

Basics

Unintended behavior

Often systems do not behave as we intend.

The unintended behaviors can be traced to:

- environmental disruption,
- operational errors,
- poor design or implementation (bugs),
- deliberate attacks.

These problems mean that systems don't meet their functional requirements.

Unintended behavior (cont.)

Some approaches to addressing these problems are:

- environmental disruption,
 - ⇒ stronger interfaces,
 - ⇒ replication,
- operational errors,
 - ⇒ operator tolerance and education,
 - ⇒ better tools,
- poor design or implementation (bugs),
 - ⇒ languages and tools,
 - ⇒ testing,
 - ⇒ verification,
- deliberate attacks,
 - ⇒ lower expectations,
 - ⇒ ???

Some threats

In order of increasing severity:

- Unintentional blunders.
- Hackers driven by technical challenges.
- Disgruntled employees or customers seeking revenge.
- Criminals interested in personal gain.
- Organized crime interested in hiding something or in financial gain.
- Organized terrorist groups.
- Foreign espionage agents.
- Information-warfare operations intended to disrupt weapons or command structures.

(Roughly from the Defense Science Board.)

Attack goals

The typical goals of attacks are not specific to computer systems:

- Publicity,
e.g., by defacing web pages.
- Fraud,
e.g., on-line scams.
- Theft of intellectual property,
e.g., DVD contents.
- Destruction,
including denial-of-service.
- Invasions of privacy; surveillance.

Some intermediate goals (e.g., stealing a password) are.

The unchanging nature of security

Security for computer systems is much like security in the rest of the real world.

Security is not black and white.

It is not about perfect defenses against well-funded, capable, and determined attackers.

The unchanging nature of security (cont.)

Security is about:

- value:
 - sometimes a simple figure
 - not always easy to calculate
- locks:
 - several kinds
 - not always cheap
 - seldom convenient
 - imperfect
- detecting attacks:
 - not always possible
 - not always possible in real time
- catching and punishing attackers
 - hard at a distance!

Vulnerabilities

Attack: A method of exploiting a vulnerability.

Vulnerability: A weakness that can be exploited to cause damage.

A trend toward vulnerable systems

Some increasingly common system characteristics enable attacks (and aggravate other problems).

- Interaction with an uncertain physical environment.
E.g., for a laptop in the enemy's hands.
- Interaction with an uncertain network environment.
Everything is connected.
- Interaction with an uncertain software environment.
E.g., with mobile code in Web pages.
E.g., with an untrusted media player.

A trend toward vulnerable systems (cont.)

- Use of an open infrastructures.
E.g., of the phone network.
- Distributed administration.
No central design and control.
- Diverse operators.
Everyone is an operator.
- Automation.
Including automated infection!

A trend toward vulnerable systems (cont.)

- Building from COTS components
(COTS = commercial, off-the-shelf).
E.g., from x86.
- Importance of time to market.
And the market seldom pays for security.
- Monocultures.
E.g., homogeneous systems based on Windows and x86.

A trend toward vulnerable systems (cont.)

These characteristics are unlikely to just go away:

- They are the result of fundamental economic or technical trends.
- Many are generally desirable.

Reading

A paper by Lampson:

- “Protection”

reachable from

www.research.microsoft.com/users/blampson/.

A paper by Saltzer and Schroeder:

- “The protection of information in computer systems”

reachable from web.mit.edu/Saltzer/www/publications/.

Homework 1 (for April 13)

Exercise 1:

Describe an actual security failure in a computer system.

State:

- a) the security property that is violated,
- b) the vulnerability that permits the violation,
- c) the attack that exploits the vulnerability,
- d) if possible, how to address the vulnerability.

You may use whatever sources you like (the Web, newspapers, the scientific literature), but please cite them. A paragraph may suffice; a page should.

Homework 1 (cont.)

Exercise 2:

Comment on how one of the principles of Saltzer and Schroeder is followed or disregarded in some aspect of a contemporary system that you know.

Again, a paragraph may suffice; a page should.

Homework 1 (cont.)

Exercise 3:

Lampson (pp. 2–3) describes a simple scheme for identifying processes in systems. Comment on how it applies, or not, when the system in question is the Web.

A paragraph should suffice.