1)

בקרת גישה

Access Control

LECTURE 4

הרצאה מס' (4)

2)

Access Control

Protecting general objects, such as files, tables, access to hardwar devices or network connections and other resources.

In general, we want a flexible structure, so that certain users can u a resource in one way (e.g., read-only), others in a different way (e.g., allowing notification) and still others not at all.

3)

Access Control Paradigm

A subject is permitted to access an object in a particular mode, and onl such authorized accesses are allowed.

- *Subjects* are human users, often represented by surrogate programs running on behalf of the users.
- *Objects* are things on which an action can be performed: Files, tables, programs, memory objects data fields, network connections and processors.
- *Access modes* are many controllable actions of subjects on objects, including, but not limited to, read, write, modify, delete, execute and sc on.

4)

Access Policies

Access control is a mechanical process, easily implemented by a table and computer process: A given subject either can or cannot access a particular object in a specified way.

Before trying to implement access control, an organization needs t take the time to develop a higher-level security policy, which will then drive all the access control rules.

ہمارے ملک میں ہر سال 14 کروڑ ٹن گندم پیدا ہوتی ہے۔ اس میں سے 1.5 کروڑ ٹن گندم ضائع ہو جاتی ہے۔ اس کا مطلب ہے کہ ہر سال 1.5 کروڑ ٹن گندم ضائع ہو جاتی ہے۔ اس کا مطلب ہے کہ ہر سال 1.5 کروڑ ٹن گندم ضائع ہو جاتی ہے۔

4)

مثال کے طور پر:

ہر-ئی، کسی کے 2 بیٹے ہیں، اور 2 بیٹیاں ہیں۔ اس کا مطلب ہے کہ ہر-ئی کے 4 بچے ہیں۔

5)

مثال کے طور پر:

ہر-ئی، کسی کے 2 بیٹے ہیں، اور 2 بیٹیاں ہیں۔ اس کا مطلب ہے کہ ہر-ئی کے 4 بچے ہیں۔

3)

مثال کے طور پر:

ہر-ئی، کسی کے 2 بیٹے ہیں، اور 2 بیٹیاں ہیں۔ اس کا مطلب ہے کہ ہر-ئی کے 4 بچے ہیں۔

- ہر-ئی، کسی کے 2 بیٹے ہیں، اور 2 بیٹیاں ہیں۔ اس کا مطلب ہے کہ ہر-ئی کے 4 بچے ہیں۔
- ہر-ئی، کسی کے 2 بیٹے ہیں، اور 2 بیٹیاں ہیں۔ اس کا مطلب ہے کہ ہر-ئی کے 4 بچے ہیں۔

5)

Access Policies

- *Effective Policy Implementation:*
  - *Check every access.*
  - *Enforce least privilege*: access to the fewest resources necessary to complete some task.
  - *Verify acceptable usage*.
- Tracking
- Granularity
- Access Log
- Limited Privilege

6)

Implementing Access Control

Access control is often performed by the operating system.

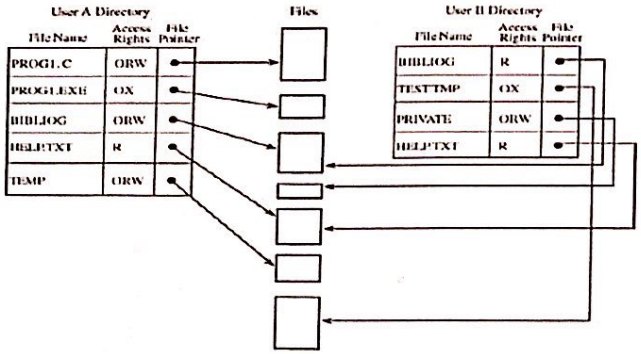
- Reference Monitor: access control that is always invoked, tamperproof, and verifiable.

- A reference monitor is a notion, not a tool you can buy to plug int a port. It could be embedded in a application (to control the application's objects), part of the operating system (for system-managed objects) or part of an appliance.

7)

מבנה לבקרת גישה

Access Control Directory

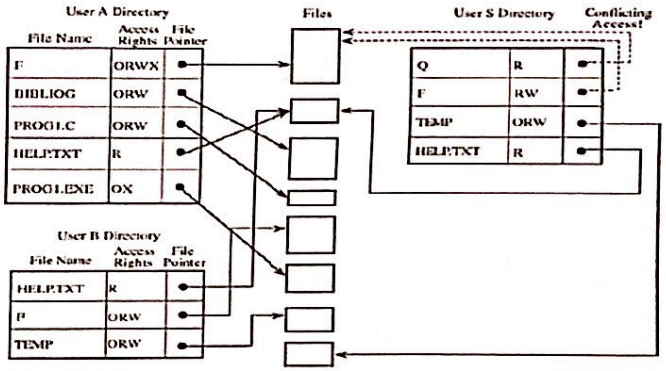


Directory Access Rights

8)

מבנה לבקרת גישה

Access Control Directory



Ambiguous Access Rights

ఆధునిక సమాజం

పారిశ్రామిక విప్లవం తర్వాత ఏర్పడిన ఆధునిక సమాజం, గతానికి భిన్నమైన కొన్ని ప్రత్యేక లక్షణాలను కలిగి ఉంటుంది.

- ఇది పట్టణ కేంద్రీకృత సమాజం. గ్రామాల నుండి పట్టణాలకు వలసలు పెరిగి, నగరాలు విస్తరించి, పట్టణ జనాభా పెరుగుతుంది.
- ఇది పారిశ్రామిక సమాజం. యంత్రాలు, కర్మాగారాలు, పెట్టుబడి, కార్మికులు ప్రధాన పాత్ర పోషిస్తారు.
- ఇది పారదర్శక సమాజం. సమాచార మార్పిడి, రవాణా సులభమవడం వల్ల సమాజం పారదర్శకంగా మారుతుంది.

(5)

సంక్షేమ రాజ్యం

- పౌరుల సంక్షేమం, భద్రత, అభివృద్ధి కోసం పనిచేసే రాజ్యం.
- విద్య, వైద్యం, పింఛన్లు, నిరుద్యోగ భృతి వంటి సేవలను అందిస్తుంది.
- పేదరిక నిర్మూలన, సామాజిక న్యాయం లక్ష్యంగా పనిచేస్తుంది.
- ఆర్థిక అసమానతలను తగ్గించి, సమతుల్య అభివృద్ధిని ప్రోత్సహిస్తుంది.

(5)

నగరీకరణ వల్ల సమస్యలు

- పట్టణ జనాభా పెరుగుదల.
- గృహ సమస్యలు.
- రవాణా సమస్యలు.
- మురికివాడల పెరుగుదల.

9) מטריצה לבקרת גישה

Access Control Matrix

objects

subjects

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Access Control Matrix

10) מטריצה לבקרת גישה

Access Control Matrix

	Bibliog	Temp	F	Help .txt	C_ Comp	Linker	Clock	Printer
USER A	ORW	ORW	ORW	R	X	X	R	W
USER B	R	—	—	R	X	X	R	W
USER S	RW	—	R	R	X	X	R	W
USER T	—	—	R	X	X	X	R	W
SYS MGR	—	—	—	RW	OX	OX	ORW	O
USER SVCS	—	—	—	O	X	X	R	W

Access Control Matrix

11) מטריצה לבקרת גישה

Access Control Matrix

Subject	Object	Right
USER A	Bibliog	ORW
USER B	Bibliog	R
USER S	Bibliog	RW
USER A	Temp	ORW
USER A	F	ORW
USER S	F	R
etc.		

List of Access Control Triples

12) איך לרשום הרשאות

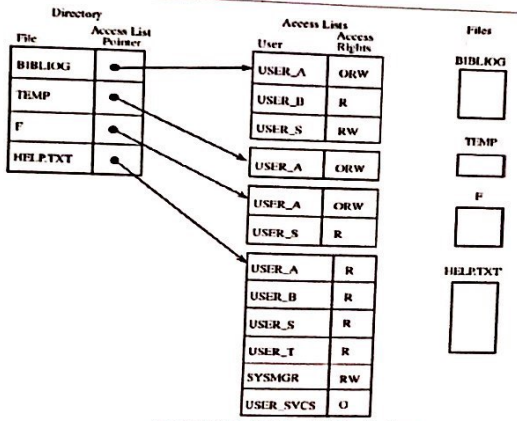
Access Control List

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Access Control List

13) גם לרשימת השליטה

Access Control List



Access Control List with Two Subjects

14) רשימת הרשאות

Privilege List

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Privilege Control List

15) יכולת

Capability

Capability: Single- or multi-use ticket to access an object or service

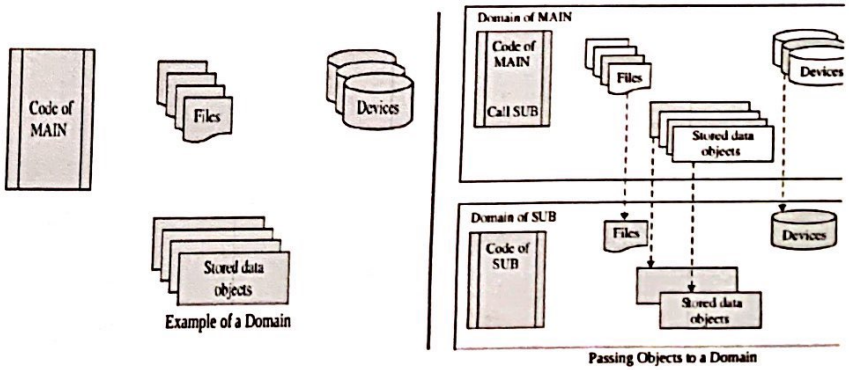
יכולת: כרטיס חד פעמי או רב שימוש לגישה לאובייקט או שירות

	File A	Printer	System Clock
User W	Read Write Own	Write	Read
Admin		Write Control	Control

Capability

16) יכולת

Capability



Example of a Domain

Passing Objects to a Domain