Access Control

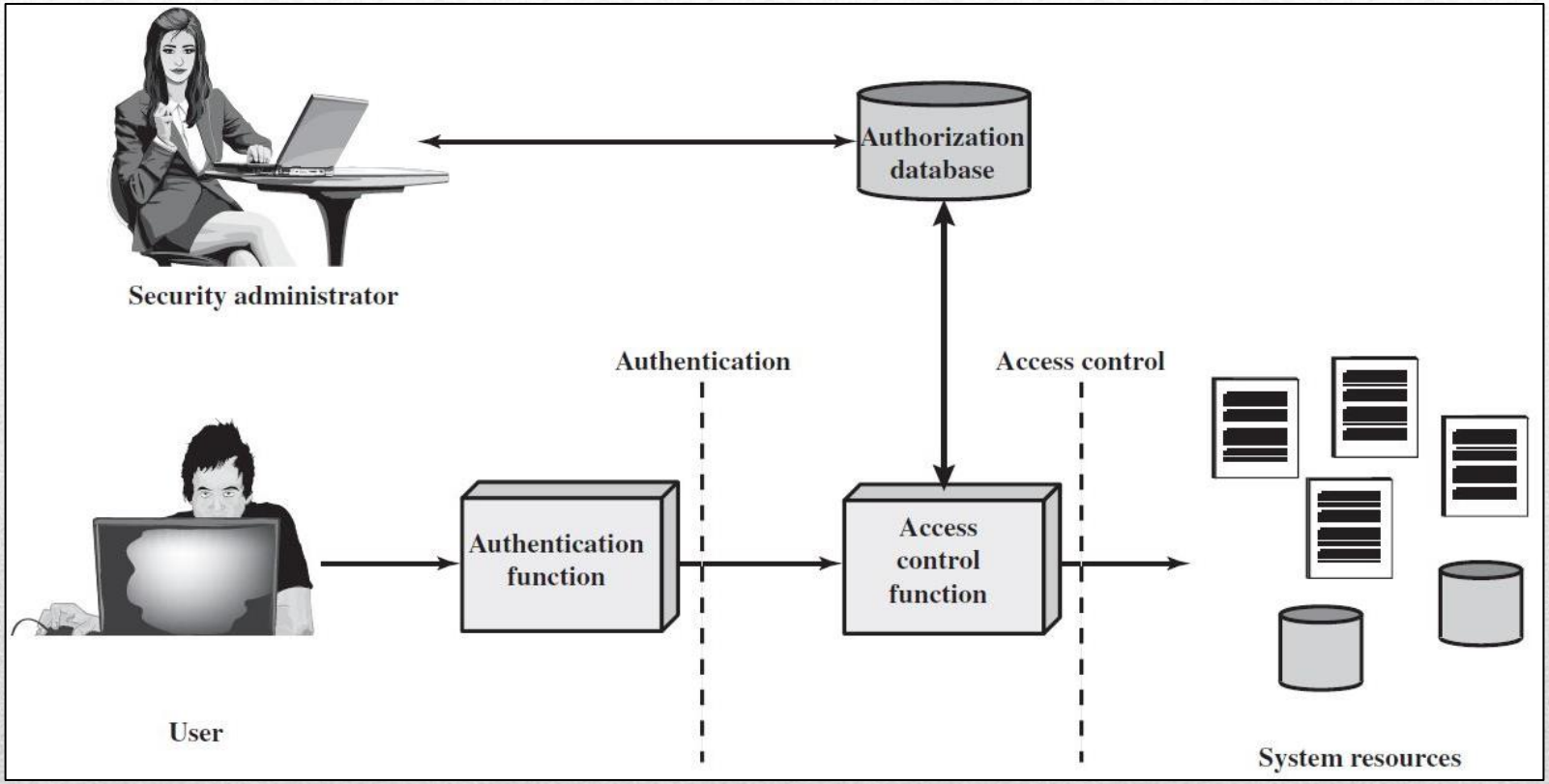
"Security Engineering" by Ross Anderson, Chapter 4

Instructor: Prof. Orr Dunkelman

Presenter: Mr. Alon Dankner

Access Control

- Access control implements a security policy that specifies who or what may have access to each system resource and which type of access that is permitted.
- The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.



Relationship among Access Control and Other Security Functions

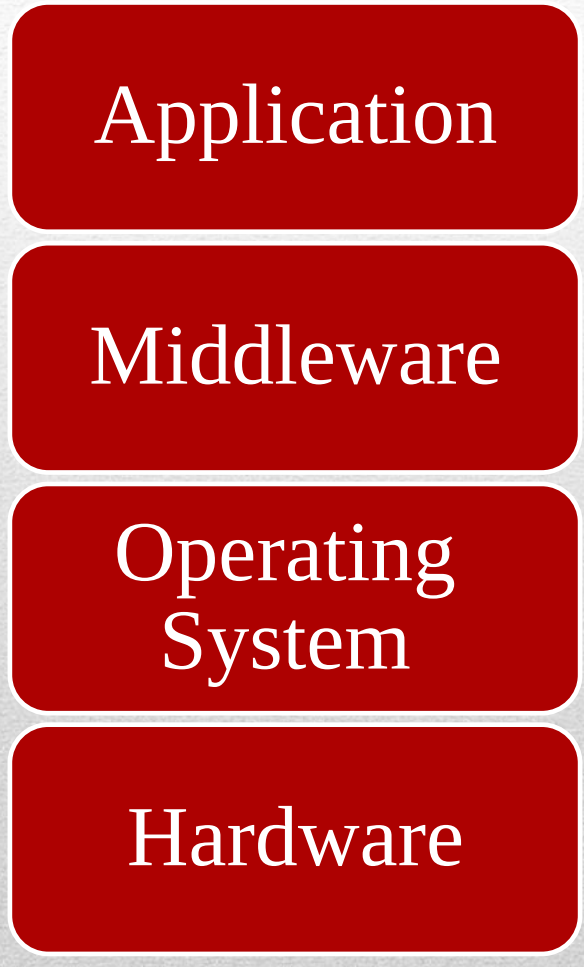
Requirements

- ✓ Reliable input
- ✓ Support for fine and coarse specifications
- ✓ Least privilege
- ✓ Policy combinations and conflict resolution
- ✓ Administrative policies

Main Problems

- **The protection problem** preventing one process from interfering with another.
- **The confinement problem** preventing programs communicating outward other than through authorized channels.

Access Control



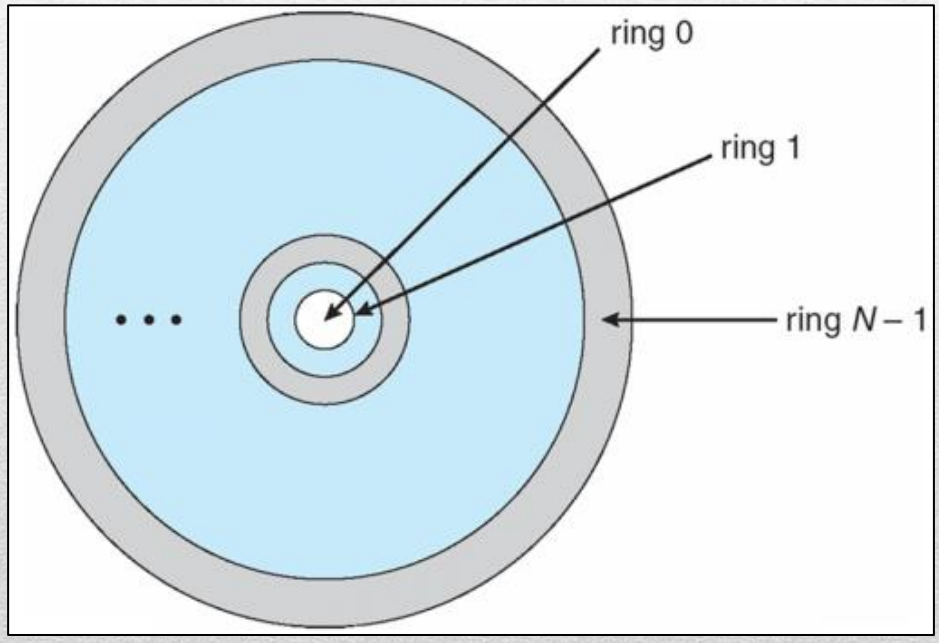
Access Control

- Application
- Middleware
- Operating System
- Hardware

- Features provided by the processor or by associated memory management hardware.

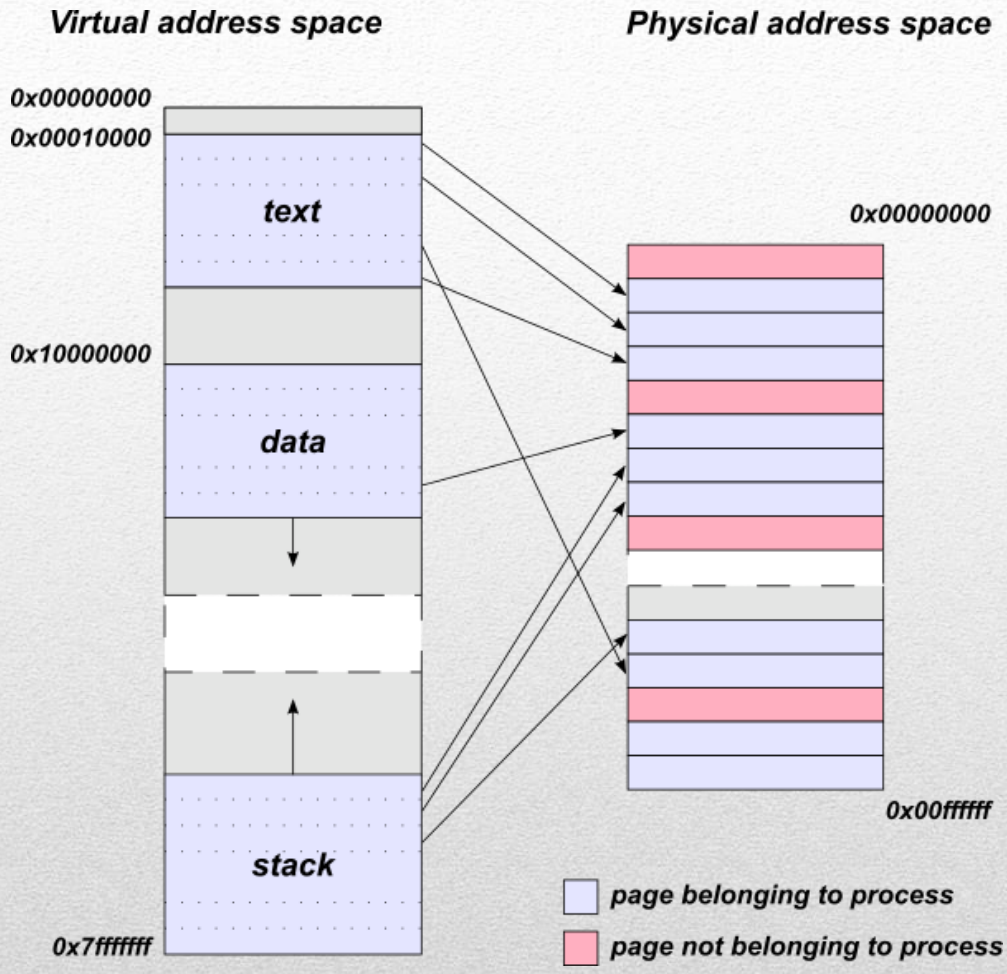
Rings of Protection

- Let D_i, D_j be two domain rings, than $j < i \Rightarrow D_i \subseteq D_j$.



Virtual Memory

- Separation of user logical memory from physical memory.
- Logical address space can therefore be much larger than physical address space.
- A page table maps virtual memory to physical memory.
- Implemented by demand paging.



Virtual Address Space and Physical Address Space Relationship

Virtual Memory

- Each page can reside in any location of the computer's physical memory.
- The page table is usually invisible to the process.
- Unallocated pages, and pages allocated to any other application, do not have any addresses from the application point of view.

Access Control

- Application
- Middleware
- Operating System
- Hardware

- Provides resources such as files and communications ports.

Access Control Matrix

- Security policy can be abstracted as a set of objects O that needs to be protected, a set of subjects S consists of all active entities and a set of rights R of the form $r(s, o)$, where $s \in S, o \in O$ and $r(s, o) \subseteq R$.

Bookkeeping Example

- You have been chosen to implement a security policy through an access control matrix, the security policy is as follows:
  - Sam, the security administrator, has universal access to all the resources.
  - Sam is not allowed to change the Accounting Data.
  - Alice, the manager, can use all of the system's resources to read and write the data.
  - Bob, the accountant, has the same privileges as Alice but can not access Insurance Data and Payroll Data.
  - Alice and Bob are allowed access to Accounting Data only through the Accounting Program, which is authorized software.

Bookkeeping Example

	Operating System	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Bob	rx	rx	rw	-	-
Alice	rx	rx	rw	rw	rw
Sam	rwx	rwx	r	rw	rw

- Sam is the security administrator
- Alice is the manager
- Bob is an accountant

Is it good enough?

Bookkeeping Example

	Operating System	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Bob	rx	rx	r	-	-
Alice	rx	rx	r	rw	rw
Sam	rwx	rwx	r	rw	rw
Accounting Program	rx	rx	rw	-	-

- Sam is the security administrator
- Alice is the manager
- Bob is an accountant

Is it good enough?

Access Control List

	Insurance Data
Bob	-
Alice	rw
Sam	rw
Accounting Program	-

- The ACL corresponding to Insurance Data.
- Split the matrix by columns and store with the object.

Capabilities

	Operating System	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Alice	rx	rx	r	rw	rw

- The C-lists corresponding to Alice.
- Split the matrix by rows and store with the subject.

ACLs vs. C-Lists

	Access Control List	Capabilities
• Runtime security checking • Delegation of rights • Revoking access	Not Efficient	Efficient
• Changing an object's status	Efficient	Not Efficient

Virtualization

- Creating a virtual (rather than actual) machine that acts like a real computer with an operating system.
- Software executed on the VM is separated from the underlying hardware resources.
- Remember VMware?

Trusted Computing

- With TC, the computer will consistently behave in expected ways, and those behaviors will be enforced by computer hardware and software.
- TC is controversial as the hardware is not only secured for its owner, but also secured against its owner.

Access Control

- Application
- Middleware
- Operating System
- Hardware

- Database or bookkeeping package, enforces protection properties.

Database Access Controls

- A database is an organized collection of data. It is the collection of schemas, tables, queries, reports, views, and other objects.
- Organizational databases concentrate sensitive information in a single logical system.

The Slammer Worm

- Exploited a buffer overflow bug in Microsoft's SQL Server and Desktop Engine database products.
- Generates random IP addresses and sends itself out to those addresses.
- A patch had been available from Microsoft for six months prior to the worm's launch.

Access Control

- Application
- Middleware
- Operating System
- Hardware

- Computer program designed for a modern online business.

Sandboxing

- Java virtual machines include a sandbox to restrict the actions of untrusted code, such as a Java applet.
- Restricted environment which has no access to the local hard disk (or at most temporary access to a restricted directory), and is only allowed to communicate with the host it came from.

Proof-Carrying Code

- Formal proof accompanies the application's executable code.
- The host can quickly verify the validity of the proof and determine whether the application match the security policy.

Some Technical Attacks

- Smashing the Stack
- Format String Attack
- SQL Injection
- Integer Manipulation Attack
- SYN Flood
- Race Condition Attack

Any Questions?

It is easier to exclude harmful passions than to rule them, and to deny them admittance than to control them after they have been admitted.

— Seneca

Thank You For Listening ☺

Bibliography: “Security Engineering” by Ross Anderson, “Computer Security: Principles and Practice” by William Stallings and Lawrie Brown, “Information Security: Principles and Practice” by Mark Stamp, “Operating System Concepts” by Avi Silberschatz, Peter Baer Galvin and Greg Gagne, Syracuse University, Wikipedia, OWASP