COMPUTER AND NETWORK SECURITY

7.1 Introduction

- Computers getting faster and less expensive
- Utility of networked computers increasing
  - Shopping and banking
  - Managing personal information
  - Controlling industrial processes
- Increasing use of computers → growing importance of computer security

Hackers and Attackers

- Original meaning of hacker: explorer, risk taker, system innovator
  - MIT's Tech Model Railroad Club in 1950s
- Modern meaning of ~~hacker~~ attacker: someone who gains unauthorized access to computers and computer networks

TYPES OF ATTACKS

MALWARE

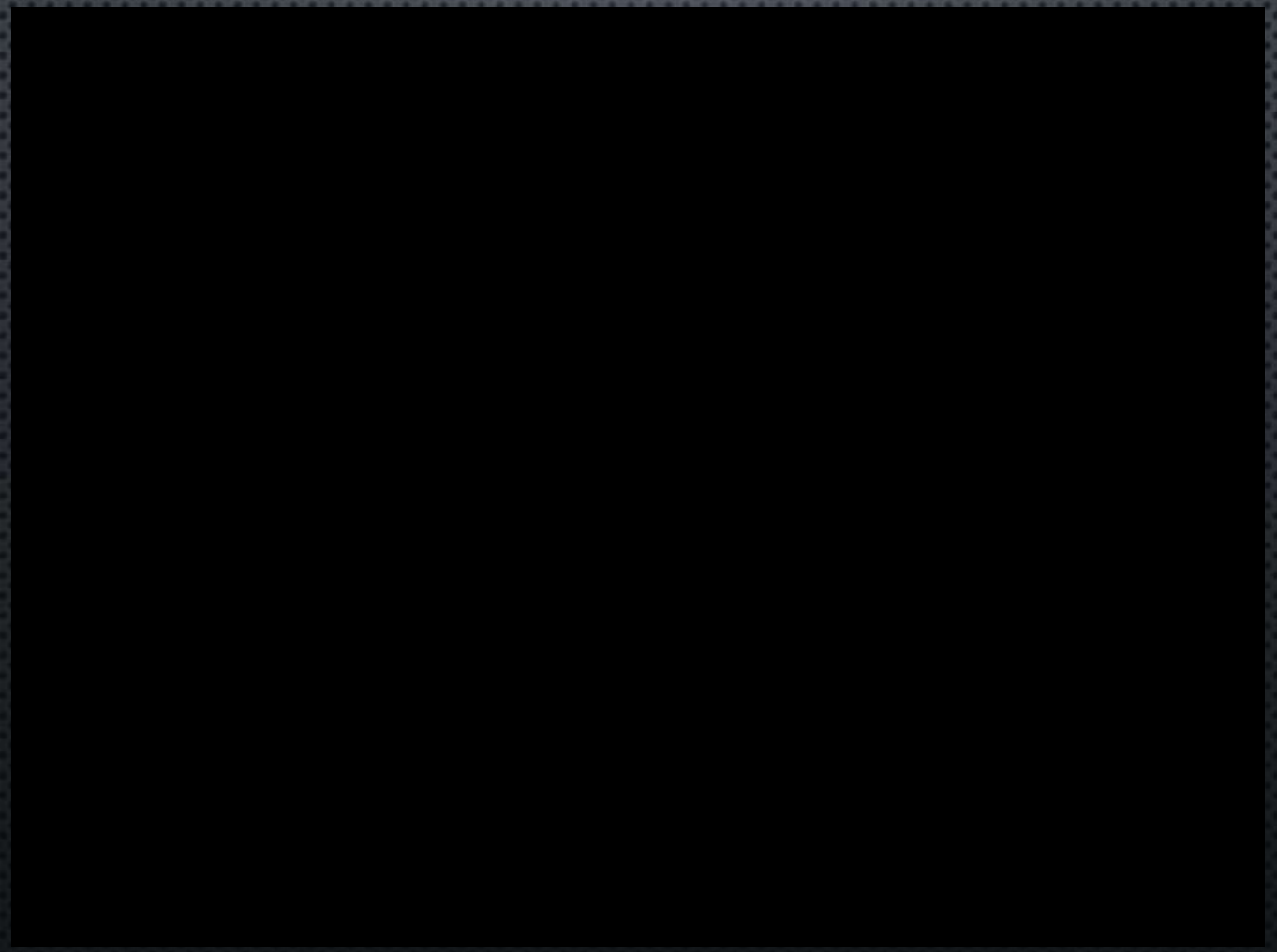
- MALICIOUS SOFTWARE
- PROGRAMS OR SCRIPTS USED TO:
  - INTERCEPT DATA
  - STEAL INFORMATION
  - LAUNCH OTHER ATTACKS
  - DAMAGE A COMPUTER
- MALWARE ATTACKS OCCUR AT AN ORGANIZATION ONCE EVERY *3 MINUTES*

SOCIAL ENGINEERING

- PSYCHOLOGICAL ATTACKING
- NON-TECHNICAL METHOD OF INTRUSION THAT RELIES ON:
  - HUMAN INTERACTION
  - TRICKERY
  - MANIPULATION
- EXPLOITING THE WEAKEST

SOCIAL ENGINEERING

AWARENESS



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

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

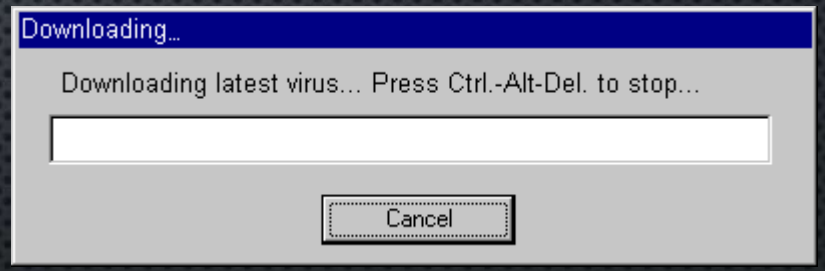
- By releasing Firesheep, Butler helped public understand lack of security on unencrypted wireless networks
- Butler's statements characteristic of someone interested in protecting privacy
- Butler demonstrated courage by taking responsibility for the program
- Butler demonstrated benevolence by making 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

- There is no standardized classification of malware but one way is by *primary* traits.
  - How it circulates to other networks
    - Email, storage peripherals, physical connections
  - How it infects files/machines
    - Memory, auto run scripts, exe, parasite vs. symbiote
  - How it conceals itself
    - Mutate(discuss more later)
  - The capabilities of its payload
    - What does it do? & Why does it do it?
    - This is endless – steal passwords, delete files, corrupt data, etc.



TYPES OF MALWARE

Question	Virus	Worm	Trojan
What is it?	Malicious computer code that replicates without human intervention	Malicious program that uses a computer network to replicate	Program that masquerades as a benign activity that delivers something malicious
How does it circulate?	Files	Network	Files
User action to circulate?	Transmit infected file to a secondary party	None	Transmit infected file to a secondary party
How does it infect?	When app is executed it replicates in a new file and delivers payload.	Vulnerability in application	When app is executed it delivers payload.

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
- 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

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

Defensive Measures

- **Security patches:** Code updates to remove security vulnerabilities
- **Anti-malware tools:** Software to scan hard drives, detect files that contain viruses or spyware, and delete these files
- **Firewall:** A software application installed on a single computer that can selectively block network traffic to and from that computer

Types of Attackers

- Cyber Terrorists
  - *Cyberterrorism*- Premeditated, politically motivated attacks
    - Designed to:
      - Cause panic
      - Provoke violence
      - Result in financial catastrophe
- Cyber Criminals
  - Individuals who launch attacks against other users and their computers
  - A loose network of attackers, identity thieves, and financial fraudsters who are highly motivated, less risk-averse, well-funded, and tenacious
  - Instead of attacking a computer to show off their technology skills (fame), cybercriminals have a more focused goal of financial gain (fortune): cybercriminals steal information or launch attacks to generate income
- Attackers
  - A person who uses advanced computer skills to attack computers

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
- Worm may have been created by Israeli Defense Forces

Cyber espionage attributed to People's Liberation Army

- Hundreds of computer security breaches 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

ANONYMOUS

- ANONYMOUS: LOOSELY ORGANIZED INTERNATIONAL MOVEMENT

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