

Chapter 4 SECURITY POLICIES

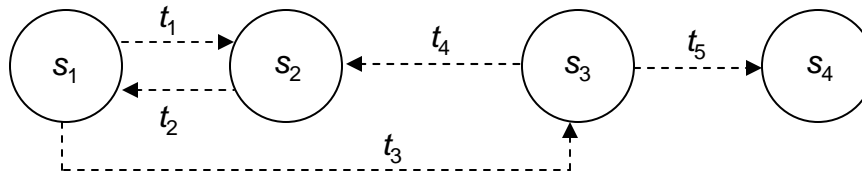
- A security policy defines “secure” for a system or a set of systems.

4.1 Security Policies

- A *security policy* is a statement that partitions the states of a system into a set of *authorized*, or *secure*, states, and a set of *unauthorized*, or *nonsecure*, states.
- A *secure system* is a system that starts in an authorized state and cannot enter an unauthorized state.
- Example: a finite-state machine

Set of authorized states: $A = \{s_1, s_2\}$

Set of unauthorized states: $UA = \{s_3, s_4\}$



This system is not secure because of the edge from s_1 to s_3 .

- A *breach of security* occurs when a system enters an unauthorized state.
- X : a set of entities, I : some information or resource. I has the property of *confidentiality* w.r.t. X if no member of X can obtain information about I .
- X : a set of entities, I : some information or resource. I has the property of *integrity* w.r.t. X if all member of X trust I .
- X : a set of entities, I : some resource. I has the property of *availability* w.r.t. X if all members of X can access I .

Chapter 4 SECURITY POLICIES

- **A security policy considers all relevant aspects of**
 - Confidentiality
 - Integrity
 - Availability
- **With respect to *confidentiality*, it identifies those states in which information leaks to those not authorized to receive it.**
- **With respect to *integrity*, it identifies authorized ways in which information may be altered and entities authorized to alter it.**
- **With respect to *availability*, it describes what services must be provided.**
- **EXAMPLE: A university disallows cheating**
 - A CS class requires the students to do their homework on the department's computer.
 - One student notices that a second student has not protected her file, and copies it.
 - Who has breached security?
 - The second student has not, despite her failure to protect her homework.
 - The first student has breached security (the security policy disallows the copying of homework!).

Chapter 4 SECURITY POLICIES

- **A *security mechanism* is an entity or procedure that enforces some part of the security policy.**
- **EXAMPLE:** In the preceding example, the policy is the statement that no student may copy another student's work.
 - One mechanism is the *file access controls*.
 - If the second student had set permissions to prevent the first student from reading her file, the first student could not have copied the file.
- **EXAMPLE: The UNIX OS**
 - Initially developed for a small research group.
 - Had mechanisms sufficient to prevent users from accidentally damaging one another's files.
 - The implied security policy for this friendly environment was “*do not delete or corrupt another's files, and any file not protected may be read.*”
 - When the UNIX OS moved into academic institutions and commercial and government environments, the previous security policy became inadequate.
- **A *security model* is a model that represents a particular policy or a set of policies.**
 - A model abstracts details relevant for analysis.
 - An analysis rarely discusses particular policies; it usually focuses on specific characteristics of policies because many policies exhibit these characteristics.
 - The more policies with those characteristics, the more useful the analysis.
 - No single nontrivial analysis can cover all policies.
 - Restricting the class of security policies sufficiently allows meaningful analysis!

Chapter 4 SECURITY POLICIES

4.2 Types of Security Policies

- Each site has its own requirements for the levels of confidentiality, integrity, and availability.
- The site policy states these needs for that particular site.
- **A *military security policy* (a governmental security policy) is a security policy developed primarily to provide confidentiality.**
 - The name comes from the military's need to keep information secret.
 - Although integrity and availability are also important, organizations use this class of policies to overcome the loss of either (e. g., by not sending orders through a computer network).
- **A *commercial security policy* is a security policy developed primarily to provide integrity.**
 - The names comes from the need of commercial firms to prevent tampering with their data.
 - **EXAMPLE:** the confidentiality of a bank's computer is compromised.
 - A customer's account balance may be revealed.
 - This would embarrass the bank, and the customer may take her business elsewhere.
 - If the integrity of a computer is compromised, the balances in customers' accounts could be altered, resulting in financial loss!
- **A *confidentiality policy* is a security policy that deals only with confidentiality.**
- **A *integrity policy* is a security policy that deals only with integrity.**

Chapter 4 SECURITY POLICIES

4.3 The Role of Trust

- The role of trust is crucial to understanding the nature of computer security.
- Theories and mechanisms for analyzing and enhancing computer security rest on certain assumptions!
- A system administrator receives a *security patch* for her computer's OS.
 - She installs it, but has she improved the security of her system?
 - She is assuming that the patch came from the vendor and was not tampered with in transit.
 - She is assuming that the vendor tested the patch thoroughly.
 - Under considerable pressure, vendors usually issue patches quickly and test them only against a particular attack.
 - The vulnerability may be deeper, and other attacks may succeed.
 - She is assuming that the vendor's test environment corresponds to her environment.
 - A vendor's patch once reset ownerships of executables to the user *root*.
 - At some installations, maintenance procedures required that these executable be owned by the user *bin*.
 - The vendor's patch had to be undone, and fixed for the local configuration.
 - She is assuming that the patch is installed correctly.
 - Some patches are simple to install because they are simply executable files.
 - Others are complex, requiring the system administrator to do several things:
 - Reconfigure network-oriented properties
 - Add a user
 - Modify the contents of a registry
 - Give rights to some set of users
 - Finally reboot the system

Chapter 4 SECURITY POLICIES

- These assumptions are fairly high-level. Invalidating any of them makes the patch a potential security problem!
- Assumptions arise also at a much lower level.
 - Formal verification provides a formal mathematical proof that a given program P is correct.
 - Suppose a security-related program S has been formally verified for the OS O .
 - The formal verification is correct.
 - The assumptions made in the formal verification of S are correct.
 - S will be transformed into an executable whose actions correspond to those indicated by the source code.
 - The hardware will execute the program as intended.

4.4 Types of Access Control

- A security policy may use 2 types of access controls (alone or in combination).
- Consider an individual user is able to set an access control mechanism to allow or deny access to an object. That mechanism is called a *discretionary access control (DAC)* (or *identity-based access control (IBAC)*).
 - DACs base access rights on the identity of the subject and the identity of the object involved.
 - **EXAMPLE:** A child keeps a diary.
 - She can grant read access or deny read access.
 - The child allows her mother to read it, but no one else.
 - This is DAC because the access to the diary is based on the identity of the subject (mom) requesting read access to the object (the diary).

Chapter 4 SECURITY POLICIES

- Consider a system mechanism that controls access to an object, and an individual user cannot alter that access. That control is a *mandatory access control* (MAC) (or a rule-based access control).
 - The OS enforces mandatory access.
 - Neither the subject nor the owner of the object can determine whether access is granted.
 - **EXAMPLE:** The law allows a court to access driving records without the owner's permission.
 - This is mandatory control.
 - The owner of the record has no control over the court's accessing the information.
- Consider the creator of an object. An *originator controlled access control* (ORCON or ORGCON) bases access on the creator of the object.
 - The goal is to allow the originator of the file to control the dissemination of the information.
 - **EXAMPLE:**
 - Bit Twiddlers, Inc.: a company that manufactures embedded systems.
 - Microhackers Ltd.: a company that produces microcodes.
 - Bit Twiddlers gives Microhackers a copy of its specifications for the processor.
 - The contract requires Microhackers to obtain permission before it gives any information about the processor to its subcontractors.
 - This is an originator controlled access mechanism.

Chapter 4 SECURITY POLICIES

4.5 Academic Computer Security

- **The explicitness of a security policy depends on the environment in which it exists.**
 - A research lab may have an unwritten policy.
 - A bank needs a very explicit policy.
 - In practice, policies begin as generic statements of constraints of the members of the organization.
 - These statements are derived from an analysis of threats.
 - As questions (or incidents arise), the policy is refined to cover specifics.
- **EXAMPLE: An academic security policy**
 - **General University Policy**
 - This policy is an “Acceptable Use Policy” for the Davis campus of University of California.
 - Computing services vary from one campus to another, so the policy does not dictate how the specific resources can be used.
 - The policy
 - Provides access to resources and to allow the users to communicate with others throughout the world.
 - States the responsibilities associated with the privilege of using campus computers.
 - The enforcement mechanisms in this policy are procedural.
 - » Minor violations: the unit resolves the problem or gives formal warnings.
 - » More serious violations: the administration may take stronger actions (e.g., denying access to campus computer systems).
 - » Very serious violations: the university may invoke disciplinary action.

Chapter 4 SECURITY POLICIES

– Electronic Mail Policy

- The electronic mail policy describes the constraints imposed on access to, and use of, electronic mail.
- The electronic mail policy is consisted of 3 parts:
 - The first is a short summary intended for the general user community.
 - The second part is the full policy for all university campuses (written as precisely as possible).
 - The third describes how the Davis campus implements the general university electronic mail policy.