CSCE48503: Information Security

Week 3: Access Control

University of Arkansas

Jan 27, 2025

Schedule [Tentative]

Week 1: Intro, Syllabus, CIA (Expectations)	[13Jan2025]	
Week 2: Security Basics	[20Jan2025]	(MLK Holiday)
Week 3: Access Control	[27Jan2025]	
Week 4: Security Policies (Week 1)	[3Feb2025]	
Week 5: Security Policies (Week 2)	[10Feb2025]	(S4x25 Conf)
Week 6: Cryptography Basics (Week 1)	[17Feb2025]	
Week 7: Cryptography Basics (Week 2)	[24Feb2025]	
Week 8: Cryptography Basics (Week 3)	[3Mar2025]	
Week 9: Mid-Term Review and Test	[10Mar2025]	
Week 10: Operating Systems Security & Malware	[17Mar2025]	
Week 11: Spring Break! (Be Safe)	[24Mar2025]	(Spring Break)
Week 12: Network Security (Week 1)	[31Mar2025]	
Week 13: Network Security (Week 2)	[7Apr2025]	(IEEE DC)
Week 14: Web Security	[14Apr2025]	
Week 15: Advanced Topics	[21Apr2025]	
Week 16: FINAL Review	[28Apr2025]	
Week 17: FINAL Exam Respondus and in Classroom	[7May2025 @ 10:15am]	

Recap

- **What is Confidentiality? Integrity? Availability? Nonrepudiation?**
  - **Which security property (or combinations of them) is/are violated?**
    - **Alice and Bob are students. Alice copies Bob’s homework.**
  - **Give an example of a situation where a compromise of confidentiality leads to a compromise in integrity.**

- **Common threats**

Recap

- **Understand prevention, detection, recovery, and mitigation**
  - **Give examples of following situations:**
    - **Prevention is more important than detection and recovery**
- **Understand assumptions & trust**
  - **Know that all security policies and mechanisms rest on assumptions**
  - **Trust involves the degree to which we have confidence that people or systems are behaving in the way we expect**
- **Understand the tradeoff between security & performance**

Exams

Module 1 – Security basics

- What is confidentiality? What is integrity, including data integrity and origin integrity (i.e., authenticity)? What is availability? What is nonrepudiation?
- Understand common threats, including eavesdropping, masquerading, modification, and replay
- Understand prevention, detection, recovery, and mitigation
- Understand trust
- Know that security should be built into the design of a system, not added on to an already implemented/deployed system

Access control

- *Access control system determines what rights an* **entity has over a set of objects**
- **Questions answered include**
  - **Does Alice have the right to write /etc/passwd?**
  - **Do you have the right to view the CSCE website?**
  - **Does Dr. Farnell have the right to change your grades?**

www.qualityquotes.co.za

Terms

- *Access control system determines what rights an* **entity has over a set of objects**

- **Subjects: active entities that do things**
  - **E.g., Alice, you, a program**
- **Objects: passive things that things are done to**
  - **E.g., EECS website, grades, data files**
- **Rights: actions taken**
  - **E.g., read, write, execute, delete, create, search**

Access Control Policy

- **Access control** ***rule:***
  - *S: subjects*
  - *O: objects*
  - *R: rights*

P(S,O,R) -> { accept, deny }

- *Access control policy contains a lot of* **these rules**
- **Many ways to represent policy**

Access Control Matrix

- Rows are subjects; columns are objects
- One table for each access right

	O1	O2	O3
S1	Accept	Accept	Deny
S2	Deny	Accept	Deny
S3	Deny	Deny	Accept

matrix.wikia.com

Access Control Matrix

- Rows are subjects; columns are objects
- One table for all access rights

	O1	O2	O3
S1	RWX	-	R
S2	R	W	RW
S3	-	-	-

matrix.wikia.com

- Advantages: fast access
- Disadvantages: large size=#subjects * #objects

Exercise

- Users: Alice and Bob; Files: X.txt and Y.exe
- Alice owns X.txt and can read and write it, Bob can read but not write it.
- Bob owns Y.exe and can read, write, and execute it, and Alice can read and execute it, but not write it.
- Generate the access control matrix

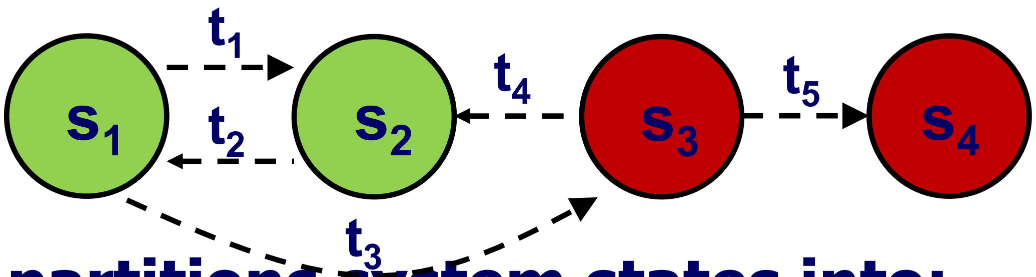
Exercise

- Users: Alice and Bob; Files: X.txt and Y.exe
- Alice owns X.txt and can read and write it, Bob can read but not write it.
- Bob owns Y.exe and can read, write, and execute it, and Alice can read and execute it, but not write it.
- Generate the access control matrix

	X.txt	Y.exe
Alice		
Bob		

Security Policy

- Computer system: a finite-state automaton with a set of transition functions

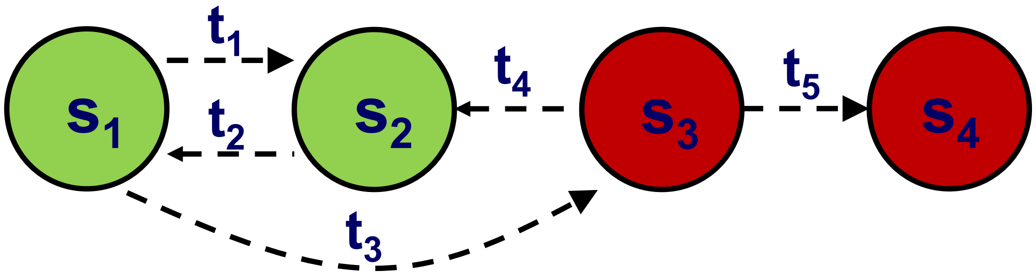


- Policy partitions system states into:
  - Authorized (secure)
    - These are states the system can enter
  - Unauthorized (nonsecure)
    - If the system enters any of these states, it's a security violation

Security Policy

❖ Secure system

- Starts in authorized state
- Never enters unauthorized state



s_1, s_2: authorized

Secure?

No, regardless of which authorized state it starts in, it can enter an unauthorized state

Secure when edge from s_1 to s_3 not present

Types of Security Policies

- **Military (governmental) security policy**
  - **Policy primarily protecting confidentiality**
- **Commercial security policy**
  - **Policy primarily protecting integrity**
- **Confidentiality policy**
  - **Policy protecting only confidentiality**
- **Integrity policy**
  - **Policy protecting only integrity**

Both confidentiality & military policies protect confidentiality
But, a confidentiality policy does NOT deal with integrity at all, while a military policy may

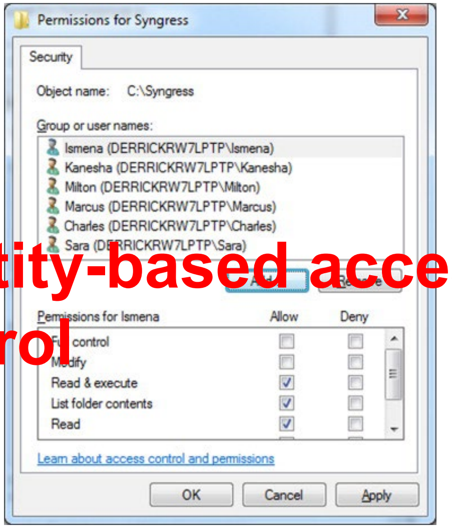
Types of Access Control

❖ Discretionary Access Control (DAC)

- individual user sets access control mechanism to allow or deny access to an object

□ Mandatory Access Control (MAC)

- system mechanism controls access to object, and individual cannot alter that access
- E.g., The law allows a court to access driving records without the owners' permission.
  - A mandatory control: the owner of the record has no control over the court's accessing the information.



Permissions for Syngress

Security

Object name: C:\Syngress

Group or user names:

Ismena (DERRICKRW7LPTP\Ismena)
Kanesha (DERRICKRW7LPTP\Kanesha)
Milton (DERRICKRW7LPTP\Milton)
Marcus (DERRICKRW7LPTP\Marcus)
Charles (DERRICKRW7LPTP\Charles)
Sara (DERRICKRW7LPTP\Sara)

Permissions for Ismena	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

identity-based access control

rule-based access control

DAC vs MAC

Discretionary Access Control

- Access policy defined by users
- Users can pass rights to other subjects and programs

Mandatory Access Control

- Access policy defined by system
- Subjects and their programs can't pass rights

What does it mean for Trojan horse?

en.wikipedia.org

Trojan Horse

- Rogue software. It contains a hidden code that performs illegitimate functions not known to the caller

Viruses and logic bombs are usually transmitted in the form of Trojan horse

en.wikipedia.org

DAC vs MAC

- **Discretionary Access Control**
  - **Access policy defined by users**
  - **Users can pass rights to other subjects and programs**
- **Mandatory Access Control**
  - **Access policy defined by system**
  - **Subjects and their programs can't pass rights**

What does it mean for Trojan horse?

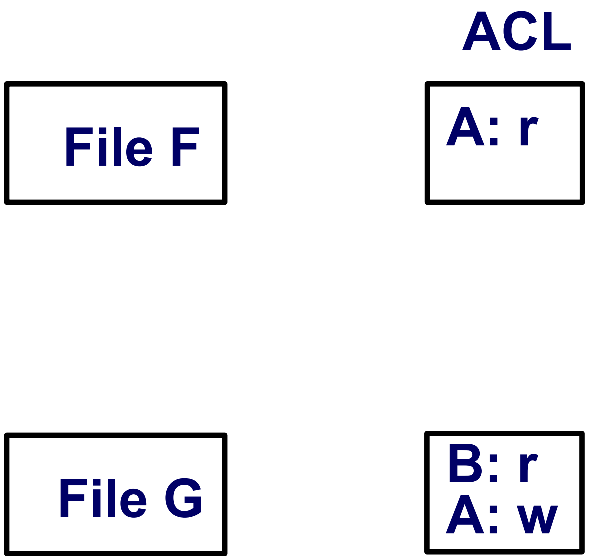
DAC is vulnerable from Trojan horses exploiting access privileges of calling subject

en.wikipedia.org

DAC vs MAC: Trojan Horse

❖ Trojan Horse Vulnerability of DAC

User B cannot read file F



ACL

File F

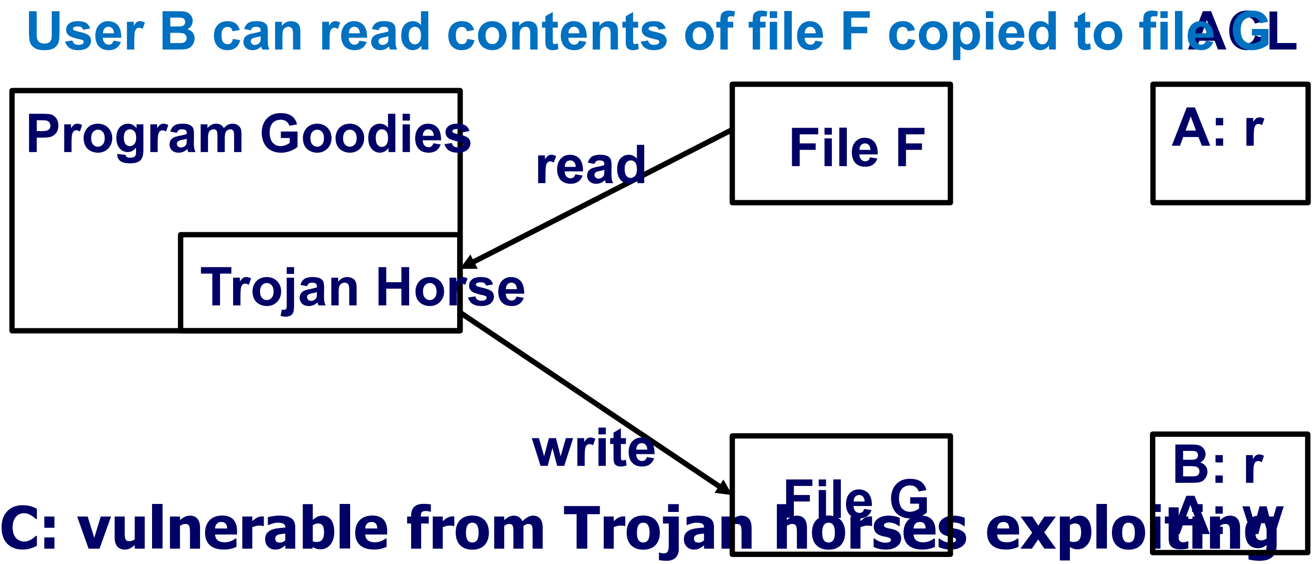
A: r

File G

B: r
A: w

DAC vs MAC: Trojan Horse

- Trojan Horse Vulnerability of DAC



User B can read contents of file F copied to file G

ACL

Program Goodies

Trojan Horse

read

File F

A: r

write

File G

B: r
A: w

- DAC: vulnerable from Trojan horses exploiting access privileges of calling subject
- MAC: impose restrictions on subjects which cannot be bypassed by Trojan Horses

Reading

- Chapter 1.2.1, 9.1.1, 9.1.2