

IBM Chat with Lab for Greater China Group

- **Executive introduction**

 - [Sal Vella](#), Vice President, Development, Distributed Data Servers and Data Warehousing

- **Presentation: Technical Introduction to DB2 Security**

 - [Yu-Ping Ding](#), Developer, DB2 LUW Security Development

 - [Walid Rjaibi](#), STSM, Chief Security Architect for DB2 LUW

- **Host:** [Frank Ning](#), Manager, DB2 LUW Install and Up/Running Development

Executive Introduction



Sal Vella

Vice President, Development, Distributed Data Servers
and Data Warehousing

IBM Software Group

Technical Introduction to DB2 Security

- Chat with Lab for the Greater China Group

Agenda

1. Refresh your understanding of DB2 9.5 Security
2. Learn how to vest security administration and database administration into two non overlapping roles
3. Learn how to prevent database administrators from accessing table data
4. Learn how to avoid granting users more privileges than what they need to perform their job tasks
5. Learn how to configure DB2 SSL to ensure the confidentiality and integrity of your data communications
6. Learn how to make a successful transition to the DB2 9.7 authorization model.

***The bigger Security picture:
Putting things into context***

The IBM Security Framework

- Securing a business process requires controls to manage risk across all IT security domains:
 - **Data and Information:** Protect critical data in transit or at rest across the lifecycle
 - **Systems Infrastructure:** Stay ahead of emerging threats across system components
 - **Applications:** Ensure Application and Business Services security
 - **Identity:** Assure the right people have access to the right assets at the right time
 - **Physical Security:** Leverage increasing capability for digital controls to secure events – on people or things – in physical space

- IBM security solutions allow you to manage risk across all IT domains



Database Security Foundations

- Database security requires implementing controls to protect data across its lifecycle
 - **Discovery:** Discovers databases and sensitive data within databases
 - **Vulnerability Assessment:** Ensures the database is configured securely
 - **Authentication:** Validates user identity
 - **Authorization:** Ensures users have the appropriate permissions to access data
 - **Data Masking:** Ensures data is masked out for non authorized users, e.g., when generating test data
 - **Auditing:** Holds users accountable for their actions
 - **Activity Monitoring:** Real-time monitoring of database activities and alerting, e.g., when an anomaly is detected
 - **Encryption:** Keeps data confidential while it is in storage or in transit

- IBM database security solutions allow you to protect data across its lifecycle



Authentication

Authentication Options

- ***Operating System***
 - User validation
 - Group membership

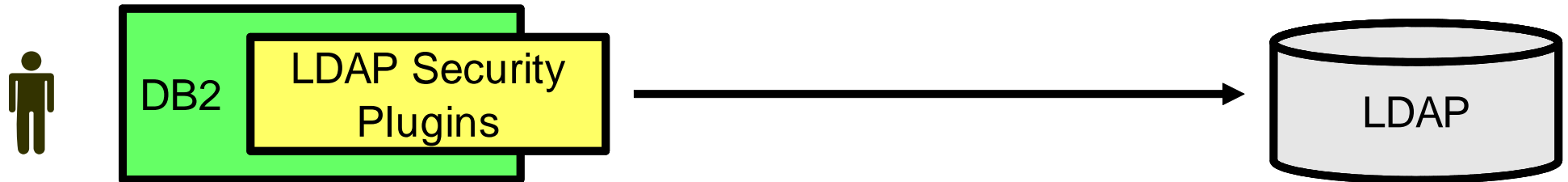
- ***Kerberos***
 - User validation only

- ***LDAP***
 - User validation
 - Group membership
 - Central user and group membership management

- ***Custom Plug-ins***
 - User validation (e.g. GSS API)
 - Group membership

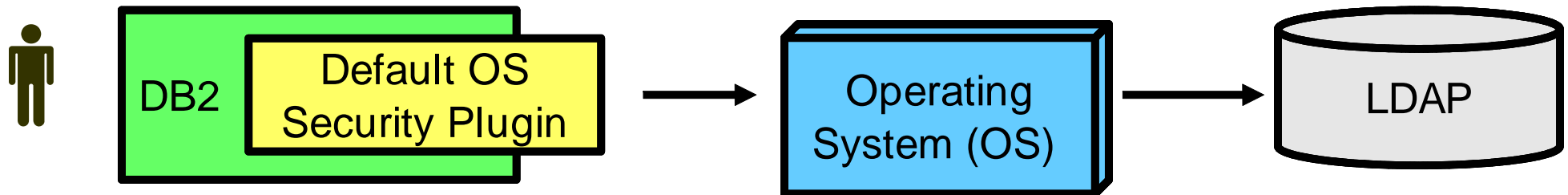
Authentication - LDAP Options

LDAP Security Plug-in Authentication



- Requires separate LDAP configuration
- Requires all users to be defined in LDAP (cannot have some in OS and some in LDAP)

Transparent LDAP Authentication*



- Integrates with existing OS LDAP configurations
- Requires minimal DB2 Configuration (1 Parameter: DB2AUTH=OSAUTHDB)

* Available in DB2 9.7 FP 1 and DB2 9.5 FP5

Authorization

Database Roles

- What is a database role?
 - A database object that may group together one or more privileges or database authorities, and may be granted to users, groups, PUBLIC, or other roles

- What are the advantages of database roles?
 - Simplification of the administration and management of privileges in a database

- When do roles take effect?
 - All the roles assigned to a user are enabled when that user establishes a connection
 - All the privileges and database authorities associated with those roles are taken into account when DB2 checks for authorization

Database Roles (Cont.)

- What can be granted to a role?
 - LBAC security labels and exemptions
 - All database privileges
 - All database authorities

- Role membership
 - Managed by SECADM and could be delegated to others using the WITH ADMIN option on role

LBAC: Row Level Authorization

president Results	
SALES_AMT	REGION
10000.50	North
12500.00	North
11100.00	West
13000.75	West
14750.50	North

n_salesmgr Results	
SALES_AMT	REGION
10000.50	North
12500.00	North
14750.50	North

e_salesmgr Results	
SALES_AMT	REGION



president (EXECS)



n_salesmgr (N_MGR)



e_salesmgr (E_MGR)

CORP.SALES Table (LBAC protected table)		
SALES_AMT	REGION	SECLABEL
10000.50	North	N_SREP
12500.00	North	N_SREP
11100.00	West	W_SREP
13000.75	West	W_SREP
14750.50	North	N_SREP


**SELECT sales_amt, region
FROM corp.sales**

LBAC: Row Level Authorization (Cont.)

➤ *When to use LBAC for row level authorization?*


- Government applications that manage classified information (intelligence, defense, etc.)
- Non government applications where:
 - Data classification is known
 - Data classification can be represented by one or more LBAC security label components
 - Authorization rules can be mapped to the security label component rules
 - If any of the above is not possible, then views are a better alternative for row level authorization.

LBAC: Column Level Authorization




hrstaff_member1 (CONFIDENTIAL)

hrstaff_member1 Results						
NAME	GENDER	DEPT_ID	PHONE	SSN	SALARY	BONUS
Paul, Nola	M	A01	91212	111-22-3333	82500.00	8500.00
Bird, Paul	F	B02	93434	222-33-4444	86000.00	7000.00
Zuzarte, Calisto	M	C03	95656	333-44-5555	89700.00	9200.00



manager1 (CLASSIFIED)

manager1 Results					
NAME	GENDER	DEPT_ID	PHONE	SALARY	BONUS
Paul, Nola	M	A01	91212	82500.00	8500.00
Bird, Paul	F	B02	93434	86000.00	7000.00
Zuzarte, Calisto	M	C03	95656	89700.00	9200.00



worker1 (UNCLASSIFIED)

worker1 Results			
NAME	GENDER	DEPT_ID	PHONE
Paul, Nola	M	A01	91212
Bird, Paul	F	B02	93434
Zuzarte, Calisto	M	C03	95656

LBAC: Column Level Authorization (Cont.)

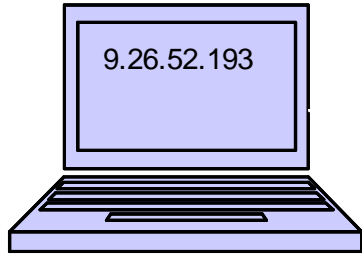
➤ *When to use LBAC for column level authorization?*

- Control access to a sensitive column (e.g., social security number, credit card number, etc.)
- Protect the data in the table from access by table owner, or DBAs
 - Assign a security label to all columns in the table
 - Assign that security label to a role
 - Assign that role to all users who need access to the table
 - Only users members in that role will be able to access data in that table

Trusted Contexts

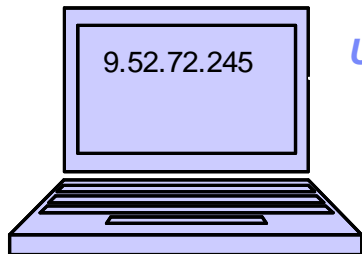
- A specification of a trust relationship between the database and an external application
- A connection that matches a trust relationship is called a trusted connection. There are 2 types:
 - An implicit trusted connection
 - An explicit trusted connection
- An implicit trusted connection allows a user to inherit a role that is not available to them outside the scope of that trusted connection
 - Allows customers to gain more control on when a privilege or an authority can be exercised by a user

Conditional Authorization Via Trusted Contexts



User: Miller

User Miller acquires the DBA role



User: Miller

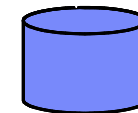
User Miller does not acquire the DBA role

DB2 Database

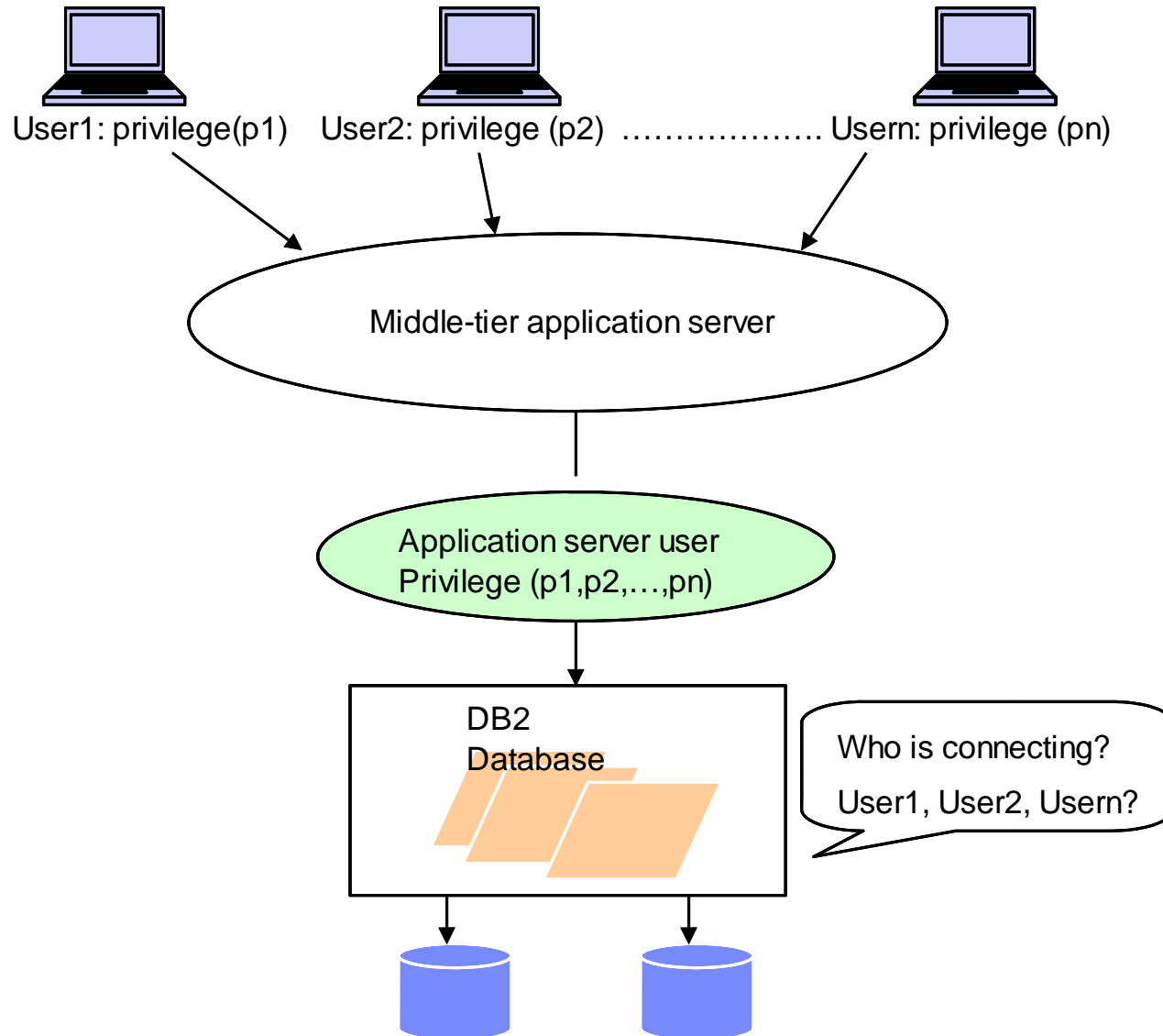
```
CREATE ROLE DBA

GRANT DBADM ON DATABASE TO ROLE DBA

CREATE TRUSTED CTX1 BASED UPON CONNECTION
USING SYSTEM AUTHID MILLER
ATTRIBUTES (ADDRESS 9.26.52.193)
DEFAULT ROLE DBA
```



Identity Propagation Challenges In Application Servers (Cont.)

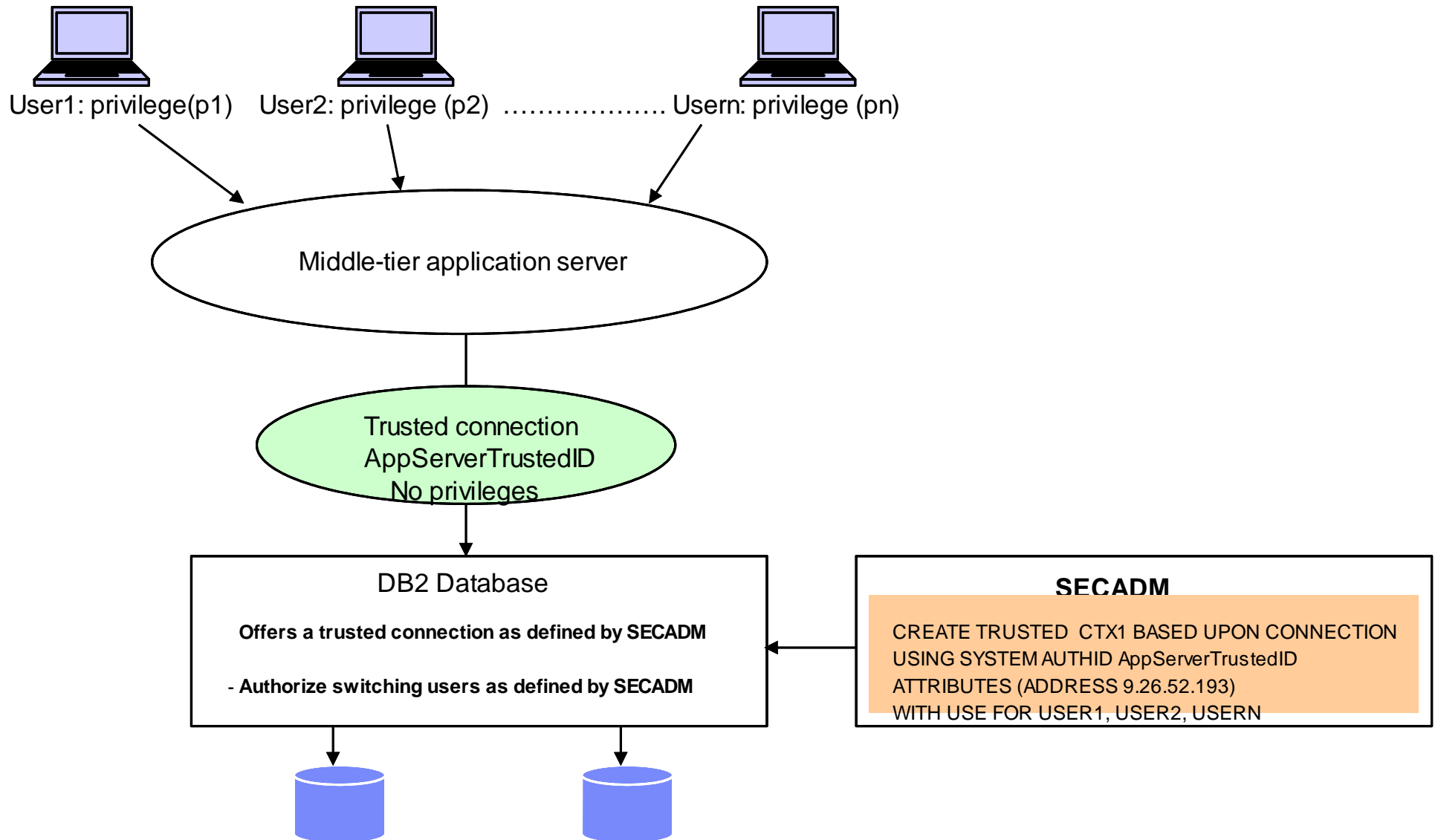


Trusted Contexts (Cont.)

- An explicit trusted connection allows a user to switch the current user on the connection
 - The user IDs to switch to are defined by the SECADM
 - Switching can optionally require authentication

- An application server uses a trusted connection to change the user id of the connection without re-authenticating the new user at the database

Application Servers With Trusted Contexts



Auditing: Native & Guardium

Native Auditing

- **Generates audit records for a series of predefined events**
- **Audit records provide insight on who did what, where, when and how**
 - **Who:** Authorization/User ID tracking
 - **What:** SQL Statement text tracking
 - **Where:** Application and IP address tracking
 - **When:** Event timestamp tracking
 - **How:** Authorization checks tracking



Native Auditing Granularity

- Audit policies can be associated with a number of database objects to control what is audited
 - The database itself
 - Tables
 - Authorities such as SYSADM, DBADM and SECADM
 - Users and groups
 - Roles
 - Trusted Contexts

- This granularity allows a narrowed focus on exactly what needs to be audited
 - Further reduction in amount of data that is logged



Native Auditing Example: Capturing who is accessing your sensitive table

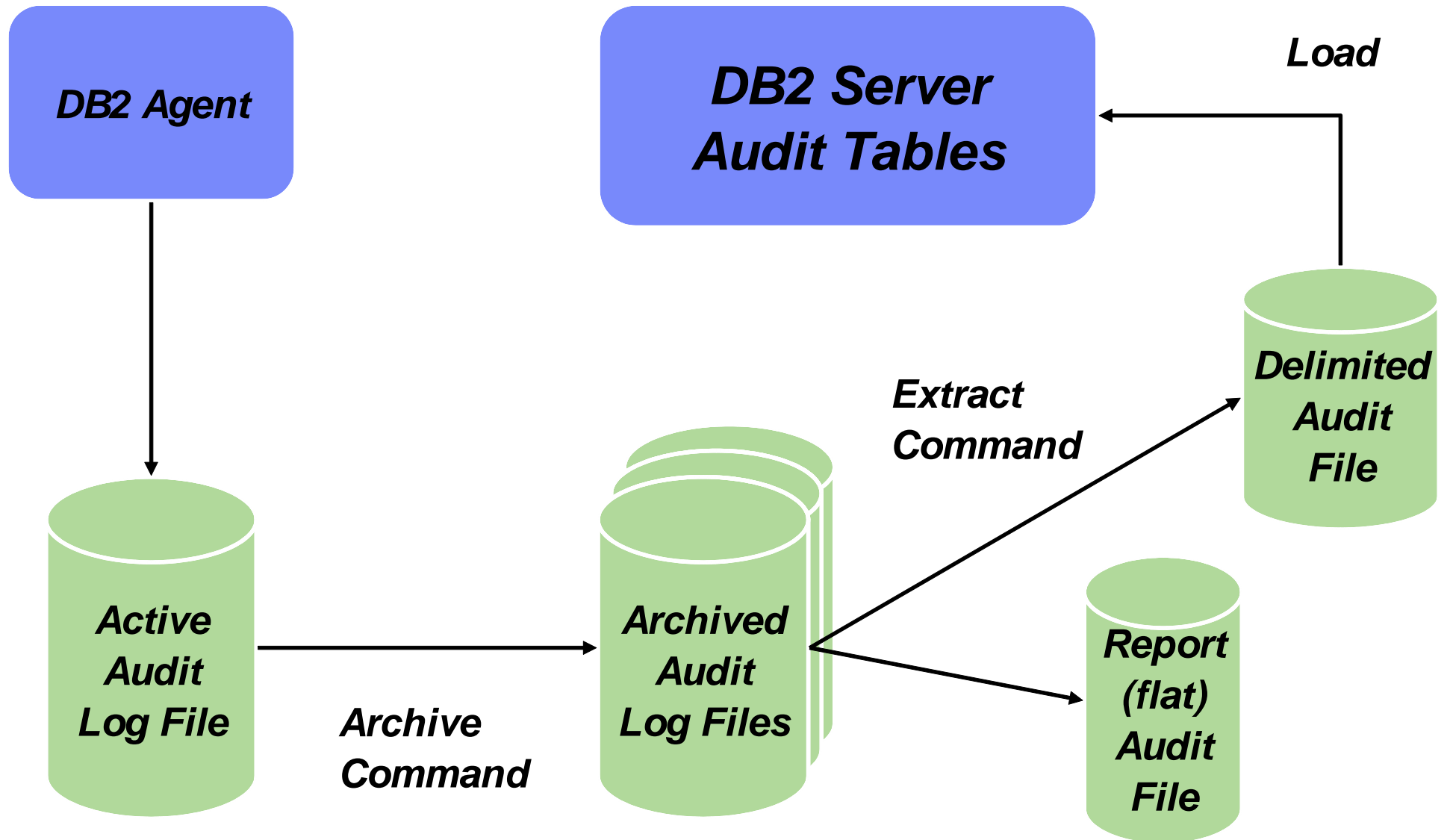
- Create an audit policy that captures EXECUTE audit events

```
CREATE AUDIT POLICY AUDITMYTABLEACCESS  
CATEGORIES EXECUTE STATUS BOTH  
ERROR TYPE AUDIT
```

- Associate the audit policy with the table

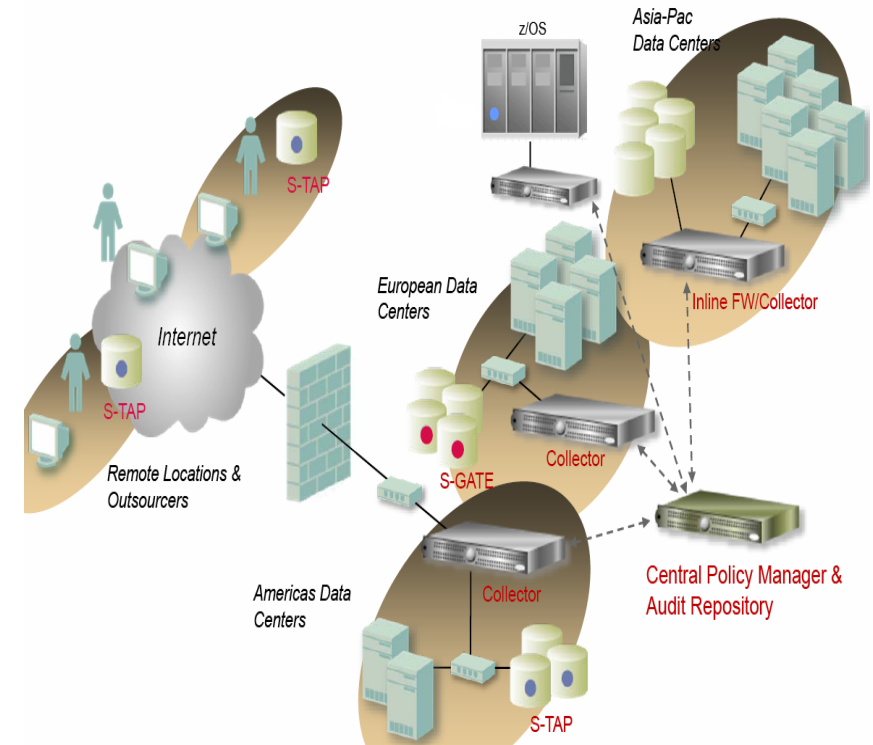
```
AUDIT TABLE MYTABLE  
USING POLICY AUDITMYTABLEACCESS
```

Native Auditing Data Exploitation



Auditing Using IBM Guardium

- Supports heterogeneous database environments – strategic direction
- Central management for all databases (DB2 and other vendors)
- No changes to databases
- Minimal overhead
- Customized reporting
 - **S-TAP**: A lightweight (2-4% server impact), host-based software probe to monitor network and local database traffic
 - **S-GATE**: A host-based agent for blocking unauthorized access to sensitive data by privileged users
 - **Collector**: Collects data from **S-TAP** and performs real-time analyses and creates audit trails to identify unauthorized activities
 - **Central Policy Manager**: Provides single unified set of audit policies, aggregates and normalizes audit information across all DBMS platforms, applications and data centers for enterprise wide compliance reporting



Data In Transit Encryption

Data In Transit Encryption

➤ ***DB2 DRDA encryption***

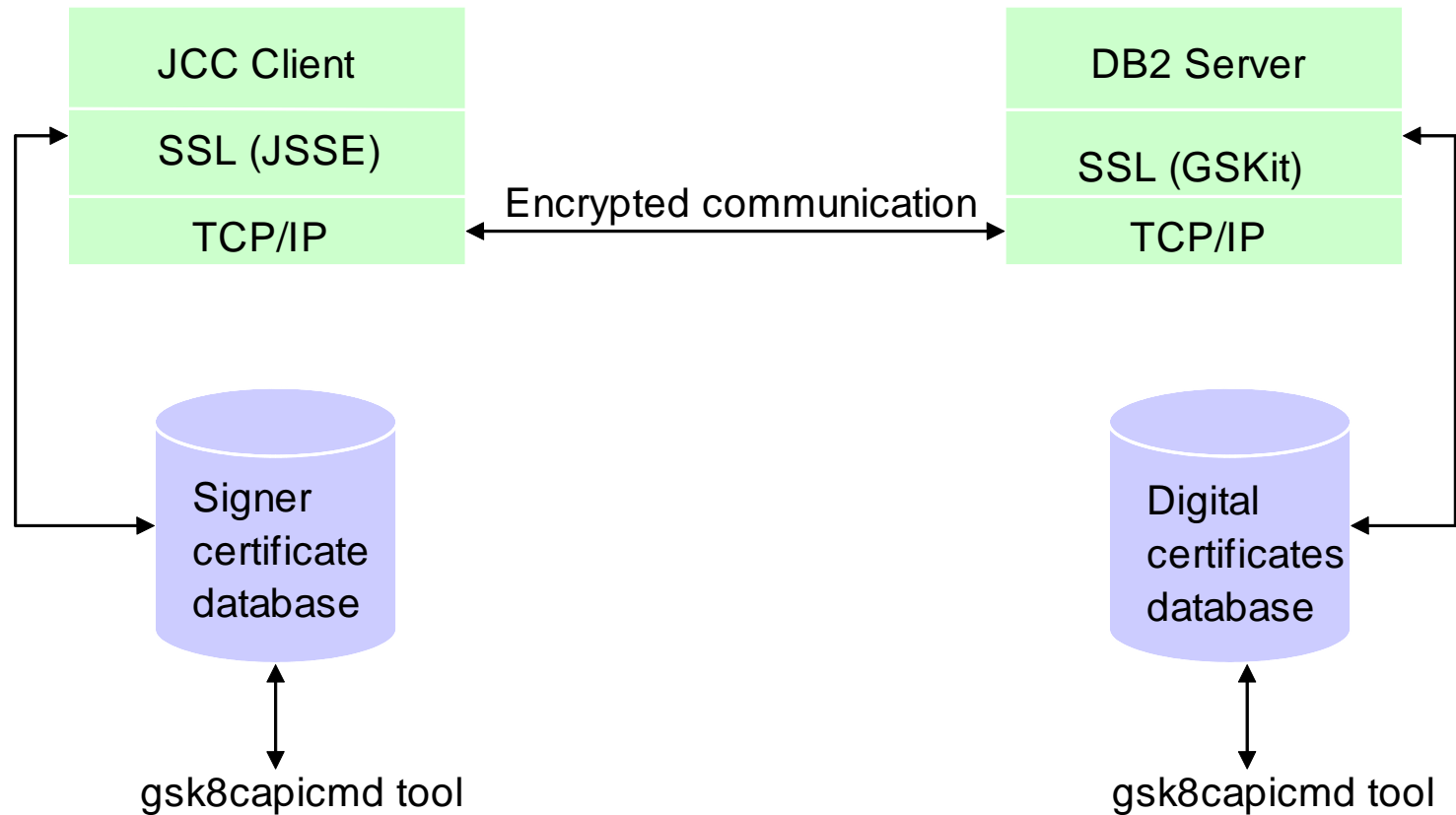
- Legacy
- DES with 56-bit keys
- Does not provide data integrity

➤ ***Secure Socket Level (SSL)***

- Strategic direction
- AES, 3DES with 128-bit (or more) keys
- Provides both data encryption and data integrity

How Does DB2 SSL Work?

JCC Client Example



How Does DB2 SSL Work? (Cont.)

➤ *The SSL handshake*

- Client requests an SSL connection listing its SSL version and supported cipher suites
- Server responds with a selected cipher suite
- Server sends its digital certificate to the client
- Client verifies the validity of the server's certificate (server authentication)
- Client and server securely negotiate a session key
- Client and server securely exchange information using the key selected above

How Does DB2 SSL Work? (Cont.)

➤ *Certificate database configuration*

- Server-side
 - Use the gsk8capicmd tool (comes with GSKit) to create a certificate database
 - Import the server digital certificate you purchased from a certificate authority (CA) into the certificate database
- Client-side
 - Use the gsk8capicmd tool to create a signer certificate database
 - Import the public key of the certificate authority into the certificate database

How Does DB2 SSL Work? (Cont.)

➤ *DB2 server configuration*

- Set the following DBM configuration parameters
 - SSL_SVR_KEYDB: Key database file
 - SSL_SVR_STASH: Stash file
 - SSL_SVCENAME: SSL port
 - SSL_SVR_LABEL: Specific certificate to use
- Optionally, select a ciphers suite
 - SSL_CIPHERSPECS: Allowed ciphers suite
- Enable SSL communication for the instance
 - db2set DB2COMM=SSL or db2set DB2COMM=SSL,TCPIP

How Does DB2 SSL Work? (Cont.)

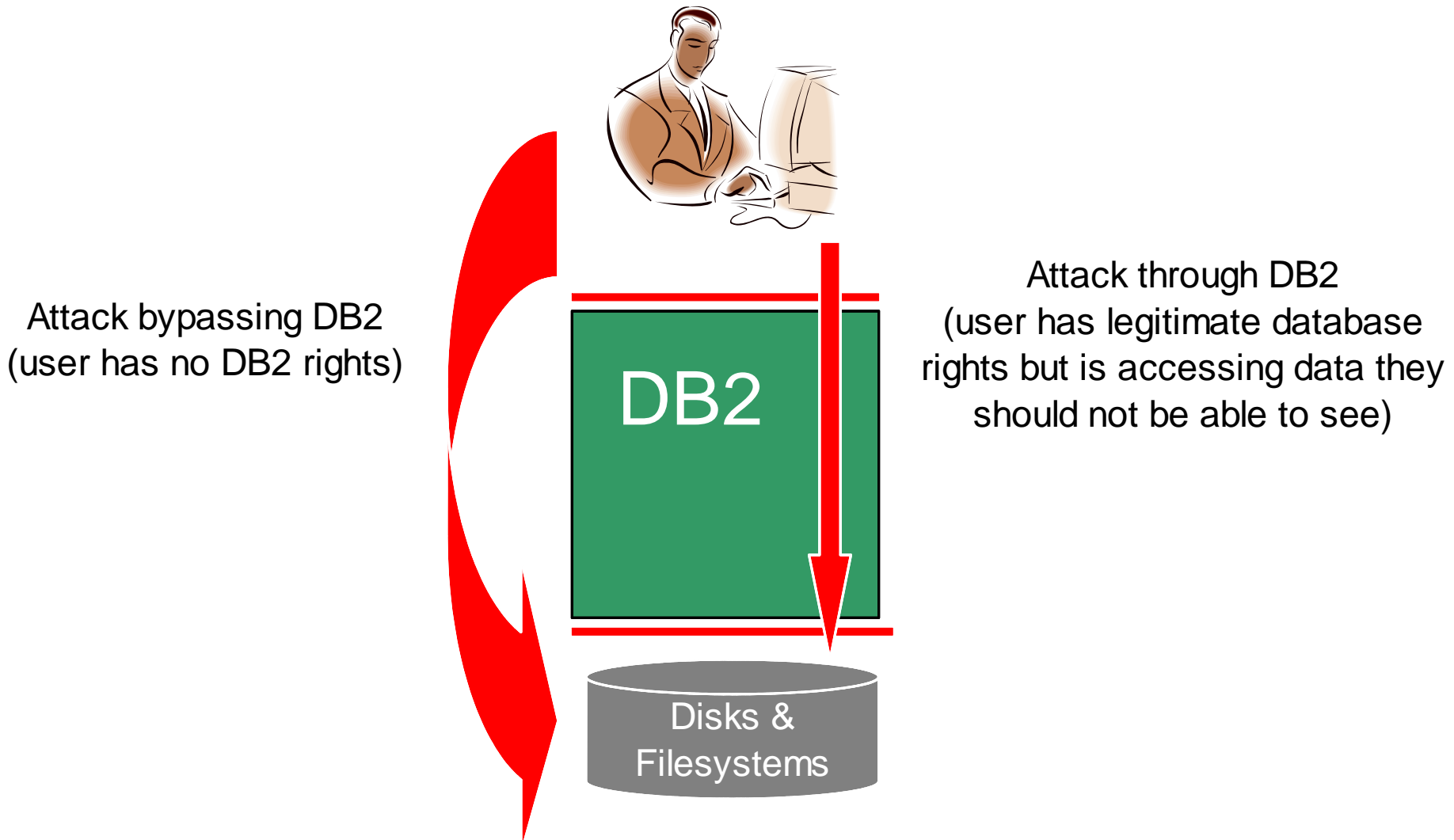
➤ *DB2 client configuration*

Java Example

```
...
properties.put("sslConnection", "true");
System.setProperty("javax.net.ssl.trustStore", "/home/wrjaibi/client.jks");
System.setProperty("javax.net.ssl.trustStorePassword", "xxxxxx");
.....
con = java.sql.DriverManager.getConnection(url, properties);
```

Data At Rest Encryption

Encryption vs. Access Control



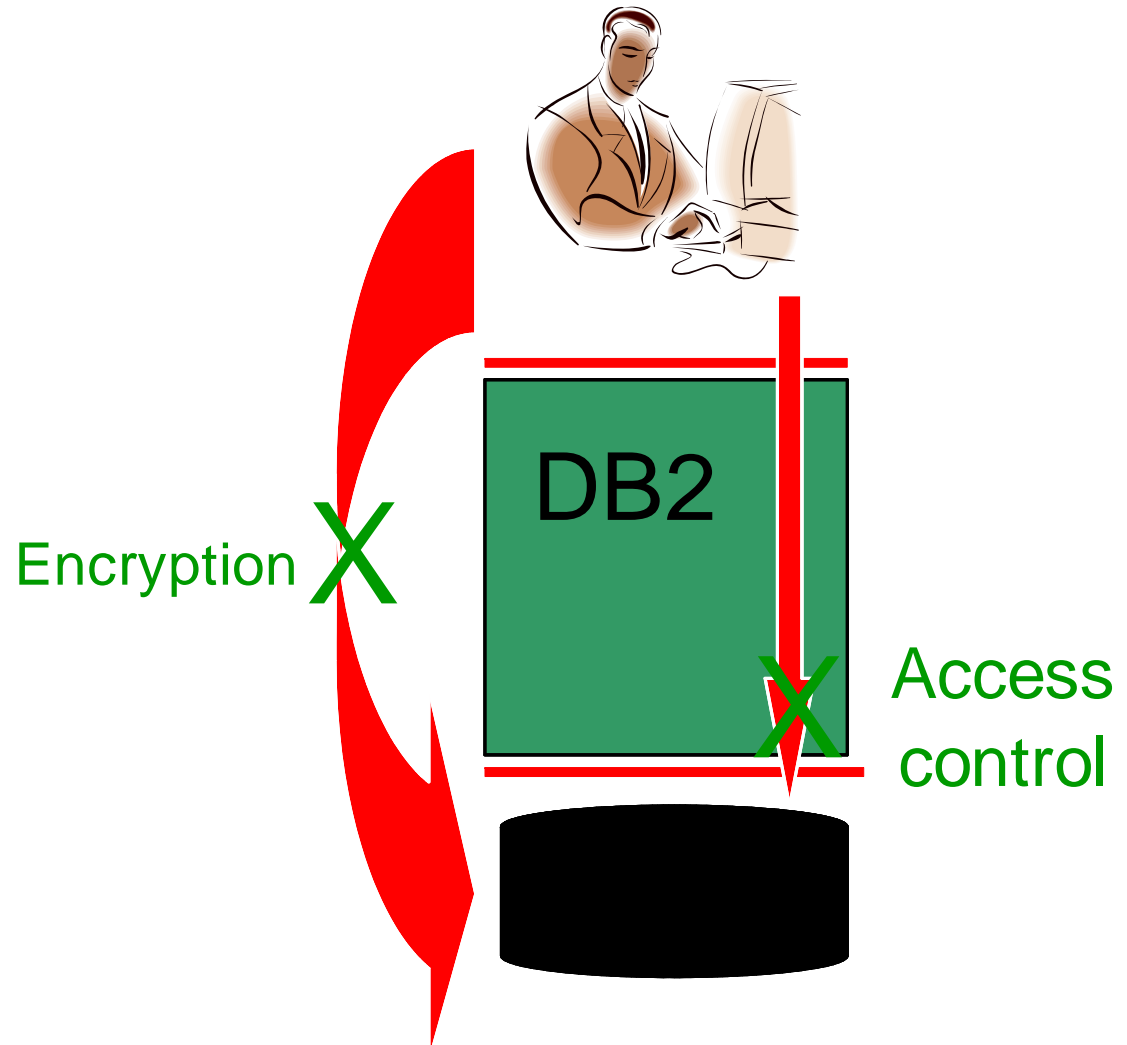
Encryption vs. Access Control (Cont.)

Use DB2 Access Controls for attacks through DB2

- Privileges/authorities
- Views/Packages/Roles
- LBAC/MLS
- Trusted Contexts

Use Encryption for attacks which bypass DB2

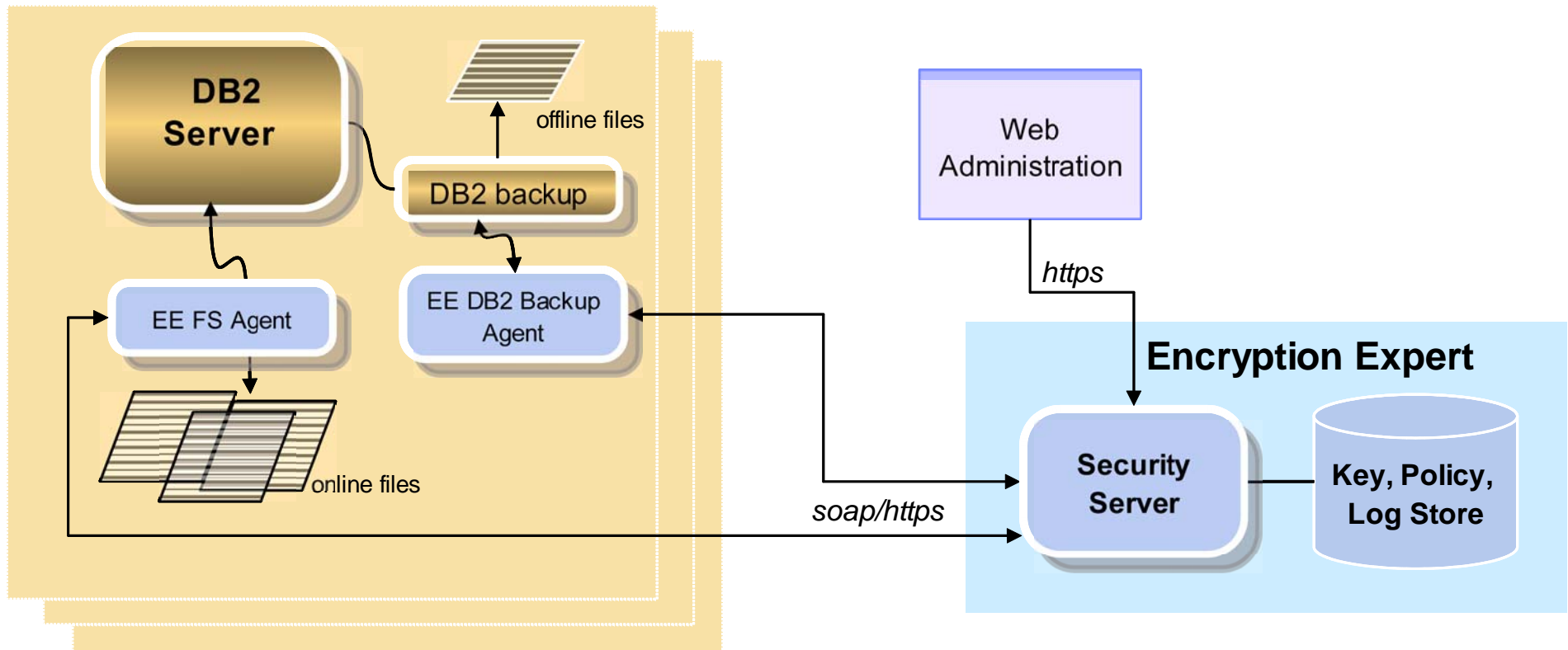
- Stealing DB2 backups
- Directly accessing OS files containing table data



Data At Rest Encryption

- *What are the requirements?*
 - Application transparency
 - Database schema transparency
 - Low performance overhead
 - Protects both on-line and off-line data (e.g. backups)
 - Addresses encryption key management issues

IBM Database Encryption Expert Architecture



■ EE Agents

- Communicates with security server to enforce policy
- Encrypt data

■ Security Server

- Key and Policy Management
- Authenticates agent communication
- Separation of duties

New in 9.7: Separation Of Duties & Least Privilege Concepts

Separation of Duties

- SYSADM no longer includes DBADM
- DBADM no longer includes the ability to do grants and revokes
 - New ACCESSCTRL authority is needed
- SECADM scope has been extended to fully manage security
 - Customers can now vest database administration and security administration into 2 non overlapping roles
 - GRANT DBADM WITHOUT ACCESSCTRL ON DATABASE TO USER JOE
 - GRANT SECADM ON DATABASE TO USER MARY

Least Privilege

- DBADM no longer includes the ability to access data
 - New DATAACCESS authority is needed
 - Customers can now set up a DBADM with no access to data
 - **GRANT DBADM WITHOUT DATAACCESS ON DATABASE TO USER ROB**

- New EXPLAIN privilege to issue EXPLAIN statements
 - No longer forced to grant actual table privileges, which allow data access

- New WLMADM authority to manage WLM objects
 - No longer forced to grant DBADM, which gives other privileges

- New SQLADM authority to perform SQL tuning
 - No longer forced to grant DBADM, which gives other privileges

- EXECUTE privilege is sufficient to run audit log management routines
 - No longer forced to grant SECADM, which gives other privileges

How do these changes affect you?

➤ SYSADM no longer a DBADM

- Any application that relies on the SYSADM being a DBADM may start encountering authorization errors. *Solution?* Grant DBADM to the appropriate SYSADM user
- Authorization errors will not happen for SYSADM users who create a database as they are automatically given DBADM and SECADM on that new database

➤ DBADM no longer includes data access and grant/revoke

- No effect on data access unless you explicitly specify WITHOUT DATAACCESS to remove the ability to access data from DBADM

GRANT DBADM WITHOUT DATAACCESS ON DATABASE TO USER JOE

- No effect on grant/revoke unless you explicitly specify WITHOUT ACCESSCTRL to remove the ability to do grants and revokes from DBADM

GRANT DBADM WITHOUT ACCESSCTRL ON DATABASE TO USER JOE

➤ SYSADM no longer includes the ability to grant DBADM and SECADM

- This ability is now vested in SECADM only

How will migration to 9.7 work?

- DB2 automatically grants DATAACCESS and ACCESSCTRL to every authorization ID that holds DBADM upon migration
- DB2 automatically grants SECADM to the user ID doing the migration if there is no authorization ID of type USER that holds SECADM in the database
- DB2 automatically grants DBADM, DATAACCESS and ACCESSCTRL to the SYSADM group upon migration

Additional Information



■ References:

- <http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp>

■ Feedback

- Presentation format and contents
- Additional DB2 topics you are interested
- Follow on questions for the presentation

■ Contact: fning@ca.ibm.com

Questions

