓DNA, blood

Why Biometrics?

- Biometrics seen as desirable replacement for passwords
- Cheap and reliable biometrics needed
- Today, a very active area of research
- Biometrics are used in security today
  - ✓Thumbprint mouse
  - ✓Palm print for secure entry
  - ✓Fingerprint to unlock car door, etc.
- But biometrics not too popular
  - ✓Has not lived up to its promise (yet)

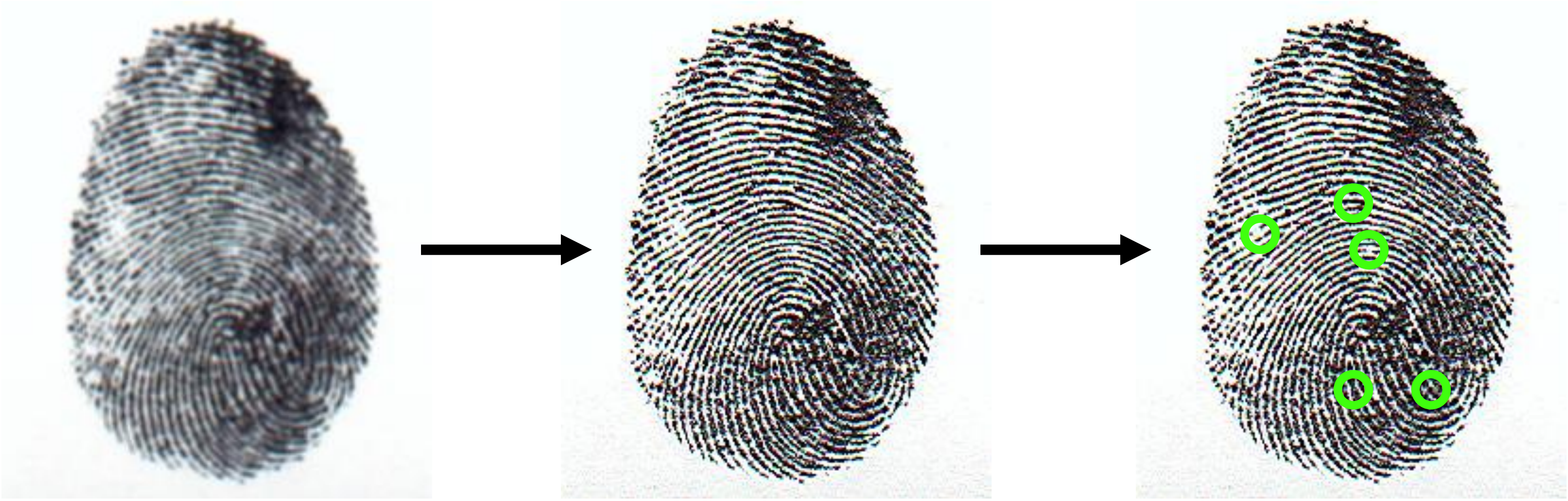
Ideal Biometric

- **Universal:** Applies to (almost) everyone
  - ✓In reality, no biometric applies to everyone
- **Distinguishing:** Distinguish with certainty
  - ✓In reality, cannot hope for 100% certainty
- **Permanent:** Physical characteristic being measured never changes
  - ✓In reality, want it to remain valid for a long time
- **Collectable:** Easy to collect required data
  - ✓Depends on whether subjects are cooperative
- Safe, easy to use, etc., etc.

Biometric Modes

- **Identification:** Who goes there?
  - ✓Compare one to many
  - ✓Example: The FBI fingerprint database
- **Authentication:** Is that really you?
  - ✓Compare one to one
  - ✓Example: Thumbprint mouse
- We are interested in authentication

Fingerprint Biometric



- Capture image of fingerprint
- Enhance image
- Identify minutia

Advantages of fingerprint-based biometrics

- Can’t be lent like a physical key or token and can’t be forgotten like a password
- Good compromise between ease of use, template size, cost and accuracy
- Fingerprint contains enough inherent variability to enable unique identification even in very large (millions of records) databases
- Basically lasts forever
- Makes network login & authentication effortless

Biometric Disadvantages

- Still relatively expensive per user
- Companies & products are often new & immature
- No common API or other standard
- Some hesitancy for user acceptance

Practical biometric applications

- Network access control
- Staff time and attendance tracking
- Authorizing financial transactions
- Government benefits distribution (Social Security, welfare, etc.)
- Verifying identities at point of sale
- Using in conjunction with ATM , credit or smart cards
- Controlling physical access to office buildings or homes
- Protecting personal property

Hand Geometry

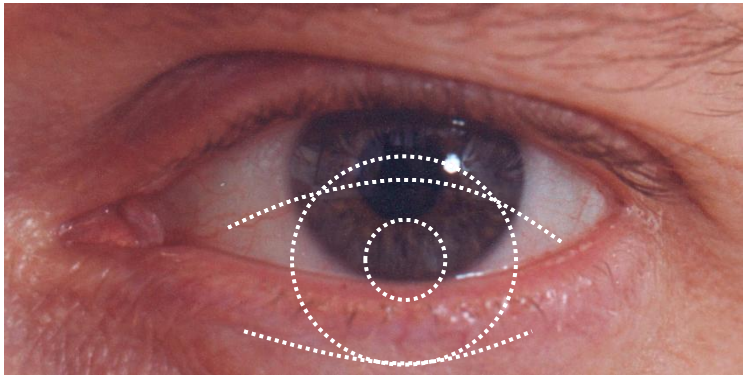
- Popular form of biometric
- Measures shape of hand
  - ✓ Width of hand, fingers
  - ✓ Length of fingers, etc.
- Human hands not unique
- Hand geometry sufficient for many situations
- Suitable for authentication
- Not useful for ID problem

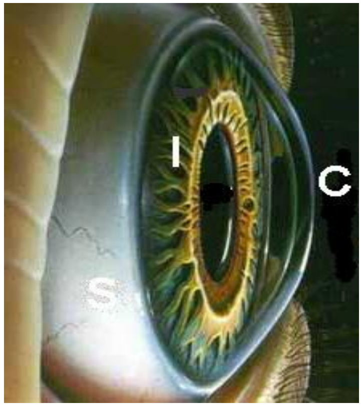
INSTRUCTIONS
PRÉSENTER VOTRE CARTE AU CENTRE DU LECTEUR
ATTENDRE QUE L'AFFICHAGE INDIQUE "POSER MAIN"
INSÉRER VOTRE MAIN DANS LE LECTEUR DE MAIN
ATTENDRE L'ACCEPTATION DU LECTEUR DE MAIN
ATTENDRE LA LUMIÈRE VERTE SUR LE TOURNIQUET
TRAVERSER LE TOURNIQUET
101/1
RSI 101/1

Hand Geometry

- Advantages
  - ✓Quick
  - ✓Hands symmetric (use other hand backwards)
- Disadvantages
  - ✓Cannot use on very young or very old
  - ✓Relatively high equal error rate

Iris Patterns





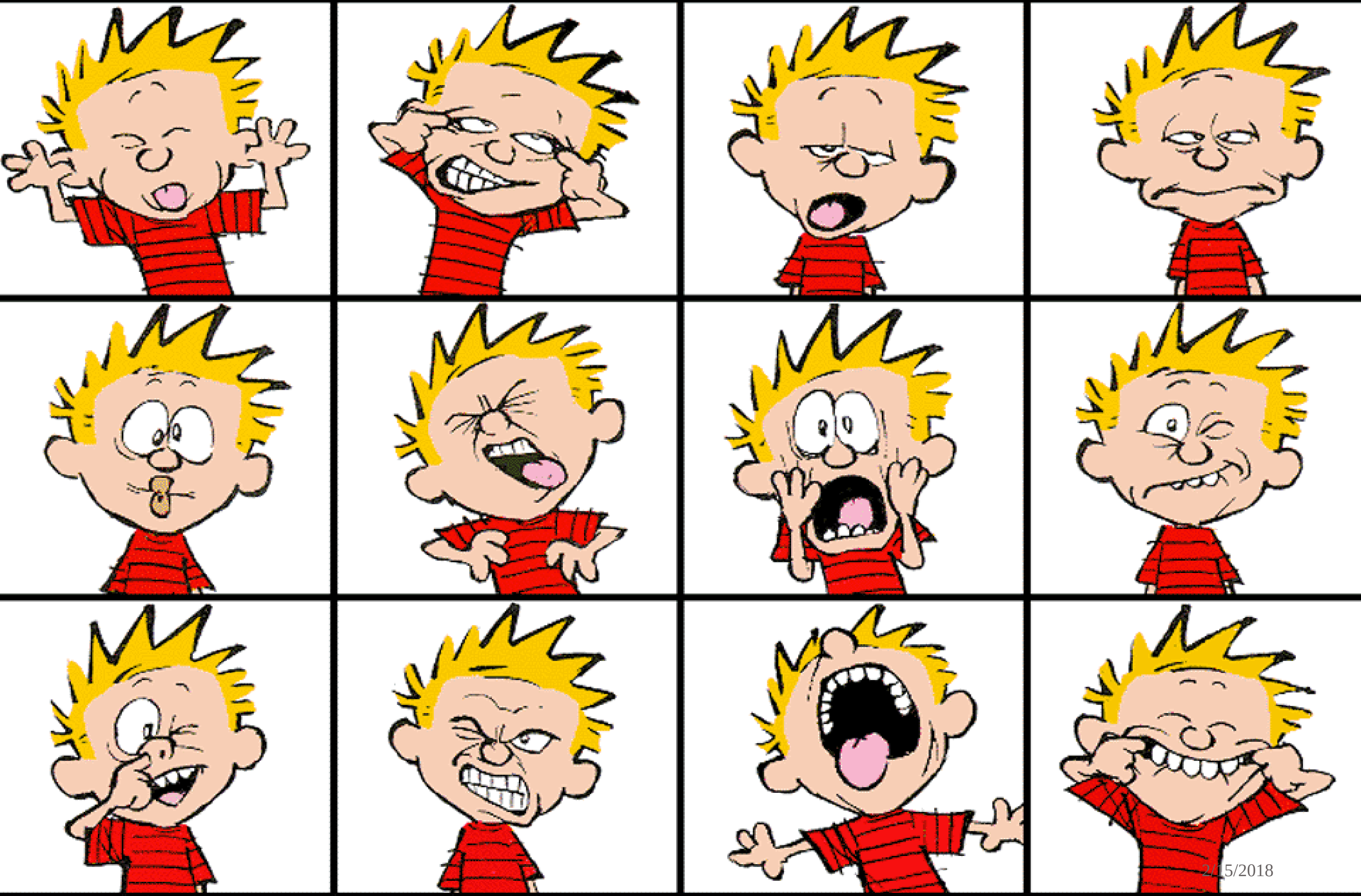
- Iris pattern development is “chaotic”
- Little or no genetic influence
- Different even for identical twins
- Pattern is stable through lifetime

Attack on Iris Scan

- Good **photo** of eye can be scanned
  - ✓ Attacker could use photo of eye
- Afghan woman was authenticated by iris scan of old photo
- To prevent photo attack, scanner could use light to be sure it is a “**live**” iris

Face Recognition

- Issues with Face Recognition?



Biometrics: The Bottom Line

- Biometrics are hard to forge
- But attacker could
  - ✓ Steal Alice’s thumb
  - ✓ Photocopy Bob’s fingerprint, eye, etc.
  - ✓ Subvert software, database, “trusted path”, …
- Also, how to revoke a “broken” biometric?
- **Biometrics are not foolproof!**
- Biometric use is limited today
- That should change in the future…

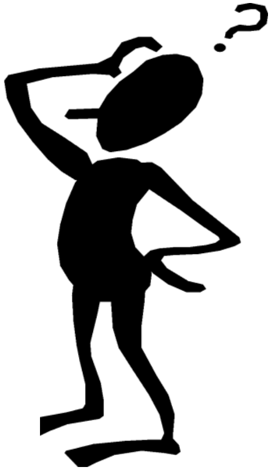
MULTI-FACTOR AUTHENTICATION

- Requires 2 out of 3 of
  1. Something you know
  2. Something you have
  3. Something you are
- **Examples**
  - ✓ ATM machine: ATM Card and PIN
  - ✓ Credit card: Card and signature
  - ✓ Smartcard with password/PIN

MULTI-FACTOR AUTHENTICATION

- **2-factor authentication:** To increase the level of security, many systems will require a user to provide 2 of the 3 types of authentication.
  - ATM card + PIN
  - Credit card + signature
  - PIN + fingerprint
  - Username + Password (Unix, NT default)

- **3-factor authentication:** For highest security
  - Username + Password + Fingerprint
  - Username + Passcode + SecurID token



END

CS 0111 LECTURE 06

CS 0111:

INTRODUCTION TO IT SECURITY

LECTURE 07

Malicious Software

Outline

- Virus and worms concepts
- Types of virus
- Computer worms
- Countermeasures

What is Malware?

Malware:

- Software intended to intercept or take partial control of a computer's operation without the user's informed consent. **OR**
- Piece of software designed with intent of compromising the security of another software
- **Also called spyware.**

What is Malware?

- **Spyware**
  - ➢ The term “spyware” taken literally suggests software that surreptitiously monitors the user. But it has come to refer more broadly to any kind of malware,
- **Malware covers all kinds of intruder software**
  - ➢Including viruses, worms, backdoors, rootkits, Trojan horses, stealware etc. These terms have more specific meanings.

The Purpose of Malware

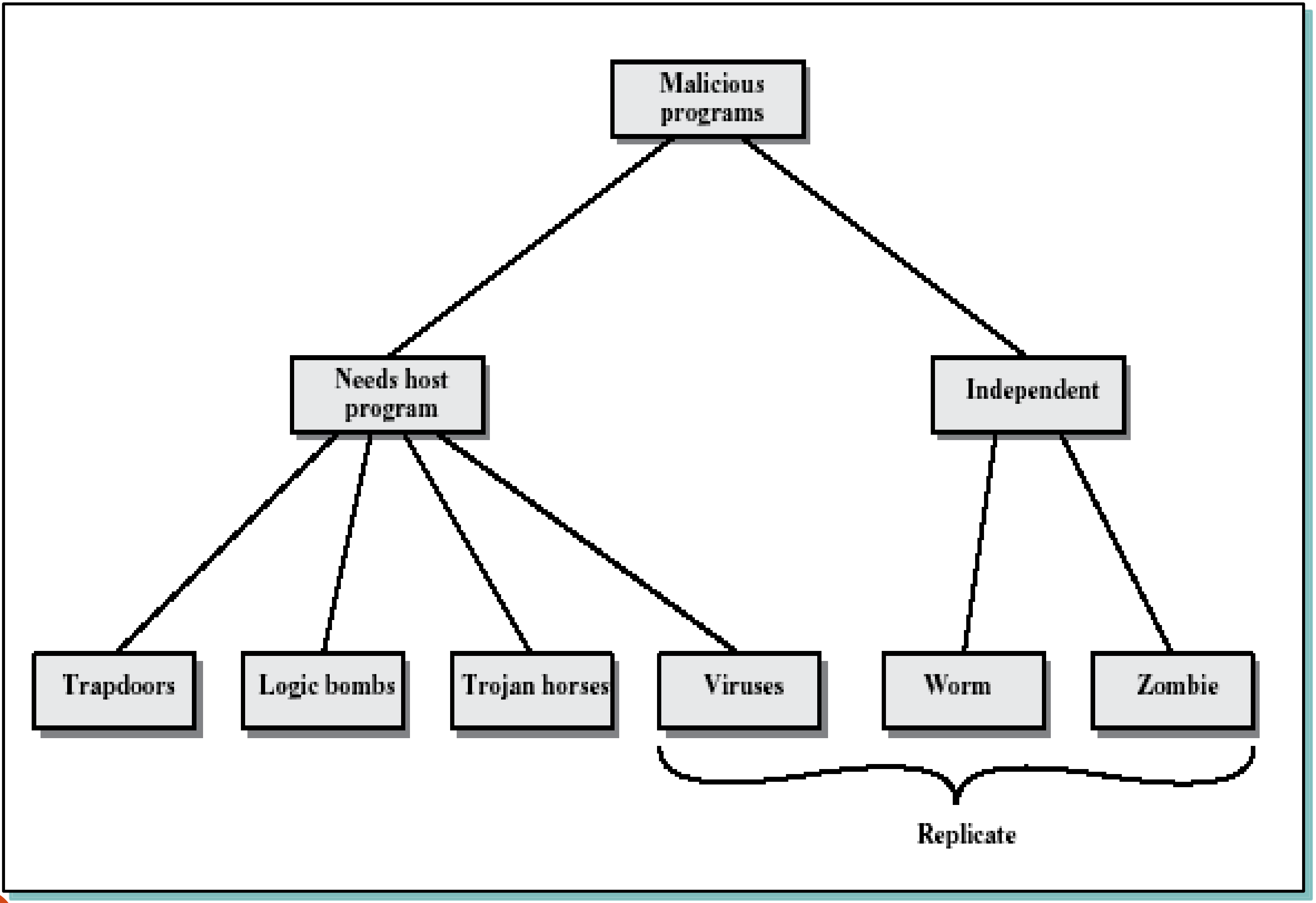
- **To partially control the user’s computer, for reasons such as:**
  - ✓To subject the user to advertising
  - ✓To launch DDoS on another service
  - ✓To spread spam
  - ✓To track the user’s activity (“spyware”)
  - ✓To commit fraud, such as identity theft and affiliate fraud
  - ✓. . . and perhaps other reasons

Malicious Programs

Two categories:

1. **Those that need a host program:** Fragments of programs that cannot exist independently of some application program, utility, or system program
2. **Those that are independent:** Self-contained programs that can be scheduled and run by the operating system (self contained)

TAXONOMY OF MALICIOUS PROGRAMS



Malicious Programs

- **Logic Bombs (**also called **slag code)**
  - ✓Logic embedded is a program that checks for a set of conditions to arise (such as the lapse of a certain amount of time or the failure of a program user to respond to a program command) and executes some function resulting in unauthorized actions.
- **Trapdoors**
  - ✓Secret undocumented entry point into a program, used to grant access without normal methods of access authentication.

Malicious Programs

- **Trojan Horse**
  - ✓Secret undocumented routine embedded within a useful program, execution of the program results in execution of the routine
  - ✓Common motivation is data destruction

- **Zombie**
  - ✓A program that secretly takes over an Internet attached computer and then uses it to launch an untraceable attack
  - ✓Very common in **Distributed Denial-Of-Service** attacks

Introduction To Virus

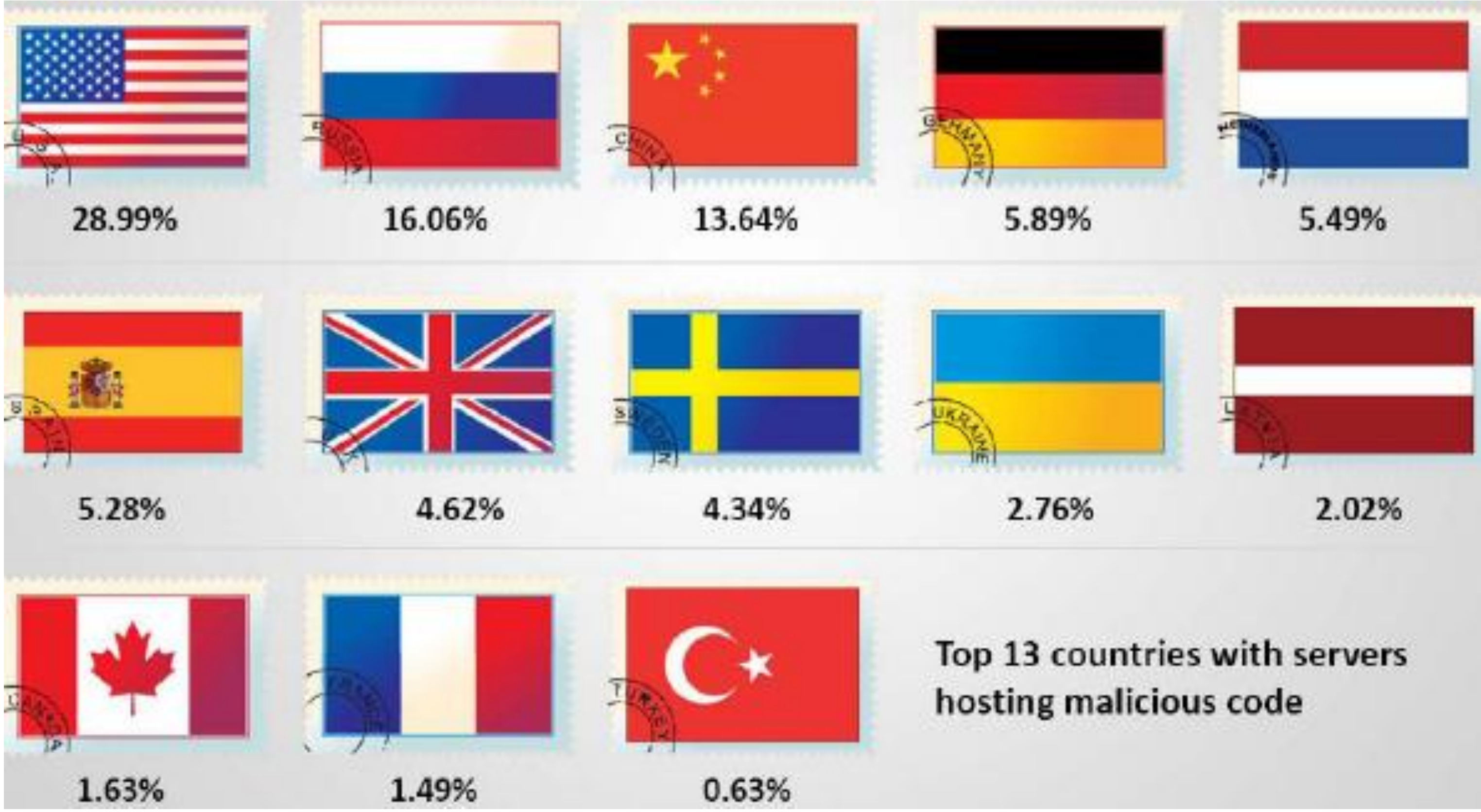
- A virus is a self-replicating program that produces its own code by attaching copies of itself into other executable codes
- Some viruses affect computers as their code is executed; others viruses lie dormant until a pre-determined logical circumstance is met.

Characteristics of Virus

- Infects other program
- Transforms itself
- Encrypts itself
- Alter data
- Corrupts files and programs
- Self propagation

Virus and worms statistics 2010

- Top 13 countries with servers hosting malicious code



Stages of virus life (6 Stages)

1. **Design stage:** developing virus code using programming languages or construction kits.
2. **Replication stage:** virus replicate for a period of time within the target system and then spreads itself
3. **Launch stage:** it gets activated with the user performing certain actions such as running an affected program.
4. **Detection stage:** a virus is identifies as threat infection target systems
5. **Incorporation stage:** ant-virus software developers assimilate defenses against the virus.
6. **Elimination stage:** users install ant-virus updates and eliminate the virus threats

NATURE OF VIRUSES (4 stages)

Four stages of virus lifetime

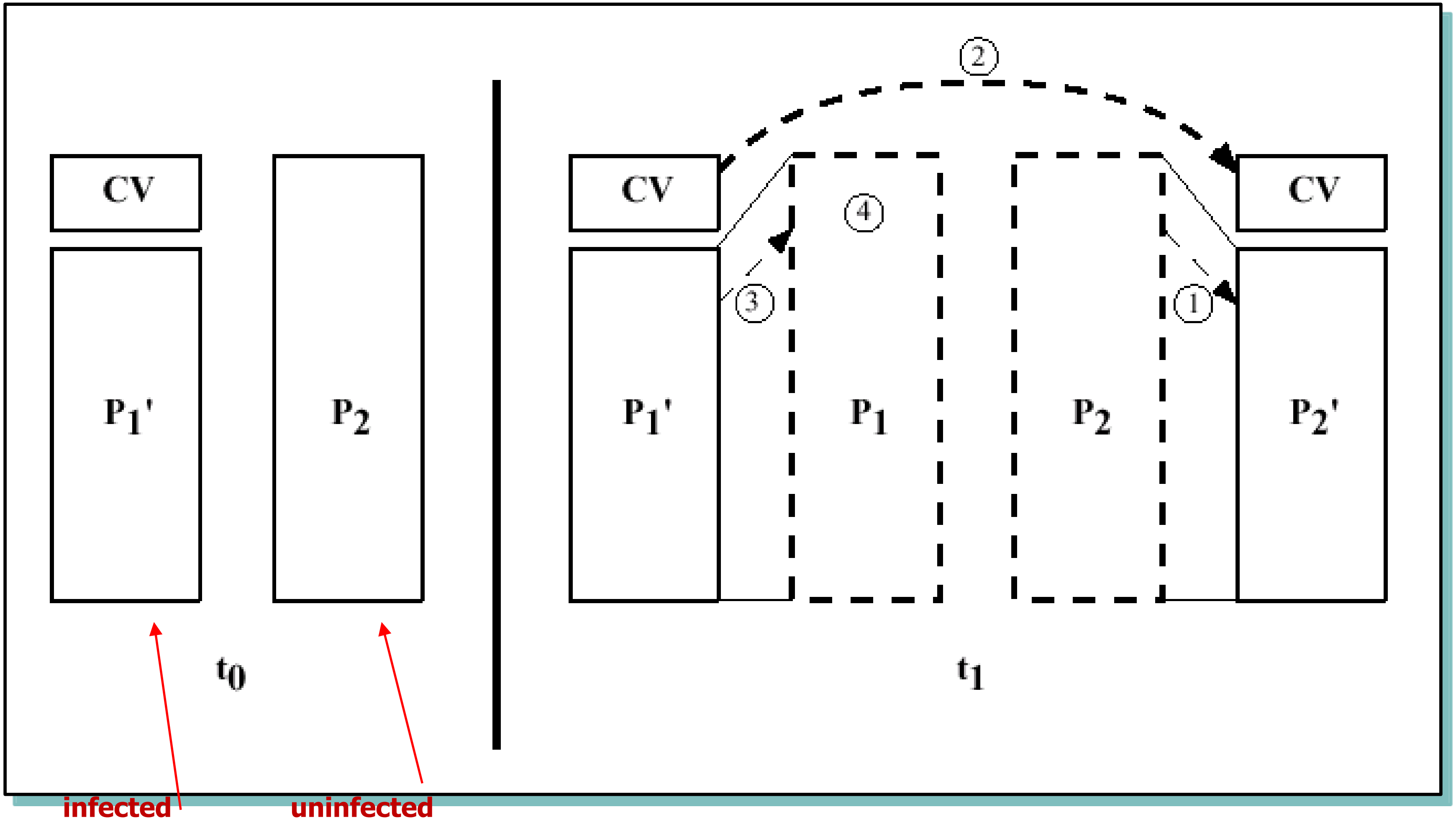
1. **Dormant phase:** virus idle
2. **Propagation phase:** cloning of virus
3. **Triggering phase:** virus activation
4. **Execution phase:** unwanted function performed

Avoiding Detection

- **Infected version** of program is **longer** than the corresponding uninfected one

- ***Solution***: **compress** the **executable file** so infected and uninfected versions are identical in length

Compression Program



infected

uninfected

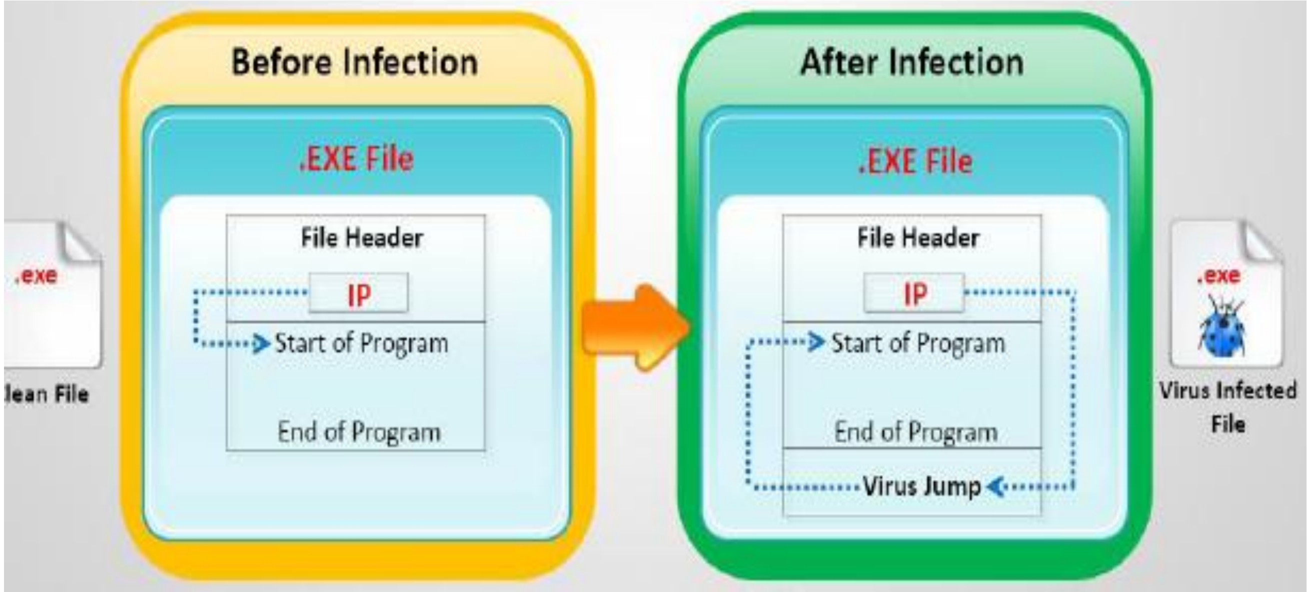
ENCRYPTION IN THE OPERATION OF A VIRUS

The role of encryption in the operation of a virus

- A portion of the virus, generally called a *mutation engine*, creates a random encryption key to encrypt the remainder of the virus.
- The key is stored with the virus, and the mutation engine itself is altered. 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.

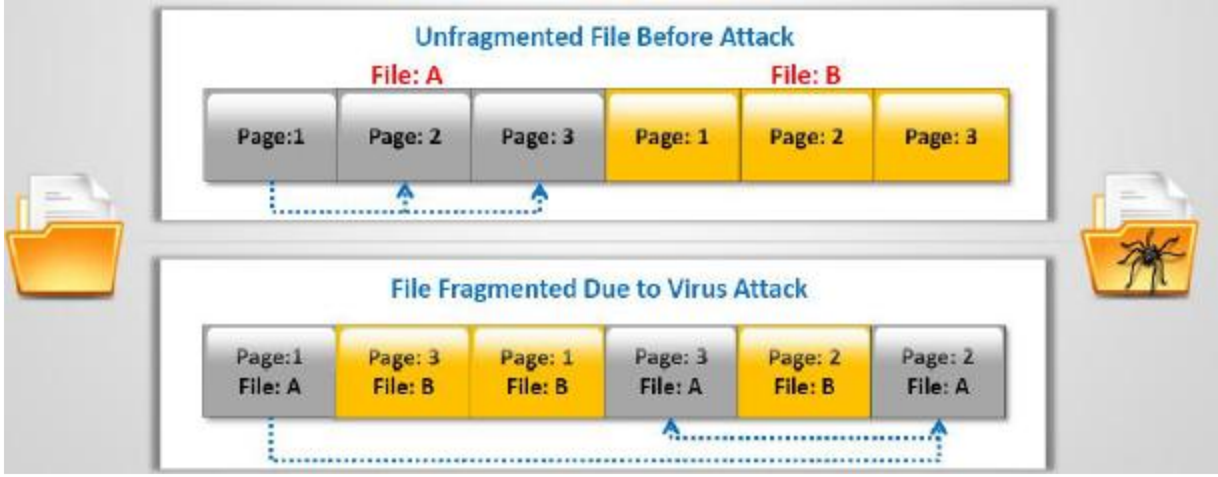
Working of viruses: Infection Phase

- In the infection phase, the virus replicates itself and attaches to an .exe file in the system.
- Some virus infect each time they are run and executed completely and others infect only when user's trigger them, which can include a day, time, or a particular event.



Working of viruses: attack phase

- Some viruses have trigger events to activate and corrupt systems
- Some viruses have bugs that replicate and perform activities such as file deletion and increase the session’s time
- They corrupt the targets only after spreading completely as intended by their developers



Why do people create computer virus?

Why do people create computer virus?

- Inflict damage to competitors
- Financial benefits
- Research projects
- Play prank
- Vandalism
- Cyber terrorism
- Distributed political massages

Indications of virus attack

Abnormal activities

- Is the systems acts in unprecedented manner, you can suspect a virus attack.
  - ✓Processes take more resources and time
  - ✓Computer beeps with on display
  - ✓Driver label changes
  - ✓Unable to load Operating System
  - ✓Anti-virus alerts

Indications of virus attack

Abnormal activities

- Is the systems acts in unprecedented manner, you can suspect a virus attack.
  - ✓Browser window “freezes”
  - ✓Hard drive is accessed often
  - ✓Files and folders are missing
  - ✓Computer freezes frequently or encounters errors
  - ✓Computer slows down when programs start.
- Note: false positive
  - ✓However, not all glitches can be attributed to virus attacks

How does a computer get infected by virus?

- Not running the latest ant-virus application
- Not updating and not installing new versions of plug-ins
- Installing pirated software
- Opening infected e-mail attachments
- When a user accepts files and downloads without checking properly for the source.

Types of viruses

- System or boot sector viruses
- Files virus
- Cluster viruses
- Macro virus
- Multipartite virus

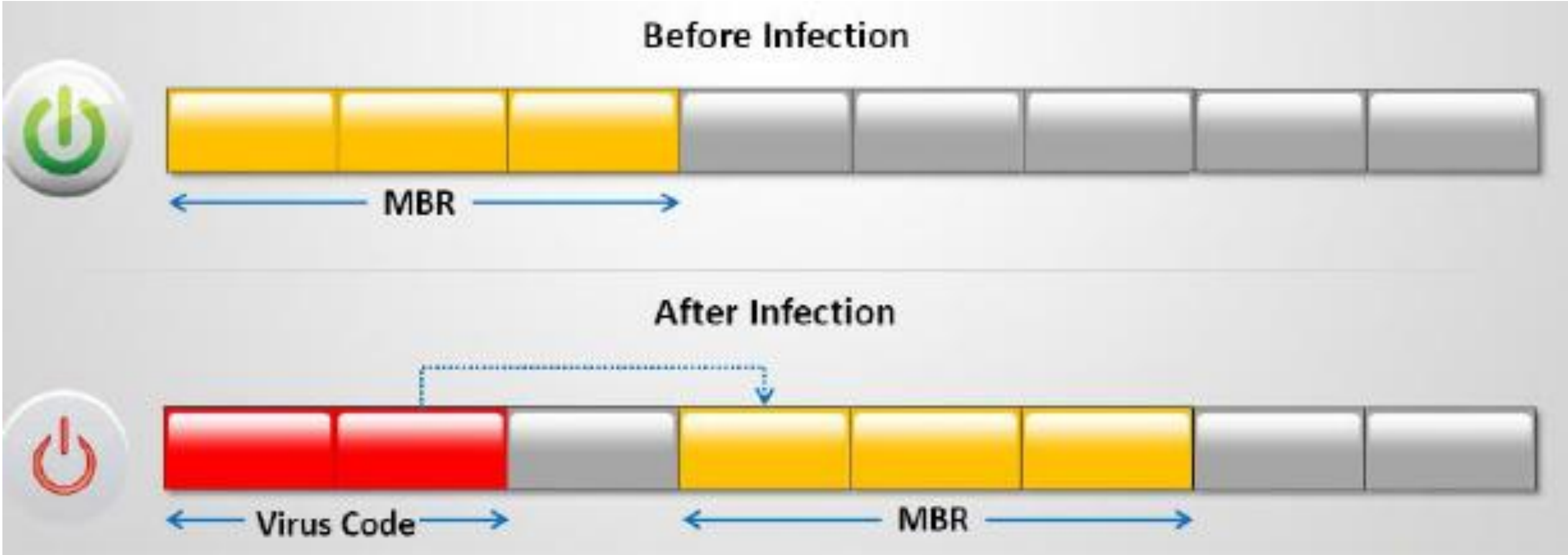
What do they infect?

How do they infect?

- Stealth virus/tunneling virus
- Encryption virus
- Polymorphic virus
- Overwriting file or cavity virus
- Sparse virus
- Companion virus/camouflage virus
- Shell virus
- File extension virus
- Add-on virus
- Intrusive virus
- Direct action or transient virus
- Terminate and stay resident virus (TSR)

System or boot sector viruses

- Boot sector virus moves MBR to another location on the hard disk and copies itself to the original location of MBR
- When system boots, virus code is executed first and then control is passed to original MBR



MBR: Master Boot Record

Files and multipartite viruses

- **File virus**
  - ✓File virus infect files which are executed or interpreted is the system such as COM, EXE, SYS, OVL, OBJ, PRG, MNU and BAT files
  - ✓Files virus can be either direct-action (non-resident) or memory resident
- **Multipartite virus**
  - ✓Multipartite virus that attempts to attack both the boot sector and the executable or grogram files at the same time

Macro virus

- Macro viruses infect files created by Microsoft Word or Excel
- Most macro viruses are written using macro language Visual Basic for Application (VBA)
- Macro viruses infect templates or convert infected documents into template files, while maintaining their appearance if ordinary document files.

Cluster viruses

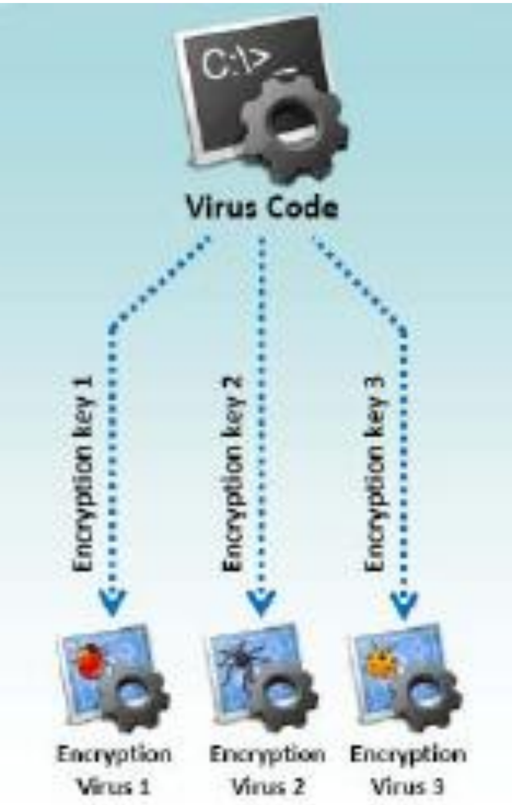
- Cluster viruses modify directory table entries so that directory entries point to the virus code instead of the actual program
- There is only copy of the virus on the disk infecting all the programs in the computer system
- It will launch itself first when any program on the computer system is started and then the control is passed to actual program

Stealth/tunneling viruses

- These viruses evade the anti-virus software by intercepting its requests to the operation system
- A virus can hide itself by intercepting the ant-virus software’s request to read the file and passing the request to the virus, instead of the OS.
- The virus can then return an uninfected version of the file to the ant-virus software, so that it appears as if the file is “clean”

Encryption viruses

- This type of virus uses simple encryption to encipher the code
- The virus is encrypted with a different key for each infected files
- AV scanner cannot directly detect these types of viruses using signature detection method.



Polymorphic code

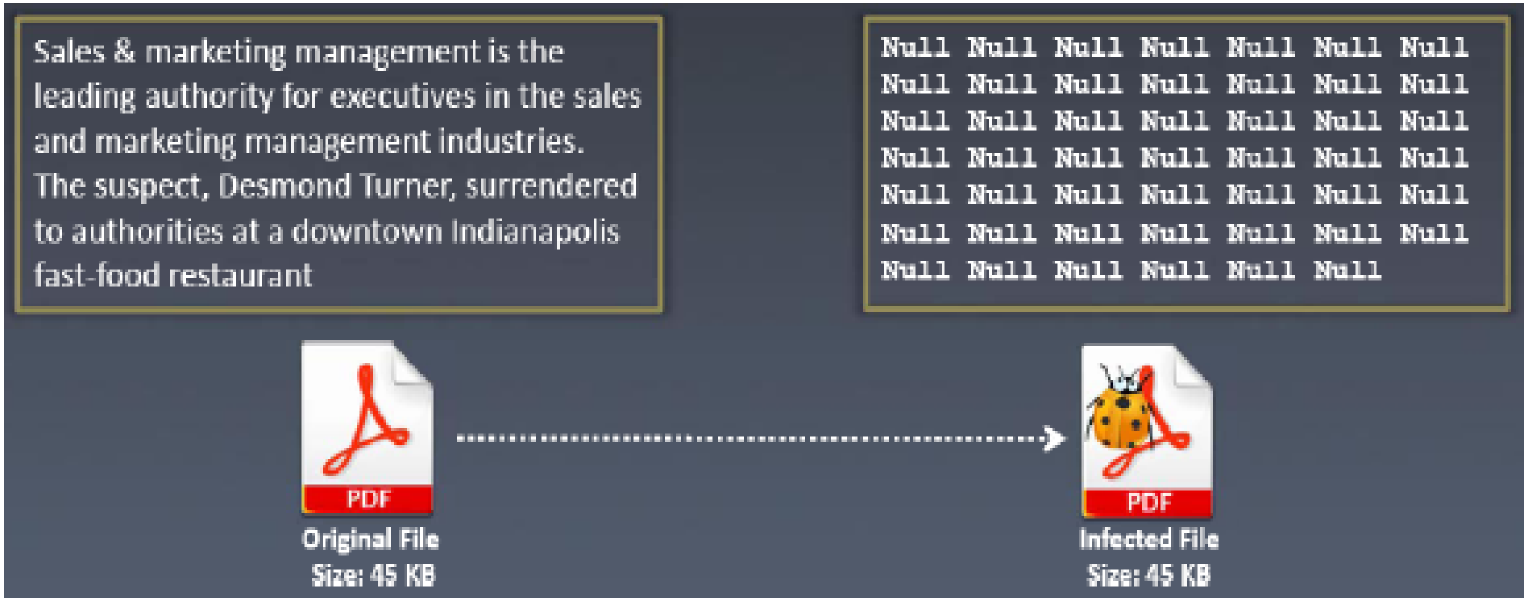
- Polymorphic code is a code that mutates while keeping the original algorithm intact
- To enable polymorphic code, the virus has to have a polymorphic engine (also called mutation engine or mutation engine)
- A well-written polymorphic virus therefore has no parts that stay same on each infection

Metamorphic viruses

- Metamorphic viruses rewrite themselves completely each time they are to infect new executable.
- Metamorphic code can reprogram itself by translating its own code into a temporary representation and then back to the normal code again.
- For example, W32/simile consisted of over 1400 lines of assembly code, 90% lines of assembly code, 90% of it is of the metamorphic engine.

File overwriting or cavity viruses

- Cavity virus overwrites a part of the host file with a constant (usually nulls), without increasing the length of the file and preserving its functionality.



Sales & marketing management is the leading authority for executives in the sales and marketing management industries. The suspect, Desmond Turner, surrendered to authorities at a downtown Indianapolis fast-food restaurant

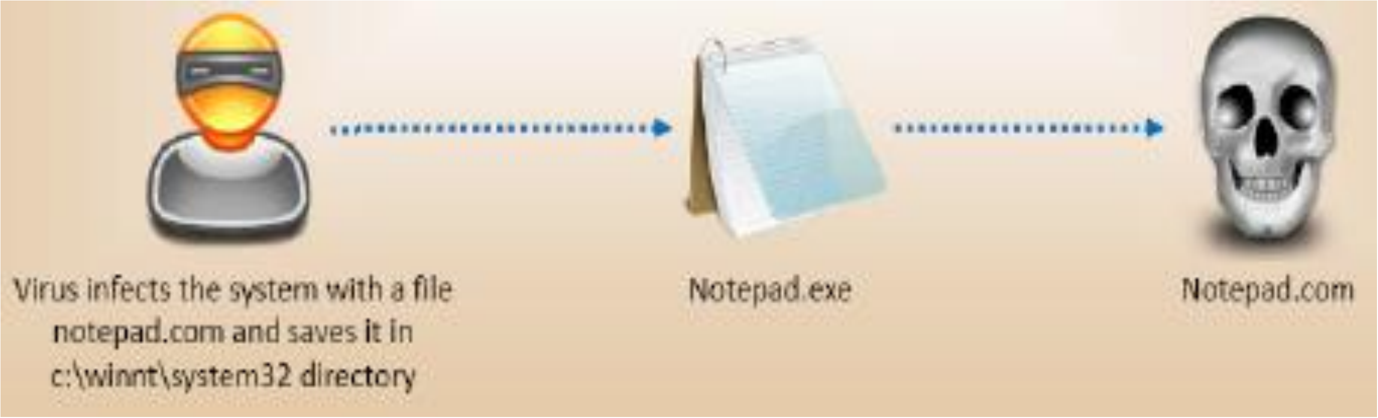
```
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null Null
Null Null Null Null Null Null
```

Sparse Infector viruses

- Sparse infector virus infects only occasionally (e.g. every tenth program executed), or only files whose lengths falls within a narrow range.
- By infection less often, such viruses try to minimize the probability of being discovered.

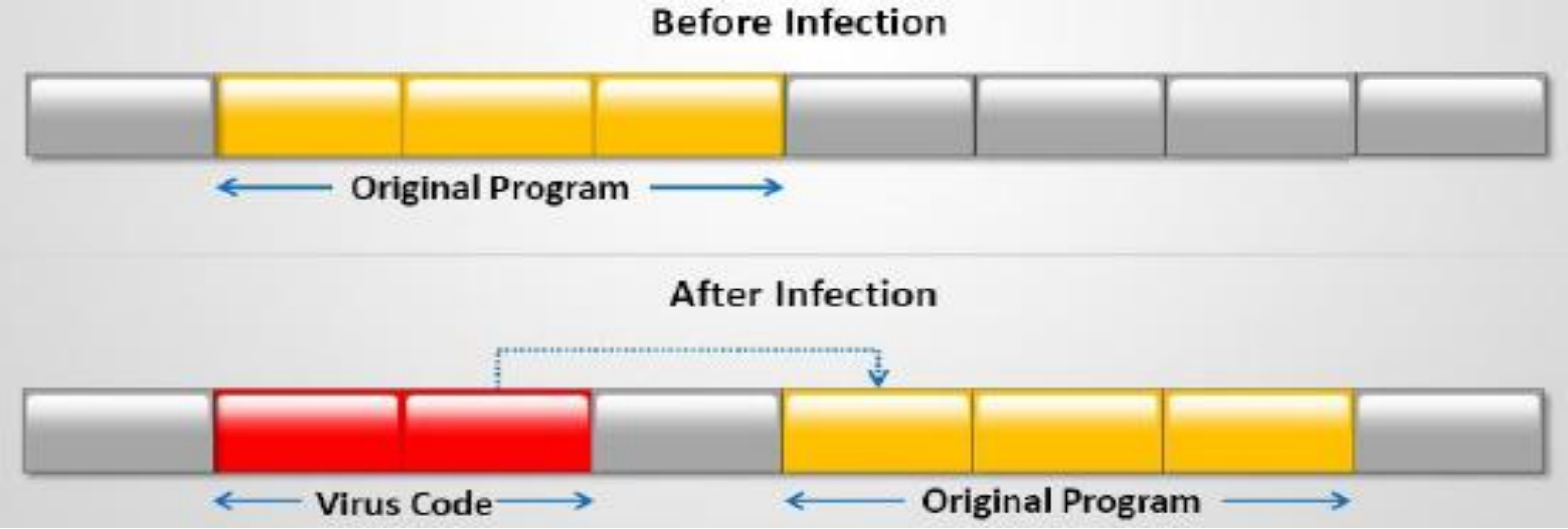
Companion/camouflage viruses

- A companion virus creates a companion file for each executable file the virus infects
- Therefore, a companion virus may save itself as notepad.com and every time a user executes a notepad.exe (good program), the computer will load notepad.com (virus) and infect the system.


Virus infects the system with a file notepad.com and saves it in c:\winnt\system32 directory
Notepad.exe
Notepad.com

Shell viruses

- Virus code forms a shell around the target host program's code, making itself the original program and host code as its sub-routine
- Almost all boot program viruses are shell viruses

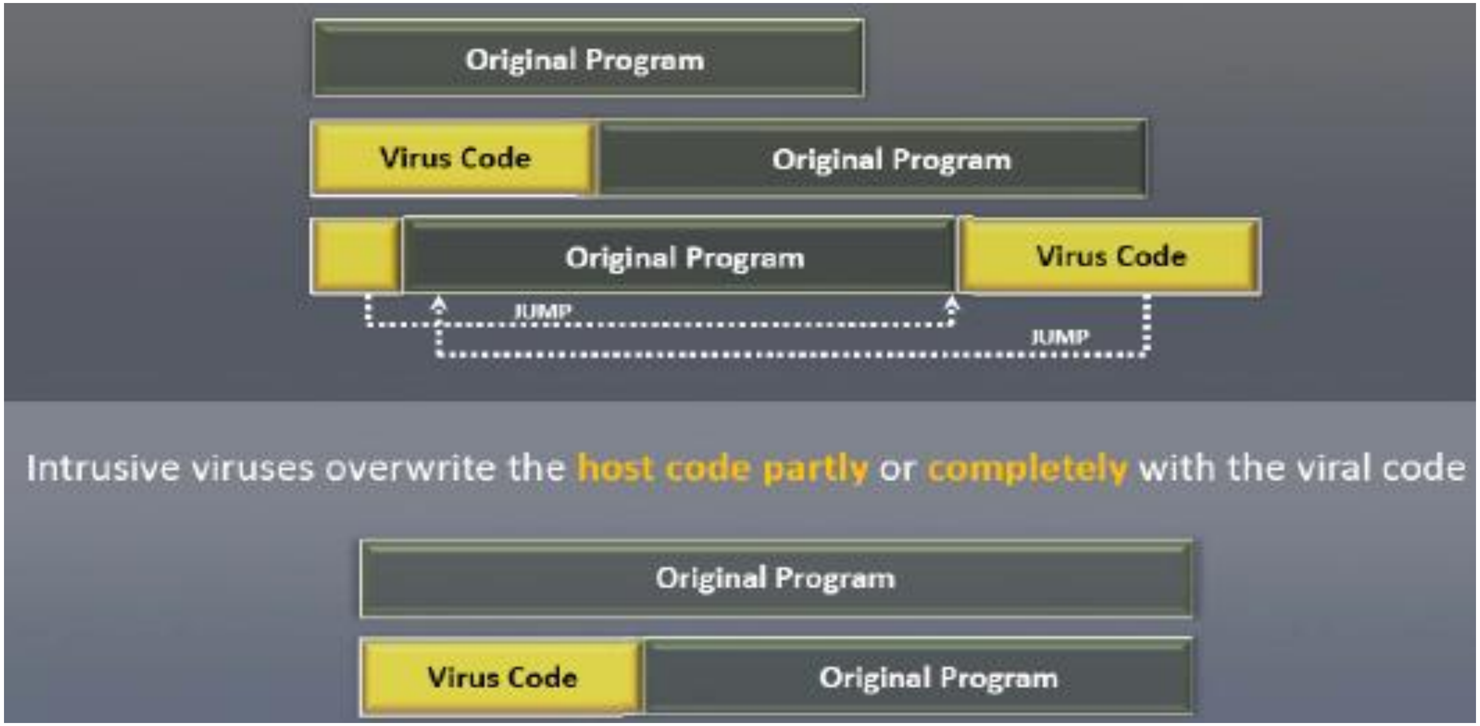


File extension viruses

- File extension viruses change the extensions of the files
- .TXT is safe as it indicates as pure text file
- With extension turned off, if someone sends you a file named BAD.TXT.VBS, you will only see BAD.TXT
- If you have forgotten that extensions are turned off, you might think is a text file and open it.
- This is an executable visual basic script virus file and could do serious damage.
- Countermeasure is turn off "Hide file extensions" in windows.

Add-on and intrusive viruses

- Add-on viruses append their code to the host code without making any changes to the latter or relocate the host code to insert their own code at the beginning.



Intrusive viruses overwrite the host code partly or completely with the viral code

Transient and terminate and stay resident viruses

Basic infection techniques

- **Direct action or transient virus**
  - ✓Transfers all the controls of the host code to where it resides
  - ✓Selects the target program to be modified and corrupt it
- **Terminate and stay resident virus (TSR)**
  - ✓Remains permanently in the memory during the entire work session even after the target host’s program is executed and terminated; can be removed only by rebooting the system.

Computer worms

- Computer worms are malicious programs that replicate, execute, and spread across the network connections indecently without human interaction.
- Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however some worms carry a payload to damage the host system.
- Attackers use worm payload to install backdoors in infected computers, which turns them into zombies and creates botnet; these botnets can be used to carry further cyber attacks.

How is worm different from a virus?

- A worm is special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.
- A worm takes advantage of file information transport features on computer systems and spreads through the infected network automatically but a virus does not.

Virus detection methods

- **Scanning**
  - ✓Once a virus has been detected, it is possible to write scanning programs that look for signature string characteristics of the virus.
- **Integrity checking**
  - ✓Integrity checking products work by reading the entire disk and recording integrity data that acts as a signature for the files and system sectors.
- **Interception**
  - ✓The interceptor monitors the operation system requests that are written to the disk.

Viruses Countermeasures

- Antivirus approaches
- Advanced antivirus techniques
  - ✓ Generic Decryption
  - ✓ Digital Immune System
- Behavior-blocking software

Viruses Countermeasures

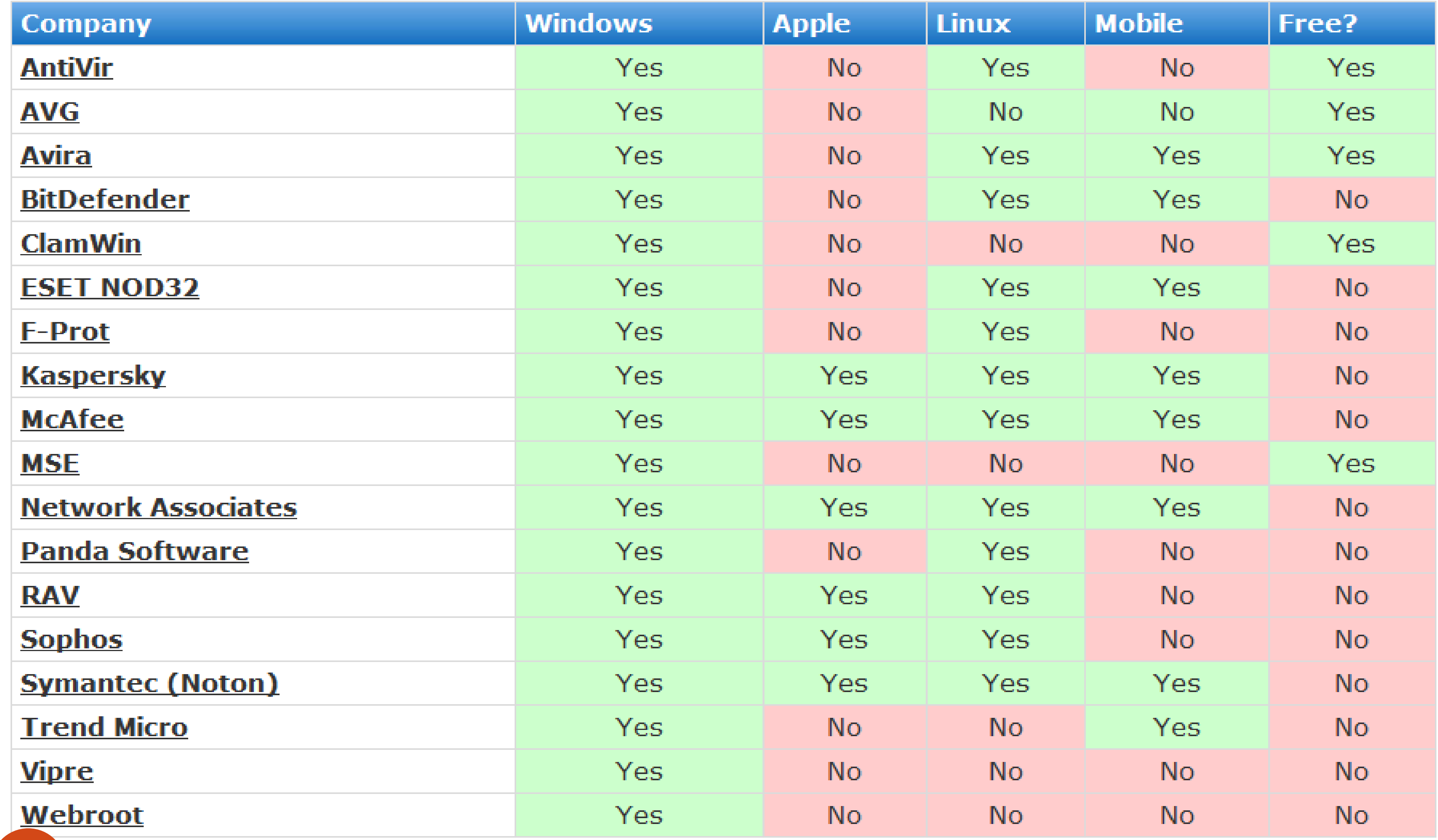
1. Antivirus Approaches

- **Detection**
  - ✓Determine that it has occurred and locate the virus
- **Identification**
  - ✓Identify the specific virus
- **Removal**
  - ✓Remove all traces and restore the program to its original state

Generations of Antivirus Software

- **First:** Simple scanners (record of program lengths)
- **Second:** Heuristic scanners (integrity checking with checksums)
- **Third:** Activity traps (memory resident, detect infected actions)
- **Fourth:** Full-featured protection (suite of antivirus techniques, access control capability)

WHAT ARE THE CURRENT AVAILABLE ANTIVIRUS PROGRAMS?



Company	Windows	Apple	Linux	Mobile	Free?
AntiVir	Yes	No	Yes	No	Yes
AVG	Yes	No	No	No	Yes
Avira	Yes	No	Yes	Yes	Yes
BitDefender	Yes	No	Yes	Yes	No
ClamWin	Yes	No	No	No	Yes
ESET NOD32	Yes	No	Yes	Yes	No
F-Prot	Yes	No	Yes	No	No
Kaspersky	Yes	Yes	Yes	Yes	No
McAfee	Yes	Yes	Yes	Yes	No
MSE	Yes	No	No	No	Yes
Network Associates	Yes	Yes	Yes	Yes	No
Panda Software	Yes	No	Yes	No	No
RAV	Yes	Yes	Yes	No	No
Sophos	Yes	Yes	Yes	No	No
Symantec (Noton)	Yes	Yes	Yes	Yes	No
Trend Micro	Yes	No	No	Yes	No
Vipre	Yes	No	No	No	No
Webroot	Yes	No	No	No	No

Viruses Countermeasures

2. Advanced Antivirus Techniques

- Generic Decryption
- Digital Immune System

Generic Decryption

- Easily **detects** even most complex **polymorphic virus**
- **No damage** to the personal computer

- Contains following elements:
  - ✓ **CPU emulator:** software based virtual computer
  - ✓ **Virus signature scanner:** scans target code for known signatures
  - ✓ **Emulation control module:** control execution of target code

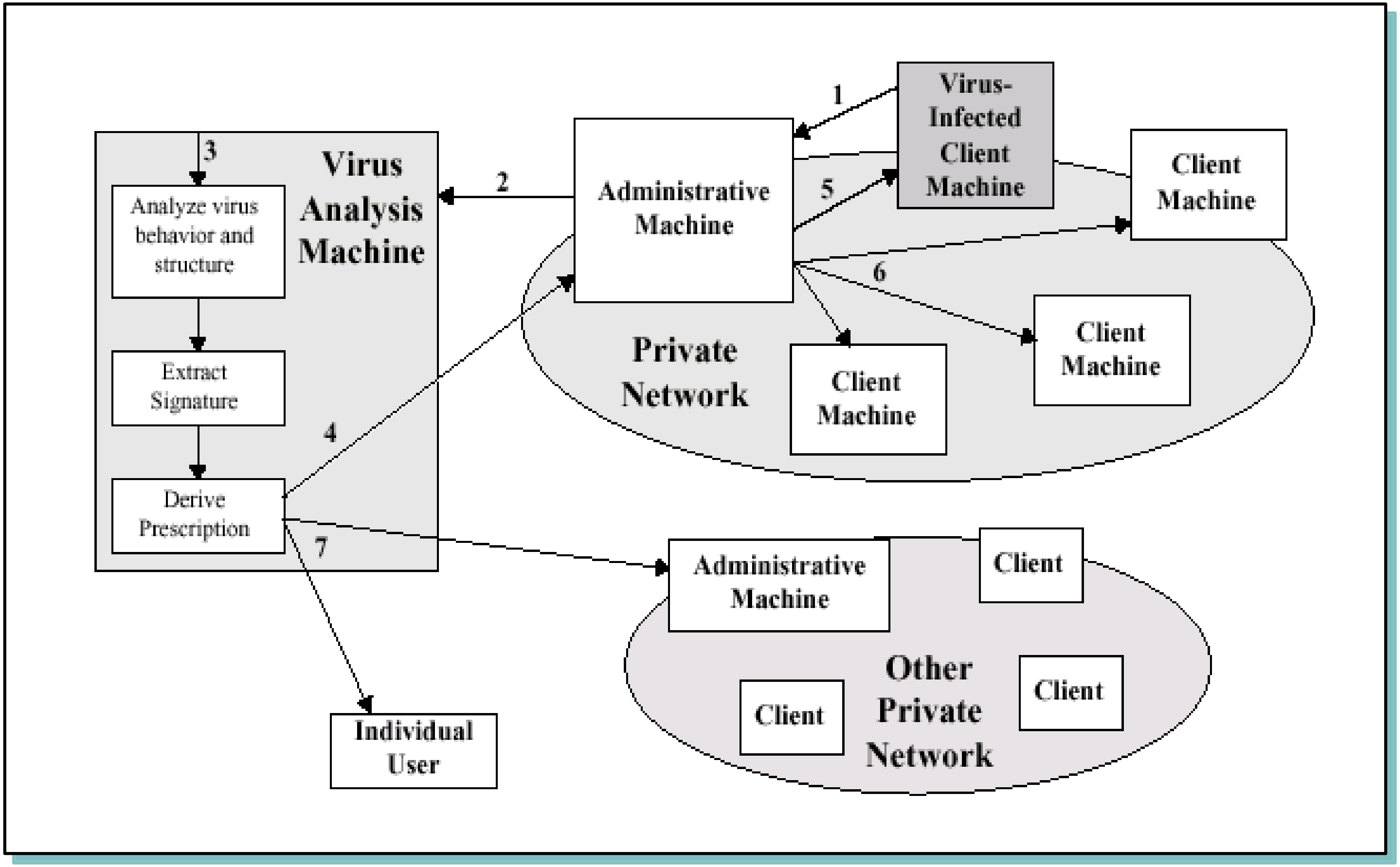
Digital Immune System

- Pioneered by **IBM**
- Response to rate of virus propagation
  - ✓ Integrated mail systems - Outlook
  - ✓ Mobile program systems – ActiveX, Java
- Expands the **use** of program **emulation**
- Depends on a **central virus analysis machines**

Digital Immune System

- This system provides a general-purpose emulation and **virus-detection** system. The objective is to provide **rapid response time** so that viruses can be stamped out almost as soon as they are introduced.
- When a new virus enters an organization, the immune system automatically captures it, analyzes it, adds detection and shielding for it, removes it, and passes information about that virus to systems running a general antivirus program so that it can be **detected before** it is allowed to run elsewhere.

Digital Immune System



Viruses Countermeasures

3. Behavior-blocking Software

- **Monitors** program behavior in **real-time** for malicious actions – part of OS
- Look for **well defined requests** to the OS: modifications to files, disk formats, mods to scripts or macros, changes in config settings, open network connections, etc.
- IPS – **Intrusion Prevention Systems**

Behavior-blocking Software

How does behavior-blocking software work?

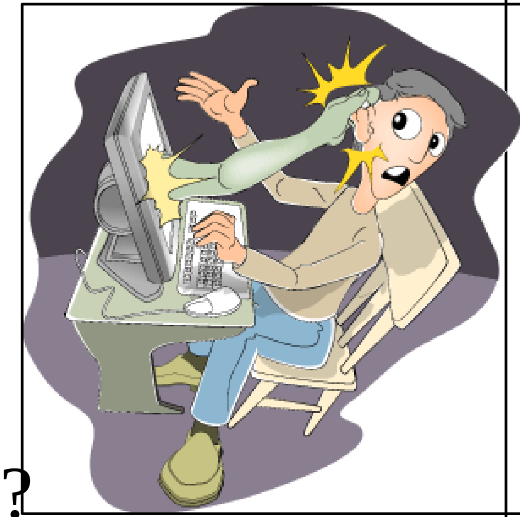
- Behavior-blocking software **integrates** with the operating system of a host computer and monitors program behavior in real-time for malicious actions.
- The behavior blocking software then blocks potentially malicious actions before they have a chance to affect the system.

Malicious Code Protection

Types of Products

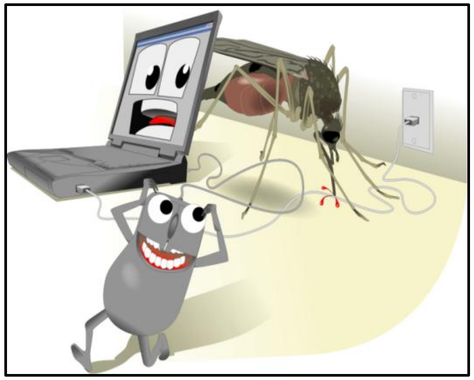
- **Scanners** - identify known malicious code - search for ***signature strings***
- **Integrity Checkers** – determine if code has been altered or changed – ***checksum*** based
- **Vulnerability Monitors** - prevent modification or access to particularly sensitive parts of the system – user defined
- **Behavior Blockers** - list of rules that a legitimate program must follow – ***sandbox*** concept

PRACTICE:
USE CARE WHEN READING EMAIL WITH ATTACHMENTS



- Executable content
- Interesting to you (social engineering)
- Violates trust
- **KRESV tests**
  - **Know test:** Know the sender?
  - **Received test:** Received email before?
  - **Expect test:** Did you expect this email?
  - **Sense test:** Does this email make sense?
  - **Virus test:** Contain a virus?
- Doesn’t pass all tests? Don’t open!
- **Level of effort: High**

INSTALL AND USE ANTIVIRUS SOFTWARE

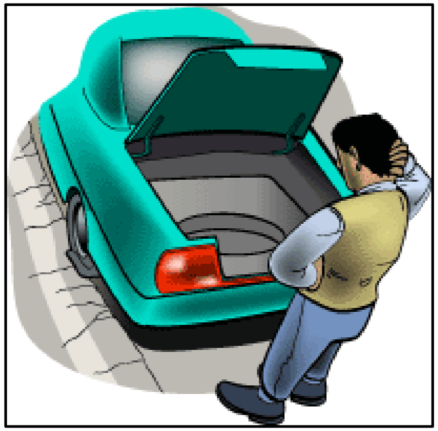


- Easy way to gain control of your computer or account
- Violates “trust”
- **DURCH tests**
  - **Demand**: Check files on demand?
  - **Update**: Get new virus signatures automatically?
  - **Respond**: What can be done to infected files?
  - **Check**: Test every file for viruses.
  - **Heuristics**: Does it look like a virus?
- **Level of effort: low**

PRACTICE:

MAKE BACKUPS OF IMPORTANT FILES AND FOLDERS

- Can you recover a file or folder if lost?
- Does your computer have a “spare tire”?
- **FOMS tests**
  - **Files**: What files should be backed up?
  - **Often**: How often should a backup be made?
  - **Media**: hat kind of media should be used?
  - **Store**: Where should that media be stored?
- Level of effort:
  - **setup: medium to high**
  - **maintaining: medium**

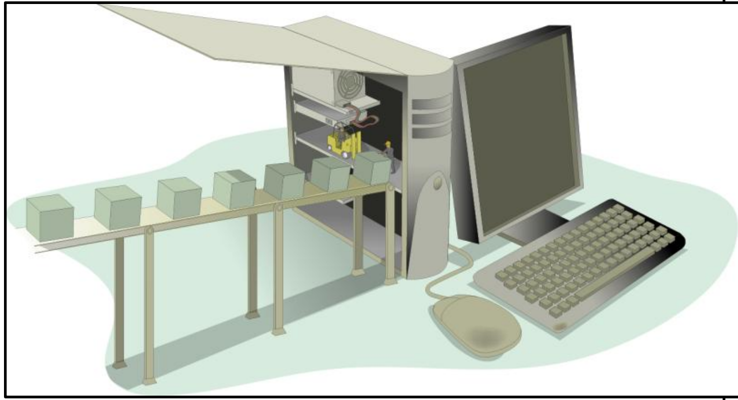


INSTALL AND USE A FIREWALL PROGRAM

- Limit connections to computer
- Limit connections from computer based on application
- Portable – follows the computer (laptop)
- **PLAT tests**
  - **Program** – What program wants to connect?
  - **Location** – Where does it want to connect?
  - **Allowed** – Yes or no?
  - **Temporary** – Permanent or temporary?
- Level of effort:
  - **install: low**
  - **maintain: high**

USE CARE WHEN DOWNLOADING AND INSTALLING PROGRAMS

Program may satisfy needs but may harm computer



- What does it *really* do?
- **LUB tests**
  - **Learn** – What does the program do to your computer?
  - **Understand** – Can you return it and completely remove it?
  - **Buy** – Purchase/download from reputable source?
- **Level of effort: high**

Virus and worms countermeasures (others)

- Ensure the executable code sent to the organization is approved
- Do not boot the machine with infected bootable system disk
- Know about the latest virus threats
- Check the DVDs and CDs for virus infection
- Ensure the pop-up blocker is returned on use an internet firewall
- Run disk clean up, registry scanner and defragmentation once a week
- Block the files with more than one file type extension
- Be caution with the files being sent through the internet messenger.

Virus and worms countermeasures (Others)

- Install ant-virus software that detects and removes infections as they appear
- Generate an anti-virus policy for safe computing and distribute it to the staff
- Pay attention to instructions while downloading files or any programs from the Internet
- Update the ant-virus software on the monthly basis, so that it can identify and clean out new bugs

Virus and worms countermeasures (others)

- Avoid opening the attachments received form an unknown sender as virus spread via e-mail
- Possibility of virus infection may corrupt data, thus regularly maintain data back up
- Schedule regular scans for all drivers after the installation of ant-virus
- Do not accept disks or programs without checking them first using a current version of anti-virus program.

END

CS 0111 LECTURE 07