Security Intro
Acknowledgements

● Gene Spafford
● Annie Anton
● Charles Pfleeger
● Marilyn Wulfekuhler
Outline

• Terminology
• Brief Introduction
• Security Planning
• Creating a Security Policy
• Threats, Attacks & Services
• Internet Privacy Policies
Terminology

• “A computer is **secure** if you can depend on it and its software to behave as you expect (intent).”

• ‘**Trust** describes our level of confidence that a computer system will behave as expected.’ (intended)

[Garfinkel & Spafford, Kasten]
What is secure?

- Does not disclose information
- Does not allow unauthorized access
- Does not allow unauthorized change
- Maintains QoS despite input and load
- Preserves audit, authenticity, control
- No surprises!

[Spafford]
Why Worry?

- Information has value
  - when combined
  - when altered
  - when disclosed

- Resource use has value
  - unauthorized use
  - denial of service

- Damage to reputation
  - damage to your personal reputation
  - damage to your group
  - damage to your company

- Your system is not alone
  - other machines on the network
  - shared resources and files
  - indirect liability

[Spafford]
Three Common Failures

• Organization has **no formal policy**. Thus, personnel cannot *consistently* make necessary decisions.
• Organization has **no reasonable response** plans for violations, incidents, and disasters.
• Plans don’t work when needed because they haven’t been *regularly tested, updated, and rehearsed*. (E.g., failure of operational security)
The Challenge

• “Without assurance that our systems will stay secure, we endanger our economies, our privacy, our personal safety and privacy, and our social institutions.” [Spafford]
How do we get there?

• Understand the needs of the users
  – Narrow focus better than broad

• Understand basic tenets of security
  – Scarcity/rareness of programs and experts

• Capture requirements for design and validation

• Design with care using good tools and methods

• Validate & Verify

[Spafford]
Understanding Security

• Good security means
  – Limiting what happens
  – Limiting who can make it happen
  – Limiting how it happens
  – Limiting who can change the system

• Users don’t tolerate limits unless there is a paradigm shift
  • Mainframes to PCs/desktops
  • to laptops
  • to handheld computers
  • to cellphones/smartphones
Psychological Acceptability

• Easy to use
  – Should be as easy to use as to not use

• False alarms should be avoided

• Frequent changes and updates are bad

• Should not require great expertise to get correct

[Spafford]
Patches

- Fixes for flaws that require an expert to install are not a good fix.
- Fixes that break something else are not a good fix.
- Frequent fixes may be ignored.
- Goal should be design, not patch

[Spafford]
Source of Problems

About 30% are buffer overflows or unchecked data

Over 90% are coding/design flaws.

Source: Securityfocus.com

[Spafford]
Quality as a Market Problem

- Good software engineers and security designers are scarce
- Productivity of coders varies:
  - Top 10% are at least 10x more productive than average coder.
  - Organizations should invest in raising skill level.
- That takes time and money, so there is a disincentive to improving quality

[Spafford]
What can we do?

• Understand that there is no “average user”
• Understand balance between features and security
• Employ better testing
• Manage complexity and change
• Build in security from the start
• Understand policy differences.

[Spafford]
Security Planning

- Security needs planning
- Risk assessment
- Cost-benefit analysis
- Creating policies to reflect your needs
- Implementation
- Audit and incident response
Planning Your Security Needs

- Confidentiality
- Data Integrity
- Availability
- Consistency
- Control
- Audit
Critical Concerns for Various Industries?

- Banking environment?
- National defense-related system that processes classified information?
- University?
- E-Commerce?
Risk Assessment

• Three questions to answer:
  – *What* am I trying to protect?
  – What do I need to *protect against*?
  – *How much* time, effort and money am I willing to expend to obtain adequate protection?

• Three key steps:
  – Identify assets
  – Identify threats
  – Calculate risks
Risk Assessment
Step 1: Identify Assets

• Tangibles
  – Computers, disk drives, proprietary data, backups and archives, manuals, printouts, commercial software distribution media, communications equipment & wiring, personnel records, audit records

• Intangibles
  – Safety & health of personnel, privacy of users, personnel passwords, public image & reputation, customer/client goodwill, processing availability, configuration information
Risk Assessment
Step 2: Identify Threats

- Illness of key people
- Loss of key personnel
- Loss of phone/network services
- Loss of utilities (phone, water, electricity) for a short or prolonged time
- Lightening or flood
- Theft of disks, tapes, key person’s laptop or home computer
- Introduction of a virus
- Computer vendor bankruptcy
- Bugs in software
- Subverted employees or 3rd party personnel
- Labor unrest
- Political terrorism
- Random “hackers”
Broad Categories of Threats

• Interruption
• Interception
• Modification
• Fabrication
Interruption

• Asset becomes lost, unavailable, unusable
• Ex:
  – Malicious destruction of HW device
  – Erasure of program or data
  – Malfunction of OS (e.g., cannot find a file)
Interception

• Unauthorized party gained access to an asset
  – Outside party: person, program, system
• Ex:
  – Illicit copying of program/data files
  – Wiretapping to obtain data in network
• Loss may or may not be detected (i.e., leave no traces)
Modification

• Unauthorized access tampers with asset
• Ex:
  – Change values in database
  – Add computation to a program
  – Modify data during transmission
  – Modify hardware
• Detection may be difficult
More Modification

- Trojan horse:
  - Overtly does one task, covertly does something else
- Virus:
  - Example of trojan horse;
  - Spread infection from one computer to next
- Trapdoor: program has secret entry point
- Information leaks: (in program)
  - Make info accessible to unintended people/programs
Fabrication

- Unauthorized party produce/generate counterfeit objects on computing system
- Ex:
  - Insert spurious transactions to a network
  - Add records to an existing database
- Detection and authentication are problems
Risk Assessment
Step 3: Quantify Threats

• Estimate likelihood of each threat occurring
• If an event happens on a regular basis, you can estimate based on your records
• Other sources:
  – Power company: official estimate of likelihood for power outage during coming year
  – Insurance company: actuarial data on probabilities of death of key personnel based on age & health
  – Etc.