Lecture 9.2
Computer and Network Security

Announcements

- LA-7 due tonight
  - Quiz only
  - Retakes available starting tomorrow
- LA-8 available Tuesday
- Oral Presentation rubric Tuesday
  - Begin research now

Last Time

- Hackers
- Computer Security Legislation
- HTTP Cookie Crimes
- Malware
  - Viruses
  - Worms
  - Trojans
  - Ransomware
  - Rootkits
  - Spyware
  - Bots and Botnets

Today

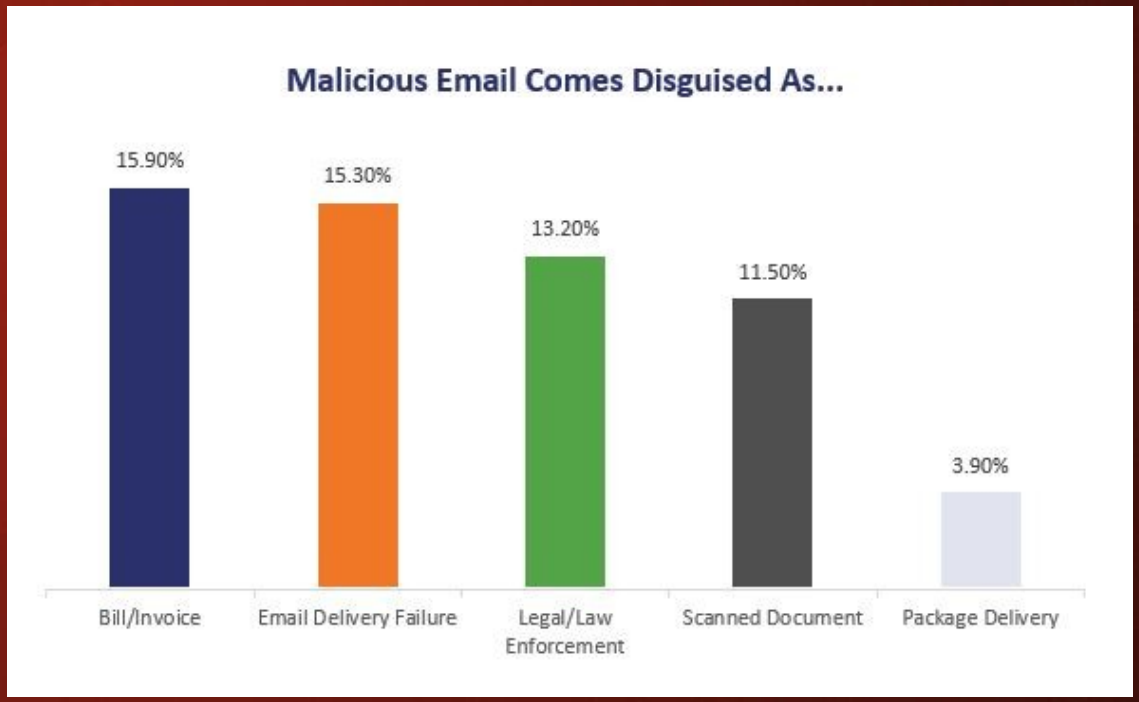
- Cybercrime Attacks
  - Phishing, Spear-Phishing, Whaling, Vishing, Smishing, Pharming
  - SQL Injection
  - DoS and DdoS
- Cybercrime Hall of Shame
- Cybercrime Hall of Lame
- Political Cyber Attacks
- Online Voting

Cybercrime

- 80 million .com domains
- Annual eCommerce exceeds $1 trillion
  - Attracts organized crime
  - Attracts political enemies
- 90% of cybercrime started via eMail
- 76% of organizations experienced phishing attack in 2017
- Average 16 malicious eMails/employee/month
- 70% US employees have no concept of cybersecurity best practices

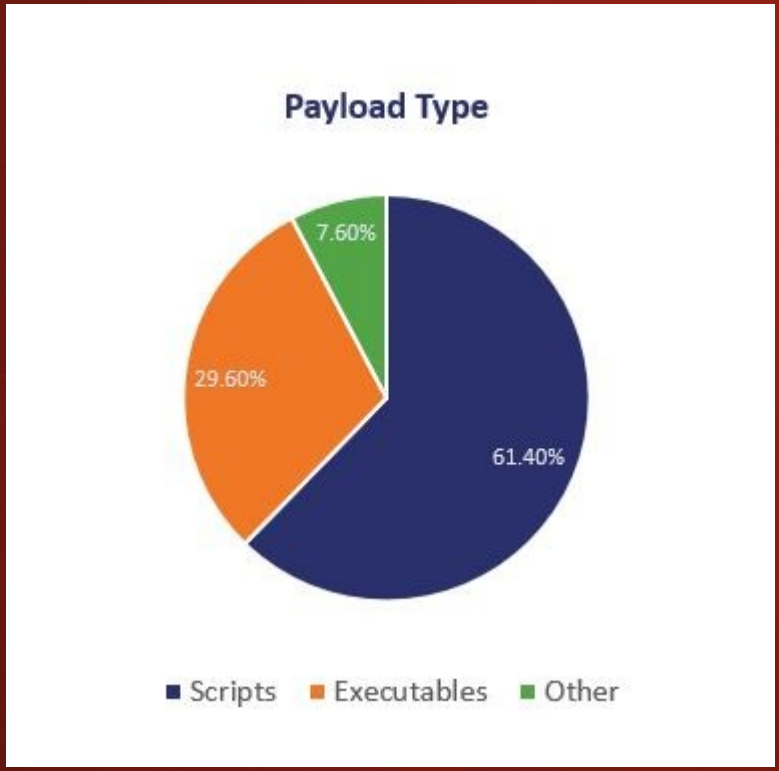
Malicious Email

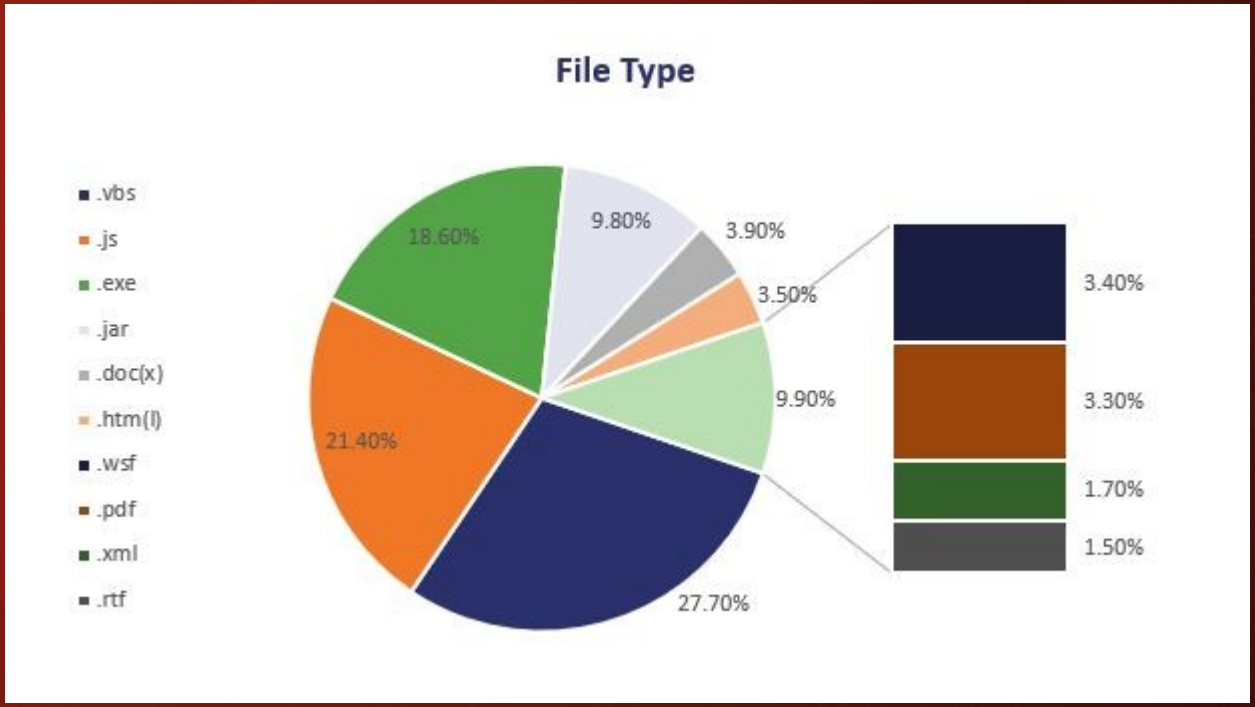
Rank	Industry	Email Malware per User
1	Public Administration	53.1
2	Wholesale Trade	34.4
3	Mining	30.0
4	Agriculture, Forestry, & Fishing	26.5
5	Manufacturing	25.5
6	Nonclassifiable Establishments	21.8
7	Retail Trade	19.9
8	Construction	18.1
9	Services	12.1
10	Finance, Insurance, & Real Estate	9.1
11	Transportation & Public Utilities	8.7



thesslstore.com/blog

Malicious Payloads





thesslstore.com/blog

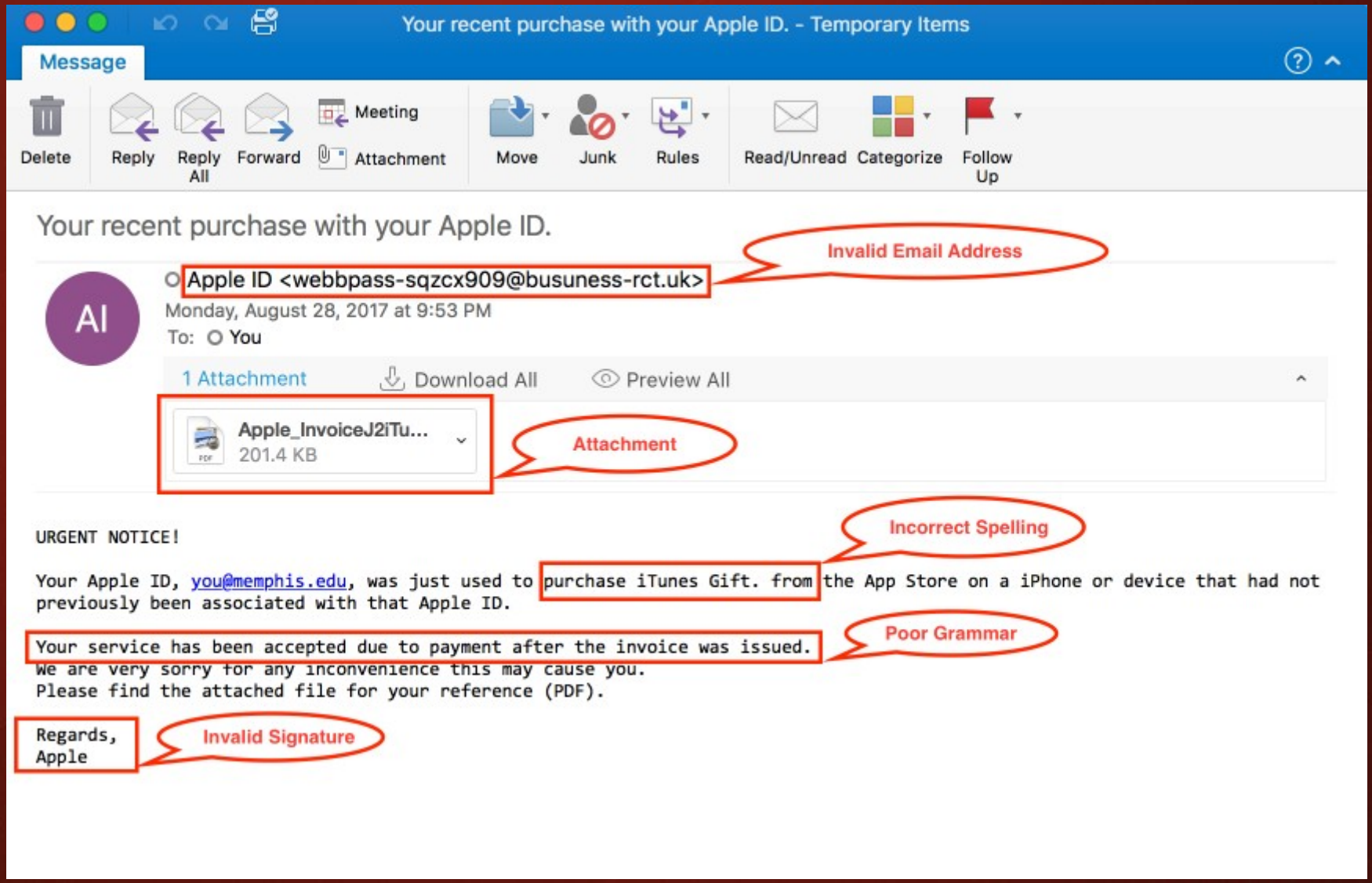
Phishing, Spear-Phishing, and Whaling

- Phishing: Large-scale effort to gain sensitive information from gullible computer users
  - At least 124,000 phishing attacks globally in second half of 2014
  - New development: phishing attacks on Chinese e-commerce sites
- Spear-phishing: Variant of phishing in which email addresses chosen selectively to target particular group of recipients
- Whaling: executives, high-level targets (big fish)

Vishing, Smishing, Pharming

- Vishing: VOIP voice-based scams
- Smishing: SMS text-based scams
- Pharming: DNS cache poisoning

Phishing Examples



https://www.memphis.edu/its/security/phishing-examples.php

From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password

Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

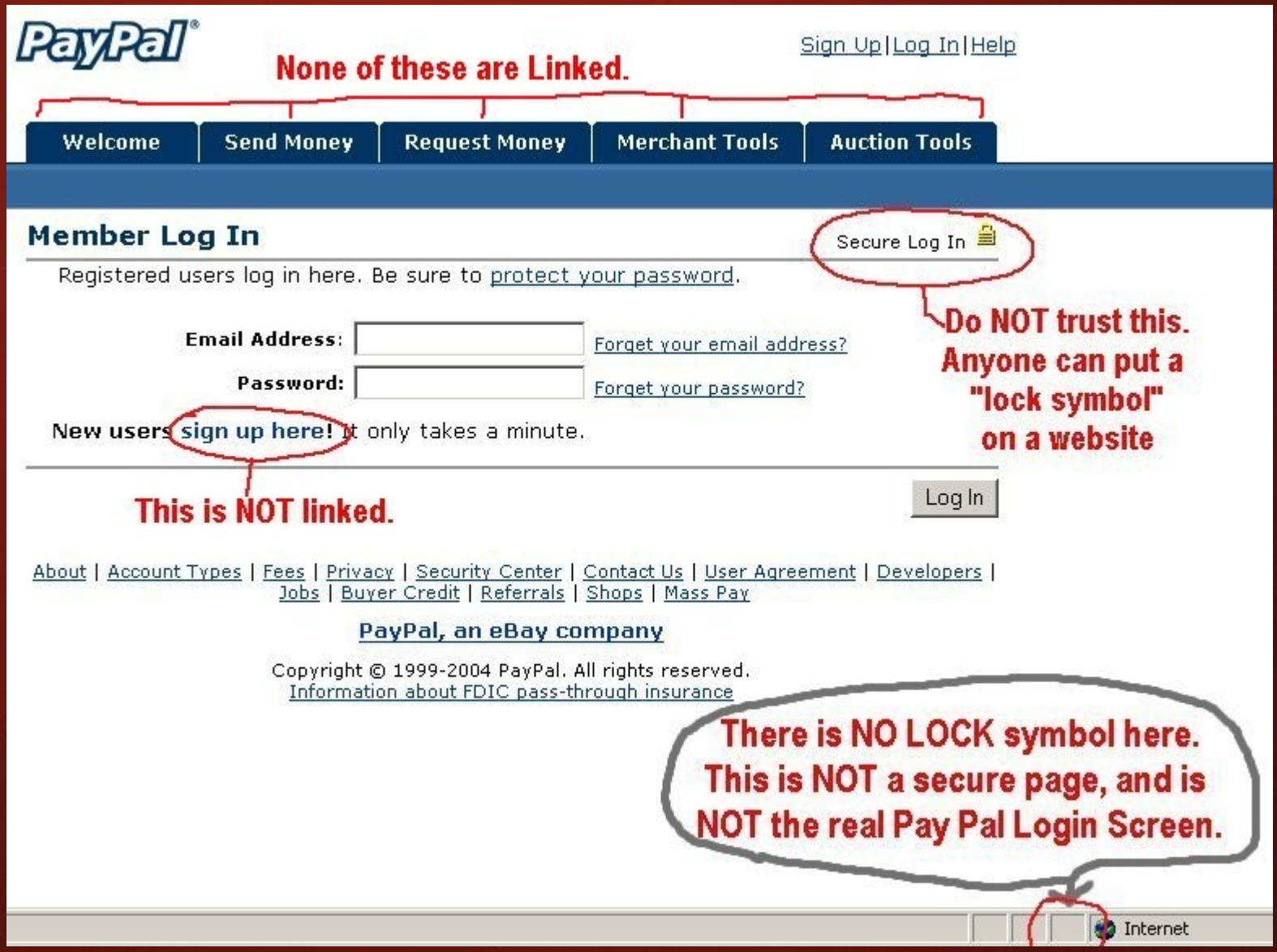
Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

Fraudulent Websites



https://www.ophtek.com/the-basics-of-how-phishing-works/

SQL Injection

- Method of attacking a database-driven Web application with improper security
- Attack inserts (injects) SQL query into text string from client to application
- Application returns sensitive information

SQL Injection Example

- Web page has form to login using email and password

SQL Injection Example

- Web page has form to login using email and password
- $email and $password sent to backend

SQL Injection Example

- Web page has form to login using email and password
- $email and $password sent to backend
- Backend queries SQL dbase

```
SELECT * FROM users WHERE email = '$email' AND password=md5('$password')
```

SQL Injection Example

- Web page has form to login using email and password
- $email and $password sent to backend
- Backend queries SQL dbase

```
SELECT * FROM users WHERE email = '$email' AND password=md5('$password')
```

- Attacker crafts a password to inject code

```
xxx') OR 1=1 --] test
```

SQL Injection Example

- Web page has form to login using email and password
- $email and $password sent to backend
- Backend queries SQL dbase

```
SELECT * FROM users WHERE email = '$email' AND password=md5('$password')
```

- Attacker crafts a password to inject code

```
xxx') OR 1=1 --] test
```

- When backend runs query, malicious side effects

```
SELECT * FROM users WHERE email = '$email' AND password=md5('xxx') OR 1=1 --] test')
```

Denial-of-Service and Distributed DoS Attacks

- Denial-of-service attack: Intentional action designed to prevent legitimate users from making use of a computer service
- Aim of a DoS attack is not to steal information but to disrupt a server’s ability to respond to its clients
- Distributed denial-of-service attack: DoS attack launched from many computers, such as a botnet

Internet-of-Things Devices Co-opted for DDoS Attack

- DDoS attack of October 21, 2016 on domain name service provider Dyn
  - Netflix, Twitter, Spotify, Reddit, PayPal, Pinterest, CNN, Fox News, the Guardian, the New York Times, the Wall Street Journal unreachable for several hours
- Attack launched by Mirai botnet, perhaps 100,000 devices
  - Network routers
  - Security cameras
  - Baby monitors
- IoT devices easy to co-opt
  - Many people never change default passwords
  - Some devices have no password protection

DDoS Attacks

- www.digitalattackmap.com
- Attack Class
  - TCP Connection
  - Volumetric
  - Fragmentation
  - Application

DDoS Attacks

- www.digitalattackmap.com
- Attack Class
  - TCP Connection
  - Volumetric
  - Fragmentation
  - Application
- Amplification
  - DNS Reflection
  - Chargen Reflection

DDoS Attacks

- www.digitalattackmap.com
- Attack Class
  - TCP Connection
  - Volumetric
  - Fragmentation
  - Application
- Amplification
  - DNS Reflection
  - Chargen Reflection
- Forms
  - Smurf
  - Teardrop
  - Pings of Death

Cyber Crime Hall of Shame

- Criminal organizations making significant amounts of money from malware
- Jeanson James Ancheta
- Pharmamaster
- Albert Gonzalez
- Avalanche Gang

Jeanson James Ancheta

- Drops out of high school 2001
- Begins working at Internet Cafe 2003
- Discovers rxbot worm
- Creates huge botnet to rent for profit
- Arrested and charged in 2005

Blue Security vs. Pharmamaster

- Blue Security: An Israeli company selling a spam deterrence system
- Blue Frog bot would automatically respond to each spam message with an opt-out message
- Spammers started receiving hundreds of thousands of opt-out messages, disrupting their operations
- 6 of 10 of world’s top spammers agreed to stop sending spam to users of Blue Frog

Blue Security vs. Pharmamaster

- One spammer (PharmaMaster) started sending Blue Frog users 10-20 times more spam
- PharmaMaster then launched DDoS attacks on Blue Security and its business customers
- Blue Security could not protect its customers from DDoS attacks and virus-laced emails
- Blue Security reluctantly terminated its anti-spam activities

Albert Gonzalez

- Hacked into NAS at 14
- ShadowCrew Identity Theives
- Operation Firewall breaks up ring, Gonzalez turns informant
- Moonlights as cyber criminal
- Convicted for TJX attacks
- Serving 20 years in prison

Avalanche Gang

- Phishing Organization
- 2009: 2/3 of world’s phishing attacks
- 2010: re-imagined as malware Zeus
- 2016: European Security Forces with privatge industry such as Symantec takes down and dismantles Avalanche botnet

Cyber Crime Hall of Lame

- DarkTrace AI detects cyber crime activity
  - 2018 detects unusual activity on fingerprint scanner in luxury goods store
  - Hacker compromising scanners and uploading *his own fingerprints* to later gain physical access
- 17-year-old launches DoS against Call of Duty online to improve his score by preventing other players logging on and killing his character
- 21-year-old student successfully hacks security firm that protects the FBI then brags about it on Twitter

Politically Motivated Cyber Attacks

- Estonia (2007)
- Georgia (2008, 2009)
- Exiled Tibetan Government (2009)
- United States and South Korea (2009)
- Iran (2009)
- Espionage attributed to People’s Liberation Army
- Anonymous

Attacks on Twitter and Other Social Networking Sites

- Massive DDoS attack made Twitter service unavailable for several hours on August 6, 2009
- Three other sites attacked at same time: Facebook, LiveJournal, and Google
- All sites used by a political blogger from the Republic of Georgia
- Attacks occurred on first anniversary of war between Georgia and Russia over South Ossetia

Fourth of July Attacks

- 4th of July weekend in 2009: DDoS attack on governmental agencies and commercial Web sites in United States and South Korea
- Attack may have been launched by North Korea in retaliation for United Nations sanctions

Supervisory Control and Data Acquisition (SCADA) Systems

- Industrial processes require constant monitoring
- Computers allow automation and centralization of monitoring
- Today, SCADA systems are open systems based on Internet Protocol
  - Less expensive than proprietary systems
  - Easier to maintain than proprietary systems
  - Allow remote diagnostics
- Allowing remote diagnostics creates security risk

SCADA Systems Carry Security Risks

Internet-based supervisory control and data acquisition (SCADA) systems can save money and make systems easier to administer, but they also carry security risks. (Dave and Les Jacobs/Kolostock/Blend Images)

Stuxnet Worm (2009)

- Attacked SCADA systems running Siemens software
- Targeted five industrial facilities in Iran that were using centrifuges to enrich uranium
- Caused temporary shutdown of Iran’s nuclear program
- United States and Israel cooperated to develop and launch the worm

Cyber Espionage Attributed to People’s Liberation Army

- Hundreds of computer security breaches over a decade in more than a dozen countries investigated by Mandiant
- Hundreds of terabytes of data stolen
- Mandiant blamed Unit 61398 of the People’s Liberation Army
- China’s foreign ministry stated that accusation was groundless and irresponsible
- US government disclosed in 2015 that SSNs and other personal information from 22 million Americans stolen from Office of Personnel Management computers
- Prime suspect: Unit 61398 of People’s Liberation Army

Anonymous

- Anonymous: loosely organized international movement of hacktivists (hackers with a social or political cause)
- Various DDoS attacks attributed to Anonymous members

Actions Attributed to Anonymous

Year	Victim	Reason
2008	Church of Scientology	Attempted suppression of Tom Cruise interview
2009	RIAA, MPAA	RIAA, MPAA's attempt to take down the Pirate Bay
2009	PayPal, VISA, MasterCard	Financial organizations freezing funds flowing to Julian Assange of WikiLeaks
2012	U.S. Dept. of Justice, RIAA, MPAA	U.S. Dept. of Justice action against Megaupload
2013	Israel	Protest Israeli treatment of Palestinians
2014	City of Cleveland	Protest killing of 12-year-old Tamir Rice by a Cleveland police officer
2015	Jihadist groups	Terrorist attack on Paris office of Charlie Hebdo magazine

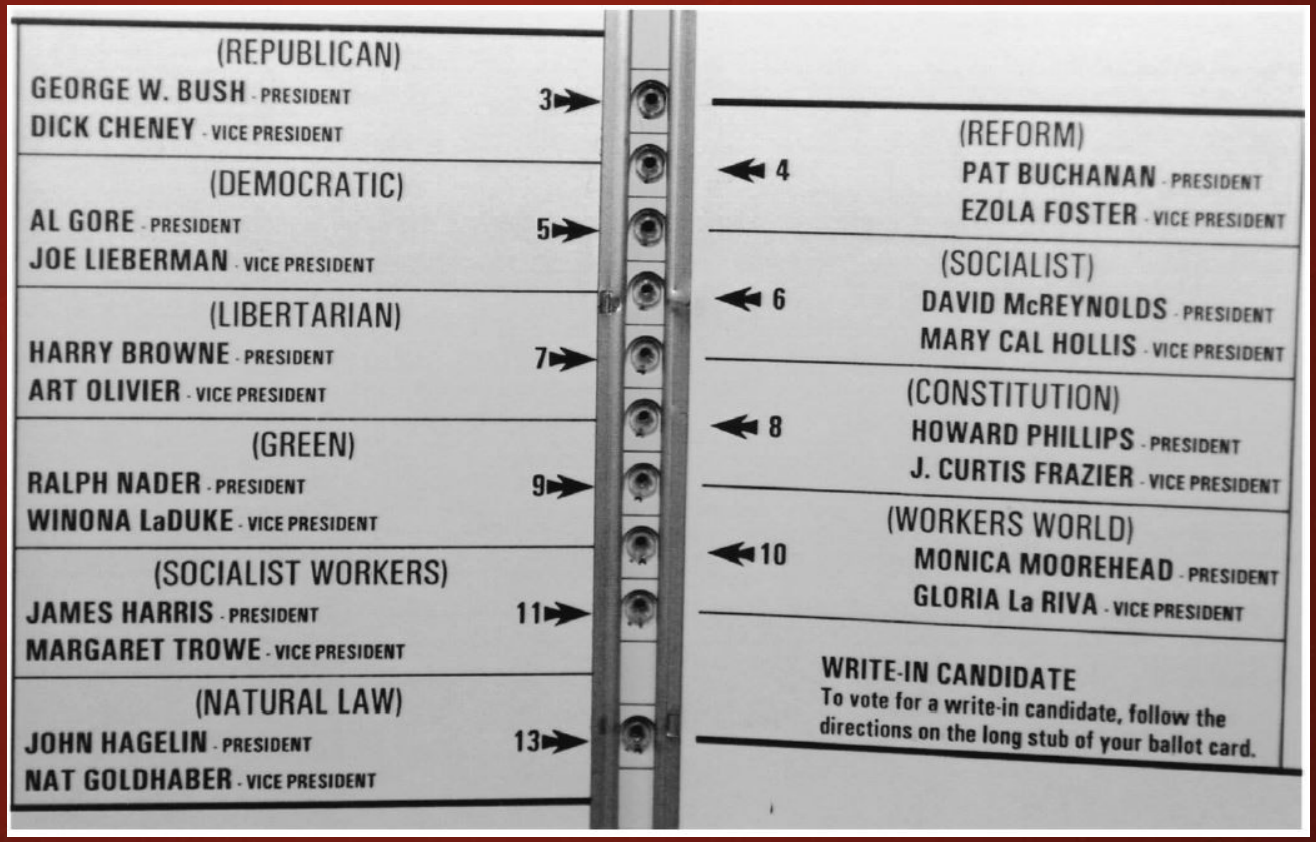
Convictions of Anonymous Members

- Dozens of people around the world have been arrested for participation in Anonymous cyber attacks
- Dmitriy Guzner (Church of Scientology attacks): 366 days in prison and $37,500 in restitution
- Brian Mettenbrink (Church of Scientology attacks): 1 year in prison and $20,000 in restitution
- Jake Davis (Sony Pictures attacks): 2 years in prison

Motivation for Online Voting

- 2000 U.S. Presidential election closely contested
- Florida pivotal state
- Most Florida counties used keypunch voting machines
- Two voting irregularities traced to these machines
  - Hanging chad
  - “Butterfly ballot” in Palm Beach County

The Infamous “Butterfly Ballot”



The layout of the “butterfly ballot” apparently led thousands of Palm Beach County, Florida, voters supporting candidate Al Gore to punch the hole associated with Pat Buchanan by mistake. (AP Photo/Gary I. Rothstein)

Benefits of Online Voting

- More people would vote
- Votes would be counted more quickly
- No ambiguity with electronic votes
- Cost less money
- Eliminate ballot box tampering
- Software can prevent accidental over-voting
- Software can prevent under-voting

Risks of Online Voting

- Gives unfair advantage to those with home computers
- More difficult to preserve voter privacy
- More opportunities for vote selling
- Obvious target for a DDoS attack
- Security of election depends on security of home computers
- Susceptible to vote-changing virus or remote access Trojan
- Susceptible to phony vote servers
- No paper copies of ballots for auditing or recounts

Utilitarian Analysis

- Suppose online voting replaced traditional voting
  - Benefit: Time savings
  - Assume 50% of adults actually vote
  - Suppose voter saves 1 hour by voting online
  - Average pay in U.S. is $21.00/hour
  - Time savings worth $10.50 per adult American
- Harm of DDoS attack difficult to determine
  - What is probability of a DDoS attack?
  - What is the probability an attack would succeed?
  - What is the probability a successful attack would change the outcome of the election?

Kantian Analysis

- The will of each voter should be reflected in that voter’s ballot
- The integrity of each ballot is paramount
- Ability to do a recount necessary to guarantee integrity of each ballot
- There should be a paper record of every vote
- Eliminating paper records to save time and/or money is wrong

Conclusions

- Existing systems are highly localized
- Widespread tainting more possible with online system
- No paper records with online system
- Evidence of tampering with online elections
- Relying on security of home computers means system vulnerable to fraud
- All in all, strong case for not allowing online voting

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
- New twist: malware infecting Internet-of-Things devices
- Cyber attacks becoming more common – at what point does a cyber attack become an act of war?

Next Time

- Best Security Practices
- No reading
- Participation Point by tomorrow at midnight:
  - What two DDoS attack forms use ICMP?

  OR
  - What was the name of the song blasted by the Stuxnet Worm on Iranian workstations?