Computers and Society

Computer Security

Notice: This set of slides is based on the notes by Professor Guattery of Bucknell and by the textbook author Michael Quinn

Computer Security

Computer security focuses on protecting the privacy of people's computers and data. Note that with the growth of cloud services, such data may not be resident only on the computer.

People who attempt to gain unauthorized access to others' computers are called *hackers*.

Goals of Hacking

Attempts to access others' data may be only curiosity. However, such attempts are often malicious and aimed at stealing services, valuables, or private information.

Hackers are often involved in identity theft, theft of financial information, theft of computer services (for example, for spamming), spying, or disruption of services.

The Original Meaning of Hacking

- According to our textbook, a *hacker* is an explorer, a risk taker, someone who is trying to make a system do something it has never done before.
  - Quinn, page 316 (5th edition)

HISTORY OF HACKING

MIT Tech Model Railroad Club

The first people who were called hackers were early computer enthusiasts such as members of the Tech Model Railroad Club (TMRC) at MIT.

The TMRC was founded in 1946 to build "things" like never before, including machinery, switching systems, control systems, and others.

http://tmrc.mit.edu/history/

Earliest Video Game: *Spacewar*

The members of TMRC created one of the earliest video games, *Spacewar* in 1962 using a DEC PDP-1 computer

The Jargon File defines *hacker* as "A person who enjoys exploring the details of programmable systems and stretching their capabilities, as opposed to most users, who prefer to learn only the minimum necessary."

http://en.wikipedia.org/wiki/Spacewar_(video_game)

http://en.wikipedia.org/wiki/Jargon_File

Hacker Ethics

Steven Levy, in his 1984 book *Hackers: Heroes of the Computer Revolution*, describes the hacker ethic as including the following:

- Access to computers should be unlimited
- All information should be free
- Mistrust authority – promote decentralization
- Judge hackers by their work, not by their credentials
- Beauty can be created on a computer
- Computers can change lives for the better

http://en.wikipedia.org/wiki/Hackers:_Heroes_of_the_Computer_Revolution

Hacking : The Dark Side

At the same time when computer hackers were trying to make the world better, a culture of telephone hackers (1950s – 1970s) was working to gain free access to telephone service and also telephone company systems.

These phone hackers stole service and, rarely, equipment from the telephone companies. On occasion they used their skills to hurt others, for example by cutting off their phone service.

The Phone Hackers: *Phreaks*

The phone hackers eventually began calling themselves *phreaks*, a corruption of the word "freak" with the "ph" from phone.

The phone phreaks were loosely organized, with their own publications (*Phrack*) and organizations (the Legion of Doom). As computers became popular in the 1980's and 1990's, phone phreaks turned more and more to computer hacking.

http://en.wikipedia.org/wiki/Phrack

http://en.wikipedia.org/wiki/Legion_of_Doom_(hacking)

Steve Jackson Games and E911

The phone phreaks stole telephone service and interfered with telephone company operations.

However, law enforcement agencies sometimes overstated their effects, and overreacted in ways that ended up damaging legitimate businesses (Steve Jackson Games, February 1989) or leading to failed prosecutions (Craig Neidorf/E911, 1989).

https://w2.eff.org/legal/cases/SJG/?f=background.sjg.html

http://en.wikipedia.org/wiki/Craig_Neidorf

Early Hacking Over the Internet

- The book of *The Cuckoo's Egg*
  - A real story!
  - Clifford Stoll traced and located a hacker in 1986 through a maze of networked computers
  - The original indication of the problem was a 75 cents discrepancy in accounting.

The book: http://en.wikipedia.org/wiki/The_Cuckoo's_Egg

The original ACM article:

"Stalking the wily hacker" by Cliffford Stoll
Communications of the ACM 31(5), May 1988 Pages 484-497

Hacking Culture Today

The hacking culture today has elements that resemble the old phone phreak culture. Information is freely exchanged on hacking websites, and there is an element of the old computer hacking culture in the respect for people with skills and knowledge to create new hacking tools.

However, organized crime and governments have also become involved.

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
- *New York Times* say it might be the work of Americans

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

Hackathon

- While "hacking" today may imply a negative sense in many situations, more and more computer science students are getting involved in "hackathons"
  - Where they get together for a few days and work intensely to solve some problems (similar to programming contests)

http://en.wikipedia.org/wiki/Hackathon

Hacking Attacks - Viruses

A *computer virus* is a piece of self-replicating code embedded in another piece of code (called the *host*).

Viruses were initially spread by copying infected software. Eventually viruses were embedded in emails, allowing viruses to actively propogate themselves.

Hacking Attacks - Worms

A *computer worm* is a self-contained program that spreads itself.

An early worm was the Internet worm developed by Robert Tappan Morris in 1988, then a graduate student at Cornell. It started as an experiment, but programming errors caused it to spread out of control, bringing down much of the internet for a day or two.

http://en.wikipedia.org/wiki/Robert_Tappan_Morris

The Conficker Worm

The Conficker worm (or Downadup) around end of 2008 is a highly sophisticated worm that has spread widely throughout the world. Its developers have watched the attempts to stop it, and have modified the Conficker program to counter attacks on the worm.

No one knows who the authors are, but evidence points to Ukranian organized crime elements.

An industry group is formed to counter the worm.

http://en.wikipedia.org/wiki/Conficker

Hacking Attacks – Denial of Service

Denial of Service attacks are intentional action designed to prevent legitimate users from making use of a computer service (Quinn).

There are a number of ways in which denial of service attacks can be launched. They typically involve overloading some resource of the attacked computer(s). This is a favorite tactic of the group Anonymous.

Hacking Attacks – Social Techniques

Social attacks take advantage of user carelessness or stupidity.

Dumpster diving attempts to find useful technical information that has been thrown in the trash.

Social engineering involves tricking people into giving away information about how to access and use systems.

Hacker Motivations

Author Bruce Sterling in *The Hacker Crackdown* suggests that many hackers think of hacking like a game. Cyberspace doesn't seem real because it's not physical. The rules for real life don't apply.

Quinn ties this to similar notions underlying media piracy. The pirated material isn't physical, it's just a copy of the bits that isn't worth what the owners think it's worth.

Hacker Motivations (2)

However, such comments apply to "hobbyist" hackers. The internet nowadays provides access to all kinds of economically valuable information. That draws in organized criminal activity as well. Organized crime is not treating this as a game.

The information may be even more valuable to governments. Recent developments have exposed government involvement in hacking exploits.

SOME CASES AND ANALYSES

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

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

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

The Internet Worm

- Robert Tappan Morris, Jr.
  - The "Morris" worm in 1988
- 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
- Morris is now a professor at MIT in CSAIL

http://pdos.csail.mit.edu/~rtm/

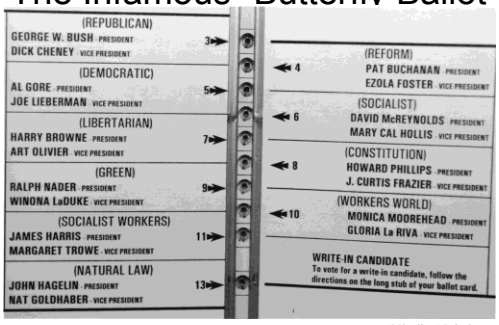
Ethical Evaluation

- 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
- Morris was wrong in all ethic framework to have released the Internet worm

Online Voting

- 2000 U.S. Presidential election closely contested
- Florida was a pivotal state, Bush won the state, thus the nation by 537 votes out of 6 million votes there
- Most Florida counties used keypunch voting machines
- Two voting irregularities traced to these machines
  - Hanging chad
  - "Butterfly ballot" in Palm Beach County
- Online voting would have eliminated these problems

The Infamous "Butterfly Ballot"



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 RAT
- 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 $18.00 / hour
  - Time savings worth $9 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