UOWD
University of Wollongong in Dubai

CSCI358
Security Engineering

Spring 2014
Tutorial #1
March 10th, 2014
Solutions

An overview of information security

Learning objectives:

- Assess the importance and the relevance of detection, recovery, and prevention
- Explain the need for implicit security policies
- Assess the potential vulnerabilities raised by the composition of security policies

Answer all questions

Some definitions

A. Basic components or services

a) Confidentiality
b) Integrity
c) availability

B. Policy and Mechanism

a) A *security policy* is a statement of what is, and what is not, allowed. It may be expressed in:

- natural language, which is usually imprecise but easy to understand;
- mathematics, which is usually precise but hard to understand;
- policy languages, which look like some form of programming language and try to balance precision with ease of understanding

b) A security mechanism is a method, tool, or procedure for enforcing a security policy. Mechanisms may be

- technical, in which controls in the computer enforce the policy; for example, the requirement that a user supply a password to authenticate herself before using the computer
- procedural, in which controls outside the system enforce the policy; for example, firing someone for ringing in a disk containing a game program obtained from an untrusted source

C. Composition of policies:

a) The composition problem requires checking for inconsistencies among policies. If, for example, one policy allows students and faculty access to all data, and the other allows only faculty access to all the data, then they must be resolved (e.g., partition the data so that students and faculty can access some data, and only faculty access the other data).

b) If policies conflict, discrepancies may create security vulnerabilities.

D. Goals of security: prevention, detection, recovery:

a) Prevention:

- To prevent attackers from violating security policy
- Prevention is ideal, because then there are no successful attacks.

b) Detection:

- To detect attackers' violation of security policy
- Detection occurs after someone violates the policy.
- The mechanism determines that a violation of the policy has occurred (or is underway), and reports it.
- The system (or system security officer) must then respond appropriately.

c) Recovery :

- Stop attack, assess and repair damage
- Continue to function correctly even if attack succeeds
- Recovery means that the system continues to function correctly, possibly after a period during which it fails to function correctly.
- If the system functions correctly always, but possibly with degraded services, it is said to be intrusion tolerant.
- This is very difficult to do correctly; usually, recovery means that the attack is stopped, the system fixed (which may involve shutting down the system for some time, or making it unavailable to all users except the system security officers), and then the system resumes correct operations.

1. Detection, recovery, prevention

For each of the following statements, give an example of a situation in which the statement is true.

a) Prevention is more important than detection and recovery.
b) Detection is more important than prevention and recovery.
c) Recovery is more important than prevention and detection.

Solution:

a) An example of when prevention is more important than detection and recovery is the nuclear command and control system. By the time an intrusion is detected and recovered from, an attacker could have launched nuclear weapons.

*b) An example of when **detection** is more important than prevention and recovery is in the protection of medical records from unauthorized emergency room personnel. If someone is brought into an emergency room, there may not be time to secure the patient's permission to access his medical records. But if the records are accessed illicitly, the security personnel should detect it.*

c) An example of when recovery is more important than prevention and detection is on a banking computer that maintains account balances. The bank must be able to recover the balance of all accounts to ensure it provides accurate service to its customers. Prevention and detection, while important, are not so important as keeping the balances accurate.

2. Policy

In addition to mathematical and informal statements of policy, policies can be implicit (not stated).

a) Why might this be done?
b) Might it occur with informally stated policies?
c) What problems can this cause?

Solution:

a) Policies may be implicit for a number of reasons.
   - The policy **may be ambiguous, and the resolution of the ambiguity left to the reader; t**hus, the exact policy is not explicitly stated.
   - The policy **may not cover all aspects of the system**; those aspects not covered by the explicit policy would presumably be covered by the implicit policy.
   - The institution own**ing the computer may simply choose t**o tell users to use "common sense"; this is also an implicit policy.

b) It is highly likely that **informally stated policies will have many areas of ambiguity and not cover all contingencies.** Hence these types of policies often lead to implicit policy components.

c) The main problem with implicit policies is that:
   - **not all users may know about them,** or may have agreed to them.
   - The statement that "common sense is so unusual because it's not common" applies here.
   - Given that people cannot refer to an oracle, or source, for an implicit policy but instead must gather opinions and make their own decisions, which may disagree with those of the system managers, a user may find **herself violating the security policy without realizing it or intending to violate it.**

3. Email-policy

Policy restricts the use of electronic mail on a particular system to faculty and staff. Students cannot send or receive electronic mail on that host. Classify the following mechanisms as secure, precise, or broad.

a) The electronic mail sending and receiving programs are disabled.
b) As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.).
c) The electronic mail sending programs ask the user if he or she is a student. If so, the mail is refused. The electronic mail receiving programs are disabled.

Solution:

a) The mechanism is **secure,** because students cannot send or receive electronic mail on the system. It is not precise, as faculty cannot send or receive electronic mail on the system, and the security policy says they are allowed to.
b) This mechanism is **precise**, because any mail from or to students is discarded. (You can argue **this is broad**, because students can execute the "send mail" command, but the mail will never leave the machine. The word "send" is **somewhat ambiguous.)**
c) This **mechanism is broad,** because a student can claim to be a faculty member when answering the question.