Computer Security
Lecture 3

Authentication and Access Control

Erland Jonsson
Department of Computer Science and Engineering
Chalmers University of Technology
Sweden

User authentication

Authentication – definition

- Authentication is *verifying a user's identity*
- cp: message authentication: is check of message authenticity (Sw. äkthet) and source
- In an OS each account has one **identifier** (e.g. username) and one **authenticator** (e.g. password)
- The identifier tells *who you are*.
- The authenticator *verifies that this is true, i.e. it provides a* secure coupling between the user and his account

User Authentication

- fundamental security building block
  - basis of access control & user accountability
- is the process of verifying an identity claimed by or for a system entity
- has two steps:
  - identification - specify identifier
  - verification - bind entity (person) and identifier
- distinct from message authentication

Authentication procedure

The ***authentication procedure*** consists of 4 stages:

1) **identification** of the user *(who is it?)*
2) provision of some kind of **authentication information,** which is secret and unforgeable.
3) **transmission of the authentication information** to the system through a secure channel.
4) **validation** of the authentication information wrt some reference information (proof of correctness)

Problems (errors, attacks) can occur in all those 4 stages

Authentication information

The authentication information can be of ***3 different, generic types,*** based on something that is unique for the user:

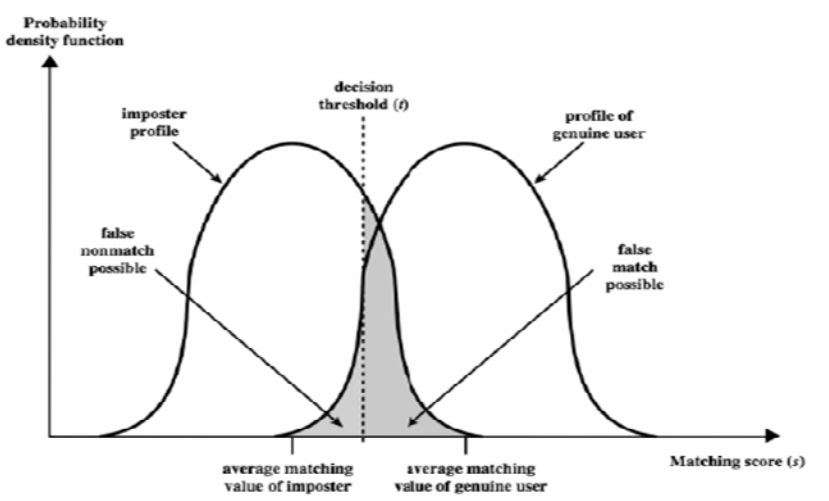
- something you **KNOW** (e.g password, PIN code)
- something you **HAVE** (e.g smartcard)
- something you **ARE (DO)** (e.g fingerprint), (biometrical methods, something characteristic about you)

(**WHERE** you are can also be used in some situations)

In general, something that you *have is called a* ***token***. i.e. something that is used for authentication

A **capability** is an **unforgeable token** that gives the possessor certain *rights* (to an object) - **authorization**

Biometric accuracy – threshold selection



The transmission channel

- The transmission channel is **often the weakest link**, especially when long distances are involved
- The transmission channel may be very short and still be vulnerable
- The "usual" transmission threats and problems apply, such as:

  - eavesdropping
  - manipuation of routers, gateways
  - replay attacks

- Consequently, the "usual" remedies also apply

Validation of authentication

- The system must have some kind of reference information in order to validate the authentication information
- An attack can be launched against the reference info, e.g.:
  - read stored password
  - change the reference info
- Protection of password reference info:
  a) store in a file with strong and limited Access Control
  b) encryption
  c) (a + b)
- Pros and Cons:
  a) - cleartext storage and comparison is in cleartext
  - back-up tapes, memory dumps reveals password
  b) + could be stored in readable files (?)
  - open for brute force attacks

Access Control

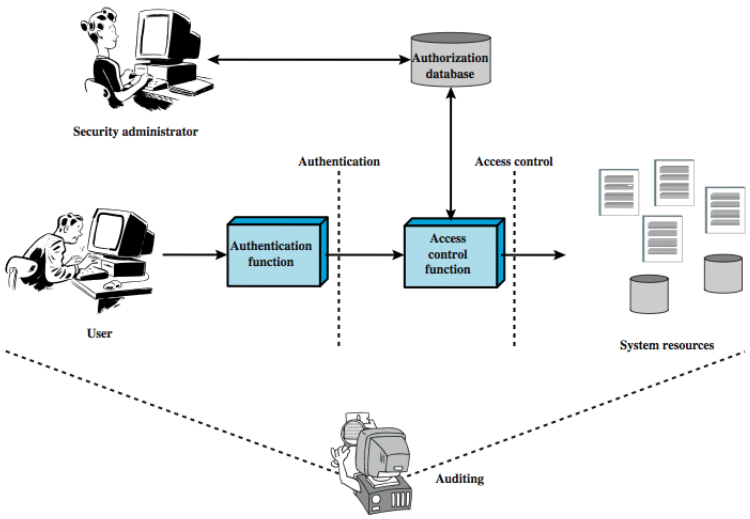
Access Control

- Definition of Access Control:
  The prevention of unauthorized use of a resource (including the prevention of use of a resource in an unauthorized manner)
- central element of computer security
  - used for boundary protection
- access control permits users and groups
  - to authenticate to system
  - to be assigned access rights to certain resources in the system i.e. authorized

Access Control Elements

- subject - entity that can access objects
  - a process representing user/application
  - often have 3 classes: owner, group, world
- object - access controlled resource
  - e.g. files, directories, records, programs etc
  - number/type depend on environment
- access right - way in which subject accesses an object
  - e.g. read, write, execute, delete, create, search

Access Control Usage



Access Control

- provided using an access control matrix
  - lists of subjects in one dimension (rows)
  - lists of objects in the other dimension (columns)
  - each entry specifies access rights of the specified subject to that object
- access control matrix is often sparse
- can decompose by either row, leading to an access control list (ACL) or column, leading to capability tickets

Access Control Matrix

		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_1	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* - copy flag set

Access Control 2

- The access control list provides a list of subjects, who can access a single object (one list "per file" or object)[1]
- The capability ticket approach presents a list of objects accessible by a single subject (one list "per user" or subject)[1]
- A capability ticket is an unforgeable token that gives the possessor certain rights to an object, i.e. it specifies the authorization for a particular user

1. See book fig. 4.3

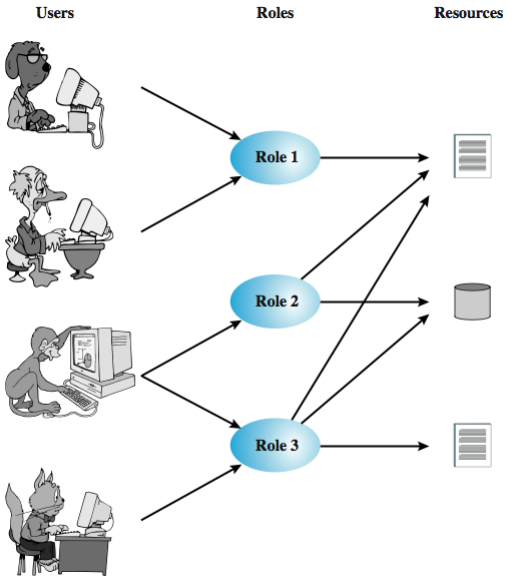
Mandatory and Discretionary Access Control

- **MANDATORY ACCESS CONTROL (MAC)** means that some central authority (e.g. the security officer) determines what information is accessible to whom
- **DISCRETIONARY ACCESS CONTROL (DAC)** means that the owner of the file (i.e. the user) determines what information is accessible to whom
- MAC and DAC can both be applied at the same time
- MAC is most commonly used in the multi-level security mechanism (MLS) in the Military Security Policy
- DAC is used in many operating systems, e.g. UNIX.

Role-Based Access Control

- In **ROLE-BASED ACCESS CONTROL (RBAC)** the rights are assigned to roles rather than to the users.
  For example in a hospital: surgeon, medical practitioner, nurse, janitor, etc
- RBAC employs MAC and has been developed to meet the needs from commercial and societal systems.
- Procedure:
  identification - authentication - selection of role - access to information (according to role).
- Advantages:
  - easy to enforce enterprise-specific security policies
  - security management is simplified
- Other policies exist, e.g Team-Based Access Control, etc

Role-Based Access Control



Role-Based Access Control

User to Role:

	R_1	R_2	...	R_n
U_1	X			
U_2	X			
U_3		X		X
U_4				X
U_5				X
U_6				X
...				
U_m	X			

Role to Access Right:

ROLES \ OBJECTS	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
...									
R_n			control		write	stop			