Terminology and Models

csci 7000-001 fall'01

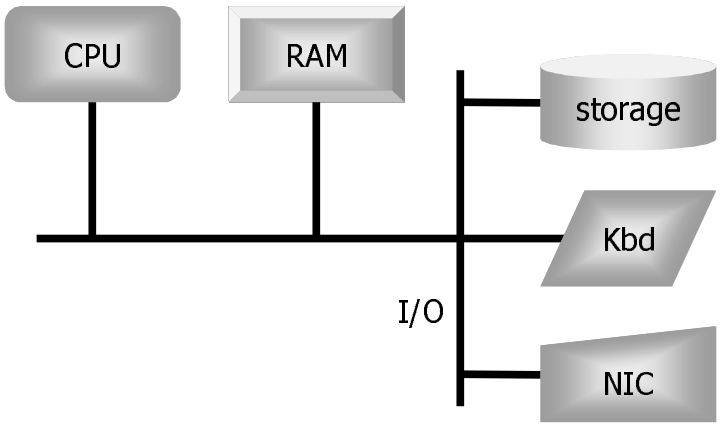
Antonio Carzaniga

Outline

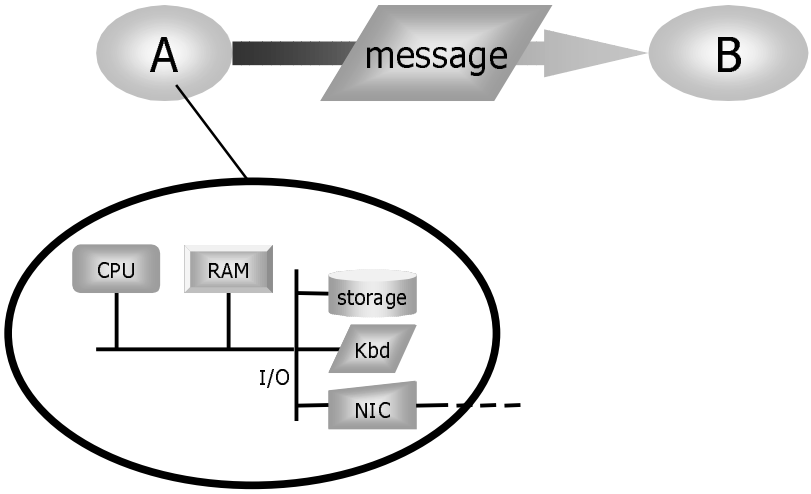
- What is computer security about?
- Terminology
- Models

What's Security?

Computer System



Distributed System



Valuable Assets

- Software
- Data
- Messages
- Computation Resources
- Communication Resources

Valuable Assets: System

- Dynamic resources
  - memory (data and software)
  - CPU
  - OS services (e.g., network ports, processes)
- Static resources
  - disk space
  - installed software
  - data files

Valuable Assets: Communication

- Communication infrastructure
  - channels
  - routing infrastructure
- Data
  - messages in transit

What's Computer Security About?

- Protecting valuable assets, and...
- Attacking valuable assets

How To Study e-Security

...like any other engineering discipline!

- Models
- Techniques
  - offense techniques (attacks)
  - defense techniques (protections)
- Tools

How To Implement e-Security

...like any other engineering discipline!

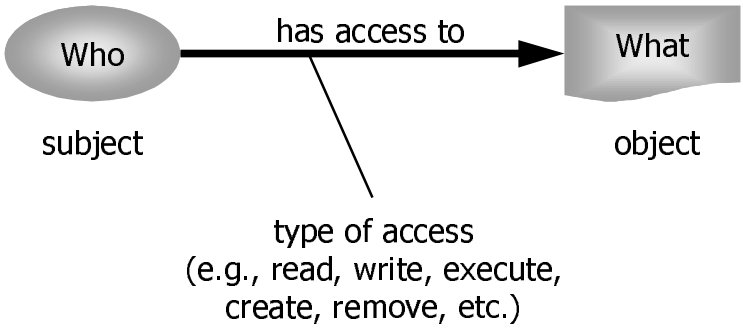
- Prevention
- Detection
- Reaction
- Analysis

B. Schneier, "Secrets & Lies—Digital Security in a Networked World," Wiley, 2000, ISBN 0-471-25311-1

What is Security, Really?

Security = Enforcing a Policy

- Policy = *access control model*



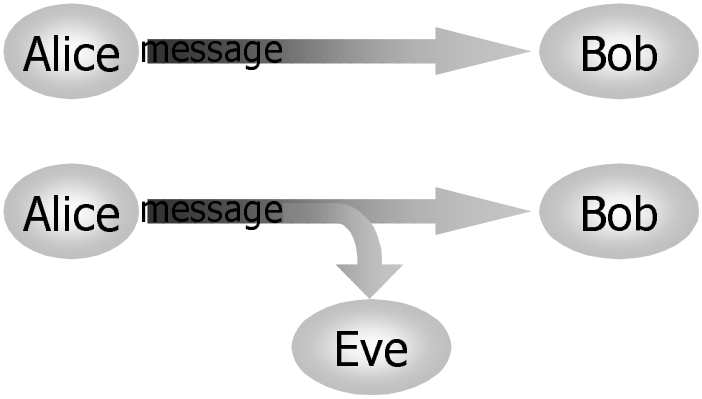
Primary Goals

- Confidentiality
  - enforcing *read* access policy
  - *A* reads object *X* $\Rightarrow$ *A* has read-access to *X*
- Integrity
  - enforcing *write* access policy
  - *A* writes object *X* $\Rightarrow$ *A* has write-access to *X*
- Availability
  - "guaranteeing access to legitimate users"

Goals vs. Threats

- Goal: to realize a policy
- Threat: to break a policy
- Unless you are an attacker...
  - threats become goals
  - and vice-versa

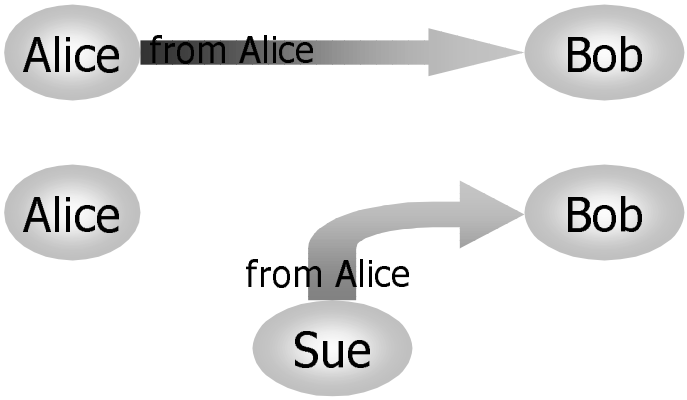
Confidentiality / Eavesdropping



Threat: *Eavesdropping*

Goal: *Confidentiality*

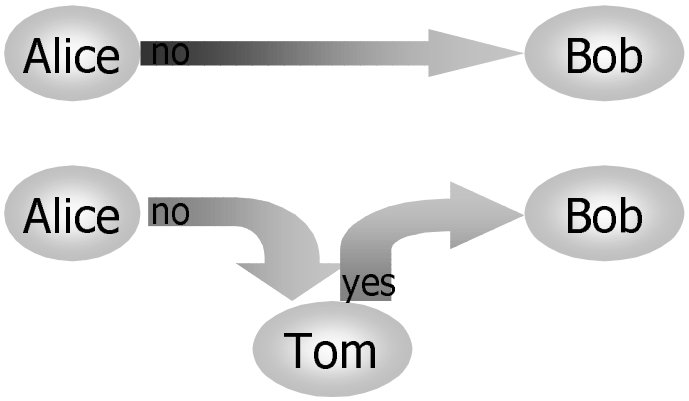
Authenticity / Spoofing



Threat: *Spoofing*

Goal: *Authentication (Integrity)*

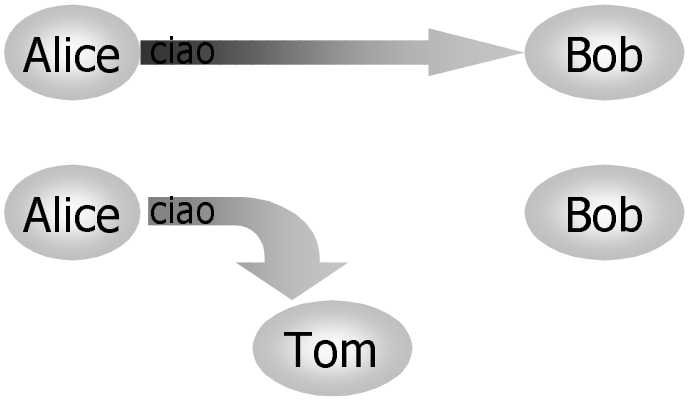
Integrity / Tampering



Threat: *Tampering*

Goal: *Integrity*

Availability / Blocking, DoS



Threat: *Blocking, DoS*

Goal: *Availability*

Threats to Software

- Deletion
- Modification
  - viruses, trojan horses, logic bombs, trapdoors, information leaks
- Theft
  - unauthorized copy

Threats to Data and Messages

- Deletion
- Modification
  - content
  - meta-data (access lists, timestamps, etc.)
- Access
  - reading
  - testing existence
- Forgery

Threats to Computation

- Performance degradation
- Interruption

Threats to Communication

- Performance degradation
- Interruption

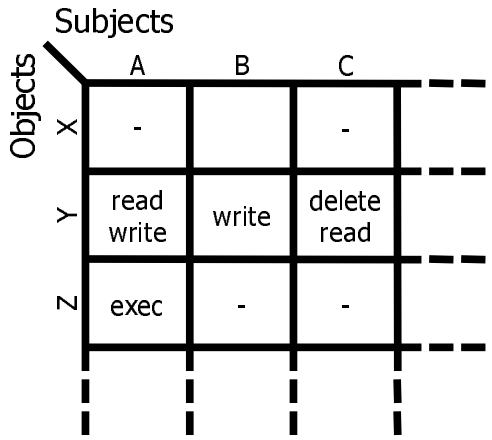
Controls vs. Weaknesses

- Defense methods: *controls*
  - facilitates or realizes a goal
  - or opposes a threat
- Attack methods: *weaknesses*, *vulnerabilities*
  - facilitates or realizes a threat
  - or...

Access Control Models

Access Control

- A number of relations, e.g.:
  - *read-access* $\subseteq$ *Subject* $\times$ *Object*
  - ...



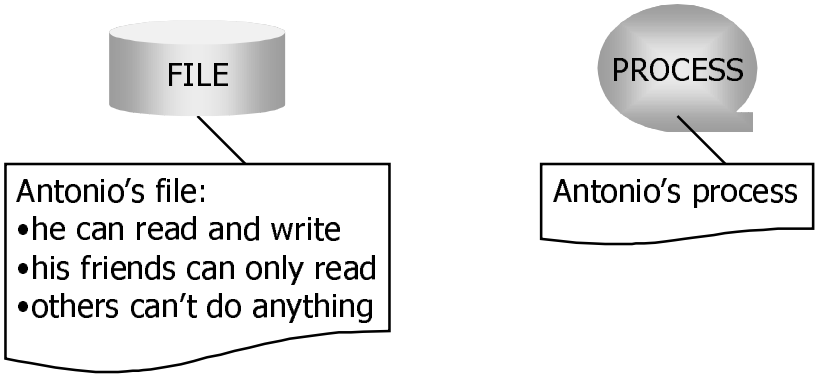
Access Control Models

- User/profile model
- Access control lists
- Multi-level security

User/Profile Model

access=0640 (-rw-r-----)
uid=19629 (carzanig)
gid=204 (serl)

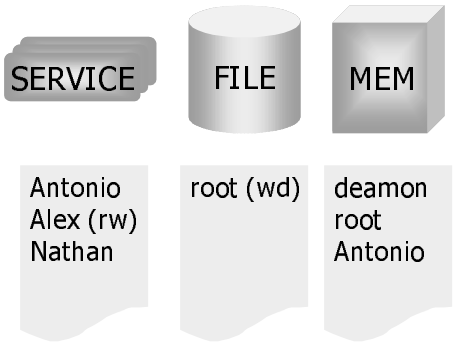
uid=19629(carzanig)
gid=204(serl)
groups=204(serl),24(visitor)



Examples

- UNIX
  - read
  - write
  - execute
  - (delete/create)
- Windows NT
  - read
  - write
  - execute
  - delete
  - create
  - change permissions
  - change ownership

Access Control Lists



- Relations stored with objects

Complex ACLs in Unix: sudo

```
# Cmnd alias specification
Cmnd_Alias  PPP = /etc/ppp/ppp-on, /etc/ppp/ppp-off

# User privilege specification
root        ALL=(ALL) ALL
carzanig    ALL=(ALL) ALL
carzanig    ALL=NOPASSWD: PPP
```

sudo

```
User_Alias    FULLTIMERS = millert, mikef, dowdy
User_Alias    PARTTIMERS = bostley, jwfox, crawl
Runas_Alias   OP = root, operator
Runas_Alias   DB = oracle, sybase
Host_Alias    SPARC = bigtime, eclipse, moet, anchor :\
              SGI = grolsch, dandelion, black :\
              ALPHA = widget, thalamus, foobar :\
              HPPA = boa, nag, python
Host_Alias    CUNETS = 128.138.0.0/255.255.0.0
Cmnd_Alias    DUMPS = /usr/bin/mt, /usr/sbin/dump, \
                      /usr/sbin/restore, /usr/sbin/rrestore
Cmnd_Alias    KILL = /usr/bin/kill
Cmnd_Alias    PRINTING = /usr/sbin/lpc, /usr/bin/lprm
Cmnd_Alias    SHUTDOWN = /usr/sbin/shutdown
FULLTIMERS    ALL = NOPASSWD: ALL
PARTTIMERS    ALL = ALL
jack          CSNETS = ALL
joe           ALL = /usr/bin/su operator
pete          HPPA = /usr/bin/passwd [A-z]*, \
                     !/usr/bin/passwd root
```

Sudo Model

- Who plays which roles
- For each object
  - who has what type of access
  - which roles have what type of access
  - who or what roles do not have what type of access (exclusions)

Multilevel Security

- Information is ranked according to its sensitivity *level*
- Information is accessed only when needed
- Information is grouped in *compartments*
- Users have *clearance levels*

Antonio: <*top secret*, {*Siena*}>

Alex: <*secret*, {*Siena, SWDock*}>

Filter.cc: <*top secret*, {*Siena*}>

grades.txt: <top *secret*, {*csci7000-001*}>

Mandatory Access Control Rules

- Mandatory access control
- You can only read at your level or lower
- You can only run processes at your level or lower
- You can only write at your level or higher

Issues in Access Control

- Delegation
- Temporary access
- Policy definition: what is the meta-policy?
- Volatility of access relations
- Run-time overhead