موسسه آموزش عالی غیردولتی غیرانتفاعی بصیر آبیک

NETWORK AND E-COMMERCE SECURITY

Basir University, 2020-2021

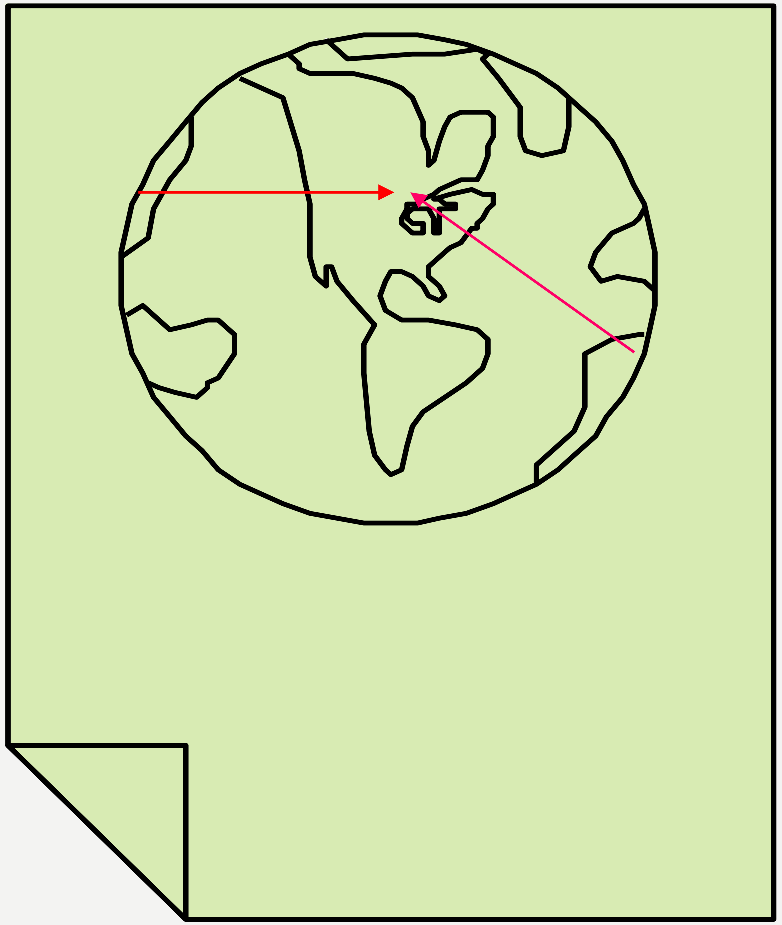
By: Prof. Dr. Mohammad Hajarian

SECURITY

THE PROBLEM OF NETWORK SECURITY

The Internet allows an attacker to attack from anywhere in the world from their home desk.

They just need to find one vulnerability: a security analyst need to close every vulnerability.



PROGRESS OF SECURITY ATTACKS

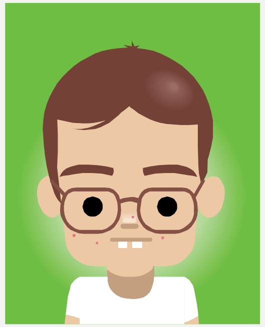
Threat Type	Year: Example Threats
Experiment	1984: Fred Cohen publishes "Computer Viruses: Theory and Experiments"
Vandalism	1988: Jerusalem Virus deletes all executable files on the system, on Friday the 13th. 1991: Michelangelo Virus reformats hard drives on March 6, M's birthday.
Hactivism	2010: Anonymous' Operation Payback hits credit card and communication companies with DDOS after companies refuse to accept payment for Wiki-Leaks.
Cyber-crime	2007: Zeus Trojan becomes 'popular'; turns computers into zbots and spyware steals credit card (CC) numbers. 2008-9: Gonzales re-arrested for implanting spyware on WLANs, affecting 171 M CC. 2013: In July 160 M CC numbers are stolen via SQL Attack. In Dec. 70 M CC numbers are stolen through Target stores. 2016-7: Ransomware charges $522 to decrypt your disk; Petya/NotPetya does not. 2017: Cryptocurrency coin mining
Information Warfare	2007, 2008: Russia launches DDOS attack against Estonia, Georgia news, gov't, banks 2010: Stuxnet worm disables 1000 of Iran's nuclear centrifuges. 2016-7: N Korea Lazarus stole $81 M Bangladesh Centralbank, releases WannaCry ransomware to fund military operations.
Surveillance State	2012: Chinese affiliations attack U.S. businesses to steal intellectual property. 2013: Lavabit closes secure email service rather than divulge corporate private key to NSA without customers' knowledge.

HISTORY OF CYBER-WAR

YEAR	FROM -> TO	ATTACK DESCRIPTION
2007	Russia -> Estonia	DOS attacks on gov't, financial inst., news
2008	Russia -> Georgia	DOS attacks on Internet, gov't websites
2008	US -> US	Malware to top aides of pres. candidates
2009	China->Embassies, foreign ministries	GhostNet malware: Command & Control software
2012	US, Israel -> Iran	Stuxnet Worm disables nuclear facilities
2010	India <->Pakistan	Hacker groups hit gov't websites
2011	China -> Canada	Spyware virus causes shutdown of economic agencies
2012	-> Iran, Middle East	Flame cyber-espionage malware
2013	N. Korea -> S. Korea	Dark Seoul Malware hits TV, banks; makes computers unusable.

CRACKERS

System Administrators
Some scripts are useful to protect networks…
Get info from hacker bulletin boards



Cracker:
Computer-savvy programmer creates attack software

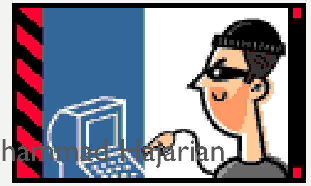
Dark Web

For Sale:
Credit Cards
Medical Insurance
Identification
Malware

Script Kiddies:
Know how to execute programs

Criminals:
Create & sell botnets -> spam
Sell credit card numbers,…

Nation States:
Cyber-warfare, spying, extortion, DDOS



Crimeware or Attack Kit=$1K-2K
1 M Email addresses = $8
10,000 PCs = $1000

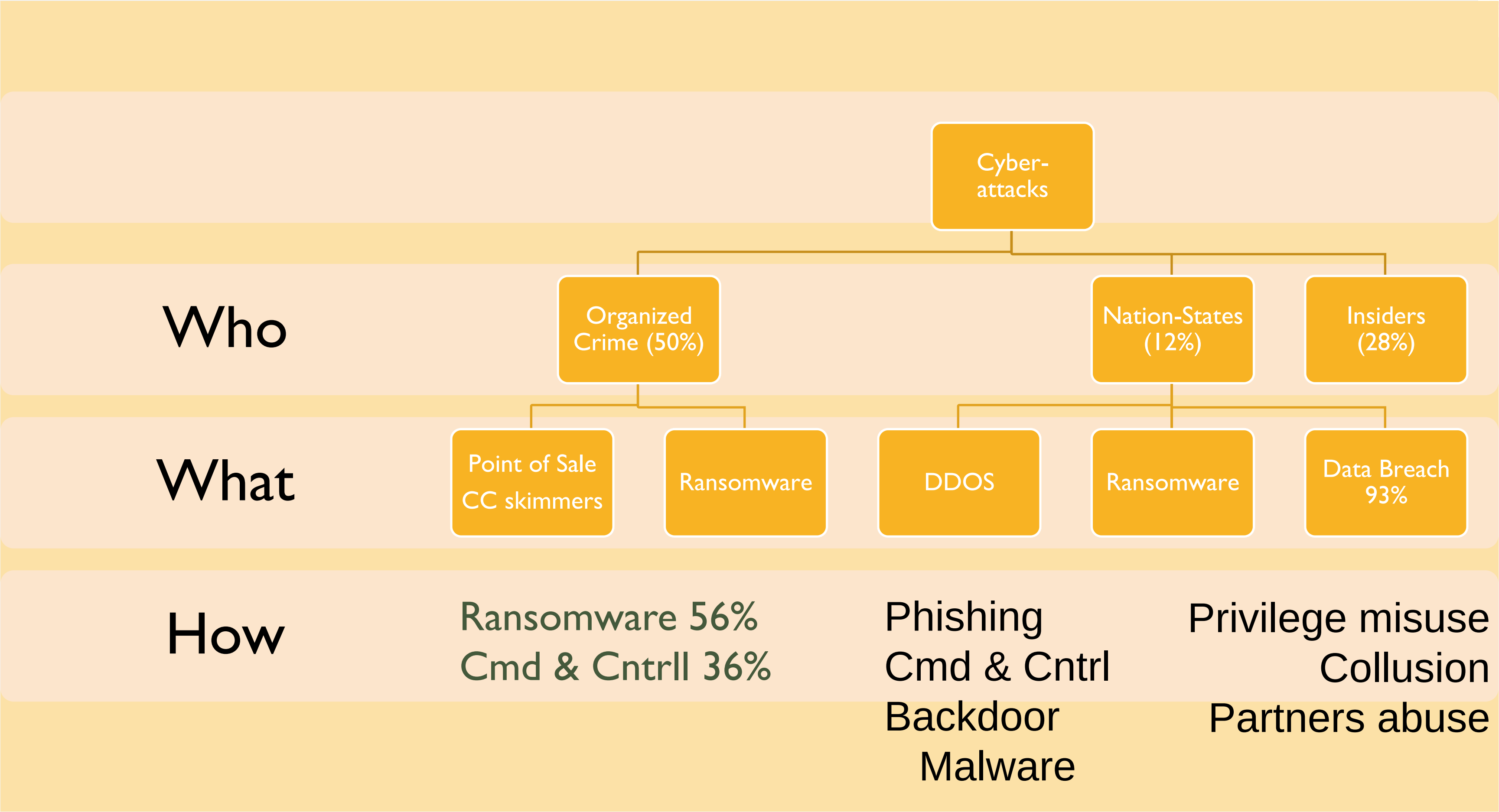
OTHER HACKERS/CRACKERS:

- **Cyberterrorists**
- **Cyberwar**: National governments attack IT
- **Espionage**: Accused: Russia, North Korea, China, France, South Korea, Germany, Israel, India, Pakistan, US.

ADVANCED PERSISTENT THREAT

- Advanced: Combination of custom & common malware
  - Target: Business or Gov’t data/operation
- Persistent: Extended period attack until target is compromised
- Threat: Organized, capable, well-funded attacker
  - Source: Gov’t or criminal enterprise

WHO-WHAT-HOW



Cyber-attacks

Who

Organized Crime (50%)

Nation-States (12%)

Insiders (28%)

What

Point of Sale CC skimmers

Ransomware

DDOS

Ransomware

Data Breach 93%

How

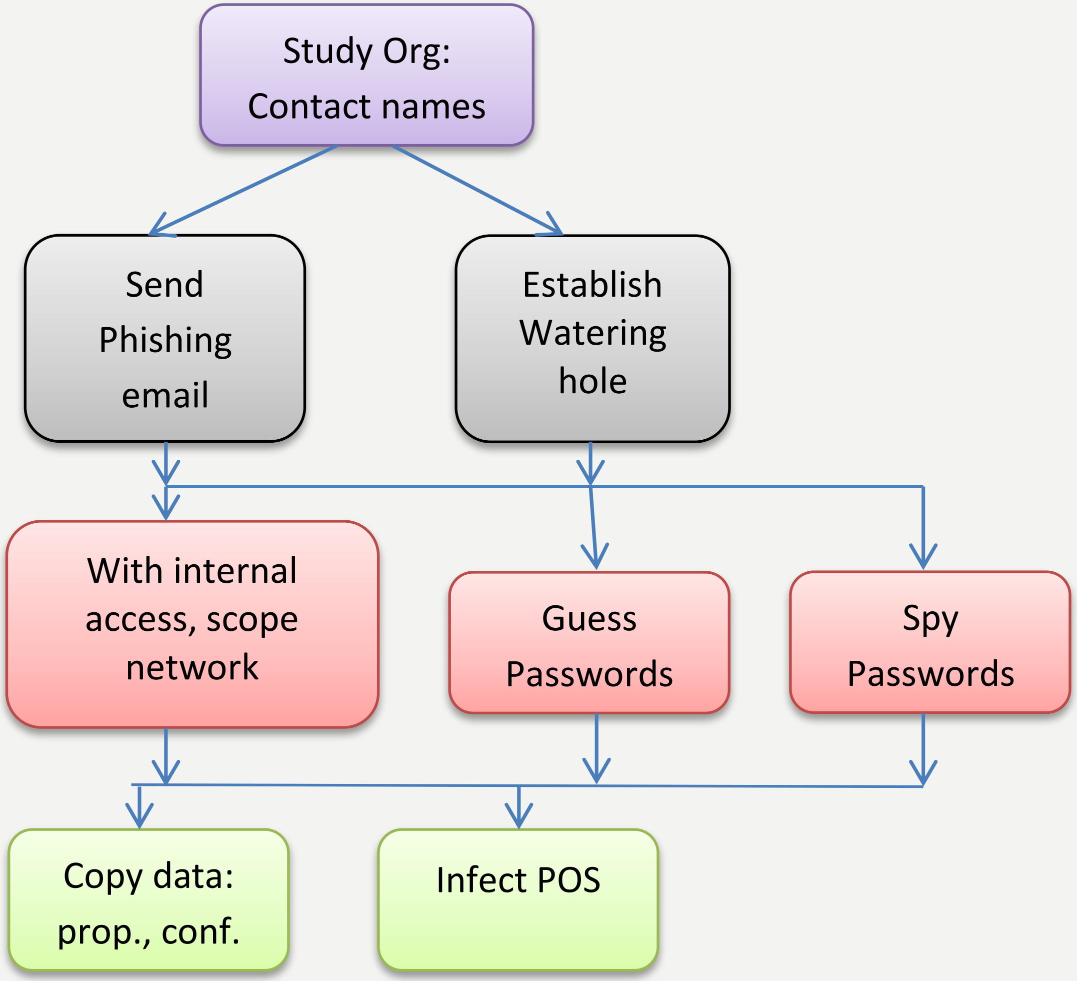
Ransomware 56%
Cmd & Cntrll 36%

Phishing
Cmd & Cntrl
Backdoor
Malware

Privilege misuse
Collusion
Partners abuse

Verizon 2018 Data Breach Investigations Report

A COMMON MEANS OF ATTACK



Study Org: Contact names

Send Phishing email

Establish Watering hole

With internal access, scope network

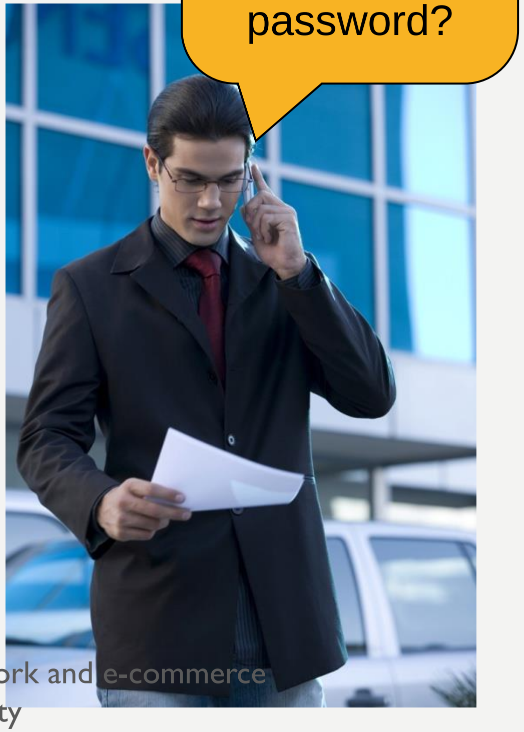
Guess Passwords

Spy Passwords

Copy data: prop., conf.

Infect POS

SOCIAL ENGINEERING



This is John, the System Admin. What is your password?

Email:
ABC Bank has noticed a problem with your account…

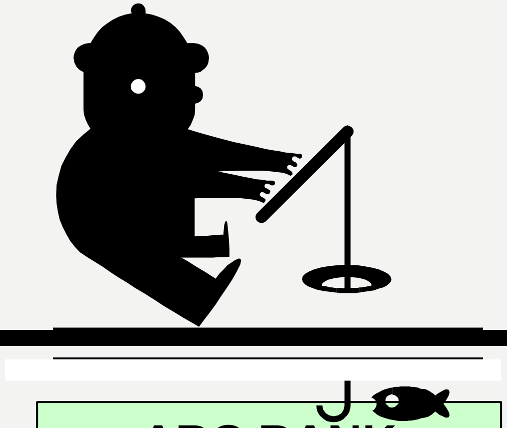
What ethnicity are you? Your mother's maiden name?

I need a password reset. What is the passwd set to?

I have come to repair your machine…

and have some software patches

PHISHING = FAKE EMAIL



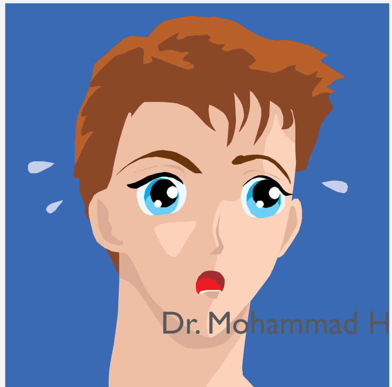
ABC BANK

Your bank account password is about to expire.
Please login…

Spearfishing

John:
Could you send Automated Services $1200?
Joe (CEO)

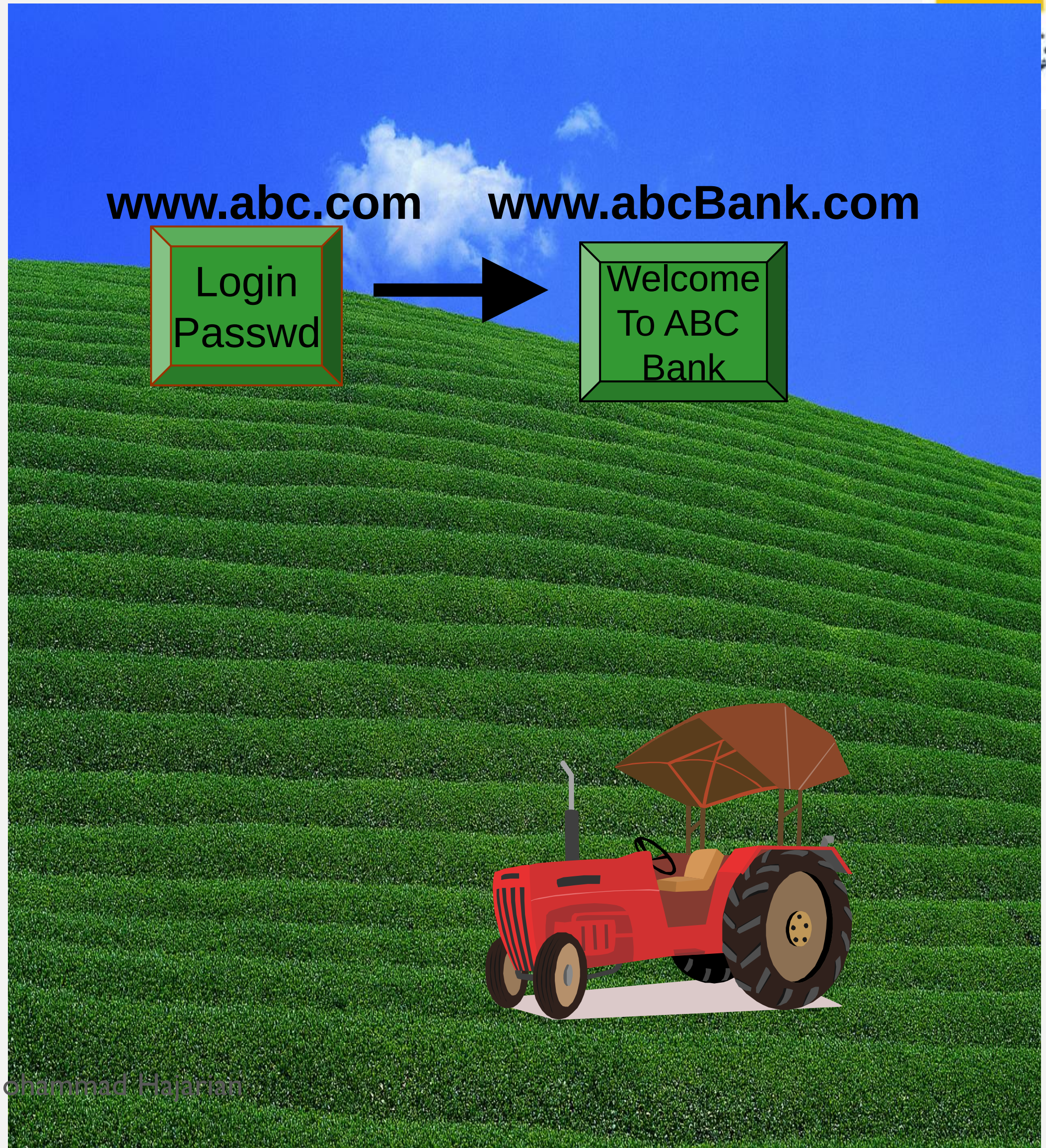
The bank has found problems with your account.
Please contact …”



PHARMING = FAKE WEB PAGES

Pharming:

- A fake web page may lead to a real web page
- The fake web page looks like the real thing
  - Extracts account information



DRIVE-BY DOWNLOAD

- A web site exploits a vulnerability in the visitor’s browser when the site is viewed

SOCIAL ENGINEERING

Phishing

- Gain Foothold
- Techniques:
  - Malware>67%
- Goals:
  - Financial 59%
  - Spying 41%

Pretexting

- Dialogue
- Obtain info, influence
- Technique:
  - CEO impersonation
  - Human resources: W2 info->fraudulent tax returns
  - Finance: transfer $
  - Malware 10%
- Goals:
  - Financial: 95%

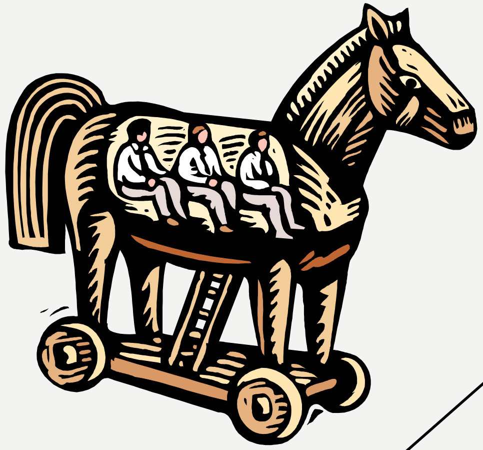
- 93% of Breaches
- Prominent technique: email 96%
  - Malicious attachment
  - Link to pharming website
- 78% do not click a single phish all year;
- 4% phish acceptance rate

Verizon 2018 Data Breach Investigations Report

ATTACK KIT - CRIMEWARE

- **Attack kit = Crimeware**: Tools which generate malware automatically
  - with varied propagation and payload mechanisms
- **Auto-rooter**: Breaks into new machines remotely
- **Downloader:** Original attack opens the door, then downloads the full attack software
- **Spammer program:** Generates large volumes of unwanted email

EXPLOIT/MAINTAIN ACCESS



Backdoor

Abnormal way to enter system, provided by Programmer or Vulnerability

Trojan Horse

Useful utility also performs malicious function

User-Level Rootkit

Replaces system executables: e.g. Login, ls, du to hide itself

Kernel-Level Rootkit

Replaces OS kernel: e.g. process or file control to hide

Bots

Slave forwards/performs commands; spreads, list email addrs, DOS attacks

Spyware/Adware

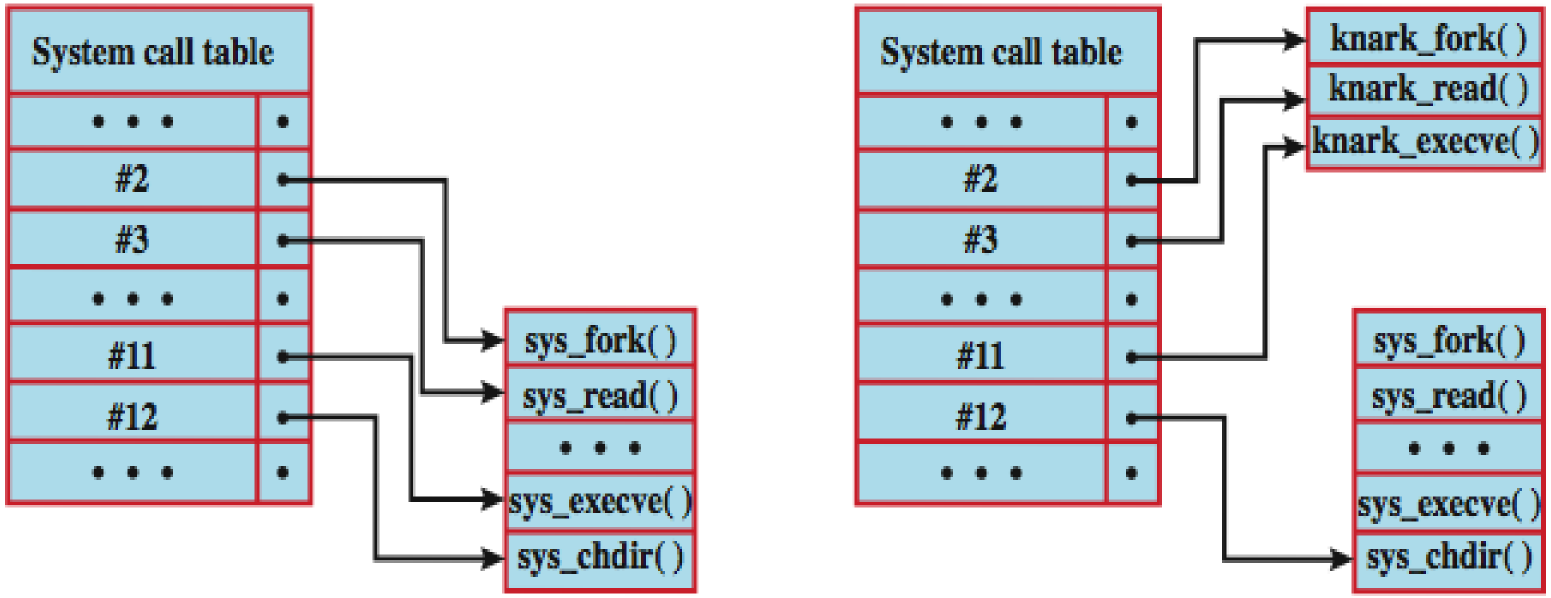
Spyware collects info: keystroke logger, collect credit card #s, **Adware**: insert ads, filter search results

ROOT KIT

Root Kit

- Upon penetrating a computer, a hacker installs a root kit
- May enable:
  - Easy entrance for the hacker (and others)
  - Keystroke logger
- Eliminates evidence of break-in
- Modifies the operating system
- Requires new OS install, when detected

ROOTKIT SYSTEM TABLE MODS



(a) Normal kernel memory layout

(b) After nkark install

OTHER MALWARE

Logic Bomb: Functional software has a built-in malicious attack or failure mechanism

- E.g., Software will malfunction if maintenance fee is not paid

Ransomware: E.g., Pay fee to decrypt software (or just pay fee)

Trojan Horse: E.g., Social Engineering: "Try this game…it is so cool"

  – Game also emails password file.

DENIAL OF SERVICE

- Single-Message DoS Attacks: Crash or disable system by attacking vulnerability
- Flooder DoS Attack: Flood victim with requests
    - **SYN Flooding**: Flood victim host with TCP SYNs (which initiate session).
    - **Smurf Attack**: Broadcast Pings to third parties with source address of victim host
    - **Amplification Attack:** Uses Broadcast address (common in 2017)
    - **Rabbit or Bacteria:** Reproduces exponentially, using up system resources
    - **Coin Mining**: Your web browser mines cryptocurrencies (e.g., Monero) for money for attacker

COVERT CHANNEL

- Exfiltrate information outside the organization
- E.g.: manipulate bits in a jpeg or mpeg
- E.g.: carry out info in a Lady GaGa CD
- E.g.: set bytes in an Excel spreadsheet

MOBILE MALWARE

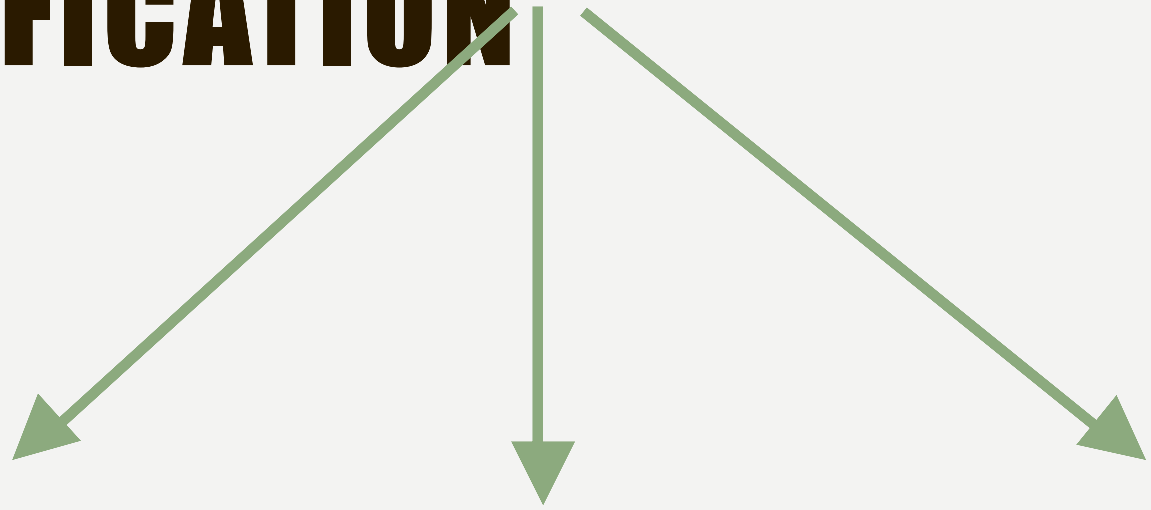
Mobile apps can be:

- Adware: Displays advertisements on other apps
- Chargeware: Charges for services without explicit notification
- Riskware: Reduces device security
- Spyware: Gathers information for another party
- Trojans: Features useful and unadvertised malicious intent

MALICIOUS SOFTWARE

- programs exploiting system vulnerabilities
- known as malicious software or malware
  - program fragments that need a host program
    - e.g. viruses, logic bombs, and backdoors
  - independent self-contained programs
    - e.g. worms, bots
  - replicating or not
- sophisticated threat to computer systems

MALWARE PROPAGATION CLASSIFICATION

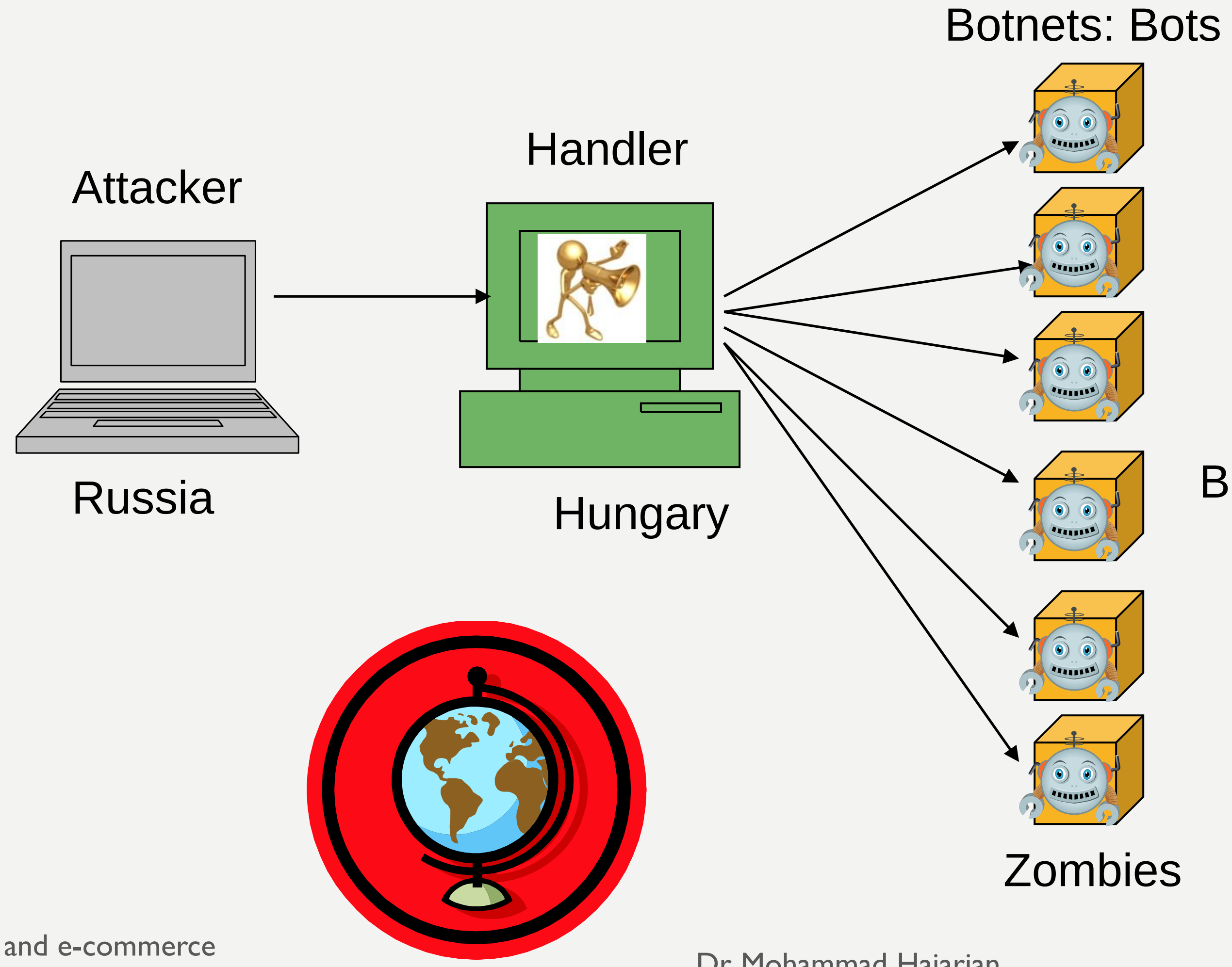


Infection
Of Executable
(e.g., Virus)

Exploit of
Software
Vulnerability
(SQL Attack,
Worm)

Social Engineering
(E.g., Phishing,
Pretexting
Watering hole,
Trojans)

BOTNETS: COMMAND AND CONTROL



Botnets: Bots

Attacker

Russia

Handler

Hungary

Zombies

Bots: Host illegal movies, music, pornography, criminal web sites, …

Forward Spam for financial gain

Sniffing traffic or Keylogging

DDOS, spread bots

Manipulate voting games

Generate clicks for ads

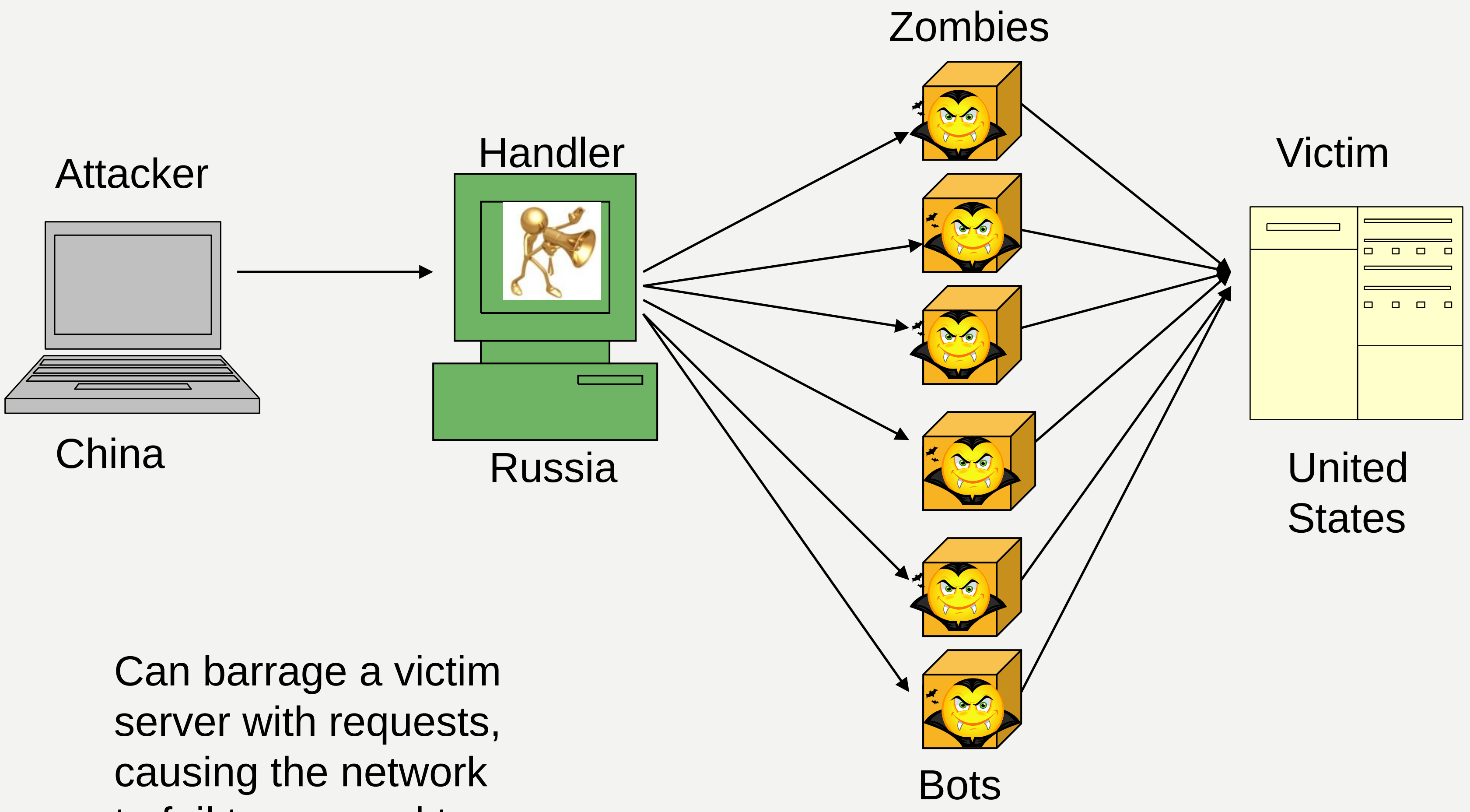
BOTS: COMMAND & CONTROL

- program taking over other computers
- hard to trace attacks
- if coordinated form a botnet
- characteristics:
  - remote control facility
    - via IRC/HTTP etc
  - spreading mechanism
    - attack software, vulnerability, scanning strategy
- various counter-measures applicable

BOT USES

- DDOS attacks
  - E.g., Internet Relay Chat overload
- Spamming
- Spying
  - Sniffing traffic
  - Keylogging
- Malware abuse
  - Spread malware
  - Install advertisement add-ons: pay-for-clicks
  - Manipulating online games

DISTRIBUTED DENIAL OF SERVICE

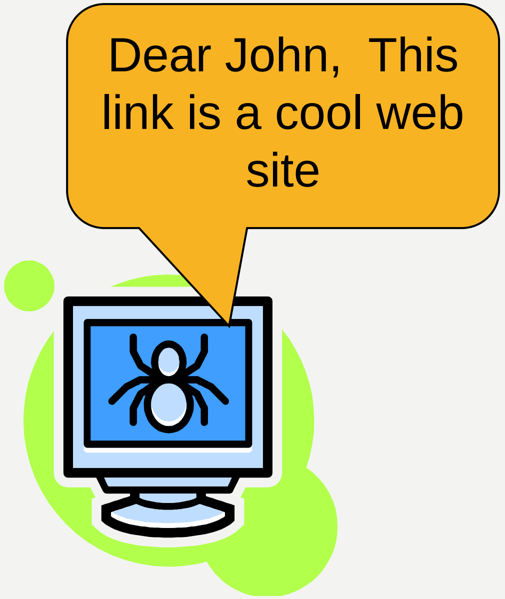


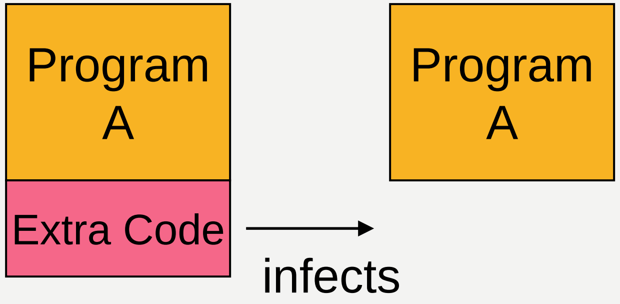
Can barrage a victim server with requests, causing the network to fail to respond to anyone

Flooder

VIRUS

- A virus attaches itself to a program, file, or disk
- When the program is executed, the virus too is executed
- When the program is given away (floppy/email) the virus spreads
- The virus may be benign or malignant but executes its load pay at some point (often upon contact)





Program A

Extra Code

infects

Program A

VIRUSES

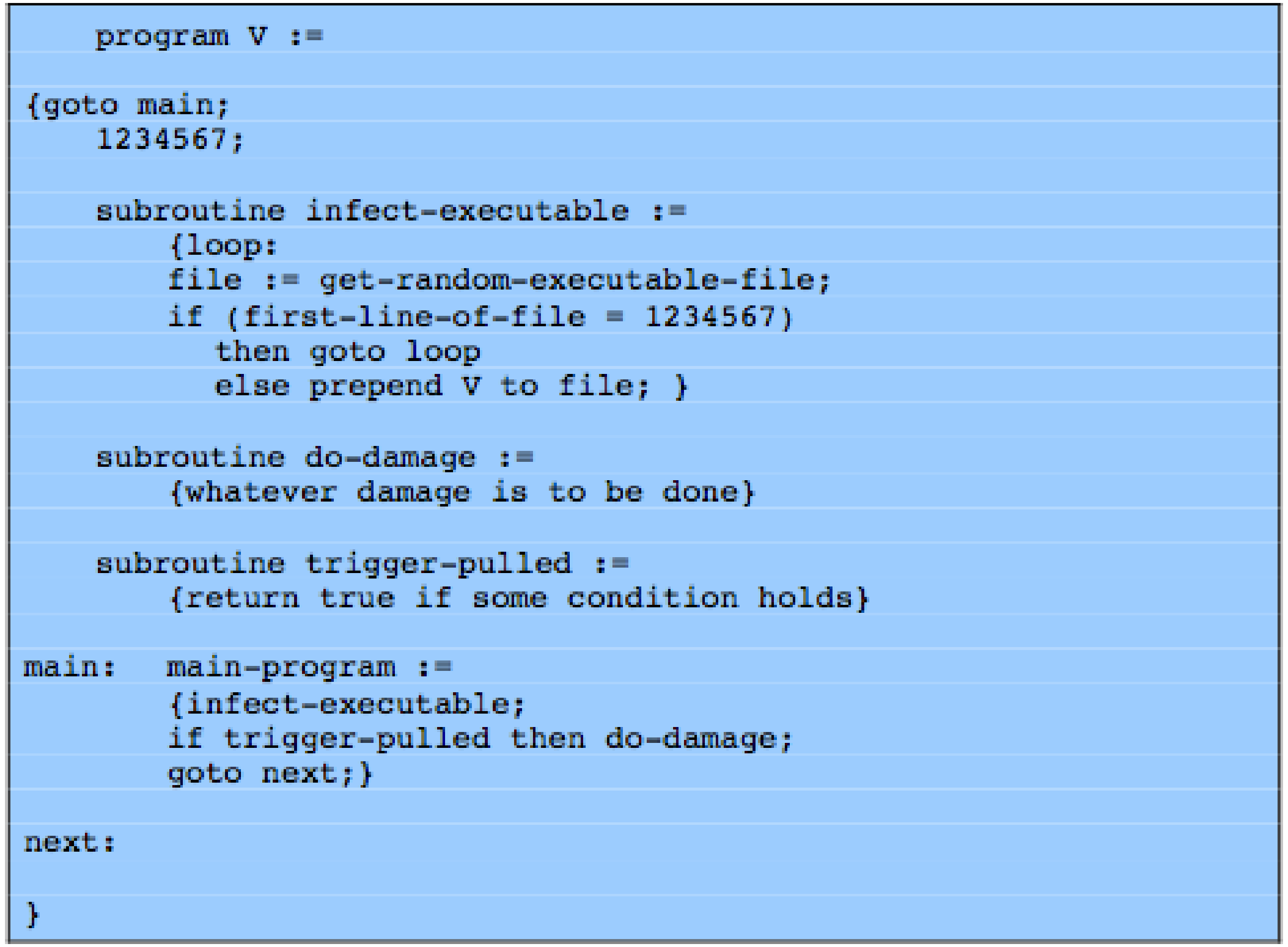
- piece of software that infects programs
  - modifying them to include a copy of the virus
  - so it executes secretly when host program is run

- a typical virus goes through phases of:
  1. Dormant: Wait for file presence, date, event,…
  2. Propagation: Spreading technique
  3. Triggering: Complete full intention
  4. Execution: Harmless or harmful

VIRUS STRUCTURE

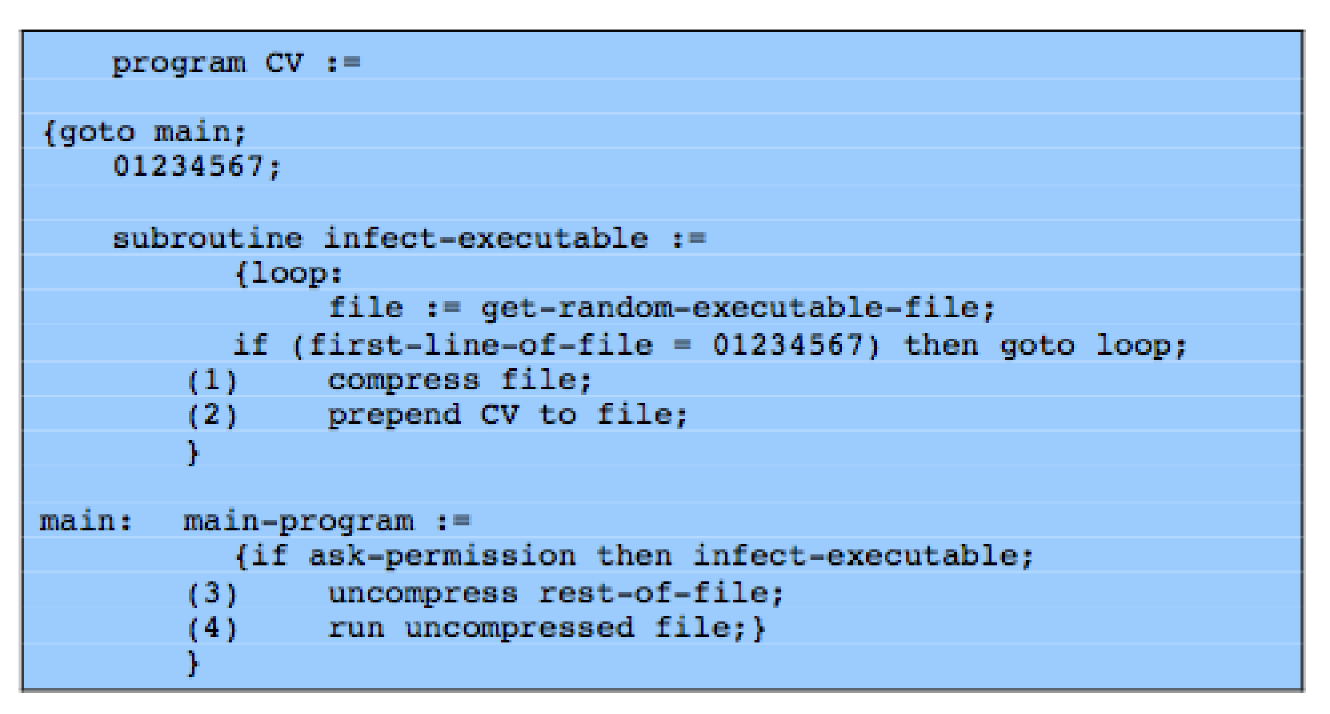
- components:
  - infection mechanism - enables replication
  - trigger - event that makes payload activate
  - payload - what it does, malicious or benign
- prepended / postpended / embedded
- when infected program invoked, executes virus code then original program code
- can block initial infection (difficult)
- or propogation (with access controls)

VIRUS STRUCTURE

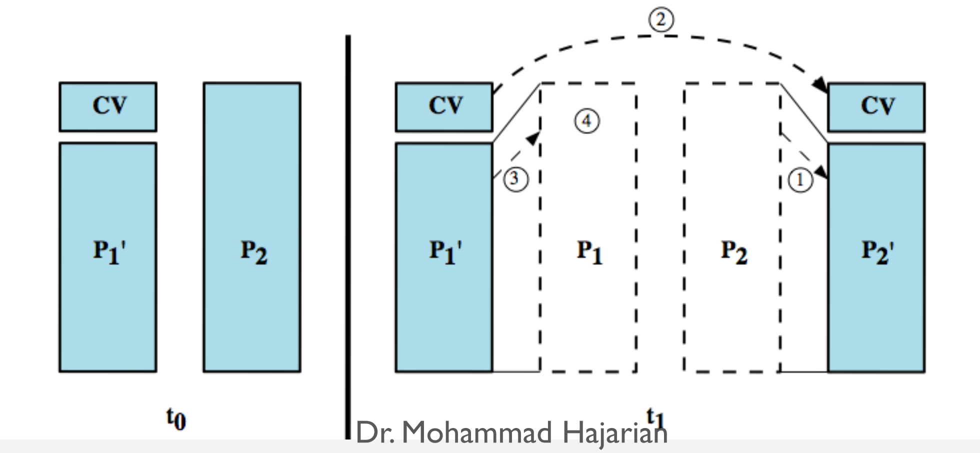


```
    program V :=

{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:

}
```

COMPRESSION VIRUS



```
    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;}
        }
```



VIRUS TARGET CLASSIFICATION

- **boot sector:** Spreads when system is booted from disk containing virus
- **macro virus**: Inserted in application file as script (e.g., MS Word doc.)
- **file infector**: Infects executable in OS or shell
- **multipartite**: Infects multiple ways/files
  - Difficult to clean, eradicate

VIRUS CONCEALMENT STRATEGIES

- **encrypted virus:** Uses a random key to encrypt virus, and stores key with virus
- **stealth virus**: Hides via encryption, file sizing, virus location, rootkit
- **polymorphic virus**: Mutates new virus with each infection
- **metamorphic virus:** Changes itself with each iteration; also polymorphic

MACRO VIRUS

- became very common in mid-1990s since
  - platform independent
  - infect documents
  - easily spread
- exploit macro capability of office apps
  - executable program embedded in MS Office doc
  - often a form of Basic
- more recent releases include protection
- recognized by many anti-virus programs

E-MAIL VIRUSES

- more recent development
- e.g. Melissa
  - exploits MS Word macro in attached doc
  - if attachment opened, macro activates
  - sends email to all on users address list
  - does local damage
  - had no Dormant phase -> faster propagation
    - 100k computers in 3 days

BRAIN VIRUS

- Lodges in upper memory then sets upper memory bound below itself
- Replaces interrupt vector for disk reads to screen disk read calls. Calls interrupt handler after screening.
- Places itself in the boot sector and six other sectors on disk
- Marks sectors as ‘bad’ so they will not get overwritten.
- Variants erase disks or destroy file allocation table

VIRUS COUNTERMEASURES

- prevention - ideal solution but difficult
- realistically need:
  - detection
  - identification
  - removal
- if detect but can’t identify or remove, must discard and replace infected program
- But what has cracker done in the mean time?

ANTI-VIRUS EVOLUTION

- virus & antivirus tech have both evolved
- early viruses simple code, easily removed
- more complex viruses -> more complex countermeasures
- 4 generations:
  - first - signature scanners
  - second – heuristics
    - Integrity checking & fragment recognition
  - third - identify actions (e.g., decompression)
  - fourth - combination packages
    - Limit access control to system & files

Antivirus, Antispyware

ANTIVIRUS

- Scheduled scans
- Antivirus updates
- Real-time file access protection
- E-mail protection
- Popular: Norton, McAfee,Panda, Fprot, AVG

ANTISPYWARE

- Real-time protection
- Scheduled scans
- Browser hijack protection
- Auto updates
- Popular: Spybot, Ad-aware, MS Windows Defender

All-in-one also includes

- URL Filter
- Content inspection: packet content

Q/A

- End of Session 1

THANK YOU!