Announcements

• HW 6 is on the web
  – Due December 10th

• Final exam:
  – Tuesday, Dec. 21
  – 11:00am-1:00pm
  – Towne 311
Access Control

- **Discretionary**: The individual user may, at his own discretion, determine who is authorized to access the objects he creates.

- **Mandatory**: The creator of an object does not necessarily have the ability to determine who has authorized access to it.
Multilevel Security

• Multiple levels of confidentiality ratings
  – Used by military and government
  – Public < Classified < Secret < Top Secret

• Information flow
  – Regulate how information is used throughout entire system
  – A document generated from Classified and Secret information must be rated Secret.
  – Label creep: Information levels tend to get higher as computation proceeds.
Information Confidentiality

Secret Inputs → Program → Secret Outputs
Public Inputs → Program → Public Outputs
Information Flow Security

• “No read up, no write down.”
  – Principals are assigned clearance levels drawn from the lattice of security labels.
  – A principal may read items with lower (or equal) security label.
  – A principal may write items with higher (or equal) security label.
Information Flow

```c
int{Alice:} X;
int{Bart:} Y;
...
if (X > 0) then {
    Y = 1;
} else {
    Y = 0;
}
//... This computation doesn’t depend on X
```
Jif = Java + Information Flow

- Confidentiality labels:
  - int{Alice:} x; "Alice's private int"
  - int{Alice:Bart} y; "Alice permits Bart as reader"

- Integrity labels:
  - int{*:Alice} z; "Alice trusts z"

- Combined labels:
  - int{Alice: ; *:Alice} w; (Both)

Insecure
- int{Alice:} a1, a2;
- int{Bart:} b;
- int{*:Alice} c;
- a1 = b;
- b = a1;
- c = a1;

Secure
- int{Alice:} a1, a2;
- int{Bart:} b;
- int{*:Alice} c;
- a1 = a2;
- a1 = c;
- c = a1;
Implementing Multilevel Security

• Dynamic:
  – Tag all values in memory with their security level
  – Operations propagate security levels
  – Must be sure that tags can’t be modified
  – Expensive, and approximate

• Static:
  – Program analysis
  – May be more precise
  – May have less overhead
Government Standards

• Department of Defense
• Trusted Computer System Evaluation Criteria (TCSEC)
  – Known as the Orange Book
  – Circa 1985
TCSEC Ratings

• **Division (D): Minimal Protection**
  – *This division contains only one class. It is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.*

• **Division (C): Discretionary Protection**
  – *Classes in this division provide for discretionary (need-to-know) protection and, through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate.*
TCSEC Ratings

• **Division (B): Mandatory Protection**
  - The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.
TCSEC Ratings

• **Division (A): Verified Protection**
  
  – *This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development and implementation.*
Example Rated Software

- Oracle Corporation Trusted Oracle7 (B1)
- Novell, Incorporated NetWare 4.11 (C2)
- Microsoft Corporation Windows NT, Version 3.5 (C2)
Digital Rights Management

- Restrict the use of digital information to protect copyright holders

- DRM attempts to control
  - File access (# of views, length of views)
  - Altering
  - Sharing
  - Copying
  - Printing or otherwise exporting
DRM Approach 1: Containment

• Encrypt the data
• Viewing the data:
  – Proprietary software
  – Proprietary hardware

• Weaknesses
  – Copy the viewing software
  – Hardware is inflexible (and fallible)
  – Reverse engineer viewing software to expose unencrypted data
  – Only takes one good hacker to create a bootleg
DRM Approach 2: Marking

- **Steganography**: (covered writing)
  - The process of secretly embedding information into a data source in such a way its very existence is concealed.

- **Digital watermarking**:
  - A short sequence of information embedded in a way that is difficult to erase.
Watermarking Basic Idea

- Pictures, Video, and Sound
  - Human perception is imperfect
  - There are a lot of “least significant bits”
  - Modifying the least significant bits doesn’t change the picture much

\[(R,G,B) = (182,54,89) \quad (R,G,B) = (182,54,90)\]

- Encode a signal in the least significant bits.
Watermarking Example

Original Image

Watermarked Image
Properties of Watermarks

• Desirable properties
  – Imperceptible
  – Robust (withstands modifications to the image)
  – High capacity
  – Efficient
  – Hard to remove (some schemes involve cryptographic operations)

• Drawbacks
  – Hard to make tamper proof
  – Can distort image/sound
DRM Examples

• DVD players/recorders
  – Keyed to a geographic region
  – DVD burners may refuse to record watermarked material

• Secure Digital Music Initiative
  – www.sdmi.org
But... SDMI hasn’t panned out

• Ed Felton of Princeton
  – “In September 2000, SDMI issued a public challenge to help them choose among four proposed watermarking technologies. During the three-week challenge, researchers could download samples of watermarked music, and were invited to attempt to remove the secret copyright watermarks.”
  – During the challenge period, our team ... successfully defeated all four of the watermarking challenges, by rendering the watermarks undetectable without significantly degrading the audio quality of the samples. Our success on these challenges was confirmed by SDMI's email server.