



Esri International User Conference | San Diego, CA
Technical Workshops | 14.07.11

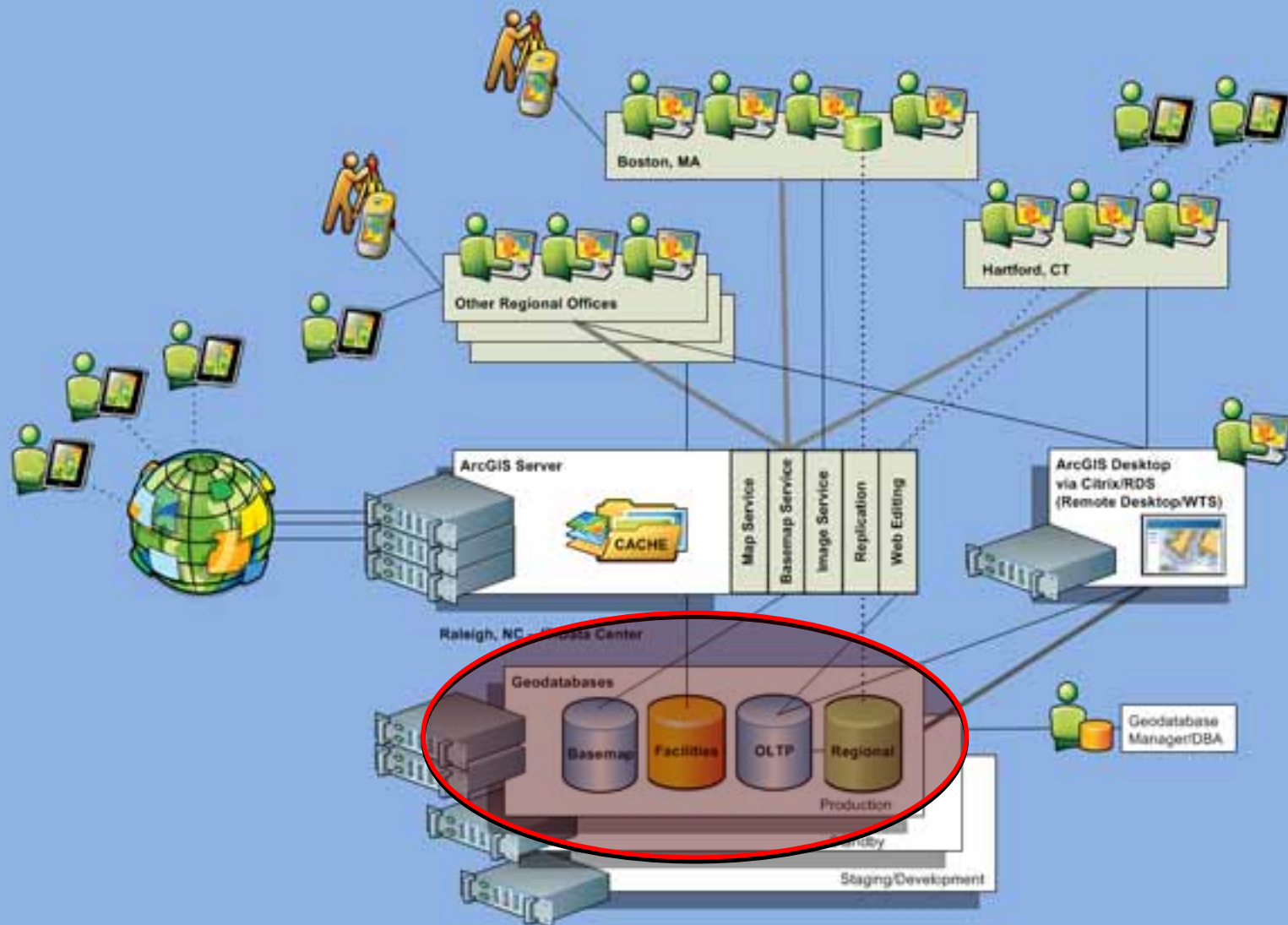
Database Security Tips

Jim McAbee

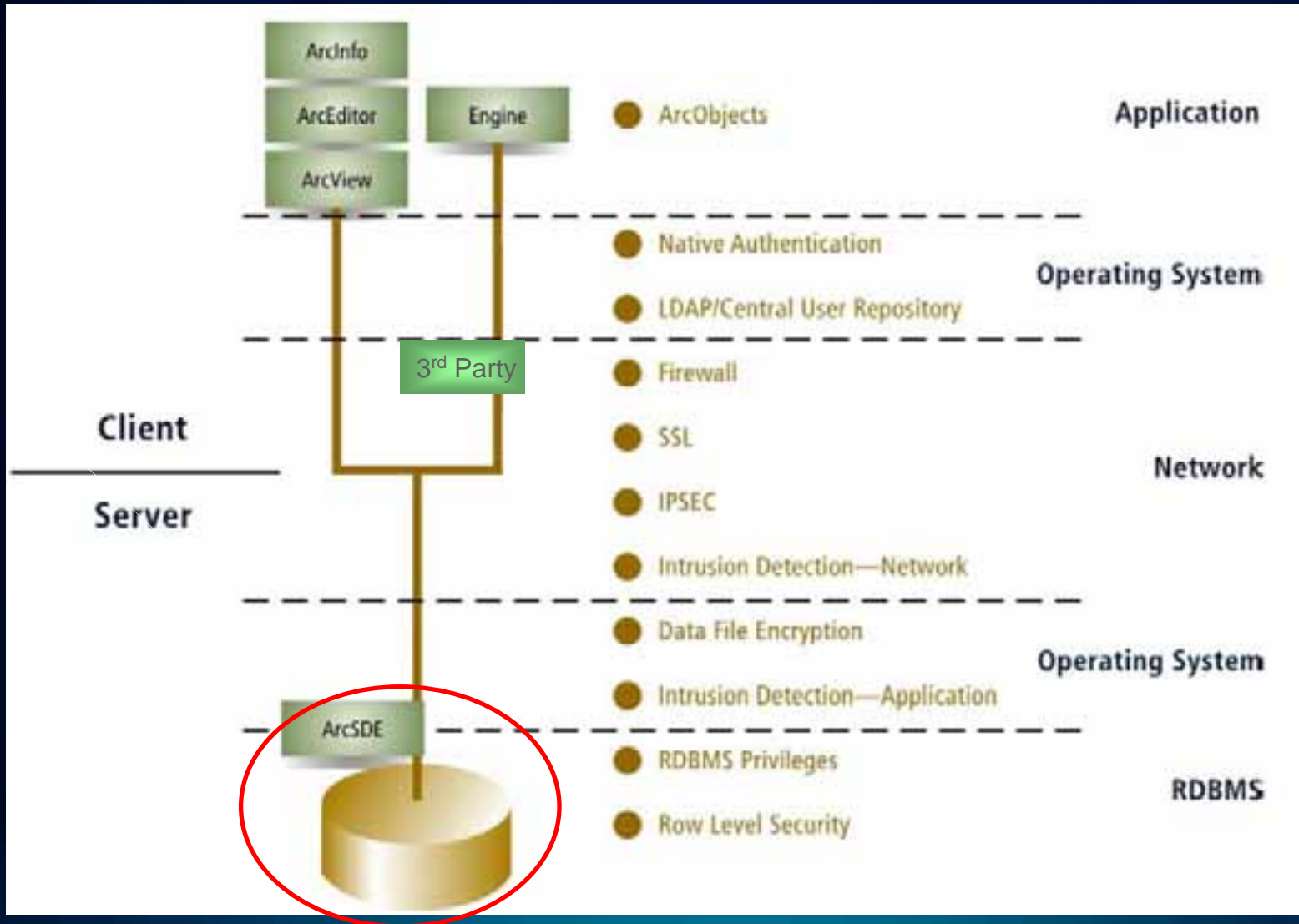
Agenda

- **Geodatabase Security: Users and Roles**
- **Authentication**
- **Authorization and Limiting Access**
- **Geodatabase Security Granularity**

Geodatabase Security



IT Security – Many Levels



Authentication Methods and Authorization

- **Authentication vs. Authorization**

- **Authentication** – “who is allowed in”

“Authentication is the process by which a system verifies a user's identity”

- **Authorization or Privileges** – “what they can do”

“Authorization indicates which database operations that user can perform, and which data objects that user can access and/or manipulate.”

- **Authentication Methods**

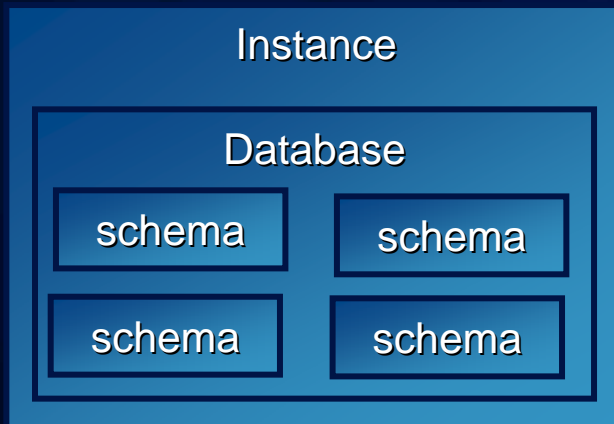
- **Database**
- **External** – Local OS, Domain, other (e.g. LDAP, etc..)
 - Cross-OS possible typically but complex

- **Authorization or Privileges**

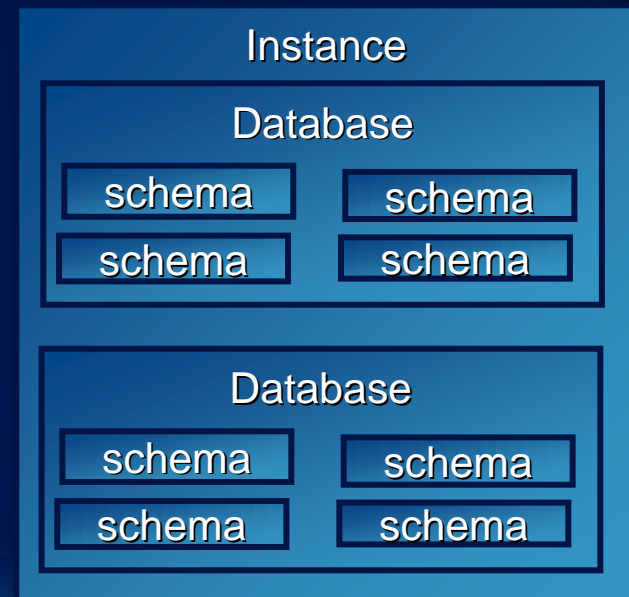
- **Object Creation (DDL – Data Definition)**
- **Object Manipulation (DML – Data Manipulation)**

Database Architecture and Authorization Differences

- Single vs. Multiple Database per Instance Architectures
- Instance vs. Database level privileges and roles



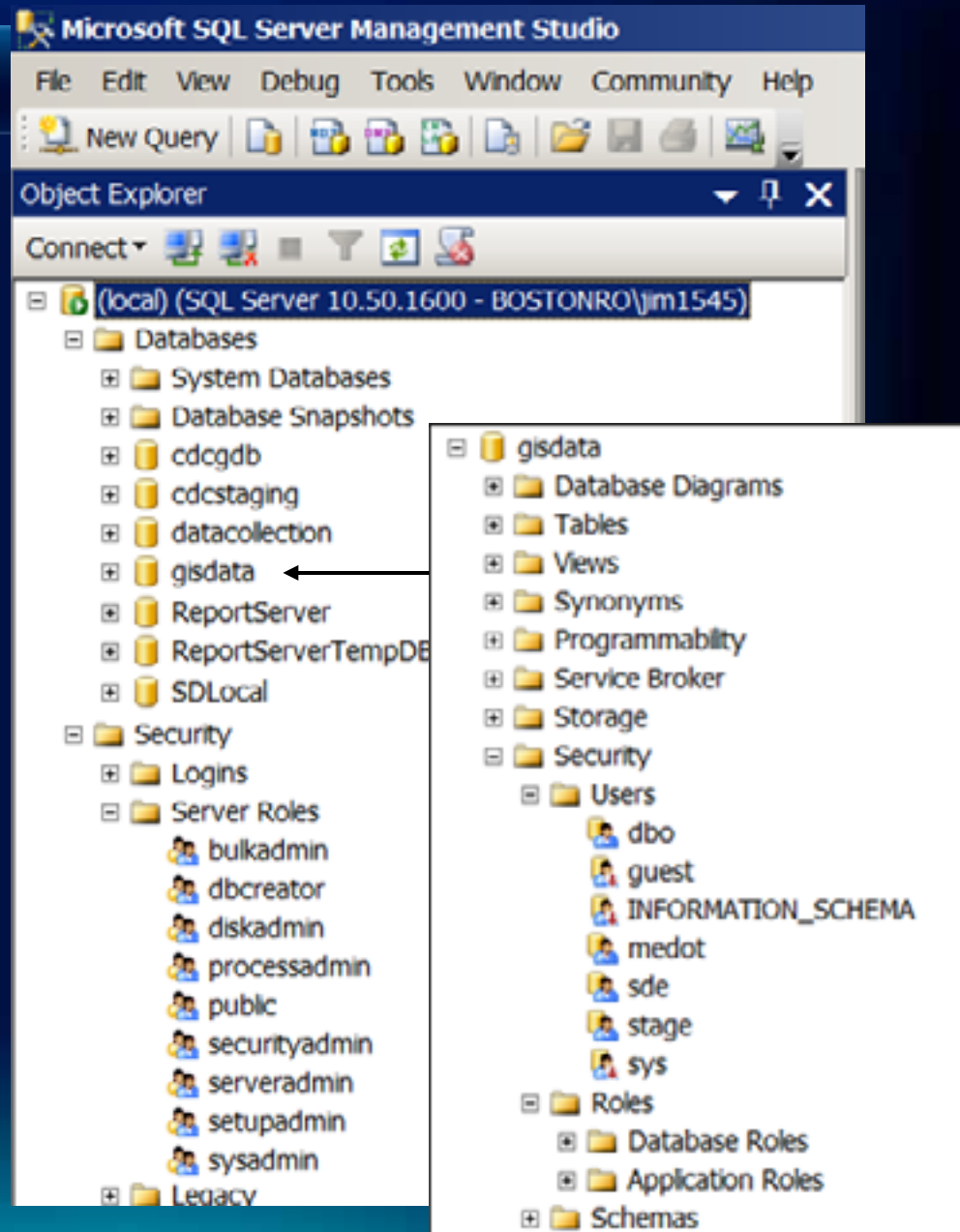
Oracle



SQL Server, DB2, Postgres

Levels of Authorization

- Instance vs. Database level




Few notes on external authentication

- Implementation very database dependent – favored by some, not by others
 - e.g. Oracle - `remote_os_authent = true` – could pose possible security issues allowing other machines an access point if they know user name, thus per Oracle 11gr2 Doc – “*it is poor security practice to use this feature.*”
 - SQL Server – windows or “mixed-mode”
 - DB2 – “*Authentication of a user is completed using a security facility outside of the DB2® database system. The security facility can be part of the operating system or a separate product.*” – DB2 9.7 Documentation
- Be aware of limitations (help.arcgis.com)

A comparison of Windows and database authentication in SQL Server

[Resource Center](#)

Windows authentication is a method for identifying a user with credentials supplied by the Windows operating system (OS) of the user's computer.

 **Tip:** Since Microsoft SQL Server databases only run on Windows operating systems, OS authentication for SQL Server is also referred to as Windows authentication.

Authorization and Policies

ORACLE Enterprise Manager 11g
Database Control

Security

[Users](#)

[Roles](#)

[Profiles](#)

[Audit Settings](#)

[Transparent Data Encryption](#)

[Oracle Label Security](#)

[Virtual Private Database](#)

[Application Contexts](#)

[Database Vault](#)

ORACLE Enterprise Manager
Database Control

[Database Instance: orcl](#) > [Users](#) >

Edit User: GISDATA

General

Name **GISDATA**

Profile **DEFAULT**

Authentication **Password**

* Enter Password *****

* Confirm Password *****

For Password choice, the role is authorized via password.

☐ Expire Password now

Default Tablespace **GISDATA**

Temporary Tablespace **TEMP**

Status ☐ Locked ☒ Unlocked

View User: GISDATA

General

Name **GISDATA**

Profile **DEFAULT**

Authentication **Password**

Default Tablespace **GISDATA**

Temporary Tablespace **TEMP**

Status **UNLOCK**

Default Consumer Group **None**

Roles

Role	Admin Option	Default
No items found		

System Privileges

System Privilege	Admin Option
CREATE INDEXTYPE	N
CREATE OPERATOR	N
CREATE PROCEDURE	N
CREATE SEQUENCE	N
CREATE SESSION	N
CREATE TABLE	N
CREATE TRIGGER	N
CREATE TYPE	N
UNLIMITED TABLESPACE	N

Object Privileges

Object Privilege	Schema	Object	Grant	Option
No items found				

Quotas

Unlimited Tablespace System Privilege granted

General

[Roles](#)

[System Privileges](#)

[Object Privileges](#)

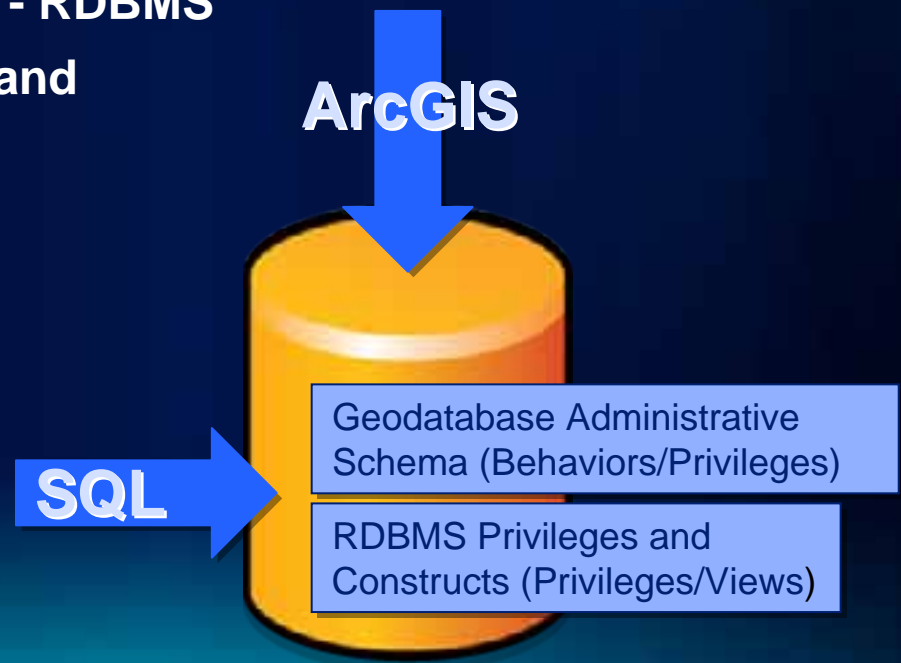
[Quotas](#)

[Consumer Group Privileges](#)

[Proxy Users](#)

Authorization/Privileges

- **DDL vs. DML – Creation vs. Manipulation**
 - Creation – create table, view, trigger, function, etc..
 - Manipulation – select, insert, update, delete
- **Management of by Database vs. Geodatabase**
 - Feature Classes and Tables - RDBMS
 - Feature Datasets, Versions and Behaviors – ArcGIS



Users - Considerations

- **User Types**
 - System
 - General vs. Specific (“head-less” vs. employee)
 - Editor, Viewer (service specific?), Departmental, Operations, etc....
- **System Roles**
 - Public
 - other
- **Locked/Unlocked accounts**
 - inactivity
- **Password Timeout**
 - automatic
 - organization policy
- **User or Role based resource management**
 - space, cpu, etc...

Other Database Level Security methods

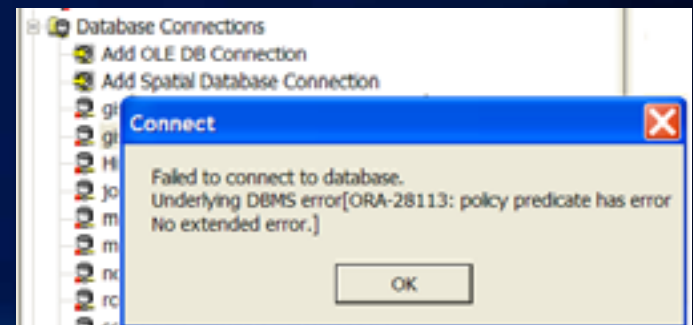
- **Row Level Security**
- **Views and Procedures**

View based RLS

- **Database implementation or custom (attribute)**
- **Do not confuse with some database specific row level security implementations.**
- **Geodatabase features are synonymous with RDBMS rows**
- **Feature level security is based on the concept of adding a column to a table that assigns a sensitivity level for that particular row.**
- **Simple Feature Classes/Layers**
- **Versioned Feature Classes require more customization (A and D tables)**

Row-Level Security in Oracle

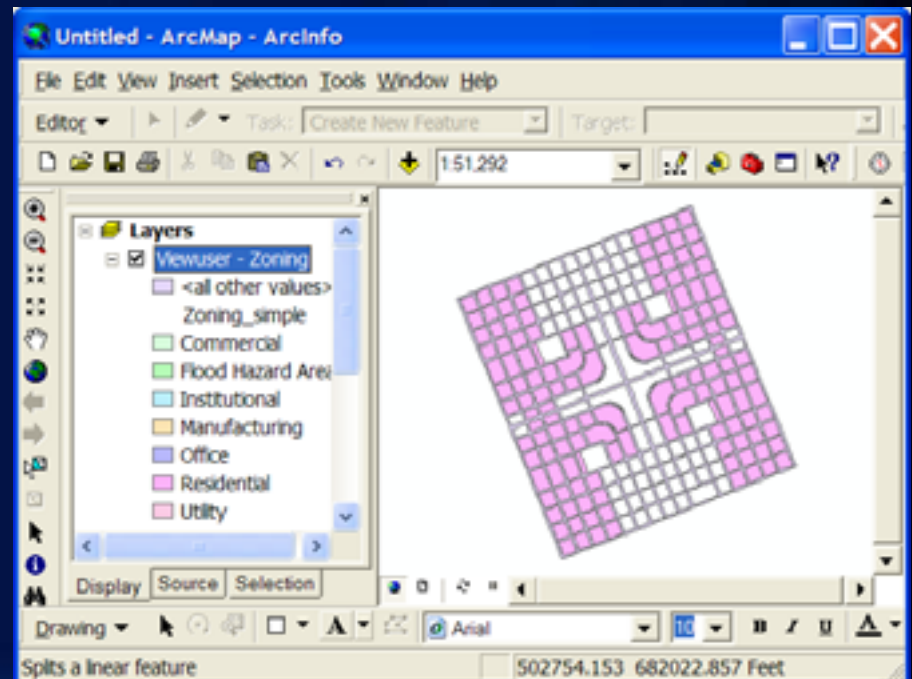
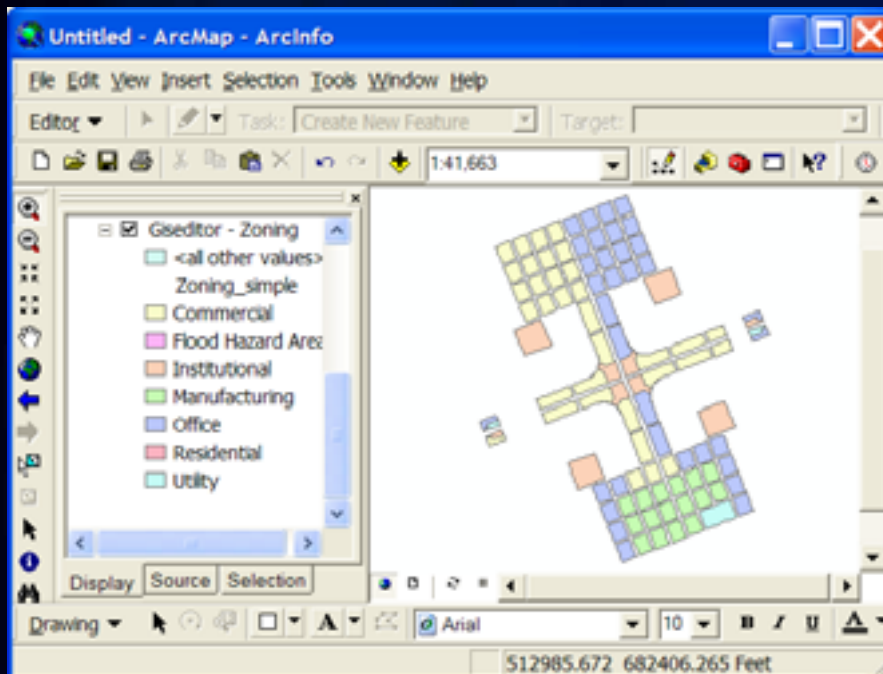
- **Terminology**
 - VPD (Virtual Private Database)
 - Fine-Grained Access Control (FGAC)
 - Oracle Label Security
- **Dynamic predicate for a table or view is generated by a PL/SQL function associated with a security policy through the DBMS_RLS package.**
- **Requires selective and careful implementation**
- **Recommended use on simple feature classes**
- **Not formally supported**
- **v\$vpd_policy, sys.rls\$ to view existing policies**



Row Level Security in Oracle

Limiting access to feature attributes

- Policy determines what features users can query
- Behavior may or may not be desired behavior (e.g. all zoning types shown in TOC)



```
dbms_ols.add_policy('giseditor','zoning','accesscontrol_zoning','sec_admin','f_policy_zoning',policy_type => dbms_ols.context_sensitive);
```


Security Tips and Tricks - Users

- **Setup Data Owners as “Head-less” organizational users**
 - type of data, departmental, application
- **Consider generic read-only/viewing users for various services or groups of services**
 - can allow for finer granularity of load and performance monitoring within database if all services are on same servers
 - can also allow for finer granularity of auditing if that is desired
- **Consider enhancing workflow enforcement through implementation of Workflow Manager (JTX)**

Thank You

<http://www.esri.com/sessionevals>



Database Origins

