SENG 360 - Security Engineering

Database Security - SQL Injection

Jens Weber

Fall 2021

University of Victoria

Learning Objectives

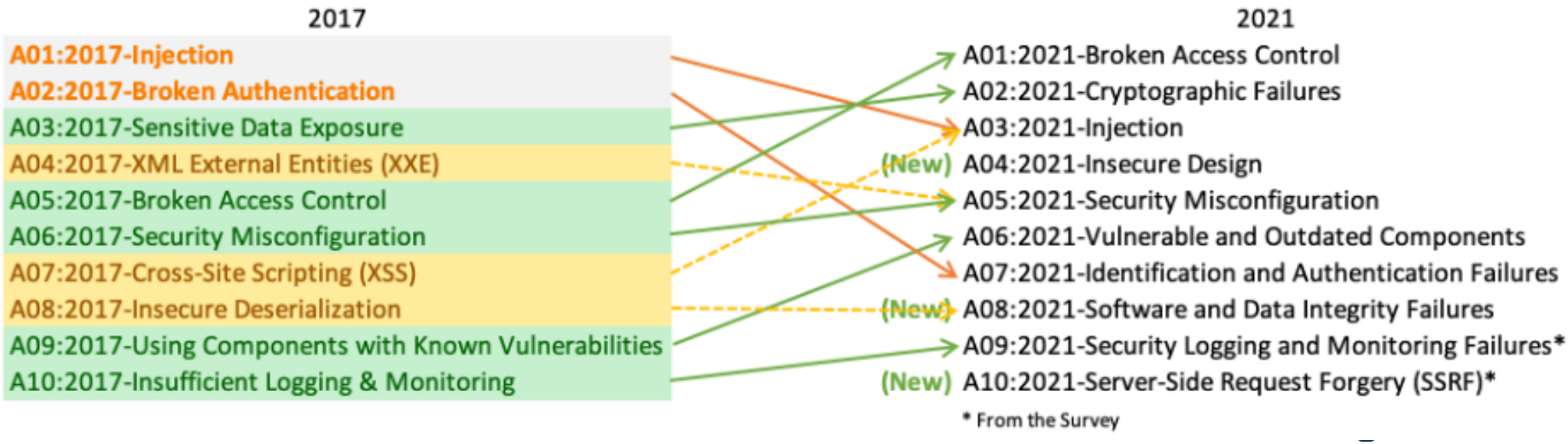
At the end of this class you will be able to

- Explain the Principle of Least Privilege (POLP)
- Describe AC inside and at the interface of databases
- Define AC policies with SQL
- Differentiate IBAC, RBAC and ABAC

University of Victoria

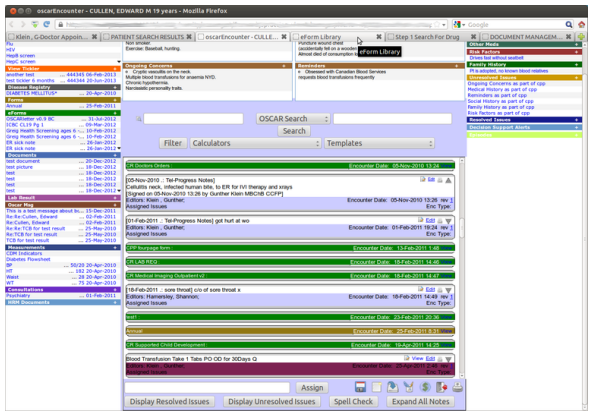
Recall from last classe

Broken access control is at the top (up from 5th)



Principle of Least Privilege (POLP)

Only the minimum necessary rights should be assigned to a subject that requests access to a resource and should be in effect for the shortest duration necessary



OscarQA_Ubuntu16 — O-out — more oscar.properties — 80×21

OSCAR | ...t@vagrant: ~ — -zsh ... | OBIB-dir -zsh ... | OBIB-VM -zsh ... | Manual

```
the renaming of columns.
# jdbcCompliantTruncation: Fields which are not included in a query, and do not
contain a default value in the database,
#                          will raise an exception in the JDBC specification. Pr
evious versions of Connector/J
#                          were not JDBC compliant and did not follow the trunca
tion specifications.
# IMPORTANT: The fields listed after the ? are required! Otherwise, OSCAR will n
ot behave properly as it depends on
#            legacy functionality. Ensure that you leave the tags behind the fie
ld when renaming the database.
db_name = oscar?characterEncoding=UTF-8&zeroDateTimeBehavior=round&useOldAliasMe
tadataBehavior=true&jdbcCompliantTruncation=false

# username
db_username = root

# password for the username above
db_password = @scar2018

:
```

Storing Database Credentials

Database credentials should never be stored in the application source code, especially if they are unencrypted. Instead, they should be stored in a configuration file that:

- Is outside of the webroot.
- Has appropriate permissions so that it can only be read by the required user(s).
- Is not checked into source code repositories.

https://cheatsheetseries.owasp.org/cheatsheets/Database_Security_Cheat_Sheet.html#database-configuration-and-hardening

University of Victoria

Permissions

- Do not use the built-in **root**, **sa** or **SYS** accounts.
- Do not grant the account administrative rights over the database instance.
- Only allow the account to connect from allowed hosts.
  - This would often be localhost or the address of the application server.
- Only grant the account access to the specific databases it needs.
  - Development, UAT and Production environments should all use separate databases and accounts.

University of Victoria

Permissions (cont'd)

- Only grant the required permissions on the databases.
- Most applications would only need SELECT, UPDATE and DELETE permissions.
- The account should not be the owner of the database as this can lead to privilege escalation vulnerabilities.
- Avoid using database links or linked servers.
  - Where they are required, use an account that has been granted access to only the minimum databases, tables, and system privileges required.

University of Victoria

Permissions (cont'd)

For more security-critical applications, it is possible to apply permissions at more granular levels, including:

- Table-level permissions.
- Column-level permissions.
- Row-level permissions
- Blocking access to the underlying tables, and requiring all access through restricted ***views***.

University of Victoria

SQL-Based Access Definition: GRANT

- Privileges include:
  SELECT, INSERT, UPDATE
  DELETE, REFERENCES
- PUBLIC means that any user has specified privileges
- "IDENTIFIED BY" specifies a password needed to revoke the rights
- "WITH GRANT OPTION" allows the specified user to grant rights to others

General form:

```
GRANT          { privileges | role }
[ON            table]
TO             { user | role | PUBLIC }
[IDENTIFIED BY password]
[WITH          GRANT OPTION]
```

Example:

```
GRANT SELECT ON ANY TABLE TO ricflair
```

SQL-Based Access Definition: REVOKE

- Privileges include:
  SELECT, INSERT, UPDATE
  DELETE, REFERENCES

- PUBLIC means that any user will lose specified privileges

General form:

```
REVOKE      { privileges | role }
[ON         table]
FROM        { user | role | PUBLIC }
```

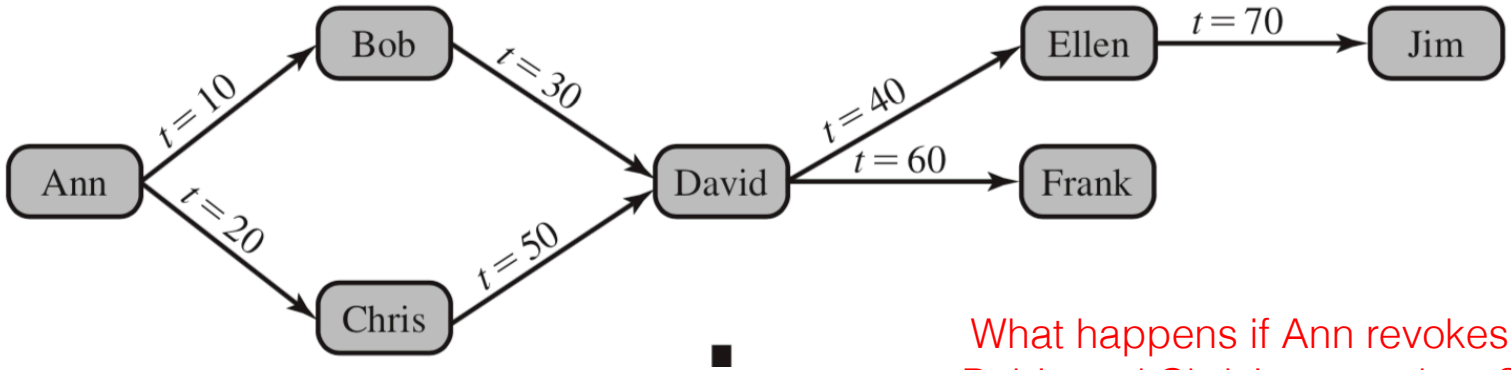
Example:

```
REVOKE SELECT ON ANY TABLE FROM ricflair
```

Cascading Authorization

The grant option enables an access right to “cascade” through a number of users

Example:
let’s assume Ann grants access to Bob at time t=10 with grant option…



What happens if Ann revokes Bob’s and Chris’ access later?

Cascading Authorization

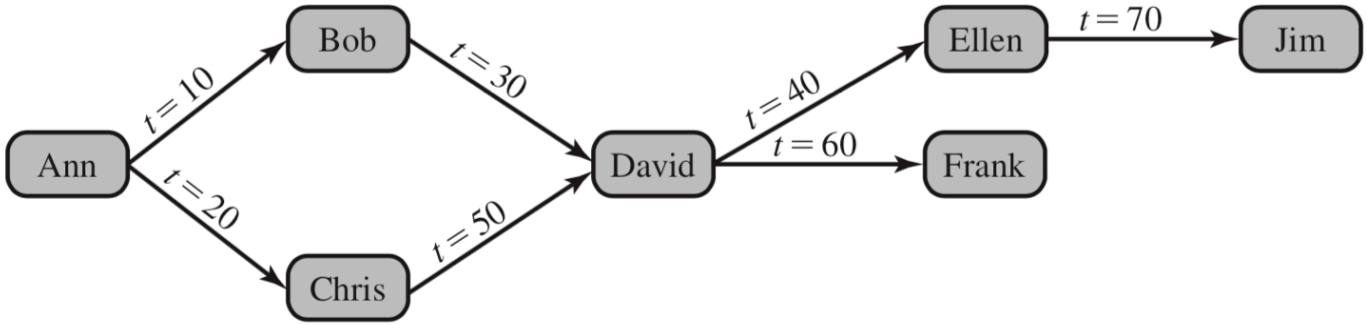
The grant option enables an access right to “cascade” through a number of users

Example:
let’s assume Ann grants access to Bob at time t=10 with grant option…

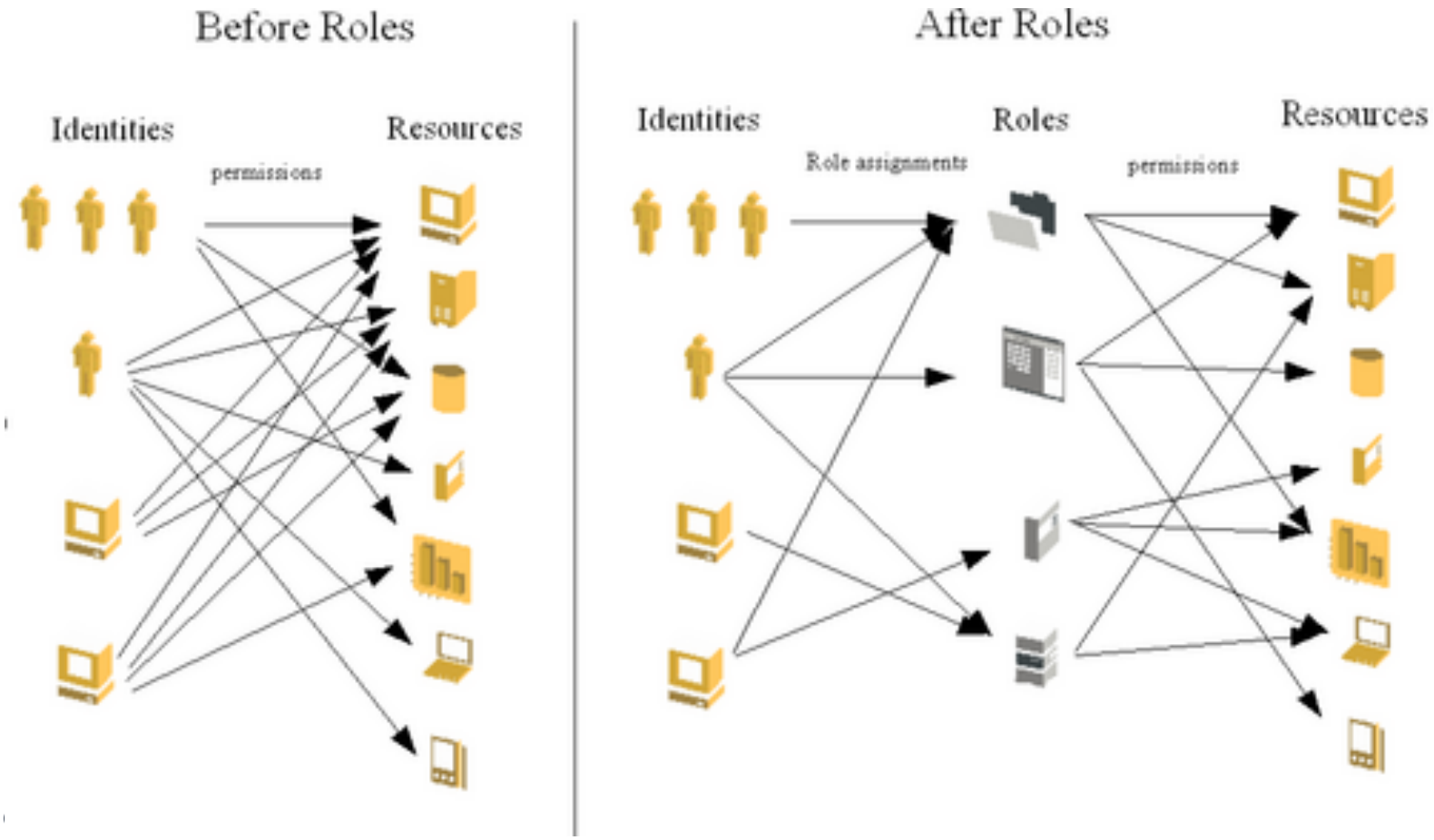
The revocation will cascade

What happens if Ann revokes
Bob’s and Chris’ access later?

What happens if Bob revokes David's right later?



IBAC vs. RBAC


Before Roles
Identities
Resources
permissions
After Roles
Identities
Roles
Resources
Role assignments
permissions

RBAC in Databases

Most DBMS support RBAC

- Fixed roles
- User-defined roles

University of Victoria

Examples

Role	Permissions
Fixed Server Roles	
sysadmin	Can perform any activity in SQL Server and have complete control over all database functions
serveradmin	Can set server-wide configuration options, shut down the server
setupadmin	Can manage linked servers and startup procedures
securityadmin	Can manage logins and CREATE DATABASE permissions, also read error logs and change passwords
processadmin	Can manage processes running in SQL Server
Dbcreator	Can create, alter, and drop databases
diskadmin	Can manage disk files
bulkadmin	Can execute BULK INSERT statements
Fixed Database Roles	
db_owner	Has all permissions in the database
db_accessadmin	Can add or remove user IDs
db_datareader	Can select all data from any user table in the database
db_datawriter	Can modify any data in any user table in the database
db_ddladmin	Can issue all data definition language statements
db_securityadmin	Can manage all permissions, object ownerships, roles and role memberships
db_backupoperator	Can issue DBCC, CHECKPOINT, and BACKUP statements
db_denydatareader	Can deny permission to select data in the database

Role Management in (MY)SQL

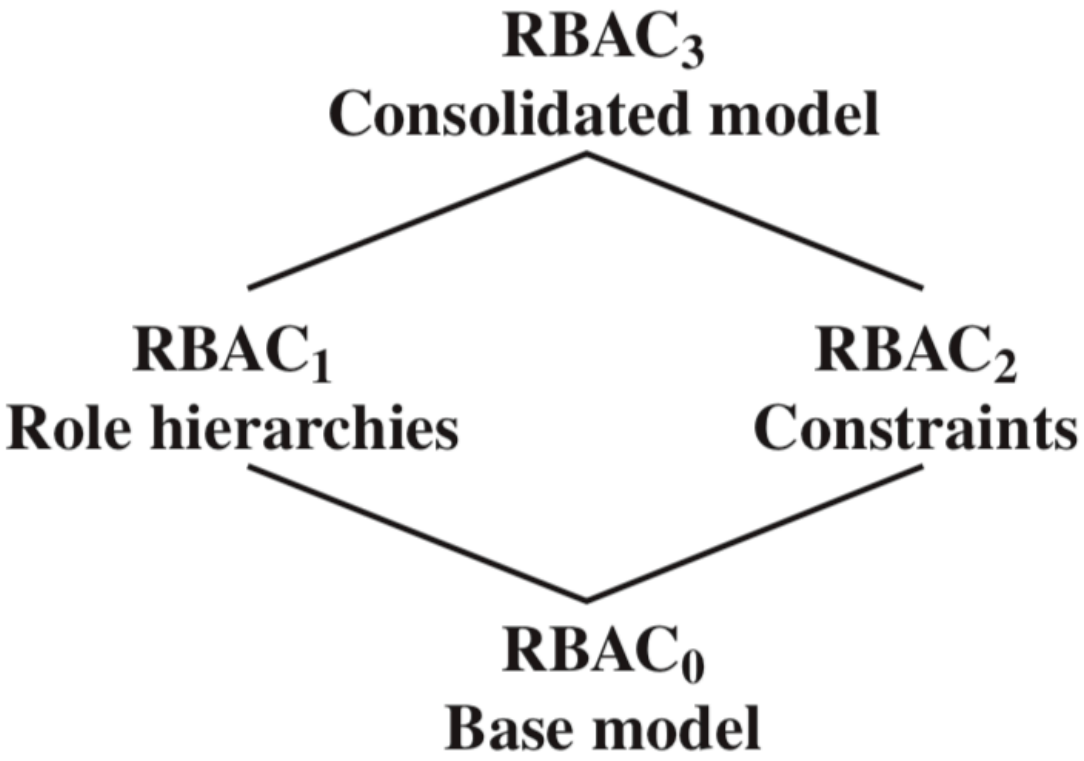
- CREATE ROLE and DROP ROLE create and remove roles.
- GRANT and REVOKE assign privileges to revoke privileges from roles.
- SHOW GRANTS displays privilege and role assignments for user accounts and roles.
- SET DEFAULT ROLE specifies which account roles are active by default.
- SET ROLE changes the active roles within the current session.
- The CURRENT_ROLE() function displays the active roles within the current session.
- The *mandatory_roles* and *activate_all_roles_on_login system* variables enable defining mandatory roles and automatic activation of granted roles when users log in to the server.

University of Victoria

RBAC Reference Models

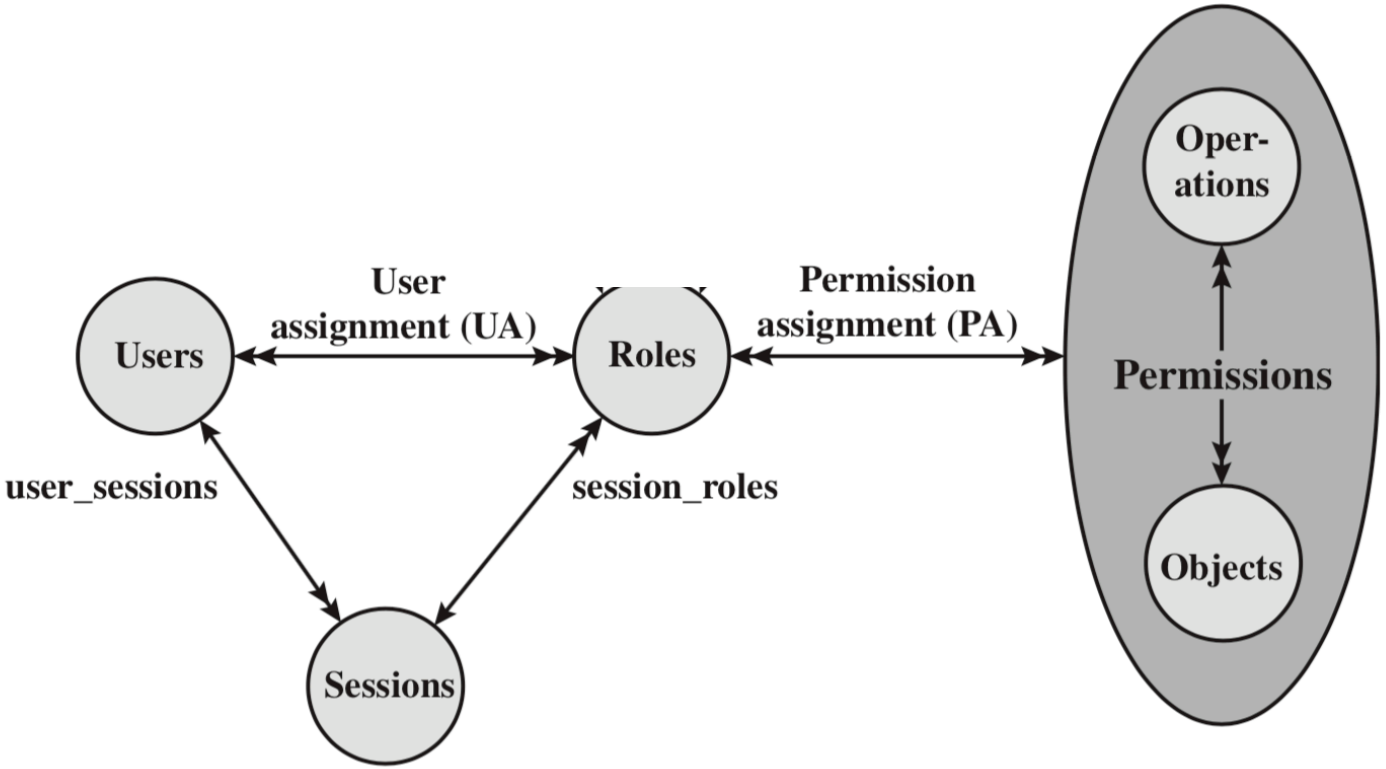
- **RBAC models come in different variations**
- **Reference models have been standardized by NIST**

RBAC Reference Models

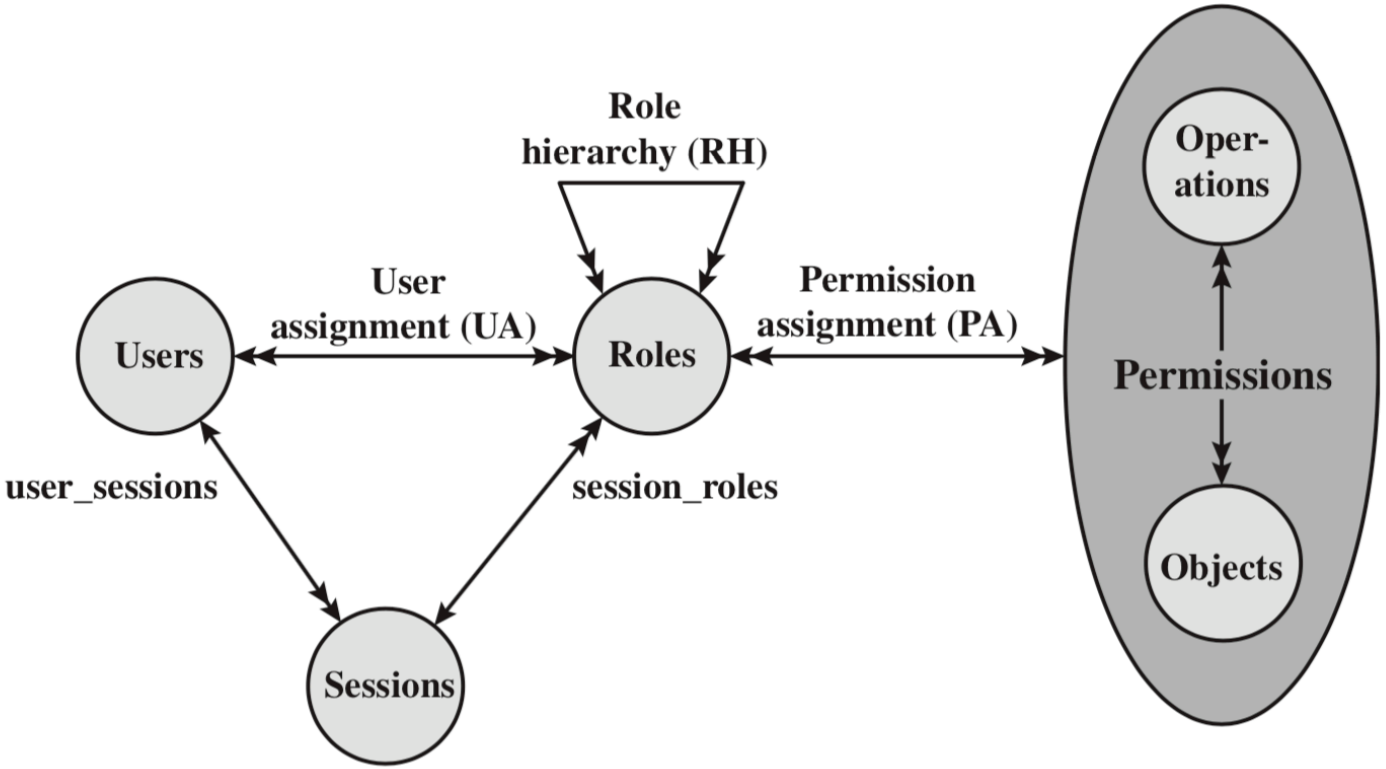


University of Victoria

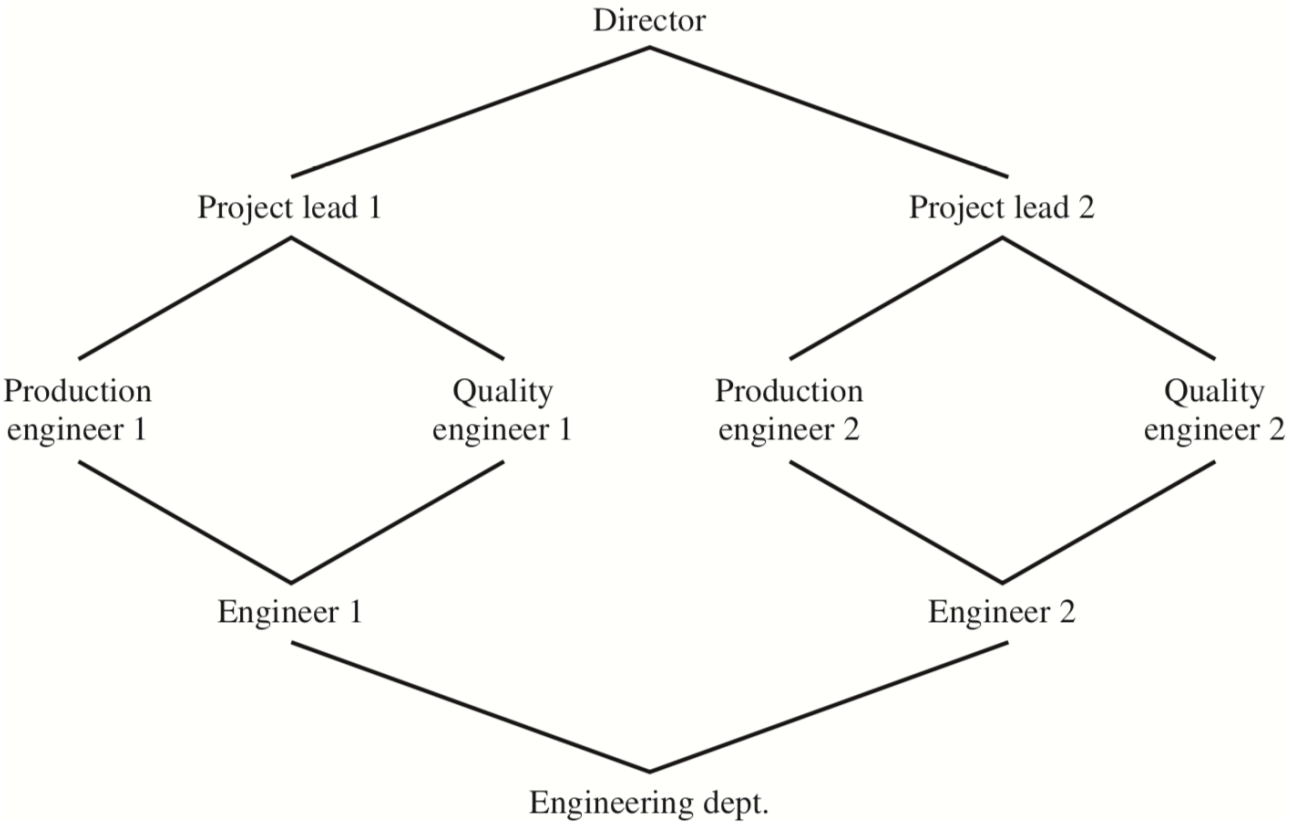
RBAC-0 – Base Model



RBAC-1 – Role Hierarchies

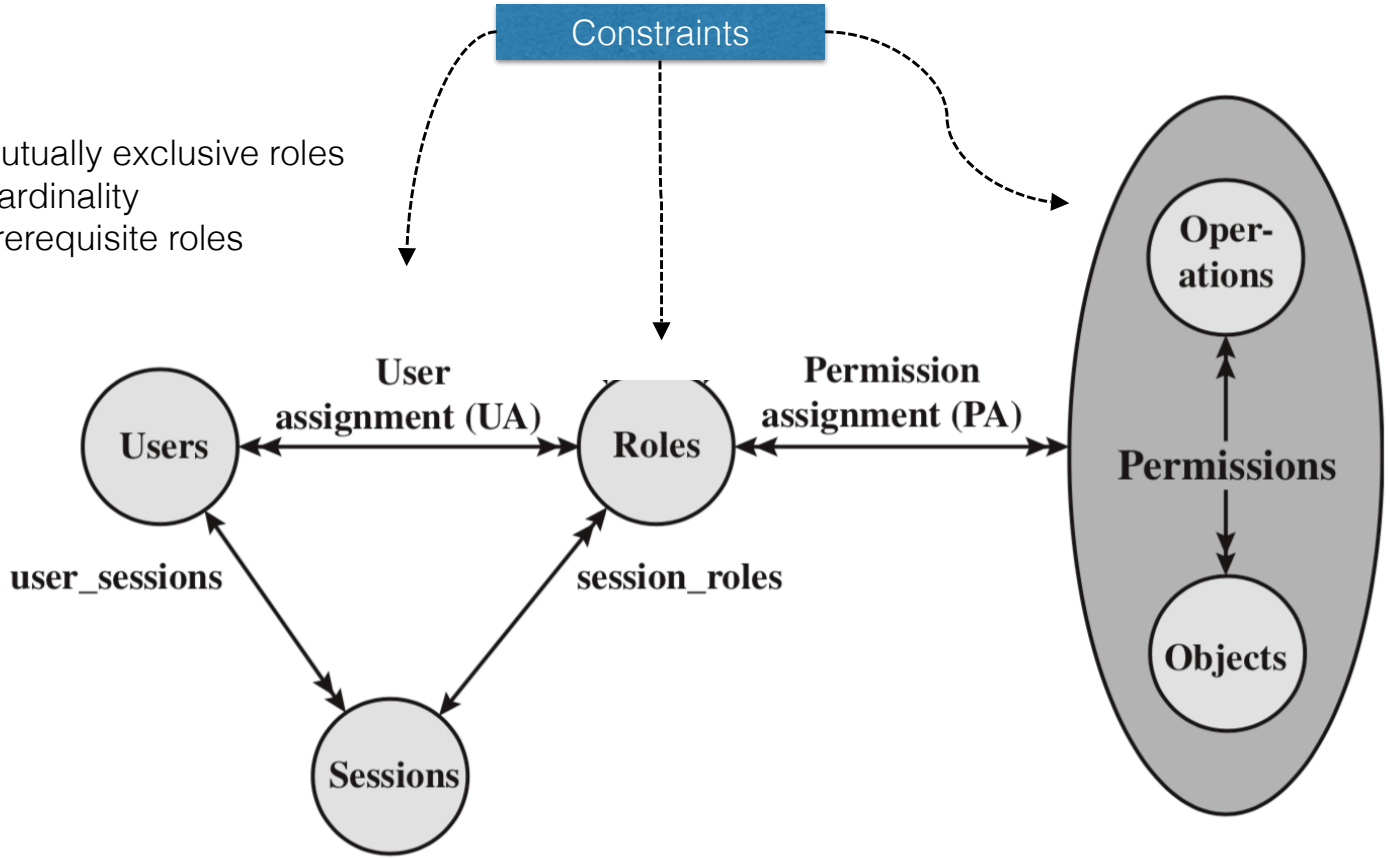


Example Role Hierarchy

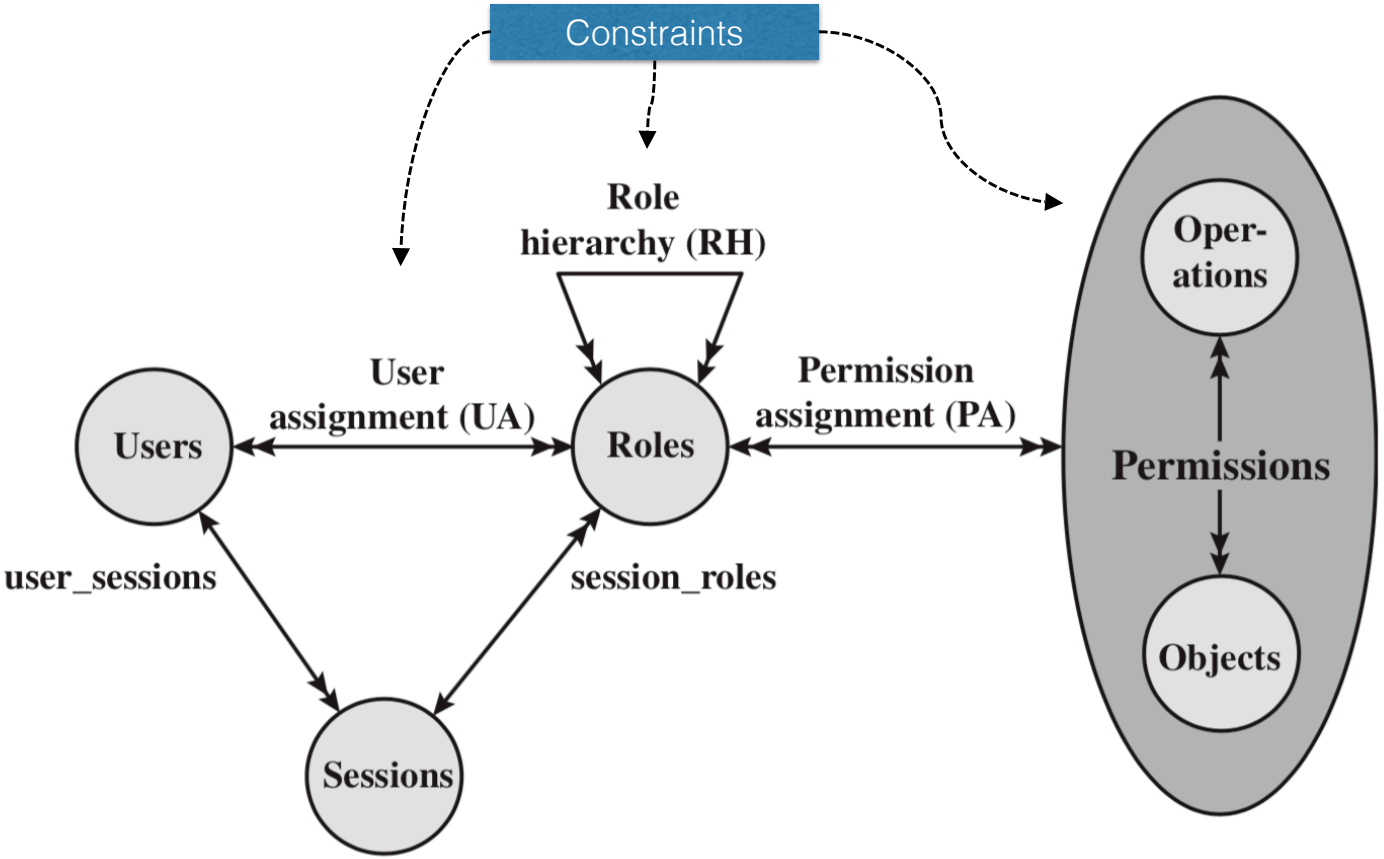


RBAC-2 - Constraints

- Mutually exclusive roles
- Cardinality
- Prerequisite roles



RBAC-3 - Consolidated



Many DBMS support RBAC-1 or higher

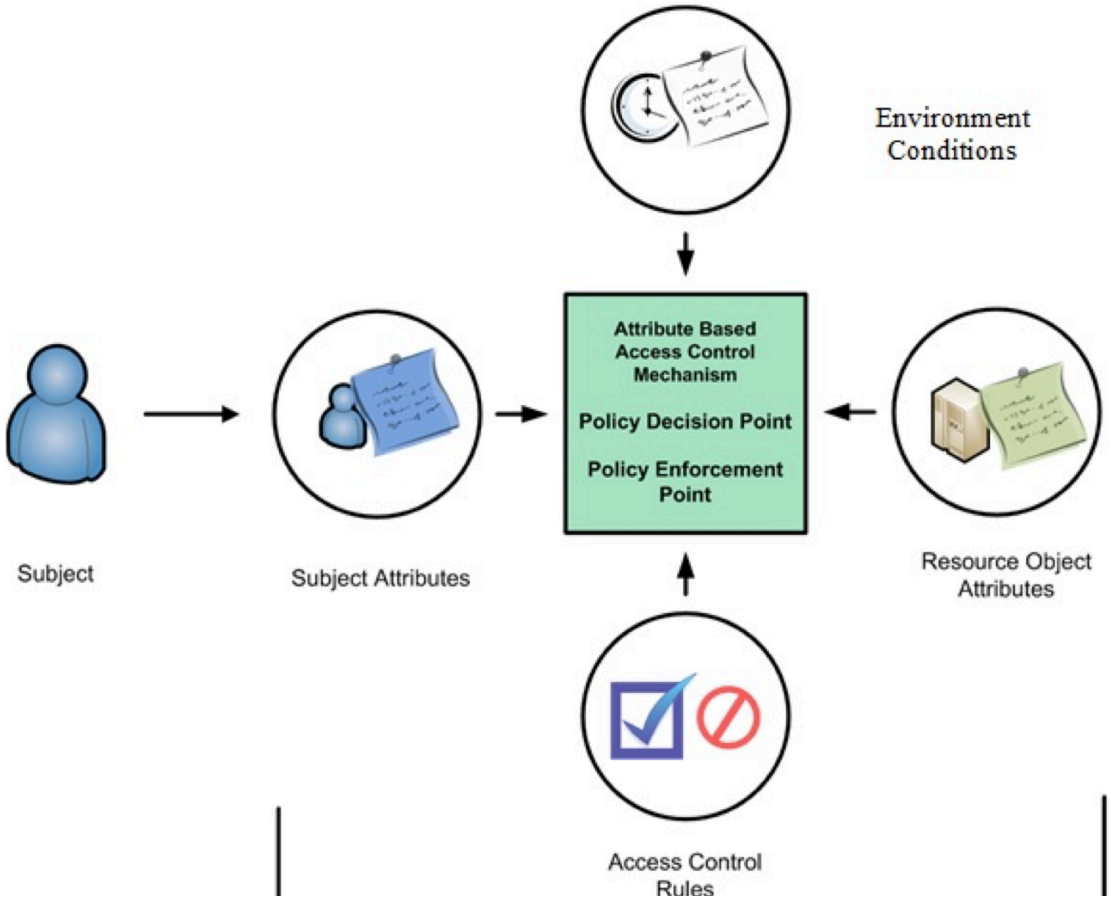
Example for building a role hierarchy:

```
CREATE ROLE DOCTOR
CREATE ROLE SPECIALIST
CREATE ROLE SURGEON

GRANT ROLE DOCTOR TO ROLE SPECIALIST

GRANT ROLE SPECIALIST TO ROLE SURGEON
```

University of Victoria

ABAC (better than RBAC)

generalizes RBAC to consider any attribute around the user (incl. role) and the context of the access



OKERA

ABAC extensions to SQL (example)

```
GRANT SELECT ON database `sales`
HAVING ATTRIBUTE NOT security.pii
TO ROLE analyst_role;
```

security: pii

uid	dob	gender	ccn
0001BDD9-EABF-4D0D-81BD-D9EABFCD0D7D	8-Apr-84	F	3771-2680-8616-9487
00071AA7-86D2-4EB9-871A-A786D27EB9BA	7-Feb-88	F	4539-9934-1924-5730
00071B7D-31AF-4D85-871B-7D31AFFD852E	22-Oct-64	F	5580-7529-3663-6698
0007967E-F188-4598-9C7C-E64390482CFB	1-Jun-66	M	6011-0440-7310-9221
000B90B2-92DC-4A7A-8B90-B292DC9A7A71	13-Jun-84	M	4532-7129-7160-3161
000C1856-994E-476B-8C18-56994E676B29	29-Dec-80	U	5580-5755-3897-8619
000F36E5-9891-4098-9B69-CEE78483B653	24-Mar-85	F	6011-0414-4078-1409
00102F3F-061C-4212-9F91-1254F9D6E39F	1-Nov-91	F	5137-5136-5053-5814
0010C6F2-8C04-450E-90C6-F28C04B50E97	20-Jun-02	U	3488-9280-3164-7164
0011C945-28C4-4D6F-B1E6-6CA7EFC14548	13-Nov-87	F	6011-7819-5600-4729

admin

uid	dob	ccn
0001BDD9-EABF-4D0D-81BD-D9EABFCD0D7D	8-Apr-84	3771-2680-8616-9487
00071AA7-86D2-4EB9-871A-A786D27EB9BA	7-Feb-88	4539-9934-1924-5730
00071B7D-31AF-4D85-871B-7D31AFFD852E	22-Oct-64	5580-7529-3663-6698
0007967E-F188-4598-9C7C-E64390482CFB	1-Jun-66	6011-0440-7310-9221
000B90B2-92DC-4A7A-8B90-B292DC9A7A71	13-Jun-84	4532-7129-7160-3161
000C1856-994E-476B-8C18-56994E676B29	29-Dec-80	5580-5755-3897-8619
000F36E5-9891-4098-9B69-CEE78483B653	24-Mar-85	6011-0414-4078-1409
00102F3F-061C-4212-9F91-1254F9D6E39F	1-Nov-91	5137-5136-5053-5814
0010C6F2-8C04-450E-90C6-F28C04B50E97	20-Jun-02	3488-9280-3164-7164

analyst

OKERA

ABAC extensions to SQL (example)

```
GRANT SELECT ON DATABASE `sales`
TRANSFORM pii.credit_card WITH mask_ccn()
TO ROLE analyst_role;
```

			pii: credit_card
uid	dob	gender	ccn
0001BDD9-EABF-4D0D-81BD-D9EABFCD0D7D	8-Apr-84	F	3771-2680-8616-9487
00071AA7-86D2-4EB9-871A-A786D27EB9BA	7-Feb-88	F	4539-9934-1924-5730
00071B7D-31AF-4D85-871B-7D31AFFD852E	22-Oct-64	F	5580-7529-3663-6698
0007967E-F188-4598-9C7C-E64390482CFB	1-Jun-66	M	6011-0440-7310-9221
000B90B2-92DC-4A7A-8B90-B292DC9A7A71	13-Jun-84	M	4532-7129-7160-3161
000C1856-994E-476B-8C18-56994E676B29	29-Dec-80	U	5580-5755-3897-8619
000F36E5-9891-4098-9B69-CEE78483B653	24-Mar-85	F	6011-0414-4078-1409
00102F3F-061C-4212-9F91-1254F9D6E39F	1-Nov-91	F	5137-5136-5053-5814
0010C6F2-8C04-450E-90C6-F28C04B50E97	20-Jun-02	U	3488-9280-3164-7164

admin view

uid	dob	gender	ccn
0001BDD9-EABF-4D0D-81BD-D9EABFCD0D7D	8-Apr-84	F	XXXX-XXXX-XXXX-9487
00071AA7-86D2-4EB9-871A-A786D27EB9BA	7-Feb-88	F	XXXX-XXXX-XXXX-5730
00071B7D-31AF-4D85-871B-7D31AFFD852E	22-Oct-64	F	XXXX-XXXX-XXXX-6698
0007967E-F188-4598-9C7C-E64390482CFB	1-Jun-66	M	XXXX-XXXX-XXXX-9221
000B90B2-92DC-4A7A-8B90-B292DC9A7A71	13-Jun-84	M	XXXX-XXXX-XXXX-3161
000C1856-994E-476B-8C18-56994E676B29	29-Dec-80	U	XXXX-XXXX-XXXX-8619
000F36E5-9891-4098-9B69-CEE78483B653	24-Mar-85	F	XXXX-XXXX-XXXX-1409
00102F3F-061C-4212-9F91-1254F9D6E39F	1-Nov-91	F	XXXX-XXXX-XXXX-5814
0010C6F2-8C04-450E-90C6-F28C04B50E97	20-Jun-02	U	XXXX-XXXX-XXXX-7164

analyst

OKERA

ABAC extensions to SQL (example)

```
GRANT SELECT ON TABLE
WHERE sets_intersect(user_attribute('territory'), territory)
TO ROLE analyst_role;
```

country	territory	ipaddress	contactname	dealsize
France	EMEA	180.235.143.173	Annette Roulet	Medium
France	EMEA	180.235.143.173	Annette Roulet	Small
France	EMEA	180.235.143.173	Annette Roulet	Small
Italy	EMEA	12.182.249.120	Paolo Accorti	Large
Italy	EMEA	12.182.249.120	Paolo Accorti	Large
Italy	EMEA	12.182.249.120	Paolo Accorti	Medium
Italy	EMEA	12.182.249.120	Paolo Accorti	Large
Italy	EMEA	12.182.249.120	Paolo Accorti	Small
Italy	EMEA	12.182.249.120	Paolo Accorti	Medium

Summary and Outlook

- Broken access control on top of OWASP Top 10
- Database AC of major importance
- Principle of Least Privilege (when configuring DB)
- SQL standard uses AC language
- IBAC, RBAC, ABAC

- Next class: Inference Control

University of Victoria

Questions?

University of Victoria