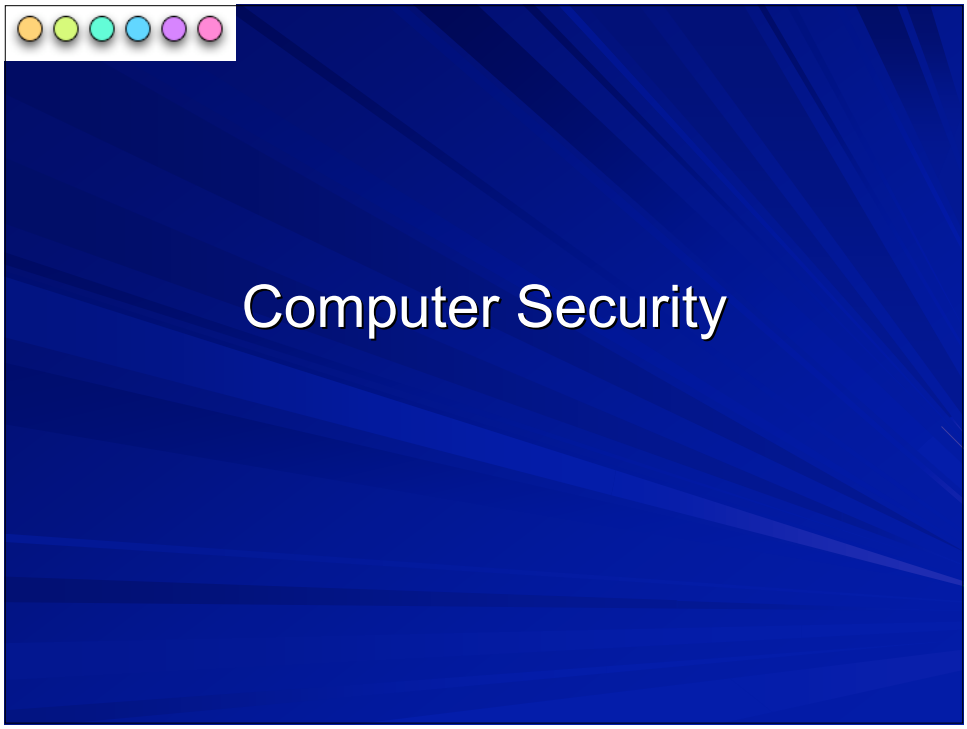
Introduction to Computer Security and Privacy

Simson L. Garfinkel, Ph.D.
simsong@csail.mit.edu
http://www.simson.net/

Today's Tutorial

Hour 1: Thinking about Security and Privacy.
Hour 2: Crypto Theory and Applications
Hour 3: Information Disclosure and Capture



What is Computer Security?

COMPUTER SECURITY:

"A computer is secure if you can depend on it and its software to behave as you expect." (Garfinkel & Spafford, 1991)

Computer security traditionally has 5 goals.

Availability
Confidentiality
Data Integrity
Control
Audit

Availability: Make sure you can use your system

Typically achieved by:

- Hardening
- Redundancy
- Reference checks on people

Confidentiality: Keep your secrets secret!

Typically achieved by:

- Physical isolation
- Cryptography
- Background checks on people

Data Integrity: Prevent others from modifying your data

Typically achieved by:

- Redundancy (2 or 3 copies?)
- Backups
- Checksums and digital signatures

Control:
Regulate the use of your system.

Typically achieved by:

- Access control lists
- Physical security

Audit:
What happened? How do we undo it?

Typically achieved by:

- Log files
- Human auditors & expert systems

Different environments have different priorities

Banking environment:

- integrity, control and audit are more critical than confidentiality and availability

Intelligence service:

- confidentiality may come first, availability last.

Military on the battlefield:

- availability may come first, audit may come last

University:

- Integrity and availability come first.

Most security texts focus on bad-guy attackers and malicious programs (worms & viruses).

Most continuity problems arise from:

- Operator, software, and configuration errors.
- Environmental problems.

The best security measures protect against both inadvertent and malicious threats.

A Security policy defines what you want to secure, from whom, and how you will do it.

Security perimeter

Because you can't secure everything

13

A Security policy defines what you want to secure, from whom, and how you will do it.

Security perimeter

Standards codify the what should be done

Guidelines explain how it will be done

14

How do you create a policy?

Option #1 Risk Assessment:

- Identify assets and their value
- Identify the threats
- Calculate the risks
- Conduct a Cost-Benefit Analysis

Option #2: Adopt “Best Practices.”

Techniques For Drafting Policies

Assign a specific “owner” to everything that is to be protected.

Be positive

Be realistic in your expectations

Concentrate on education and prevention

Threats to Consider:

Human error
"Hackers"
- technical gurus, script kiddies, criminals looking for gain.

Disgruntled employees
Organized crime
- increasingly a threat! Breaking into hospitals, e-commerce sites, etc.

Foreign espionage (it happens!)
Cyber terrorists (it hasn't happened yet)
Information warfare attacks (depends on how you count)
Microsoft / RIAA / MPAA
Mom

Risk Cannot Be Eliminated

You can purchase a UPS…

- But the power failure may outlast the batteries
- But the UPS may fail
- But the cleaning crew may unplug it
- But the UPS may crash due to a software error.

Spaf's first principle of security administration:

"If you have responsibility for security,
but have no authority to set rules or punish violators,
your own role in the organization is to take the blame
when something big goes wrong."

(Garfinkel & Spafford, 1991)

Saltzer & Schroeder's Design Principles

"The Protection of Information in Computer Systems," (Saltzer & Schroeder, 1975)

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least Privilege
- Least Common Mechanism
- Psychological Acceptability

Creating for securing operating systems, but generally applicable.

Economy of mechanism

"The design of the system should be small and simple so that it can be verified and correctly implemented."

- Example: A mechanical lock.

Fail-safe defaults

"Base access decisions on permission rather than exclusion."

By default, do not grant access.

- Example: Disabling services on a web server when the program is first installed..

Complete Mediation

"Every access should be checked for proper authorization."

Example: *Access control inside the corporate firewall.*

Open Design

"Security should not depend upon the ignorance of the attacker. This criterion precludes back doors in systems, which give access to users who know about them."

Example: Linux.

Separation of privilege

"Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key."

Counter-example: root

Principle of Least Privilege

"Every user and process should have the minimum amount of access rights necessary. Least privilege limits the damage that can be done by malicious attackers and errors alike."

Example: A key for the cleaning closet.

Least Common Mechanism

"Minimize the amount of mechanism common to more than one user and depended on by all users… Users should be isolated from one another by the system. This limits both covert monitoring and cooperative efforts to override system security mechanisms."

Example: The operating system kernel.

Psychological acceptability

"The security controls must be easy to use so that users routinely and automatically apply the protection mechanisms correctly…"

Also, mental models should match the underlying mechanisms.

Example:

29

Privacy

The word “privacy” means different things in different contexts.

Freedom from intrusion.

Control of personal information.
(“False light.”)

Control of one’s image or name.
(“Misappropriation.”)

The nature of the privacy threat has changed over the past 50 years.

Threat #1: The Media.
- See *The First Amendment Handbook,* http://www.rcfp.org/handbook

Threat #2: Government
- Wiretaps, database searches

Threat #3: Business
- Unwanted phone calls & mail
- Credit databanks
- Employee monitoring

The historic driver of the privacy problem was the "bad people" problem.

The world is filled with bad people.

You can't put them all in jail.

We are surrounded by evidence of "bad people:"

Decreasing inventory at stores

- Shoplifting?
- Employee theft?

Merchandise purchased with "lost" credit cards

- Perhaps the card was stolen
- Perhaps the card wasn't stolen

A simple way to solve the “bad people” problem is to make a list.

Make a list of the bad people.

Don’t do business with anybody on the list.

Examples of Solution...

Retail Credit (est. 1899)
- List of people “known” not to reply their debts

Medical Information Bureau (est. 1902)
- List of people with “known” medical problems

Chicago-area merchants (1950s)
- List of “known” shoplifters

Typical Credit Report

"Retired Army Lieutenant Colonel"

- "A rather wild-tempered, unreasonably, and uncouth person….
- "who abused his rank and wasn't considered a well-adjusted person.
- "He was known to roam the reservation at Ft. Hood and shoot cattle belonging to ranchers who had leased the grazing land from the Army."

—Hearings on the Retail Credit Company, 1968

Credit reports of the 1960s contained information that was hearsay or just wrong.

Records confused between individuals.

No "statute of limitations" on the information.

People frequently prohibited from seeing their own records.

Approaches to Privacy Enforcement

Governmental Standards
- Enforcement by regulatory agencies, states, etc.

Industry Standards
- "Codes of conduct"
- Limited enforcement through licensing
- Limited enforcement from government

Unregulated Market
- Reputation, or Caveat emptor

Technology can help in all of these cases.

Fair Credit Reporting Act, 1970

Right to:
- See your credit report.
- Challenge incorrect information.
- Information automatically expire after 7 years.
- Know who accesses your report.
- Free credit report if you are denied credit.

The Code of Fair Information Practice (1973) clarified these "data protection" rights.

#1 No Secret record-keeping systems.

#2 Right to see your record.

#3 Information obtained for one purpose may not be used for another purpose.

#4 Right to correct or amend incorrect records.

#5 Organizations must assure the reliability of data and take precautions to prevent misuse.

Fair Information Practice has evolved over the last 35 years…

1970 – FCRA

1980 – OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." (8)

1995 – EU 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the movement of such data."

2000 – Canada "C6" "Personal Information Protection and Electronic Documents Act." (PIPEDA)

2000 – US FTC: "Notice, Choice, Security and Access"
(plus: industry-specific legislation.)

HIPAA (Health Insurance Portability and Accountability Act of 1996*)

Key Provisions:

- Largely about health insurance portability, not about privacy
- Privacy mandates are largely about security:
  - Firewalls, anti-virus, etc.
  - Designate a privacy officer
  - Post privacy policy
  - Require outsourcing companies to protect information.
  - Access to health information; procedures for correcting errors.
- Enforced by the States (unfunded mandate); HHS enforces in "extreme cases."

(*privacy rule passed 2002)

COPPA: Children's Online Privacy Protection Act of 1998.

Key Provisions:

- Applies to online collection of info on children under 13
- Requires "verifiable parental consent"
  - Very hard in most cases; letter, fax or phone call
  - Some exceptions — one time response to "homework help"
- Privacy notice must be posted on website

http://www.ftc.gov/opa/1999/9910/childfinal.htm

Gramm-Leach-Bliley Act of 1999

Consumers must be informed of privacy policies

- Initial notice
- Annual notice
- Notices were mostly ignored!

Consumers must have a chance to "opt-out"

- Many different ways to "opt-out"
- Have you ever opted out?

45

Sarbanes-Oxley: "Public Company Accounting Reform and Investor Protection Act" of 2002

Section 101: Established Public Company Accounting Oversight Board

Section 201: Prohibits Auditors from providing non-audit services "contemporaneously with the audit"

Section 203: Lead auditor must rotate every 5 years

Sarbanes-Oxley: Clarified and strengthened many rules on publicly-traded corporations.

- Insider Trading
- Conflict of Interest
- Public disclosures
- Assessment of internal controls
- Mandatory disclosures

Not really a privacy or security law.
Internal controls should help protect personal information

Policy vs. Technology:

Policy solutions can be more flexible than technical solutions

- Policy can be “technology-neutral”
- Policy doesn’t need to be upgraded
- Policy doesn’t crash when there are typos
- Policy can enable lawsuits that attack the *human* root of problems

Policy vs. Technology:

On the other hand:

- Policy doesn't work across national boundaries.
- Privacy-invading firms have a seat at the table when legislation is drafted. (Sometimes they draft it.)
- Policy must be enforced.
  (Criminal provisions of HIPPA were recently gutted.)

Technical solutions can short-cut many of the problems in the policy arena.