SENG 360 - Security Engineering
Access Control

Jens Weber

Fall 2022

University
of Victoria

Recall from last week

Database Access Control

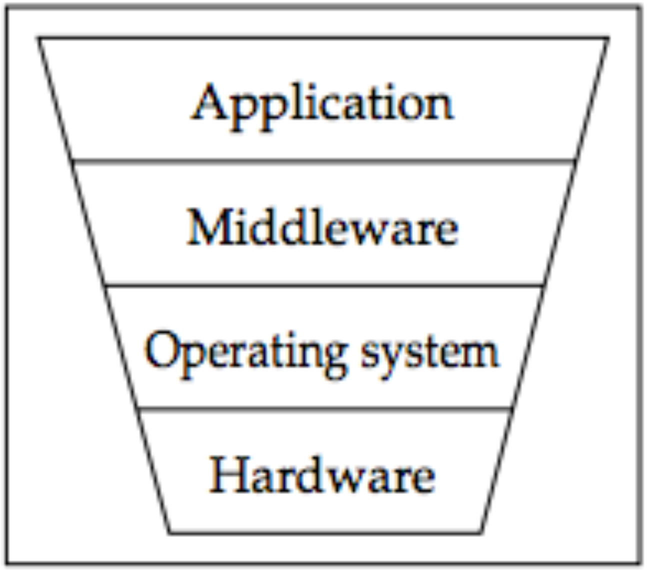
➡ *Discretionary access control (DAC)*

➡ *SQL*

Today

➡ *AC on other levels*

➡ *Mandatory Access Control (MAC)*

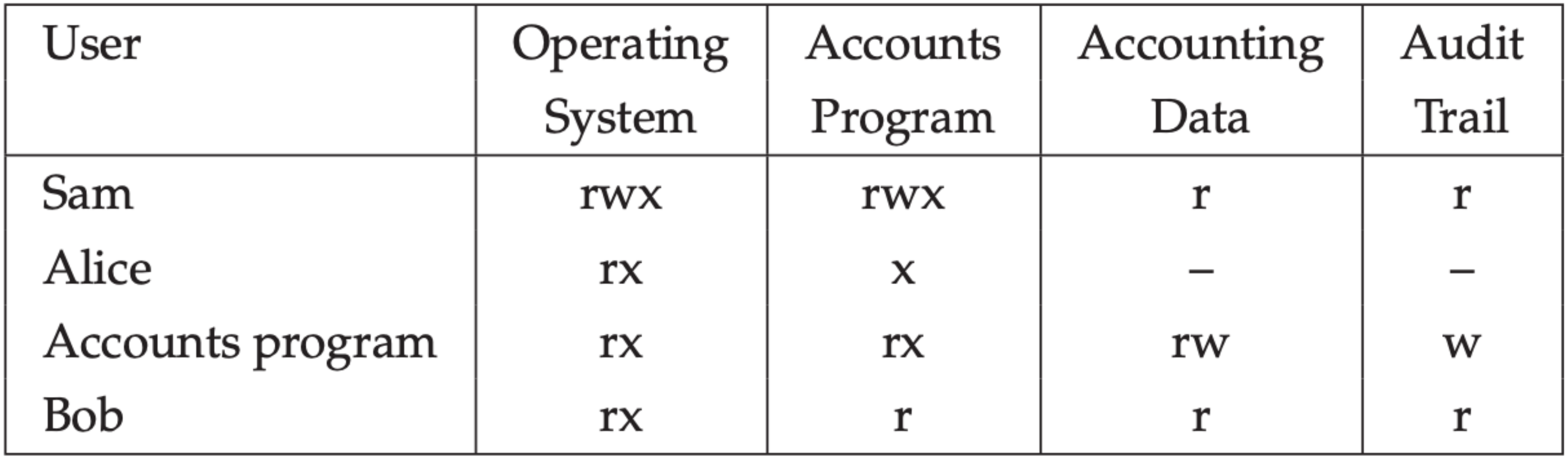


Learning Objectives

At the end of this class you will be able to

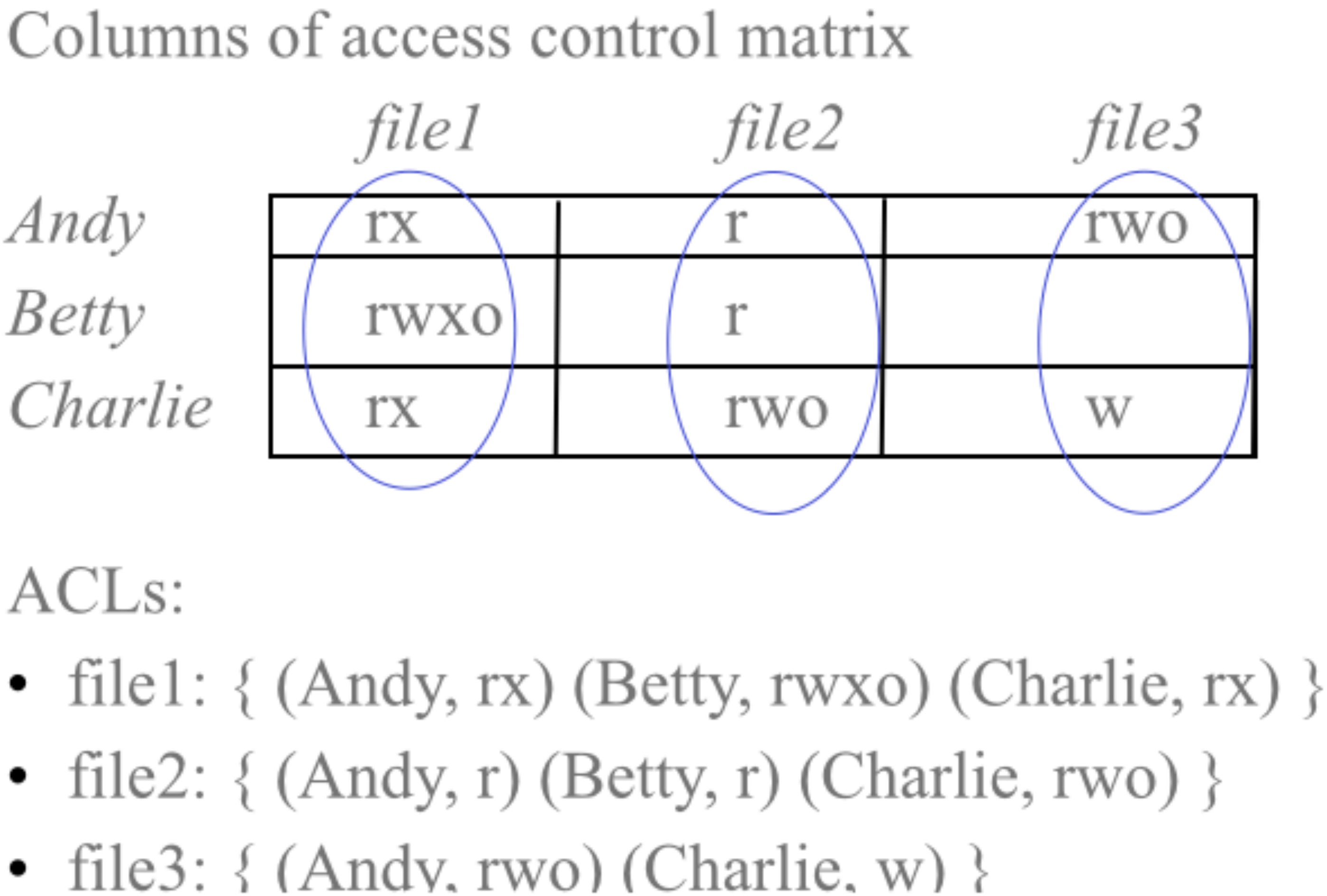
- Describe representations for discretionary AC policies
  - ACM, ACL, C-list
- Distinguish between mandatory and discretionary AC
- Use formal multilevel/multilateral security models

Access Control Matrix



User	Operating System	Accounts Program	Accounting Data	Audit Trail
Sam	rwx	rwx	r	r
Alice	rx	x	–	–
Accounts program	rx	rx	rw	w
Bob	rx	r	r	r

Access Control Lists (AC lists)



Columns of access control matrix

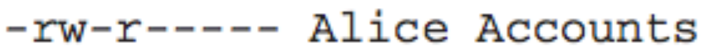
	file1	*file2*	*file3*
Andy	rx	r	rwo
Betty	rwxo	r	
Charlie	rx	rwo	w

ACLs:

- file1: { (Andy, rx) (Betty, rwxo) (Charlie, rx) }
- file2: { (Andy, r) (Betty, r) (Charlie, rwo) }
- file3: { (Andy, rwo) (Charlie, w) }

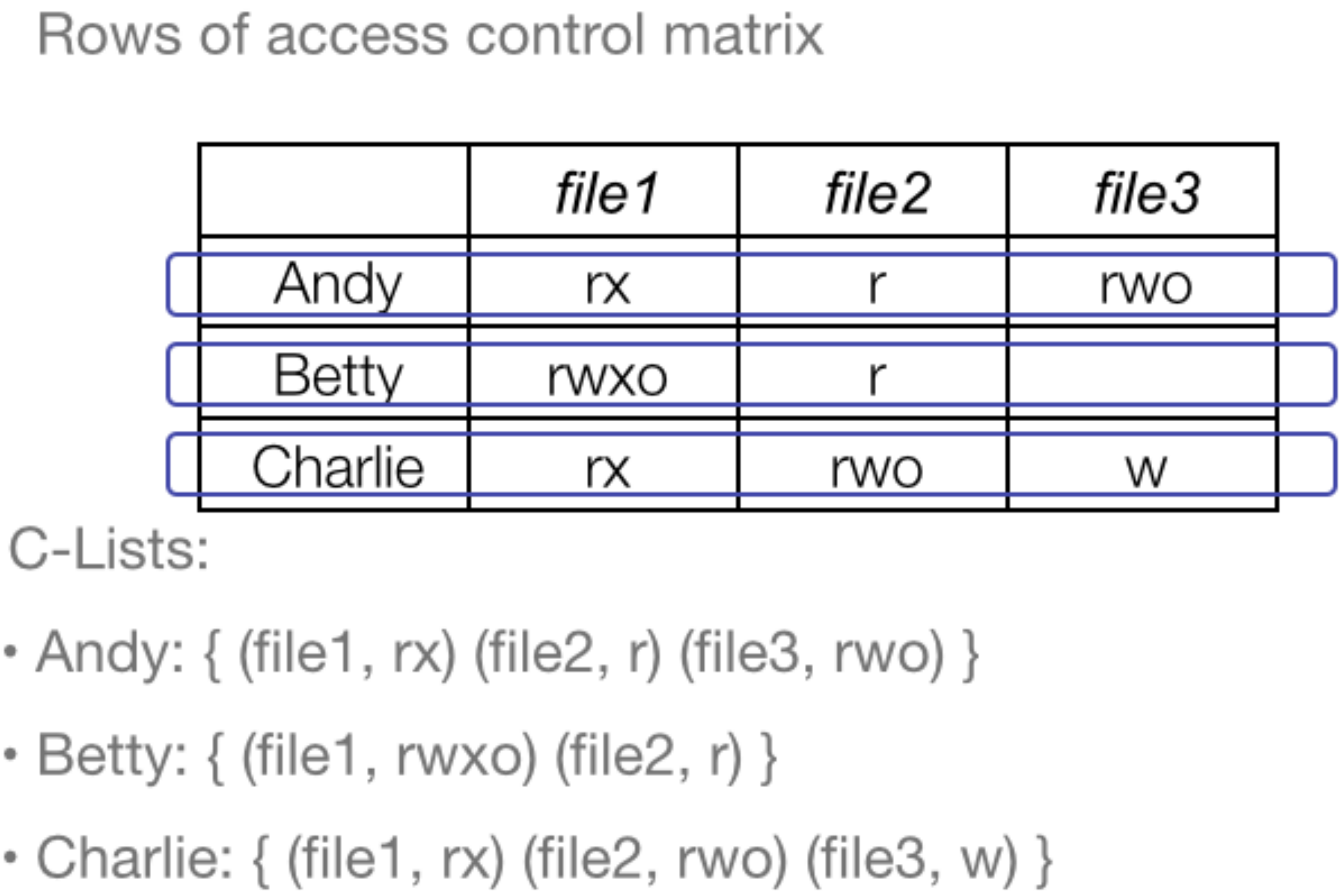
AC Lists in Operating Systems

- ACLs can be long … so combine users
  - UNIX: 3 classes of users: **owner**, **group**, **rest**
    - rwx rwx rwx
  - Ownership assigned based on creating process
  - Group set to current group of process
  - Can change it to any other group the user belongs to



```
-rw-r----- Alice Accounts
```

Capability Lists (C lists)



Rows of access control matrix

	file1	*file2*	*file3*
Andy	rx	r	rwo
Betty	rwxo	r	
Charlie	rx	rwo	w

C-Lists:

- Andy: { (file1, rx) (file2, r) (file3, rwo) }
- Betty: { (file1, rwxo) (file2, r) }
- Charlie: { (file1, rx) (file2, rwo) (file3, w) }

C-Lists vs ACLs

Advantages C-Lists

- efficient run-time checking
- easy delegation

Advantages ACLs

- efficient revocation / rights management
- not easy to forge

In practice: OS often combine both
(e.g., file descriptor, kerberos ticket)

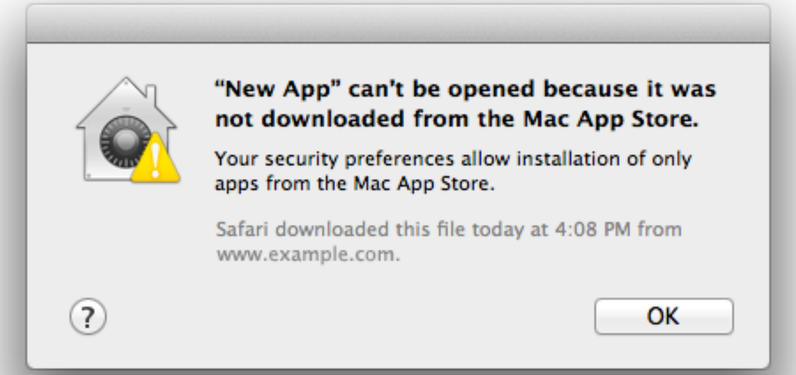
Discretionary vs. Mandatory Access Control

Discretionary Access Control (DAC):

- Users decide how they want to share their data

Mandatory Access Control (MAC): System (administrators) enforce AC policy

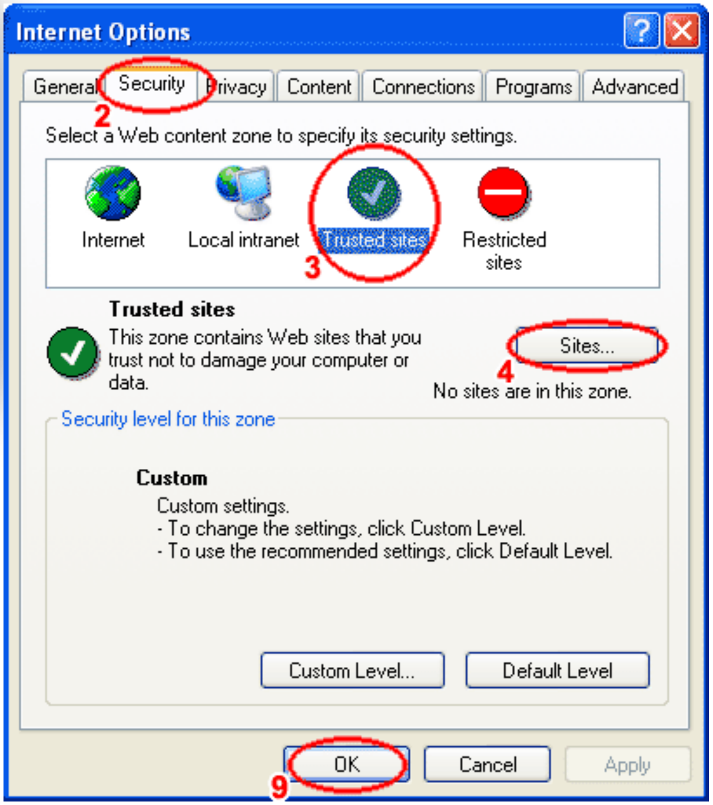
Multi-level secure systems



"New App" can't be opened because it was not downloaded from the Mac App Store.

Your security preferences allow installation of only apps from the Mac App Store.

Safari downloaded this file today at 4:08 PM from www.example.com.



Select a Web content zone to specify its security settings.

Trusted sites

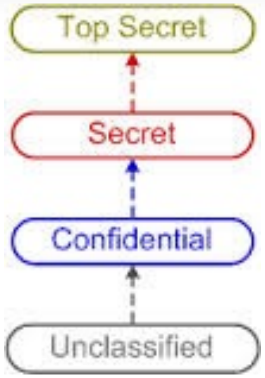
This zone contains Web sites that you trust not to damage your computer or data.

No sites are in this zone.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.



Top Secret

Secret

Confidential

Unclassified

AC Policy Models

Generic “model” that of protection properties common to a class of security policies. May lend itself to mathematical analysis.

- Bell-Lapadula Model (confidentiality)
- Biba Model (integrity)
- Brewer Nash Model (integrity / conflict of interest)
- Clark-Wilson Model (integrity / procedural)

Bell LaPadula Model

David Elliott Bell and
Leonard J. LaPadula

Introduced in 1973

- Air Force was concerned with security in time-sharing systems
- Many OS bugs
- Accidental misuse

Basic idea: Information should not flow downward

Main Objective:

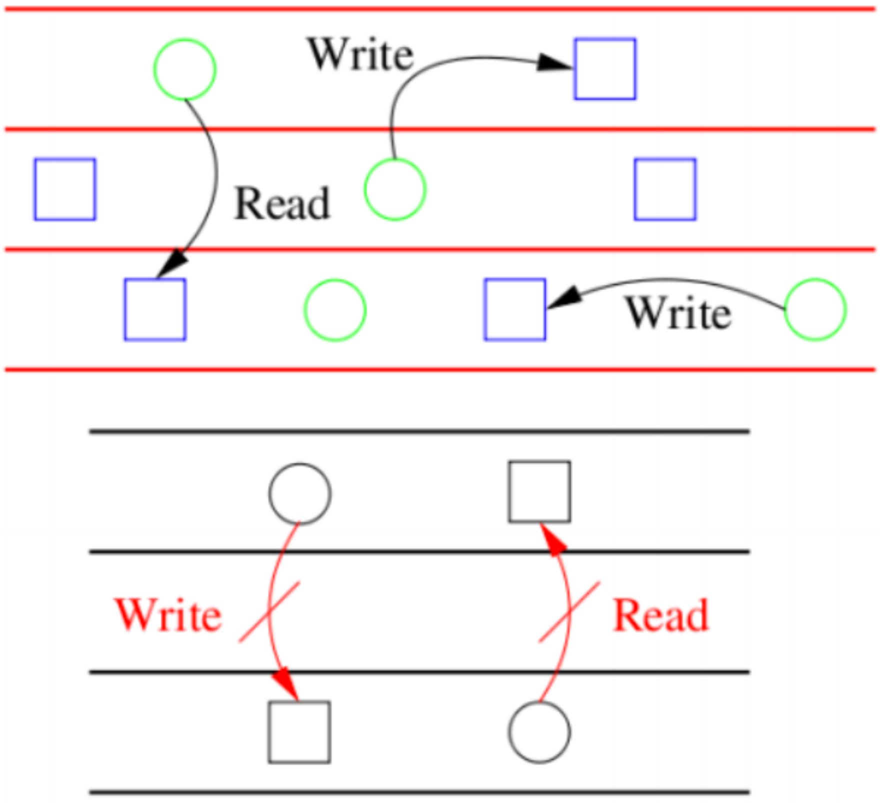
- Enable one to show that a computer system can securely process classified information

Bell-LaPadula Rules

- Subject S can read object O *if and only if* the subject's security clearance $l_S \geq l_O$, which is the security classification of O, and S has discretionary read access to O.
  (called *security condition or NRU*)

- S can write O *if and only if* $l_S \leq l_O$ and S has discretionary write access to O.
  (called **-property or NWD*)

Bell Lapadula Visualized



Example: Bell-LaPadula

Security Levels	Subjects	Objects
Top Secret (TS)	Tamara, Thomas	Personnel Files
Secret (S)	Sally, Samuel	E-Mail Files
Confidential (C)	Claire, Clarence	Activity Log Files
Unclassified (UC)	Ulaley, Ursula	Telephone List Files

– What objects can can Thomas read?

– Can Sally write email files? Can she read personnel files?

– Which files can Claire read and write, respectively?

– Who can read telephone lists?

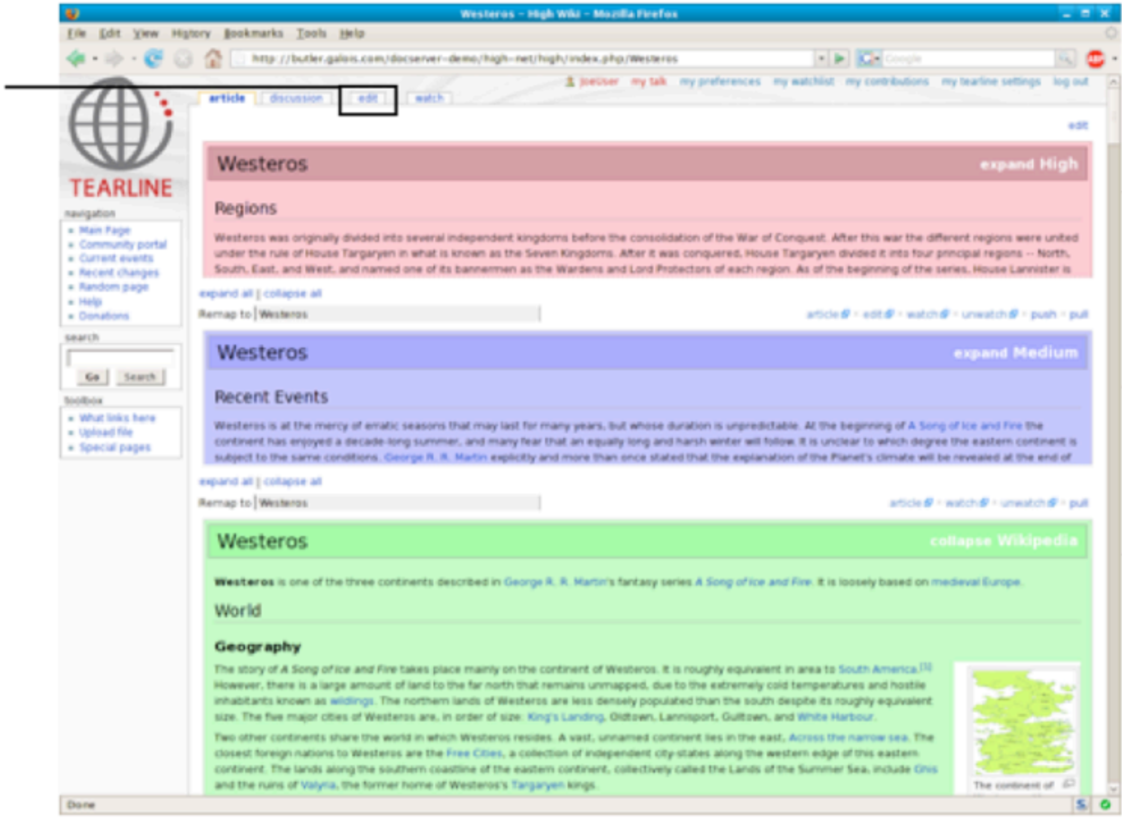
Tranquility

Criticism: user may ask admin to declassify object (or subject)

- *Tranquility property*
  - *Strong tranquility*: security labels remain unchanged during the operation of the system
  - *Weak tranquility*: security labels do not change in ways where they would violate the AC policy (preferred because of POLP)

Example application: ML Wiki

Merged Wiki View: High


Westeros – High Wiki – Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://butler.galois.com/docserver-demo/high-net/high/index.php/Westeros
Google
joeuser my talk my preferences my watchlist my contributions my tearline settings log out
article discussion edit watch
TEARLINE
navigation
Main Page
Community portal
Current events
Recent changes
Random page
Help
Donations
search
Go Search
toolbox
What links here
Upload file
Special pages
edit
expand High
expand all | collapse all
Remap to Westeros
article · edit · watch · unwatch · push · pull
expand Medium
article · watch · unwatch · pull
collapse Wikipedia
Done

Westeros

Regions

Westeros was originally divided into several independent kingdoms before the consolidation of the War of Conquest. After this war the different regions were united under the rule of House Targaryen in what is known as the Seven Kingdoms. After it was conquered, House Targaryen divided it into four principal regions -- North, South, East, and West, and named one of its bannermen as the Wardens and Lord Protectors of each region. As of the beginning of the series, House Lannister is

Westeros

Recent Events

Westeros is at the mercy of erratic seasons that may last for many years, but whose duration is unpredictable. At the beginning of A Song of Ice and Fire the continent has enjoyed a decade-long summer, and many fear that an equally long and harsh winter will follow. It is unclear to which degree the eastern continent is subject to the same conditions. George R. R. Martin explicitly and more than once stated that the explanation of the Planet's climate will be revealed at the end of

Westeros

Westeros is one of the three continents described in George R. R. Martin's fantasy series *A Song of Ice and Fire*. It is loosely based on medieval Europe.

World

Geography

The story of *A Song of Ice and Fire* takes place mainly on the continent of Westeros. It is roughly equivalent in area to South America.[1] However, there is a large amount of land to the far north that remains unmapped, due to the extremely cold temperatures and hostile inhabitants known as wildings. The northern lands of Westeros are less densely populated than the south despite its roughly equivalent size. The five major cities of Westeros are, in order of size: King's Landing, Oldtown, Lannisport, Gulltown, and White Harbour.

Two other continents share the world in which Westeros resides. A vast, unnamed continent lies in the east, Across the narrow sea. The closest foreign nations to Westeros are the Free Cities, a collection of independent city-states along the western edge of this eastern continent. The lands along the southern coastline of the eastern continent, collectively called the Lands of the Summer Sea, include Ghis and the ruins of Valyria, the former home of Westeros's Targaryen kings.

The continent of

High can edit High content only

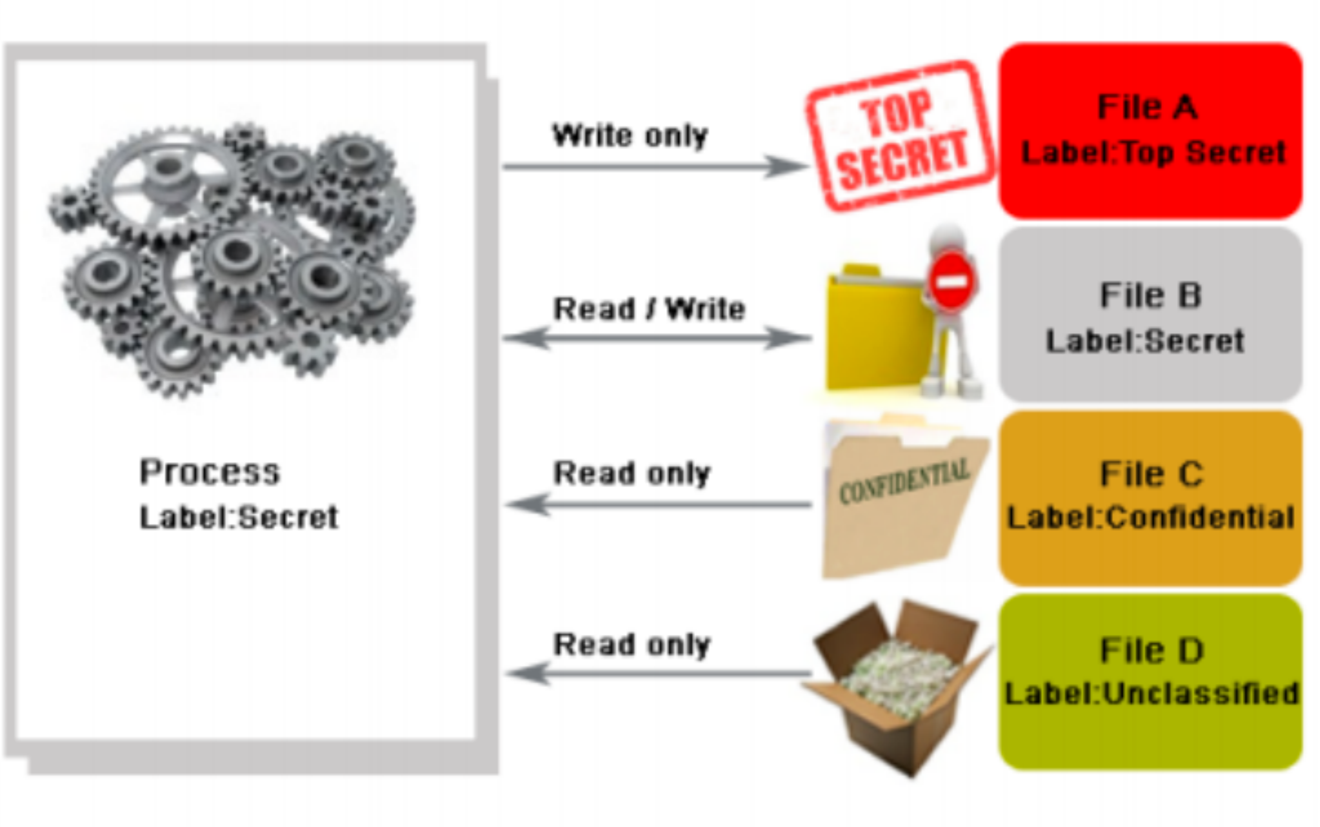
Banners separate content at each level

The wiki page begins with High content

Medium content

Low content

Example OS: SELinux



© Jens H. Weber

Adding Compartments to Levels

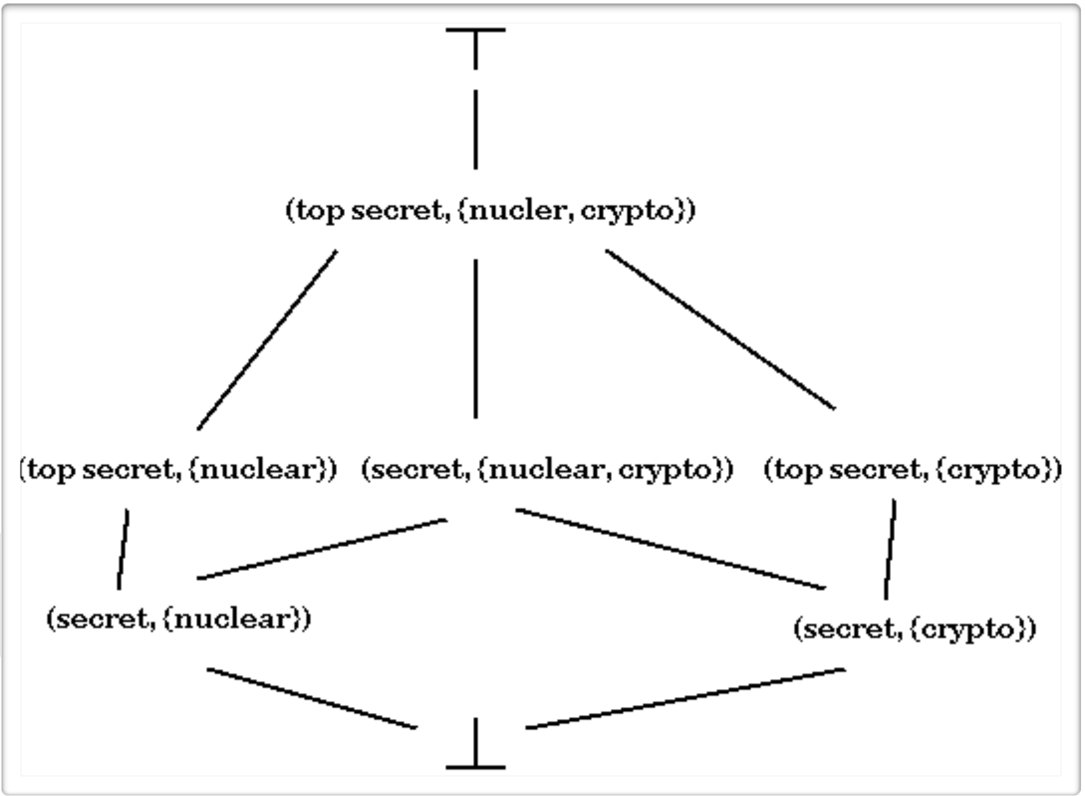
Creates a partial order

vertical levels

TOP SECRET
SECRET
CONFIDENTIAL
OPEN

horizontal compartments

nuclear	crypto	navy	army



© Jens H. Weber

Biba Integrity Model

Ken Biba, 1975

Can be seen as Bell-Lapadula Model (upside down)

read up - write down

- The higher the level, the more confidence...
  - that a program will execute correctly
  - that data is accurate and/or reliable
- Note relationship between integrity and trustworthiness
- Important: *integrity levels are **not** confidentiality levels*

University of Victoria

Strict Integrity Policy - Typically called “The” Biba Model

Analog to Bell-LaPadula model

1. $s \in S$ can read $o \in O$ iff $i(s) \leq i(o)$
2. $s \in S$ can write to $o \in O$ iff $i(o) \leq i(s)$
3. $s_1 \in S$ can execute $s_2 \in S$ iff $i(s_2) \leq i(s_1)$

University of Victoria

Biba's Low Watermark Policy

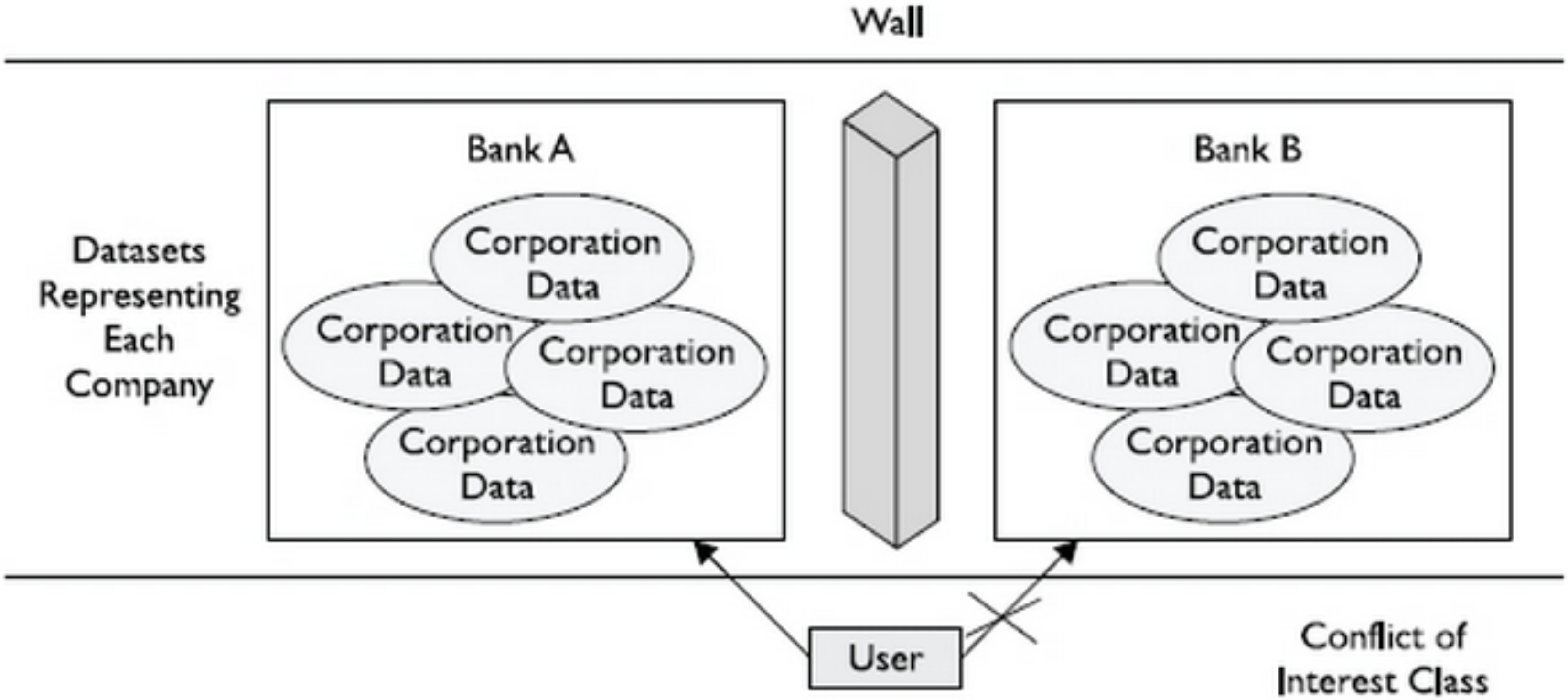
- Subjects get "tainted" by reading low integrity information

- When s reads o, $fs(s) = min(fs(s), fo(o))$
  s can only write objects at lower levels

Problem: Subject integrity levels decrease over time.
(Need some way to restore integrity.)

Brewer Nash Model

Goal: There must be no information flow that causes a conflict of interest



Brewer Nash Model

Goal: There must be no information flow that causes a conflict of interest

- **Sets**: Companies **C**, Subjects **S**, Objects **O**
  (Think Subjects = Analysts and Objects = Documents)
- $y: O \rightarrow C$ *returns the company that belongs to a given object*
- $x: C \rightarrow P(C)$ *returns the Conflict of Interest set for a company*
- **Security label** for an object o is defined as ***(x(o), y(o))***
- $N: S \times O \rightarrow BOOL$ *returns True if **s** has had access to **o***

Brewer Nash Model

Simple security property (ss-property):

- A subject **s** is allowed access to an object **o** only if $\forall$ o’: N(s,o’) $\Rightarrow$ y(o)=y(o’) or y(o)$\notin$x(o’)

For example, consider the following conflict classes:

- { Ford, Chrysler, GM }
- { Bank of America, Wells Fargo, Citicorp }
- { Microsoft }

For example, if you access a file from GM, you subsequently will be blocked from accessing any files from Ford or Chrysler. You are free to access files from companies in any other conflict class.

Brewer Nash Model

Simple security property (ss-property):

- A subject s is allowed access to an object o only if $\forall$ o’: N(s,o’) $\Rightarrow$ y(o)=y(o’) or y(o)$\notin$x(o’)

*-property:

- A subject s is allowed ***write*** access to an object o only if $\forall$ o’: N(s,o’) $\Rightarrow$ y(o)=y(o’) or x(o’)=$\oslash$