CIS 4360
Secure Computer Systems

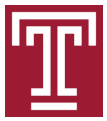
Malware

Professor Qiang Zeng

Spring 2017

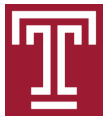
Previous Class

- Implementation Principles
  - Policy and Mechanism Decoupling
  - Reference Monitor
- Bell-LaPadula (BLP) Secrecy Model
  - No read up
  - No write down
- Biba Integrity Model
  - No read down
  - No write up
- Chinese Wall Model
  - If you have accessed the data of a corporation, you cannot read the data of its competitors



Writing Assignments

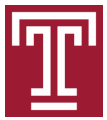
- Can a user cleared for (S, {dog, cat, pig}) read documents classified in the following ways under the BLP model?
  - (TS, {dog})
  - (S, {dog})
  - (S, {dog, cow})
  - (S, {monkey})
  - (C, {dog, pig, cat})
  - (C, { })
- (S, {dog}), (C, {dog, pig, cat}), and (C, { })



Previous Class

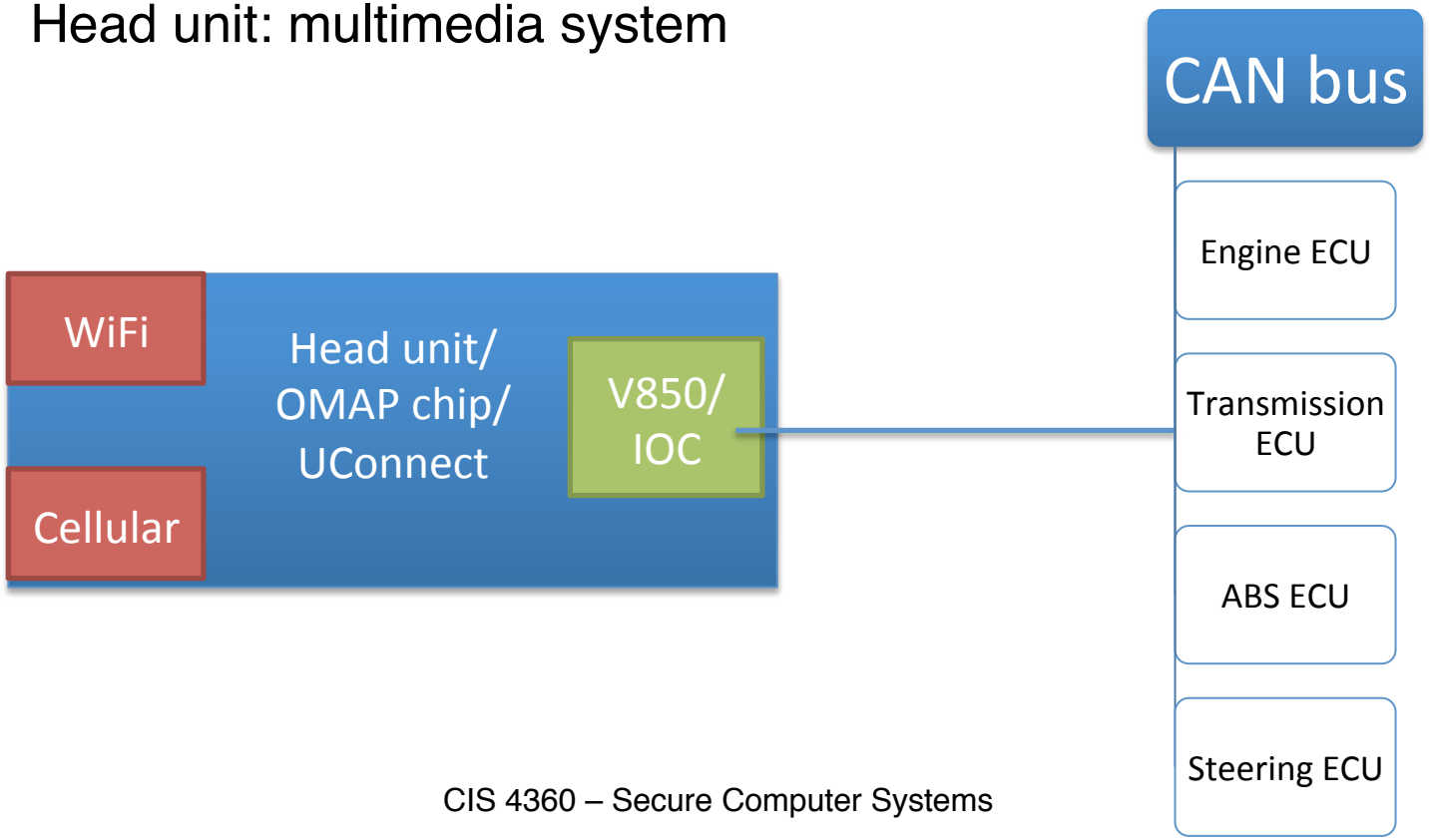
Can BLP and Biba be enforced in the same system?

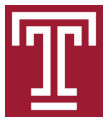
Theoretically, you can do that. But it would be very inflexible, as a user can only access objects that have exactly the same security class as the user



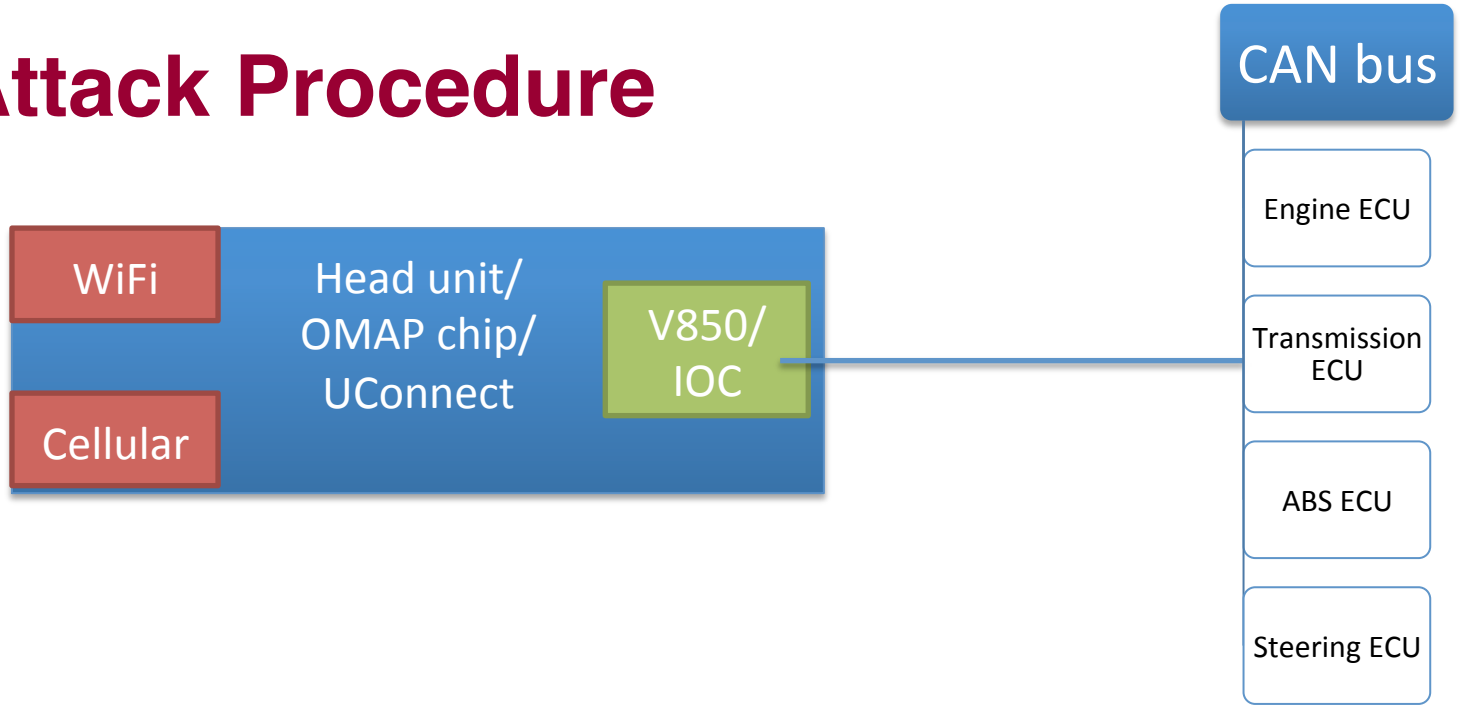
Terms and Architecture

- Terms:
  - CAN: Controller Area Network. A message bus in vehicle for inter-component communication
  - ECU: Electronic Control Unit. Each is an embedded system. E.g., engine ECU, transmission ECU, airbag ECU, ABS ECU
  - Head unit: multimedia system

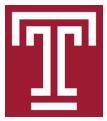




Attack Procedure

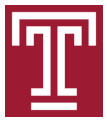


1. Establish network connection with victim car: either guess WiFi password, or scan cars connected to the Sprint cellular network
2. Port scanning and find a vulnerable service listening at some port
3. Exploit the service to login the computer for the head unit
4. Command the head unit to "update" the firmware at V850
5. Now you can send messages to the ECUs to control the car



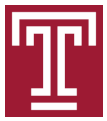
Outline

- Virus vs. Worm vs. Trojan
  - Detailed discussion about Worms
- Spyware vs. Ransomware vs. Botnet vs. Rootkit



Malware

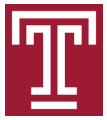
- Malware: malicious software
- A large variety
- A huge number of terms:
  - Trojan, Virus, Worm, Rootkit, Spyware, Botnet, Logic bomb, Drive-by-download, Backdoor, Adware, …




malware
infection
infected
trojan
firewall
spam
hacker
detection
virus
intruder
spyware
phishing
attack
internet
crime
hackers
service
network
illegal
target
groups
networks
communications
information
cyber
criminal
department
hacking
international
terrorism
computer
pornography
offensive
unauthorized
activities
theft
individuals
child
warfare
crimes
cyberspace
mail
data
security
purposes
system
altering
allegedly
million
including
used
rooms
content
cases
access
fraud
use
drug
investigators
websites
between
several
services
systems
devices
copyright
university
major
face
documented
encrypted
defined
trafficking
way
time
group
website
specific
scams
detect
malicious
technical
traffickers
electronic
sending
unsolicited
topology
needed
during
financial
committed
harm
facilitated
server
physical
identity
considered
obscene
surrounding
directly
future
cyberterrorism
stalking
distributed
resources
packages
victim
refers
limits
organized
infected
problems
defense
citation
individual
government
jurisdictions
high
ring
derogatory
included
using
variety
harassment
document
increasingly
counts
hate
officials
race
well
technology
trades
main
form
include
combatting
nation
companies
concern
going
profile
stored
code
federal
entering
kinetic
people

Classification is important

- Classification based on propagation; i.e., how has the malicious software reached victims?
  - Trojan
  - Virus
  - Worm
  - Drive-by-download
- Classification based on payload; i.e., what malicious actions does the malware take?
  - Spyware: to steal (info.)
  - Ransomware: to extort
  - Botnet: to control
  - Rootkit: to hide
  - …

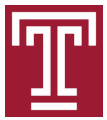


Trojan

- Named after the wooden horse the Greeks used to cheat and infiltrate Troy

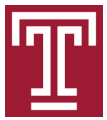
Trojan

- A malicious program that *looks* innocent
  - It looks like, e.g., a browser, music player, or calendar
- It does not replicate itself, so it relies on user interaction to install it
  - E.g., the malware author may publish Trojans in the form of "free" software; then, users are lured to download and install them



Virus

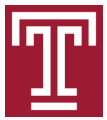
- A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program
  - Like a biological virus, a computer virus cannot live independently; it has to be part of a host program
- It *actively* replicates itself by infecting other files once reaching a computer
- It *passively* infects other computers, when, e.g.,
  - A victim user sends the infected file through emails
  - An infected USB drive is inserted to another computer



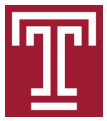
How to infect?

- An infected file example
- The first line "1234567;" is a flag showing that the file has been infected to avoid duplicate infection
- The function "*main action block*" is the entry point of the program

```
program V
1234567;

procedure attach-to-program;
begin
   repeat
        file := get-random-program;
   until first-program-line ≠ 1234567;
   prepend V to file;
end;

procedure execute-payload;
begin
   (* perform payload actions *)
end;

procedure trigger-condition;
begin
   (* return true if trigger condition is true *)
end;

begin (* main action block *)
   attach-to-program;
   if trigger-condition then execute-payload;
   goto main;
end;
```

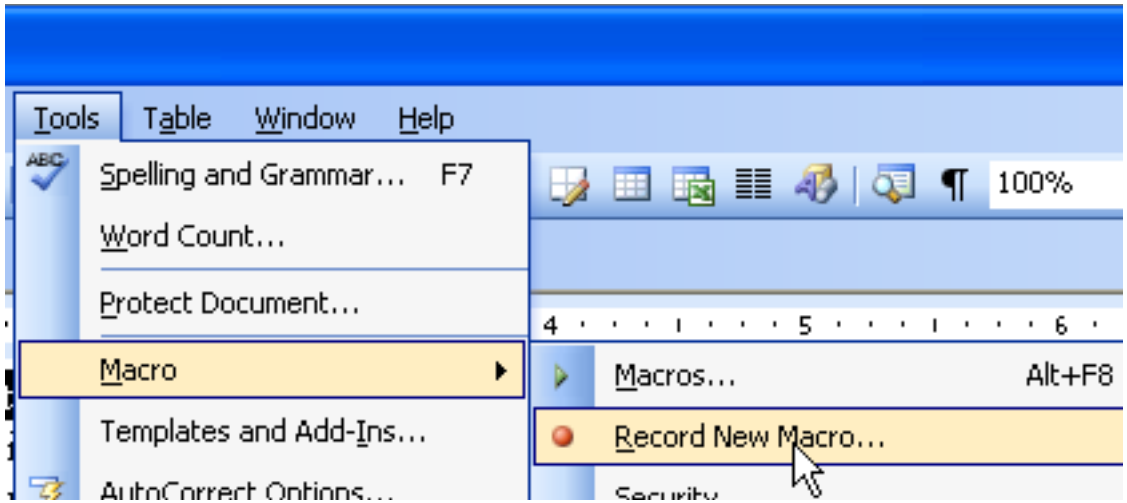


While some viruses infect executable files, many infect word, excel, power point files

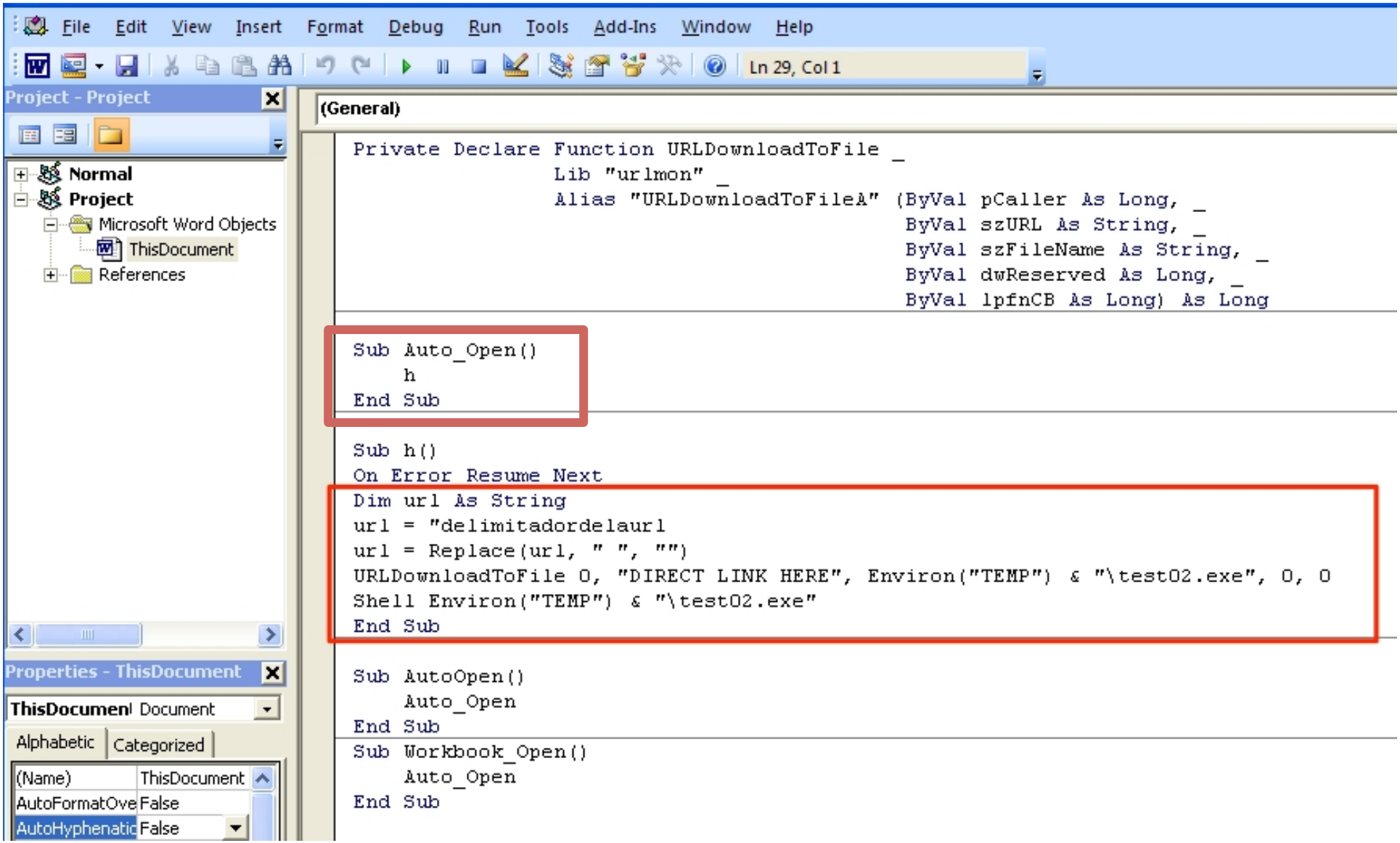


Macro Viruses

- What is a Macro?
  - A Macro is a series of commands defined for automation
  - Used in Microsoft Office
  - Useful example: “Company Letterhead” macro
  - Can even create “AutoExec”, “AutoNew”, “AutoOpen” macros
- What are the advantages of macro viruses compared to viruses infecting native executables?
  - They are platform-independent; a macro virus in a document can run on both Mac and PC
  - Very often, word/ppt/excel files are attached in emails

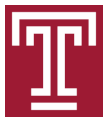


An “AutoOpen” Macro virus example



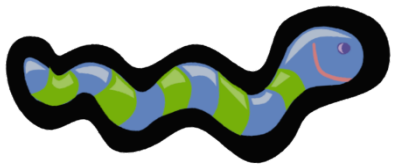
Thus, don't open documents, such as email attachments, from untrusted sources; some companies even disable Macros in Office products via policy

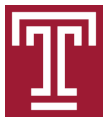
Macro Viruses do not rely on vulnerabilities, while Scripting Viruses usually exploit vulnerabilities of the script interpreters, such as browsers and PDF readers. They become more popular nowadays.
We will touch more on this when discussing Drive-by Downloads



Worm

- A Worm is malicious code which replicates automatically itself over a network
- Worms generally exploit vulnerabilities in remote services or local email clients to spread





Recent Worm Attacks

Melissa	1998	e-mail worm first to include virus, worm and Trojan in one package
Code Red	July 2001	exploited Microsoft IIS bug probes random IP addresses consumes significant Internet capacity when active
Code Red II	August 2001	also targeted Microsoft IIS installs a backdoor for access
Nimda	September 2001	had worm, virus and mobile code characteristics spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL Slammer	Early 2003	exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	Late 2003	exploited open proxy servers to turn infected machines into spam engines
Mydoom	2004	mass-mailing e-mail worm installed a backdoor in infected machines
Warezov	2006	creates executables in system directories sends itself as an e-mail attachment can disable security related products
Conficker (Downadup)	November 2008	exploits a Windows buffer overflow vulnerability most widespread infection since SQL Slammer
Stuxnet	2010	restricted rate of spread to reduce chance of detection targeted industrial control systems

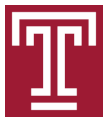
Case Study – Code Red

- 2001; exploited a buffer overflow vulnerability in Microsoft IIS
  - Surprisingly, the patch was actually released one month earlier than the attack. What is the lesson?
- Infected 360,000 servers in 14 hours

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0
```

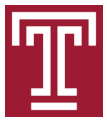
Trojan vs. Virus vs. Worm

	Trojan	Virus	Worm
Self-replicated	N	Y	Y
Self-contained	Y	N	Y
Relying on exploitation of vulnerabilities	N	Maybe (e.g., scripting viruses)	Y

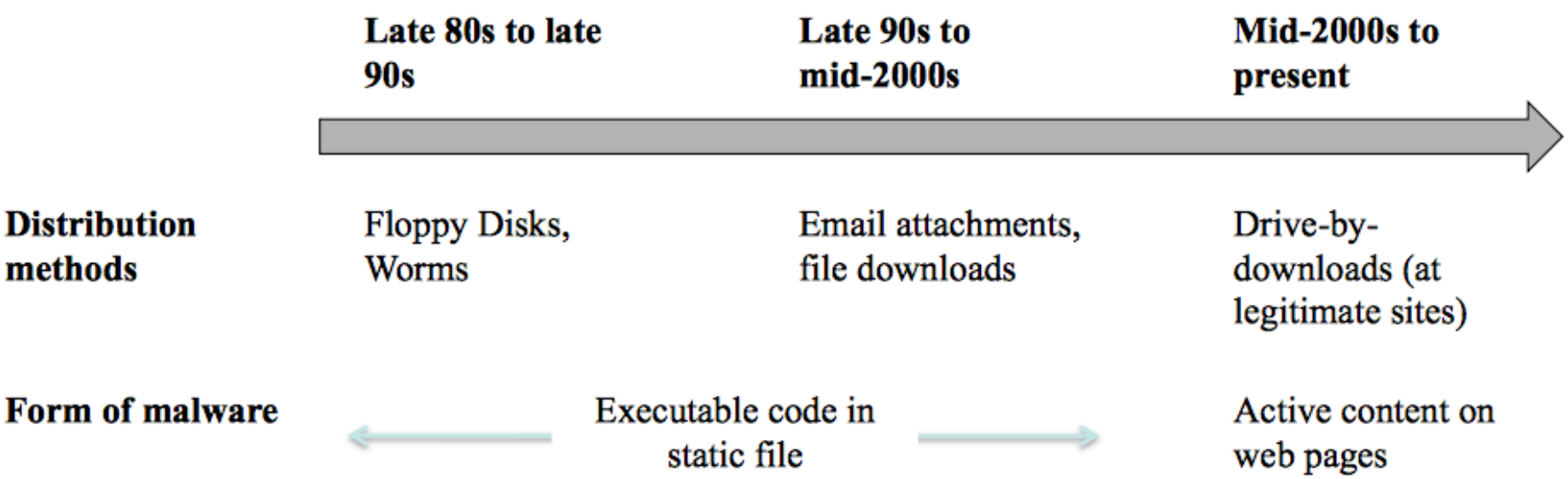


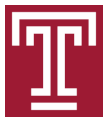
Drive-by Download

- It is not malware but is a way to distribute malware
- A drive-by download refers to the unintended download of malware onto your computer
  - Typically, attackers first compromise a popular website, and insert malicious code into webpages
  - Next, when a user visits the webpages, the malicious code (usually, scripting viruses) is downloaded and executed in the browser
  - Finally, the malicious code exploits vulnerabilities of the browser to download and install malware without the user's permission or knowledge
- Some variants exploit bugs in PDF readers and email client to download malware stealthily



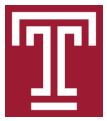
Fundamental Change in Malware Distribution





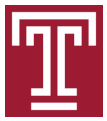
Demo

- Drive-by Download through invisible iFrames
  - https://youtu.be/_cBed6-ufIQ
- Malvertising: you can even buy advertisement service from a website; instead of advertising products, you distribute malware through the ads
  - This way, you even do not need to compromise the website to achieve drive-by downloads



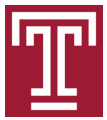
What makes Drive-by Download particularly dangerous is that it infects your computer by simply a link.

So, open any link with caution and keep your browser and operating system up to date!



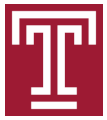
Classification is important

- Classification based on propagation; i.e., how has the malicious software reached victims?
  - Trojan
  - Virus
  - Worm
  - Drive-by-download
- Classification based on payload; i.e., what malicious actions does the malware take?
  - Spyware: to steal (info.)
  - Ransomware: to extort
  - Botnet: to control
  - Rootkit: to hide
  - …

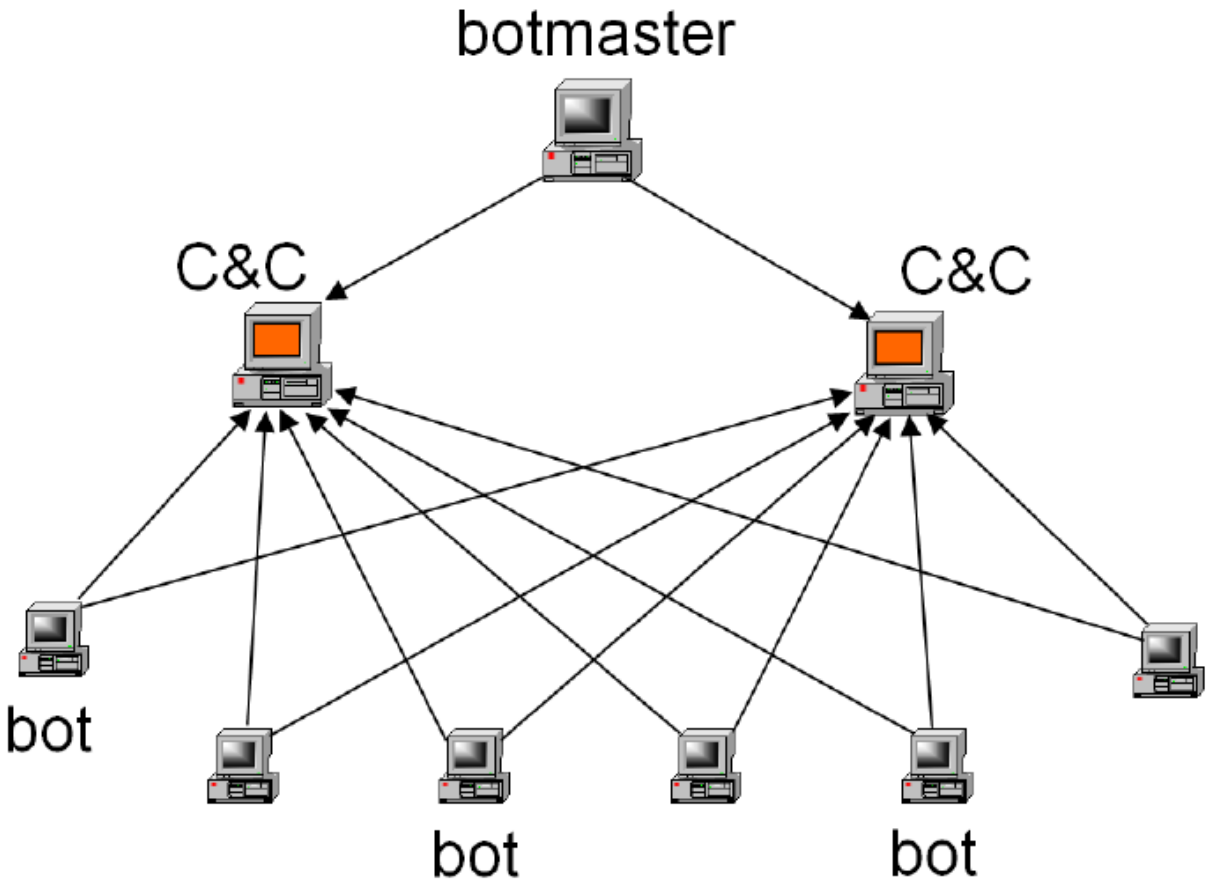


Botnet

- Botnet – a collection of compromised computers that are controlled by hackers for organized attacks
  - BOTNET: roBOT + NETwork
- In a Botnet, a compromised computer is called a "Zombie", "Bot", "Robot", or "Drone", while a botnet owner is called a "bot header" or "bot master"
- Uses:
  - Steal privacy information
  - Distributed denial-of-service (DDoS) attacks
  - Spamming
  - Spreading new malware
  - Manipulating online polls/games
  - Bitcoin mining
  - Click fraud
  - …



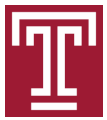
Classic Botnet Structure



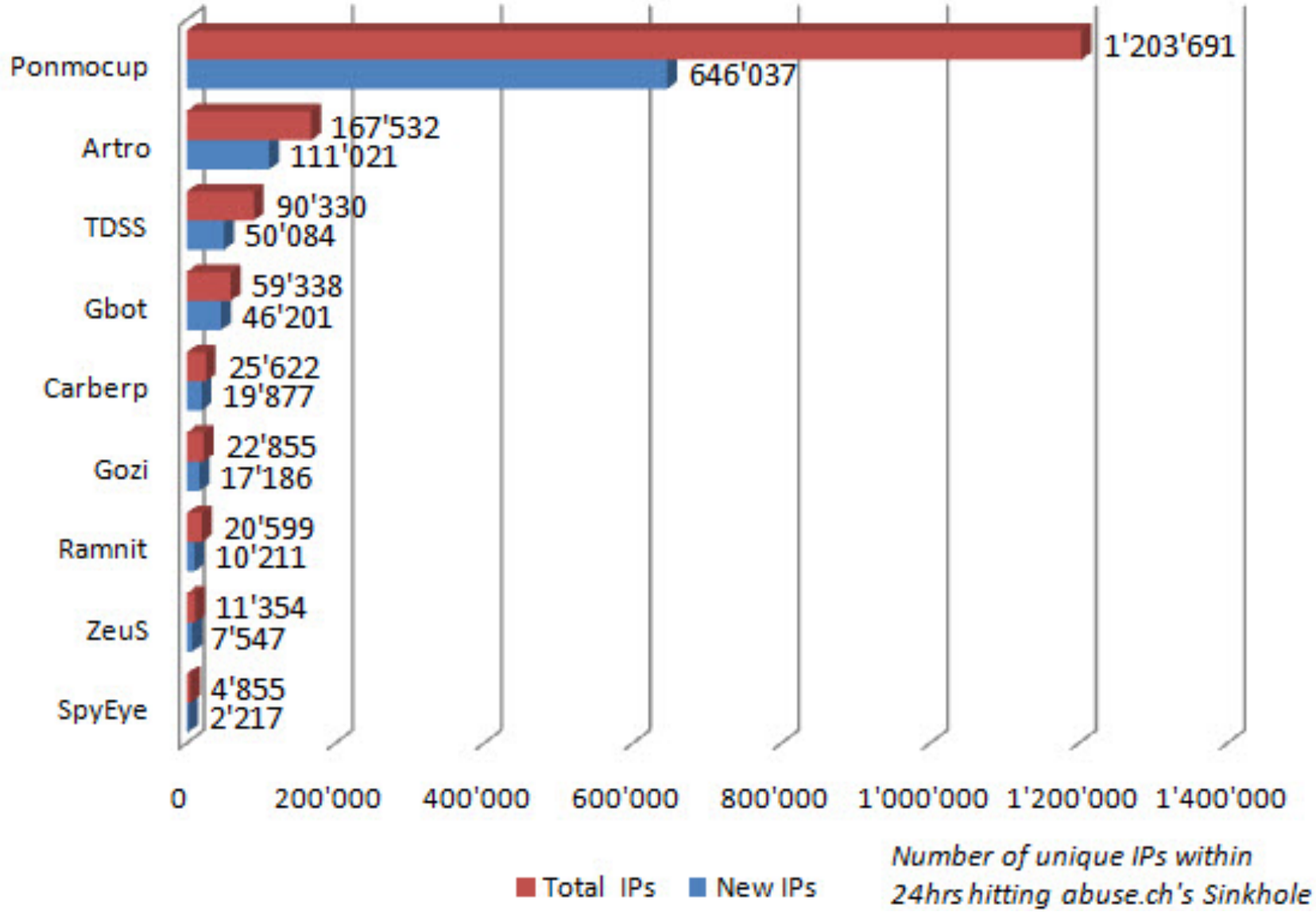
Recently, the topology has evolved to P2P, so that you cannot simply take down the C&C servers to defeat a botnet

How to “recruit” bots?

- Drive-by downloads
- Trojans
- Worms
- …

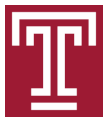


Botnet Statistics (3/3)



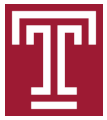
Countermeasures against Botnets

- Keep your systems up to date
- Blacklisting domains/IPs of C&C servers
- Taking down the C&C servers
- Packet filtering
- Law enforcement



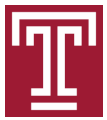
Rootkit

- A rootkit is an application (not necessarily malware) that hides its presence or the presence of another application (worm, spyware, etc)
  - Using some of the low-level functionalities, e.g., rewriting system calls, intercepting lib calls, to change the return results of the calls
    - E.g., a rootkit may intercept the call that returns the list of all alive processes and remove the malicious process from the list
    - E.g., a rootkit may modify the call that return the list of files in a directory and remove the malicious file from the list
  - Hard to detect via anti-virus software, as AV software call the crooked system/API calls



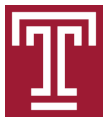
Types of Rootkits

- User mode
- Kernel mode
  - A variant is called bootkits that interfere with the boot process to gain control before the kernel starts
- Hypervisor level
- Firmware level



Summary

- Virus vs. Worm vs. Trojan
- Drive-by download
- Botnet
- Rootkit



Writing Assignments

- It is absolutely possible that an experienced attacker may combine the techniques of viruses and worms. Could you find one concrete example in the list of famous worm attacks?
- Does a drive-by download attack always succeed when you open a malicious webpage?
- Describe the main components in a classic botnet structure