Lecture 1 Notes; March 31, 1997; Notetaker: Michael Clifford

BACKGROUND OF COMPUTER SECURITY

Question: If a student takes a copy of a homework assignment file from another student in CSIF, and the file is not read protected, is the action a violation of security?

Answer: This depends on the policy of the facility

Policy: What actions are permissible
- At UCD, the policy states that students may not copy each other's homework

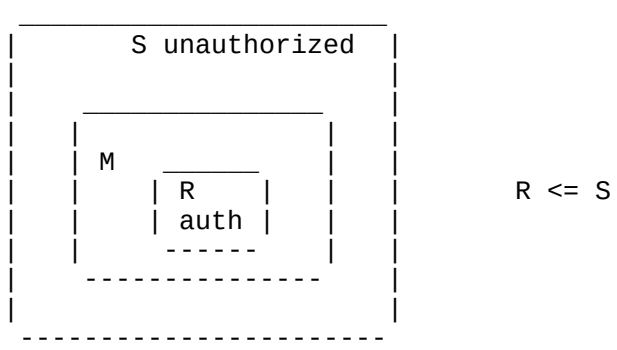
Mechanism: Those things which enforce policy
- In the example, a security breach occured because UCD's academic honesty policy was violated.
- A mechanism may not adequately enforce a policy, or may over enforce a policy.

Precision: A mechanism is precise if no unauthorized actions may be taken

Secure: A mechanism is secure if no actions that the policy does not permit can be taken

Given a set of system states:

S = unauthorized actions
M = states permitted by a mechanism
R = states permitted by a policy



Precise: M = R
Secure: M is a subset of R
Not secure: M contains elements not in R

COMPONENTS OF SECURITY POLICY

-Confidentiality

-Integrity:
- Data integrity: data has not been changed
- Origin integrity: data comes from the place that it is supposed to have come from

-Availability: Why is data (in)accessible?

-Snooping: gathering data

-Modification: altering data as it flows by

-Masquerading: pretending to be someone that you are not

-> Delegation: authority can be delegated, but both the identity and validity of the delegation must be confirmed

-Repudiation of origin (plausible deniability): denying that you sent something
-> how do you prove an origin? Technical details conflict with laws and human nature

-Denial of Receipt: You can deny that you got something

-Delay: making something take longer to occur

-Denial of service: infinite delay - you can be prevented from using a system, by blocking access to that system's services

Which threats are important in a security policy depends on what you are doing.

Possible attack: masquerade as a secondary server, then deny access at the primary server.

THREE GOALS OF SECURITY

1) Prevention: preventing problems

2) Detection: identifying that a problem exists

3) Recovery: dealing with problems in an appropriate manner

TRUST

-how much do you trust your system monitoring?

-well placed trust is good

-poorly placed trust leaves you without security

-know what you trust, and what your security mechanisms trust

Trust occurs at four levels:

1) People level
2) Software level
3) Operations level
4) Hardware level (example: Pentium FPU bug)

What are your basic assumptions?
What is your attacker capable of?

OPERATIONS

-Social engineering (lying): Convincing people to follow certain patterns of behavior, such as giving you access to a system

-Organizational problems: A company does not have an organization which effectively supports system security

-People problems: The people who work at a company may not know what they are doing. People who leave a company may know too much about the security policies and mechanisms at the company that they have left

ANALYSIS

-Cost / benefit analysis: Does it cost more to put a system in place than to do

nothing at all?

-Risk assessment: What are the potential problems?
How likely are problems to arise?
mechanisms: which methods of dealing with problems are best?

-Laws and culture: What rules apply to operating in a certain company or environment?
-what will people put up with? Would the requirement of passing a drug test in order to access a computer be acceptable?