


CSE312/ISE312
A Gift of Fire, Fourth edition by Sara Baase

Read Chapter 5: Crime
(5.1-5.2)

Slides prepared by Cyndi Chie and Sarah Frye, and Sharon Gray. Revised by R. Kelly



What We Will Cover

- Hacking
- Identity Theft and Credit Card Fraud
- Whose Laws Rule the Web

Corresponding page number: 229



Hacking Terms

- Intentional, unauthorized access to computers
- The term has changed over time
- Phase 1: Early 1960s to 1970s
 - A positive term
 - A "hack" was an especially clever piece of code
- Phase 2: 1970s to mid 1990s
 - Hacking took on negative connotations
 - Breaking into computers for which the hacker does not have authorized access
- Phase 3: Beginning in mid 1990s
 - The growth of the Web changed hacking; viruses and worms could be spread rapidly
 - Large scale theft of personal and financial information

Corresponding page number: 230-231



Is Hacking a Crime

Is "harmless hacking" harmless?

- Responding to nonmalicious or prank hacking uses resources.
- Hackers could accidentally do significant damage.
- Almost all hacking is a form of trespass.

Corresponding page number: 235



Hacktivism (Political Hacking)

- Use of hacking to promote a political cause
- Disagreement about whether it is a form of civil disobedience and how (whether) it should be punished
- Some use the appearance of hacktivism to hide other criminal activities

Should hacktivism be treated as simple vandalism?

Corresponding page number: 236-237



Security Research

- “White hat hackers” use their skills to demonstrate system vulnerabilities and improve security

Is it ethical for a Stony Brook Computer Science security class to hack into an external company’s computers?

Corresponding page number: 237-239

Government Sponsored Hacking

- Examples
 - USSR gas pipeline
 - Russian border disputes
 - China industrial espionage
 - Possible US attack on Iranian nuclear facility
 - Russian tampering with 2016 US Election
- Hacking by governments has increased

Ability to identify origin of hacks
(not DDOS attacks) has improved

At what stage do you consider a government
sponsored hack to be an act of war?

Corresponding page number: 239-240

Security

- Variety of factors contribute to security weaknesses:
 - History of the Internet and the Web
 - Inherent complexity of computer systems
 - Speed at which new applications develop
 - Economic and business factors
 - Human nature

Corresponding page number: 241-244



Definitions

- Politically motivated hacking to conduct sabotage and espionage
 - Cyber espionage – obtaining secrets from individuals, rivals, governments, and enemies using illegal exploitation of computers, networks, and software
 - Cyber sabotage – disruption of equipment such as power, water, fuel, communications and transportation

The Director of US National Intelligence defines cyber-sabotage as the top security threat to the United States



Cyber Weapon Potential

- Cause physical damage (e.g., USSR pipeline, 1000+ Iran centrifuges)
- Disable power systems over a large scale – for an extended time period
- Disable financial systems
- Disable transportation (e.g., air traffic control, trains)

Think of cyber weapons as consistent with nuclear weapons



Current State

- Limited public US cyber war strategy
- Recent attacks on US
 - RSA
 - Military contractors
 - NY Times
 - 2 week power plant outage
 - 2016 election
- Recent attack on Iran (Olympic Games)
- History of “preemptive strike” against Iraq

Corresponding page number:



Cyber War Capabilities

- US – Olympic Games attack
- China – NY Times, RSA, aerospace contractors, CNN (when reporting on Tibet)
- Russia – 2007 Estonia attack
- Iran - possible attack against financial institutions, using a commercial data center botnet
- North Korea – 2013 attack on South Korea (banks, broadcast, and 30,000 computers)
- Israel – participation in Olympic Games attack
- Germany and India – now adding cyber warfare and cyber security capabilities



Examples

- 2009 reports of infiltration of US power grid (possibly only administrative systems)
 - By China and Russia (denied by China)
 - Left software that could potentially disrupt the grid
 - North American Electric Reliability Corporation issued a warning that grid is not adequately protected from cyber attack
- 2007 physical attack on Syria by Israel reported to be coordinated with a cyber attack on Syrian air defenses

Corresponding page number:



Issues


- Attribution of an attack is very difficult
 - DoD investing heavily in attribution capabilities
 - 2012 (e.g., DoD Secretary) statements indicate attribution can be done and (anonymous) has been done
- Current effectiveness of “zero day” malware
- Cyber threat can neutralize the US military advantage (e.g., China/Taiwan confrontation in 1996)
- US political and business resistance to imposition and enforcement of security standards
 - P&L issues
 - Global corporations



US Cyber Responsibilities


- Department of Defense (DoD) Cyber Command (established 2010)
- Department of Homeland Security (DHS)
- Central Intelligence Agency (CIA)
- National Security Agency (NSA)

Boundaries of US vs. non-US
intelligence and wartime vs.
peacetime actions




Legal Background

- Lag in laws and policies governing US conduct in cyber warfare
- Recent policy review (2013) - US President can order a pre-emptive strike if the US has credible evidence of a major cyber attack
- US military can openly carry out antiterrorism missions in nations where US operates under rules of war (e.g., Afghanistan)
- Intelligence agencies have authority to strike in undeclared war zones (e.g., Pakistan, Yemen)




Clarke's Questions (paraphrased)

1. What do we do when part of the US is blacked out due to a cyber attack?
2. Does the advent of a cyber war place the US at a disadvantage?
3. Do we envision the use of cyber war weapons only in response to the use of cyber war weapons against us?
4. Are cyber weapons something that we will employ routinely in both large and small conflicts?




Clarke's Questions (paraphrased)

5. Will we plan to conduct a cyber war even when there is not a physical engagement?
6. Do we see cyberspace as another domain in which we must be militarily dominant?
7. How certain must we be to identify who attacked us before we respond?
8. Will we ever hide the facts when we attack with cyber weapons?




Clarke's Questions (paraphrased)

9. Should we be hacking into other nations' networks in peacetime?
10. What do we do if we find that other nations have hacked into our networks in peacetime?
11. Do we intend to use cyber weapons primarily or initially against military targets only?
12. Do we see the utility of cyber weapons being their ability to inflict destruction on the economic infrastructure of an enemy or on their society at large?




Clarke's Questions (paraphrased)

13. What is the importance of avoiding collateral damage with our cyber weapons?
14. If we are attacked with cyber weapons, when do we respond with kinetic weapons (and do we publicly state our strategy)?
15. What kind of goals do we achieve with cyber war?



Clarke's Questions (paraphrased)

16. Should the line between peace and cyber war be brightly delineated (or blurred)?
17. Would we fight cyber war in a coalition with other nations?
18. What level of command authority will authorize weapons and approve targets?
19. Are there types of targets that we believe should not be attacked?



Clarke's Questions (paraphrased)


20. How do we signal our intentions – in peacetime and in crisis? Can we use our cyber weapons as a deterrent?
21. If an enemy is successful in an attack, how does that affect our other military and political strategies?



Defensive Triad Recommendations

1. Greatly increase security of the Internet backbone
2. Separate and secure the controls for the US power grid
3. Vigorously pursue security upgrades for DoD IT systems

Greatly aided by small, secure non-public Intranets




Internet Backbone

- 90% of Internet traffic flows through the backbone
- Only about a half dozen backbone providers
- Backbone ISPs have current business reasons not to drop botnet participants
- Strategy:
 - Stop an attack when it enters the backbone
 - Deep packet inspection (fast scanning of headers and data) is feasible
 - Privacy issues
 - Inspection at backbone peering points



US Power Grid

- Department of Homeland Security announced that a US power station was crippled for weeks by cyber attacks
- Most of the US power grid is Internet connected (and increasing with development of Smart Grid)
- Audits show grid is easily attacked (some commands to components are not encrypted)
- Strategy:
 - Deep packet inspection on control grid interconnect
 - Encryption and authentication of control commands



DoD IT Systems

- Increasing use of COTS software
 - Non-US HW components
 - Proprietary OS (e.g., Windows)
- Easily attacked classified and unclassified networks (e.g., 2008 Russian attack on DoD network)
- Strategy:
 - Upgrade DoD systems



Black Hat Consensus

- Recommended actions
 - Expanded cyber security research & development
 - Smart regulation (e.g., guidelines for backbone carriers)
 - Focus on resilience instead of attribution
 - No connectivity between utility networks and the Internet
 - Forceful leadership



Responsibility for Security

- Businesses have a financial responsibility to use security tools and monitor their systems to prevent attacks from succeeding
- Home users have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware)

Businesses are potentially liable for losses if security is not current

Do system developers have an ethical responsibility to develop with security as a goal?

Corresponding page number: 244-245



The Law

Catching and Punishing Hackers

- 1984 Congress passed the Computer Fraud and Abuse Act (CFAA)
 - Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet
 - Under CFAA, it is illegal to access a computer without authorization
 - The USA PATRIOT Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems

Corresponding page number: 245



Catching Hackers

- Law enforcement agents monitor hacker sites
- Security professionals set up 'honey pots' which are Web sites that attract hackers, to record and study
- Computer forensics specialists can retrieve evidence from computers, even if the user has deleted files and erased the disks
- Investigators trace viruses and hacking attacks by using ISP records and router logs

Corresponding page number: 246