Lesson 3

Security policies and Bell-LaPadula

The tree is contained in the seed

Security policies and the Bell-LaPadula Model

Chapters 4 and 5

Overview

- A security policy defines what is secure
- A security mechanism implements a security policy
- There are two different types of security policies:
  - those dealing with *confidentiality*
  - those dealing with *integrity*
- However, real world security policies also have to deal with availability

Overview

- The Bell-LaPadula model is a confidentiality policy.
  - Subjects and objects are assigned security levels.
  - A security level includes
    - a security clearance (top secret, secret, etc.)
    - a category (e.g., EUR, NUC, GER) indicating need to know within the security clearance
- Security clearances are mandatory access controls.

Overview

- Bell-LaPadula also allows for discretionary access controls like we described in the previous lecture, but these are checked only after the security clearances are checked
  - A "lower" security level cannot read from a "higher" security level. (no read up)
  - A "higher" security level cannot write to a "lower" security level (no write down)

- Previously we informally described the three basic properties or components of security
- What are they?

Three Security Components

- Confidentiality
- Integrity
- Availability

- Now we want to define them formally

Formal Security Definitions

Definition 4-1 A *security policy* is a statement that partitions the states of the system into a set of *authorized*, or *secure*, states and a set of *unauthorized*, or *non-secure*, states.

Definition 4-2 A *secure system* is a system that starts in an authorized state and cannot enter an unauthorized state.

Definition 4-3 A *breach of security* occurs when a system enters an unauthorized state.

Definition 4-7 A *security mechanism* is an entity or procedure that enforces some part of the security policy.

Definition 4-8 A *security model* is a model that represents a particular policy or set of policies.

Main Point

1. A security policy defines what is secure. Where there is duality there is insecurity. True security is only possible in unity consciousness.

Policy vs. Mechanism

- Distinction between security policy and security mechanism is important
  - **Example:** Student A copies a file of student B because B did not read protect it. The security policy forbids copying so A has violated the policy. Had B used the mechanism of setting the file permission, then student A could not have copied. However, B is not in violation of the security policy.
  - **Example:** Security policy must specify procedures to handle backups of confidential data.

Confidentiality

Definition 4-4 Let X be a set of entities and let I be some information. Then I has the property of *confidentiality* with respect to X if no member of X can obtain information about I.

Integrity

Definition 4-5 Let X be a set of entities and let I be some information. Then I has the property of *integrity* with respect to X if all members of X trust I.

- If I is data, then trust means data integrity
- If I is the origin of something, then trust means origin integrity (or authentication)
- If I is a resource, then trust means assurance that the resource operates according to its specification

Availability

Definition 4-6 Let X be a set of entities and let I be a resource. Then I has the property of *availability* with respect to X if all members of X can access I.

- "access" is relative (1 hour delay okay for Amazon, not okay for medical data)

Types of Security Policies

- Military (or governmental) policies
- Commercial policies
- Confidentiality policies
- Integrity policies

Military Security Policies

Definition 4-9 A *military security policy* (also called a *governmental security policy*) is a security policy developed primarily to provide confidentiality.

- Integrity and availability are also important, but confidentiality is most important for the military/government.

Privacy

- Confidentiality is a major part of privacy, but privacy also restricts what information the government can ask of an individual.
- Privacy "denotes a zone of inaccessibility" of mind or body, the right to be left alone and to maintain individual autonomy, solitude, intimacy, and control over information about oneself.

Confidentiality

- Confidentiality "concerns the communication of private and personal information from one person to another."
- The key ingredients of confidentiality are trust and loyalty.
- Professionals rely on the promise of confidentiality to inspire trust in their clients and patients.
- In the case of lawyers, psychiatrists, and clergy, communications are legally designated "privileged."

Commercial Security

Definition 4-10 A *commercial security policy* is a security policy developed primarily to provide integrity.

- Example: Banks can't afford to have accounts altered incorrectly.

Commercial Security

- However, commercial organizations are also interested in confidentiality, e.g., they would like to control who looks at:
  - personnel data
  - marketing plans
  - formulas
  - manufacturing and development techniques

Definitions

Definition 4-11 A confidentiality policy is a security policy dealing only with confidentiality

Definition 4-12 An integrity policy is a security policy dealing only with integrity

Confidentiality vs. Integrity

- The role of trust highlights their difference
- Confidentiality policies: unrelated to trust in the content of objects, only care about disclosure
- Integrity policies: determine level of trust in objects or their content (more nebulous than confidentiality because harder to calibrate)

Example

- Transactions (as in database transactions) are important to many integrity policies.
- Note that trust plays a major role here, i.e., the concern here is about the accuracy of an object.
- This contrasts with a confidentiality policy whose focus is restricting access to an object; it "officially" doesn't care whether the object is accurate or not.

The Role of Trust

- The role of trust is crucial to understanding the nature of computer security.
- Any theory or mechanism rests on certain assumptions.
- The accuracy of those assumptions affects the trust we have in the system.

The Role of Trust

Example:

Assumptions in effect when applying a security patch (e.g. an update to Windows)

1. Patch originated from Microsoft and that it wasn't modified in transit.
2. Microsoft tested the patch thoroughly.
3. Microsoft's test environment corresponds to the environment in which the patch is being applied. (e.g., same previous patches are in effect)
4. Patch is installed correctly.

The Role of Trust

Example:

What assumptions are in effect for a formally verified program S?

1. The formal verification of S is correct.
2. The assumptions made in the formal verification of S are correct.
3. S is compiled correctly (compiler is correct)
4. Hardware that runs compiled version of S is functioning correctly.

Types of Access Control

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Originator controlled access control (ORCON or ORGCON)

Discretionary Access Control

Definition 4-13 If an individual user can set an access control mechanism to allow or deny access to an object, that mechanism is a *discretionary access control* (DAC), also called an identity-based access control (IBAC).

Example:

Access control in Windows is discretionary.

Mandatory Access Control

Definition 4-14 When a system mechanism controls access to an object and an individual user cannot alter that access, the control is a *mandatory access control* (MAC), occasionally called a rule-based access control.

Example: The military might use an OS that sets the access rights of a document based on the security clearance of the person who created the object. The person who created the document cannot change the access rights.

Example: The law allows a court to access driving records without the owner's permission.

Originator Controlled Access Control

Definition 4-15 An *originator controlled access control* (ORCON or ORGCON) bases access on the creator of the object (or the information it contains).

Example: Digital Rights Management

Example: Contractor signs a NDA (non-disclosure agreement) which requires him to get permission before giving certain information to somebody else.

Bell-LaPadula

Chapter 5

Example of a confidentiality policy

Goals of Confidentiality Policies

- A confidentiality policy, also called an information flow policy, prevents the unauthorized disclosure of information.
- It is not concerned with the integrity or availability of the information.

Military: Enemy must not know battle plans.

Government: The U.S. Privacy Act requires that certain personal data, e.g., income tax returns, be kept confidential.

The Bell-LaPadula Model

- Corresponds to military style classifications.
- It has influenced much of the development of computer security technologies.

Informal Description

- The simplest type of confidentiality classification is a set of security clearances arranged in a linear (total) ordering.

Total Ordering

Definition:

For all a, b and c in a set X (in this case the set of security clearances or classifications):

if a R b and b R a then a = b (antisymmetry)
if a R b and b R c then a R c (transitivity)
a R b or b R a (totality or completeness)

Example:

X=integers (or natural numbers)
R is the binary relation <=

The Bell-LaPadula Model

Let X = {top_secret, secret, confidential, unclassified}
Let R =
{
(unclassified, unclassified), (unclassified, top_secret),
(unclassified, secret), (unclassified, confidential),
(confidential, confidential), (confidential, top_secret),
(confidential, secret), (secret, secret),
(secret, top_secret), (top_secret, top_secret)
}

- Then R defines a total ordering on X
- Read a R b as a has a lower security clearance than b.

Easier way to specify a linear ordering

Suppose the relation is <=

Then R would be specified as

unclassified <= confidential <= secret <= top_secret

For integers it would be

… <= -1 <= 0 <= 1 <= …

- A linear ordering can be specified like this because of transitivity and every element is related to every other element (and to itself which is implicit)

The Bell-LaPadula Model

- A subject has a security clearance
- An object has a security classification
- The goal of the Bell-LaPadula model is to prevent read access to objects at a security classification higher than the subject's clearance
  - No read up
- For example, in the following policy model, Clarence cannot read Electronic Mail or Personnel files

Example

Clearance/ Classification	Subjects	Objects
TOP SECRET (TS)	Tamara, Thomas	Personnel Files
SECRET (S)	Sally, Samuel	Electronic Mail Files
CONFIDENTIAL (C)	Claire, Clarence	Activity Log Files
UNCLASSIFIED (UC)	Utaley, Thomas	Telephone List Files

Main Point

2. The Bell-LaPadula model is based on subject, objects and security classifications. Maharishi's Vedic Science is based on knower (Rishi), process of knowing (Devata) and the known (Chandas) and the wholeness from which they arise.

Adding Discretionary Access Controls to Bell-LaPadula

- The Bell-LaPadula security model combines mandatory and discretionary access controls.
  - The mandatory controls dominate
  - The discretionary controls in the access control matrix are applied only if the mandatory controls indicate that the subject can access the object

Simple Security Condition, Preliminary Version

Let L(S) = ls be the security clearance of subject S

Let L(O) = lo be the security classification of object O

S can read O if and only if

lo <= ls and S has discretionary read access to O

No Write Down (Star Property)

- However, we need to prevent copying a high security file into a lower security file.

*-Property (Star Property), Preliminary Version

S can write O if and only if

ls <= lo and S has discretionary write access to O

- This means that subjects with a UNCLASSIFIED clearance can write to a TOP SECRET file assuming they have write access to the file.

Results in a Secure System

Theorem 5-1 Basic Security Theorem (summarized). If a system starts out secure and each state transition respects the two above conditions, then the system is secure.

- The two conditions are “no read up” and “no write down”
  - as defined in the preliminary versions of the Simple Security Condition and Star Property

Adding Categories to Bell-LaPadula

- Add categories to each security clearance/classification.
- Each category describes a kind of information.
- Categories model "need to know".
- A subject can only read/write objects in categories associated with the subject.
- Each security clearance/classification and category form a security level.

Example

If Clarence is in (CONFIDENTIAL, {EUR, US}) then he can read CONFIDENTIAL documents about EUR (Europe) or US (U.S.).

See below for other documents that he has access to.

Definition 5-1 The security level (L, C) dominates the security level (L', C')
if and only if L' <= L and C' subset of C

Example,
If George is cleared into security level (SECRET, {NUC, EUR}) and
DocA is classified as (CONFIDENTIAL, {NUC}) and
DocB is classified as (SECRET, {EUR, US}) and
DocC is classified as (SECRET, {EUR})

then
George dom DocA
George !dom DocB (George doesn't have need to know about US information)
George dom DocC

Final Improved Version with Categories

Simple Security Condition
S can read O if and only if
S dom O and S has discretionary read access to O.

*-Property
S can write to O if and only if
O dom S and S has discretionary write access to O.

- If S is cleared into (UNCLASSIFIED, {}), then S can write to a (TOP_SECRET, {NUC}) file
  - (assuming that S has write access to that file)

Results in a Secure System

Theorem 5-2
Basic Security Theorem (summarized).
If a system starts out secure and each state transition respects the above two conditions, then the system is secure.

- The two conditions are the Simple Security Condition and the Star Property

Properties of a Bell-LaPadula Security System

- A subject S has a maximum security level and a current security level.
- The maximum security level must dominate the current security level.
- A subject S effectively decreases its security level from the maximum in order to communicate with subjects at lower security levels.

Summary

- Bell-LaPadula is an abstract model and can be adapted to various environments
- "read" conventionally means "allowing information to flow from the object being read to the subject reading".
  - Thus "read" usually includes "execute" because the subject could monitor the instructions in the object
- "write" conventionally means "allowing subject writing to the object written"
  - "write" normally includes "appends".

Main Point

3. In Bell-LaPadula there is no "write down" and no "read up". The teaching of a spiritual technique (a technique for developing the subject) requires great skill. There is a saying, "the wise should not delude the ignorant". This an example of "write down very carefully".

CONNECTING THE PARTS OF KNOWLEDGE WITH THE WHOLENESS OF KNOWLEDGE

1. Income tax returns are confidential.
2. Income tax returns have a security level.

3. Transcendental Consciousness is an integrated field of all the laws of nature.
4. Wholeness moving within itself: in Unity Consciousness duality is vanquished; one has total knowledge of the object, namely it is known to be a manifestation of one's own Self.