Name : Subhendu Maji
Reg. no: 18ETCS002121

course code : 19CSC315A
course : Information Security and Protection

CSE - C - section.

Date : 10-6-2021

TT - 2

1.

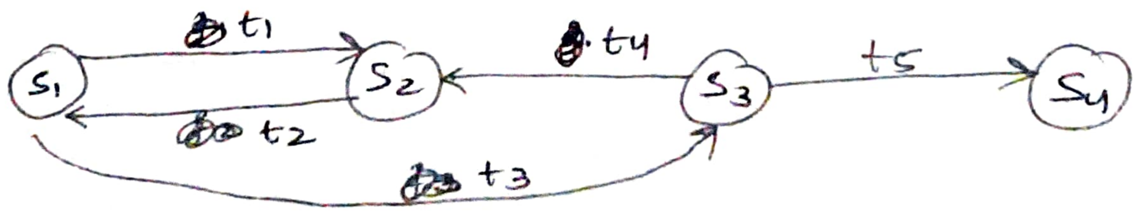
A security policy defines "secure" for a system or a set of systems. Security policies can be ~~informed or~~ informal or highly mathematical in nature.

consider a computer system to be a finite-state automation with a set of transition functions that change state. Then.

A security policy is a statement that partitions the states of the system into a set of authorized, or secure, states & a set of unauthorized, or non-secure states.

Security policy sets the context in which we can define a secure system. What is secure under one policy may not be secure under a different policy

Consider a finite-state machine ~~state~~ e.g. below.



A secure system is a system that starts in an authorized state & cannot enter an unauthorized state.

Name : Subhendu Maji   Reg. no. 18ETCS002121

(the finite state machine is in last page)
It consists of four states & five transitions. The security policy partitions the states into a set of authorized states. $A = \{s_1, s_2\}$ and a set of unauthorized state $A = \{S_3, S_4\}$.

This system is not seure, because regardlers of which authorized state it starts in, it can enter an unauthorized state.

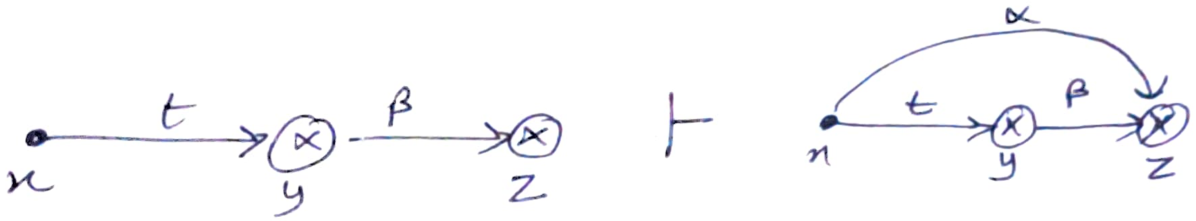
However if the edge from S_1 to S_3 were not ~~presence~~ present, the system would be secure, because it could not enter an unauthorized state ~~for~~ from an authorized state.

we know, A breach of security occurs when a system enters an unauthorized state.

5. Take-grant Protection model.

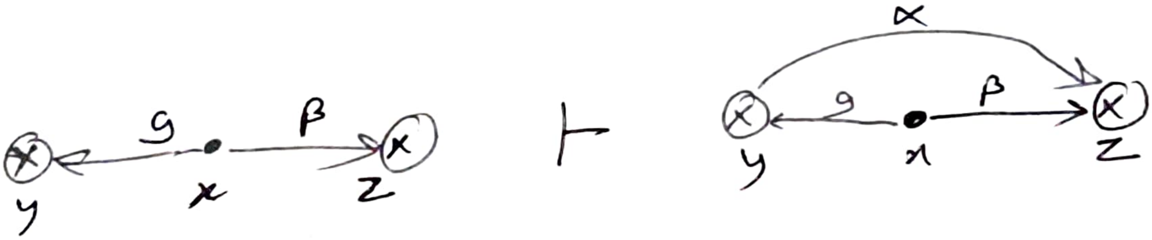
take: let x, y and z be three distinct vertices in a ~~protetection~~ protection graph G_0, and let x be a subject. Let there be an edge from x to y labelled γ with $t \in \gamma$, an edge from y to z labelled β, and $\alpha \subseteq \beta$.

Then the take rule defines a new graph G_1 by adding an edge to the protection graph from ~~[illegible]~~ x to z labelled α,



The rule is written "x takes (α to z) from y"

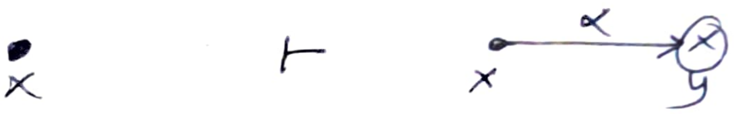
grant : let x, y, & z be three ~~prote~~ distinct vertices in a protection graph G_0, and let x ~~be~~ a Subject, let there be an edge from x to y labelled γ with $g \in \gamma$. an edge from x to z labelled β and $\alpha \subseteq \beta$. Then the ~~grant~~ ~~#~~ grant rule defines an new graph G_1 by adding ~~an~~ edge to the protection graph from y to z labelled α,



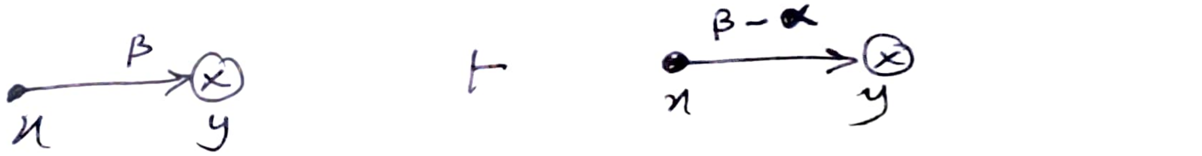
The rule is written "x grants (α to z) to y".

create : let x be any subject in a protection graph G_0 and let . create defines a new graph G_1 by adding a new vertex y to the graph by an edge from x to y labelled α.

The rule is written "x creates (α to new vertex) y".



remove : let x & y be any distinct vertices in a protection graph G, such that x is a subject. Let there be an explicit edge from x to y labelled β, and let. ~~That~~ Then remove defines a new graph G1 by deleting the α labels from β. If β becomes empty as a result, the edge itself is ~~dele~~ deleted.



4). Mendatory Access Control (MAC)

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), also known as rule-based access control.

- operating system enforces this.
- Neither the subject nor the owner of the object can determine whether access is ~~granted~~ granted.

E.g

The law allows a court to access driving records without any owner's permission. This is MAC, because owner of the record has no control over the court's access to the information.

Discretionary Access Control (DAC)

If an individual user can set an access control mechanism to allow or deny access to an object, that mechanism is a DAC, also known as indentity based access control.

DAC base base access rights on the identity of the subject & the identity of the object involved. Identity is the key.

E.g ~~Set~~ Suppose a child keeps a diary. The controls access to the diary because she can allow someone to read it (grat read access) or not allow someone to it (deny read access). The child allows her mother to ~~reed~~ read it, but no one else. This is DAC because access to the diary is based on the identity of the object (mom) requesting read access to the object (the ~~diary~~ diary).

Name : Subhendu Maji Reg : 18ETCS002121

Originator Controlled Access control (ORCON/ORGCON)

A originator controlled access controll bases access on the creator of an object (or the information it contains).

Eg.

let a company (ABC Ltd). is famous for ~~[illegible]~~ embedded systems, contract with (BCD Ltd), a company equally famous for microcoding abilities.

The ~~[illegible]~~ contract requires microhacker to develop a new microcode long. for a particular processor designed to be ~~[illegible]~~ used in embedded systems.

ABC gives microhacker a copy of its specification for processor. The ~~[illegible]~~ terms of what require microhackers ~~to~~ obtain permission before it gives any info about the processor to its subcontrators.

This is an ORCON, because even though BCD ~~[illegible]~~ own the files specification, they are not allow anoyone to anyone to acces info without ABC's permission.

2. a)

let a computer system allow the network administrator to read all network traffic. It disallow all other users from reading this traffic. The system is designed in such a way that the network administrator cannot communicate with other users. Thus there is no way for the right or of the network administrator over the network device to leak. This system is Safe.

Unfortunately, the OS has a flaw, If a user specifies a certain file name in a file deletion system call, that user can obtain access to any file on the system (bypassing all file system access ~~to~~ controls). This is an implementation flaw, not a theoretical one. It also allows the users to read data from the network

So, the system is not secure.

Subhendu Maji 18ETCS002121

2. b) (i) Mandatory access Control / Descretiroary acces Control.

The system contols access & an individual cannot change that..
If there is a owner of the 'military facility' and this person also had the ability to promote military people to 'general'. In this way the facility owner could grant access to their facility. If DAC, general is the identity & ~~the~~ the particular room is the object.

(ii) Originator Controlled access & discretionary access control policy
(ORCON) (DAC).

DAC because, the student ~~grat~~ grants the permission to the faculty to see the grades. If he doesn't grant permission to a particular faculty member, that faculty member can't see the grads.

ORCON because, the originator, which is the registrar, contols dissemination of data, but the student also had some control, and allows access to an individual record based upon the identity of the faculty member.

Name : Subhendu Maji Reg. no.: 18ETCS002121

3.

b) Military Security Policy

- The military security Policy is based on protecting classified information with respect to confidentiality.
- each piece of information is ranked at a particular sentivity Level :
  - unclassified
  - restricted
  - confidential
  - secret
  - Top secret
- each piece of information may be associated with one or more projects called compartments.
- A person has a clearance ~~level~~ to access information up to a certain level of ~~sent~~ sensitivity.
- the user may not alter classification, i.e the policy requires Mandatory Access Contol.

Commercial Security Policy

- Commercial security policies generally have a broader Scope than the military security policy.
- they are ~~norm~~ normally less formal. There is no ~~formalize~~ formalized notion of clearance & ~~to~~ consequently are the ~~rules~~ rules for ~~apt~~ allowing access less regularized
- the degree of sensitivity are normally (but variants exist).
  - public
  - propriedary
  - Internal

- They may ~~not~~ address issues such ~~incidents~~ as industrial espionage, conflicts of interest & rules for how activities must be performed within a company. Also they extend the scope to integrity & ~~availability~~ availability.

3 a) $x_1, x_2, x_3 \Rightarrow$ entities
$i_1, i_2, 3 \Rightarrow$ resources

Suppose x_1 is an entity (students) and is i_1 (teachers salary) is information 0/resource should not be able to access to anyone in the set other than x_2 (Accountant), This is called confidentiality

let x_1 be a person accessing a data analysis about some product 'z'. The data analysis is i_2. There is some one external (lets say x_2) who manipulates the record (i_2 is changed). This is breach of ~~integrity~~ integrity.

Suppose x_3 be the person who wants to access portal to view of question papers (i_3). The portal is as some error. ~~Though~~ though x_3 is a student is not able to open. This is breach of availability.

let x_1 be the student submitting his assignment i_1, the i_1 is being ~~accessed~~ accessed by x_2 & x_3. This is breach of confidentiality.