Security

(more details…)

Security Goals

- **Confidentiality:**
  - Assets are accessible only by authorized parties
  - Read-type access: read, view, print, existence
  - secrecy and privacy

- **Integrity:**
  - Modified only by authorized parties in authorized ways
  - Modification: write, change, change status, delete, create

- **Availability:**
  - Assets accessible to authorized parties
  - denial of service
Vulnerabilities

- Reverse the 3 security objectives
- Major assets:
  - Hardware
  - Software
  - Data
- Their interconnection is also an asset

Threats to Hardware

- Physical device is visible – easy target

- “Involuntary computer-slaughter”
  - Accidental acts not intended to do harm
  - Ex: natural acts, human-oriented accidents (spilling of food/drink), dust, smoke, physical abuse

- “Voluntary computer slaughter” – machinicide:
  - Shoot or stab machines, bombs/fires/collisions, short out circuit boards (pens, knives, etc.), stolen
  - Theft and destruction major mechanisms for attack
Threats to Software

• Computing Equipment worthless without software
• Deletion: easy to delete
  – Motivate need for configuration management
• Modification:
  – Trojan horse: overtly does one task, covertly does something else
  – Virus: type of Trojan horse; spread infection from one computer to another
  – Trapdoor: program has secret entry point
  – Information leaks: makes information accessible to unintended people/programs
• Theft: unauthorized copying of SW

The internet worm of 1988


Internet worm of 1988

- exploited vulnerabilities in unix, finger, sendmail
- copied /etc/passwd file, then guessed passwords
- used any credentials found to infect other systems

Internet worm of 1988

Goal was to set up a botnet, but several mistakes prevented it from happening
Other notorious worms

- Melissa
- ILOVEYOU
- SirCam

Objective: trick users into clicking executable email attachment (requires human assistance)

An actual botnet

Conficker worm:
- first appeared 2008
- infects a computer, opens a channel to worm’s creator, then awaits instructions

- Still around after 8 years…
Conficker in action

Worm connects computers across network.
Computers without property security updates
Computers with open shares
Computers with removable media (e.g., USB drives, external hard drives)
Computers with weak passwords

Protect with updated security patches, anti-virus SW, strong passwords, and secured shares.

Threats to Data

- Printed data can be readily interpreted by general public
- Data attack more widespread than either HW or SW
- Data has cost:
  - Confidential data has value to competitors
  - Incorrectly modified data lead to loss of human life
  - Poor security can lead to financial liability
    - Personal data is leaked to public
- Data may have short life:
  - High value: (e.g., economic data and effect on stock market)
Threats to Data

- **Confidentiality:**
  - Preventing unauthorized disclosure
  - **Problems:** wiretapping, bugs in output devices, monitoring electromagnetic radiation, bribing key employees. (Data is often human readable.)

- **Integrity:**
  - Preventing unauthorized modification
  - **Problems:** malicious programs, erroneous file system utilities or flawed communication systems

- **Availability:**
  - Preventing denial of authorized access
  - **Problems:** denial of service attacks. (flood server)

Other threatened entities

- **Storage media**
  - Need backups of data and physical protection of backups

- **Networks:**
  - Involve HW, SW, and data

- **Access:** access to computing equipment (unauthorized use of processing cycles, network, etc.)

- **Key People**
  - Crucial weak points
In the news…

What big recent retail data breach has made news?

Ransomware

Was BWL prepared for a ransomware attack?

Lansing State Journal

Langston - The April 25 cyberattack against the Board of Water & Light was devastating, expensive and embarrassing, but seven months later BWL leaders say the utility is moving forward with heightened cybersecurity awareness among its more than 700 employees.

The attack involved an employee opening an email attachment that contained a ransomware virus. The virus locked the utility’s email and accounting systems. Eleven days passed before BWL said those systems were operating normally.

In addition to paying a $35,000 ransom to unidentified foreign hackers, BWL incurred costs of cyber forensics, the cleaning and testing of 790 to 800 laptops, desktops and servers, the replacement of an extensively infected server and $440,000 in cybersecurity upgrades that brought the total to about $2.4 million.
People Involved

- **Amateurs:**
  - Observed flaw in security
  - Normal/regular employees
  - Exploit system (innocently?)

- **Crackers:**
  - Students who attempt to access facilities
  - “victimless” crime?
  - Serious offense: causes millions of dollars in damage

- **Career Criminals:**
  - Start as computer professionals who engage in computer crime and have good payoffs
  - Electronic spies
  - Response: lack of criminal prosecution trend

Methods of Defense

- **Controls:**
  - **Encryption:** transform data to unintelligible format to outside observers.
  - **SW controls:**
    - Internal program controls: parts of program enforce security restrictions (e.g., access limits)
    - Operating system controls: limitations enforced by OS to protect users from each other
    - Development controls: quality standards for design, code, test, and maintenance.
  - May use HW components, encryption, or info collection.
    - Affect users directly, so is usually first solution considered
    - Care must be taken in **design** because it affects the way systems are used
    - Balance between ease of use and effectiveness.
Methods of Defense (cont’d)

- Hardware Controls:
  - HW or smartcard implementations of encryption
  - Locks limiting access
  - Circuit boards that control access to disks in PCs

- Policies:
  - Added HW or SW features
  - Frequent changes of passwords
  - Must have training and administration
  - Legal and ethical controls (lack of understanding and standards for both)

- Physical Controls:
  - Locks on doors, guards at entry points,
  - backup copies of important artifacts,
  - physical site planning to avoid natural disasters

Effectiveness of Controls

- Awareness of problem
  - People using controls must understand the need

- Likelihood of Use:
  - **Principle of Effectiveness**: Controls must be used to be effective. They must be efficient, easy to use, and appropriate.

- Overlapping Controls:
  - Security for a PC may involve security for access to data, physical access to machine/storage media, and file locking mechanisms.

- Periodic Review:
  - Few controls are permanently useful.
  - Need to review and update.
Cost Benefit Analysis

• Cost of Loss
  – Assigning cost range is sufficient
• Cost of Prevention
  – Cost of preventing each loss
• Adding up the Numbers
  – Matrix w/ assets, risks, possible losses
  – Includes: probability, the predicted loss, $ required to defend against the loss
• Convincing Management
  – Risk assessment helps you make proper justifications for management

What does all this mean for a software engineer?

• evaluate risks and costs
• create and follow a security policy
• from a practical standpoint,
  ▪ don’t take defaults
  ▪ don’t take shortcuts
Creating Policy

- Defines what you consider to be valuable and what steps should be taken to safeguard those assets.
- General Policy
- Policy for Different Sets of Assets
  - Email, personnel data, etc.

The Role of Policy

- Makes clear what is being protected and why
- States the responsibility for that protection
- Provides grounds upon which to interpret and resolve any later conflicts that might arise
- Should be general and change little over time
- Should not list specific threats, machines or individuals by name
Standards

• Standards codify successful practice of security in an organization.
• Generally phrased in terms of “shall”
• Platform independent
• Imply a metric to determine if they have been met
• Developed to support policy
• Change slowly over time

[Garfinkel & Spafford]

Four Easy Steps to a More Secure Computer

1. Decide how important security is to your site
2. Involve and educate your user community
3. Devise a plan for making and storing backups of your system data
4. Stay inquisitive and suspicious

[Garfinkel & Spafford]