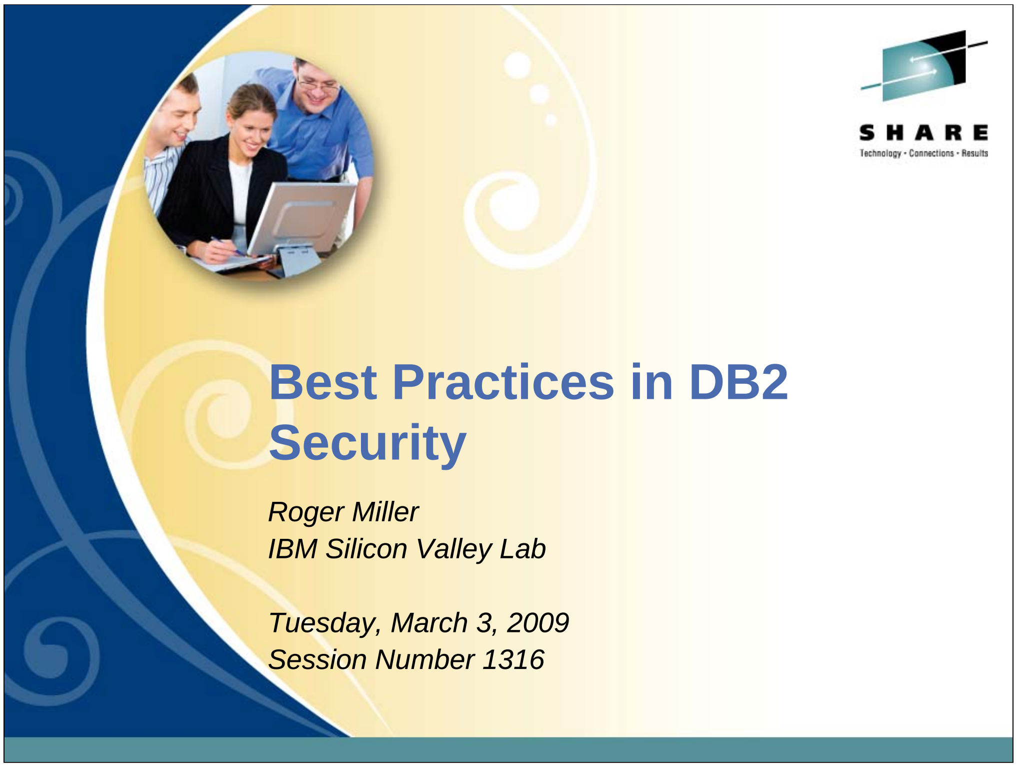


Best Practices in DB2 Security

Roger Miller
IBM Silicon Valley Lab

Tuesday, March 3, 2009
Session Number 1316

Security is in the headlines and growing much more important. This session will discuss various practices for security and discuss how you can make improvements. The discussion includes various security objectives. Most sites have a range of needs and objectives. For some situations, basic security is adequate. For others better or standard security techniques are needed. In other cases, best security practices are demanded. Our tools range from very tight system security to basic techniques, applicable with public information on the web.   Application security techniques are more flexible, but require much more work by more people, so they are generally weaker. Choices and guidelines will be our primary points, discussing how to provide improved security for your situation. The objective is to help customers understand the range of choices for security, the improvements and how to make incremental enhancements.

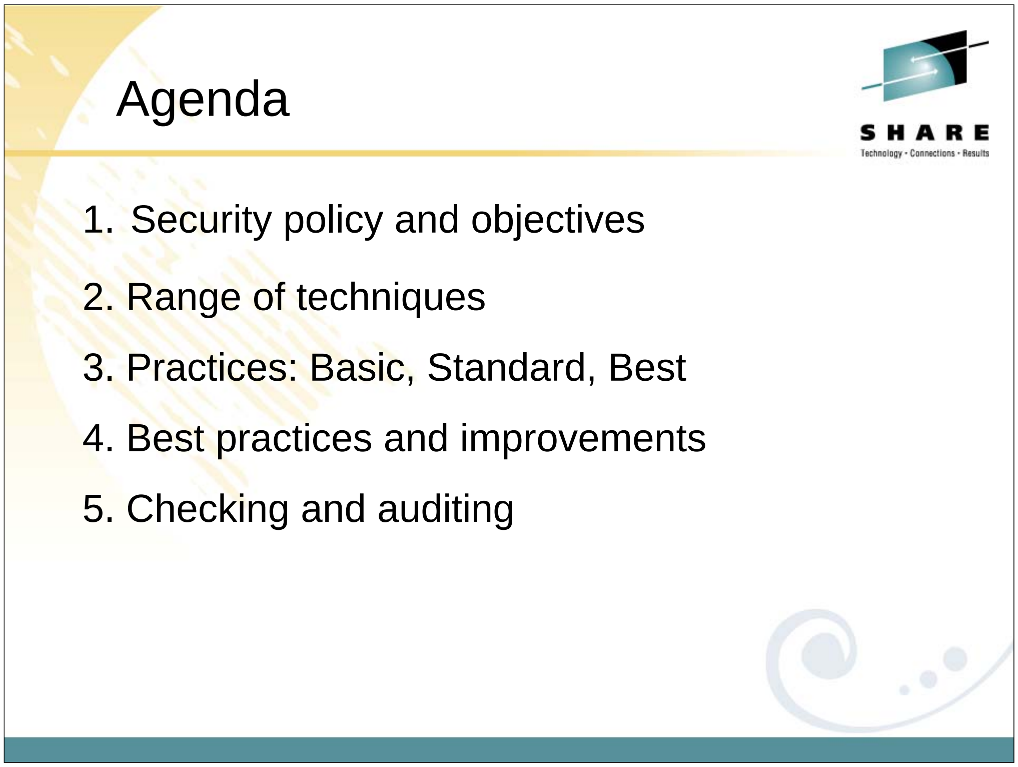
For other details on DB2 for z/OS security, there are many suggested resources, such as the Protect Your Assets presentation:

http://www.ibm.com/support/docview.wss?rs=64&uid=swg27001877

Best practices: http://www.ibm.com/support/docview.wss?uid=swg27007842&aid=1

Library for security:

http://publib.boulder.ibm.com/infocenter/dzichelp/v2r2/topic/com.ibm.db2.doc.admin/bjndmstr124.htm



Agenda

SHARE

Technology • Connections • Results

1. Security policy and objectives
2. Range of techniques
3. Practices: Basic, Standard, Best
4. Best practices and improvements
5. Checking and auditing

This is the agenda for the presentation, beginning with a discussion of possible objectives, then looking through guidelines and techniques, while distinguishing the best practices from other security techniques. We will discuss ways to improve situations that I have seen before and emphasize the need for checking and auditing.

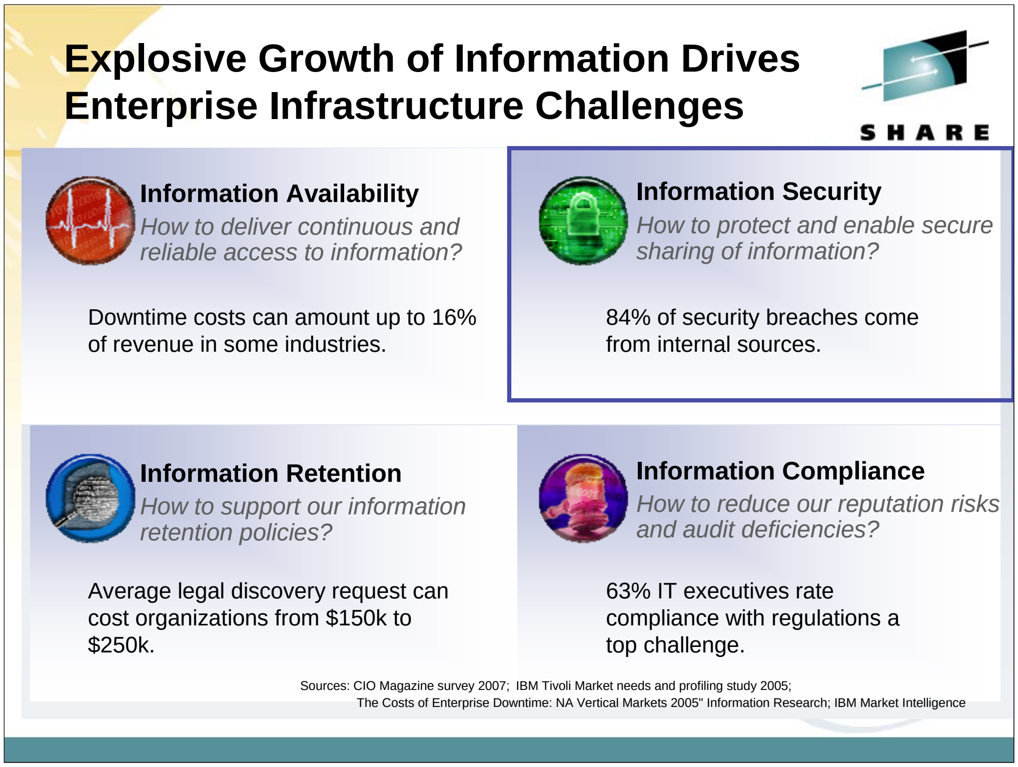
For more detail on DB2 security, see

ftp://ftp.software.ibm.com/software/db2storedprocedure/db2zos390/techdocs/db2sec1001p.pdf

This presentation will be updated and placed on the DB2 web site. Check for it before and after conference time to get additions, corrections and many more notes.

http://www.ibm.com/software/data/db2/zos/support.html

Then click on Technical Presentations and put security into the additional search terms, sort results by date – newest first.



Explosive Growth of Information Drives Enterprise Infrastructure Challenges

SHARE

Information Availability
How to deliver continuous and reliable access to information?

Downtime costs can amount up to 16% of revenue in some industries.

Information Security
How to protect and enable secure sharing of information?

84% of security breaches come from internal sources.

Information Retention
How to support our information retention policies?

Average legal discovery request can cost organizations from $150k to $250k.

Information Compliance
How to reduce our reputation risks and audit deficiencies?

63% IT executives rate compliance with regulations a top challenge.

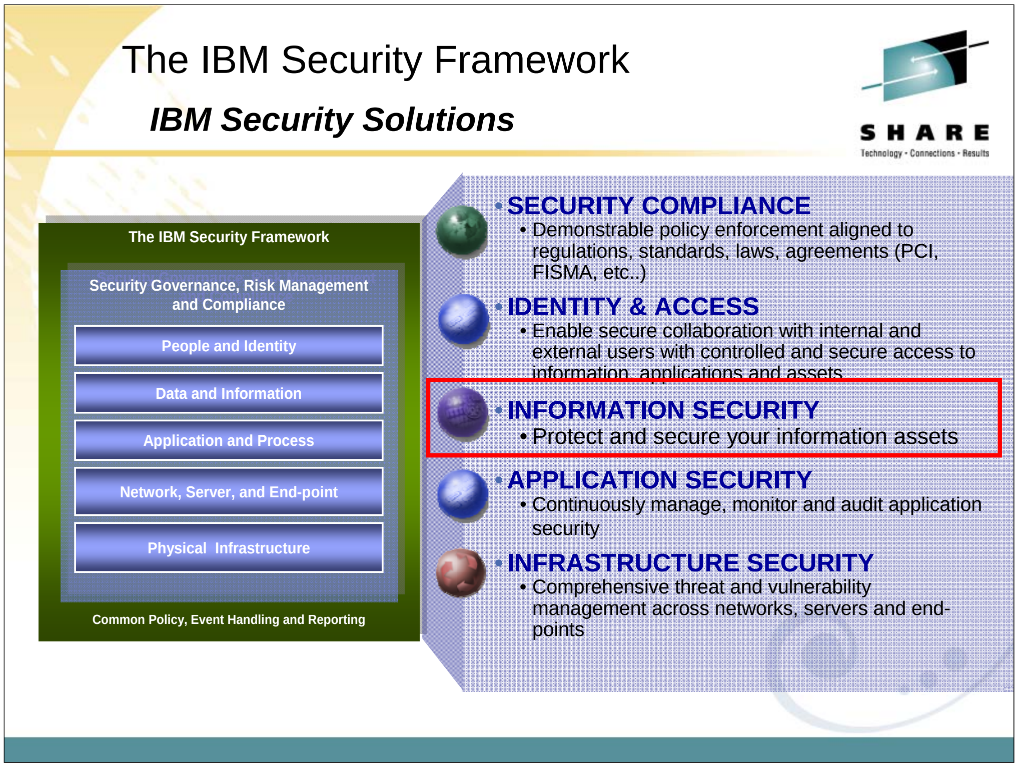
Sources: CIO Magazine survey 2007; IBM Tivoli Market needs and profiling study 2005;
The Costs of Enterprise Downtime: NA Vertical Markets 2005" Information Research; IBM Market Intelligence

What we're proposing is that enterprises that want to succeed in such a challenging business climate need to focus on four key areas to ensure their information infrastructures can support the goals of the business. The 4 key areas are:

- Information Availability
- Information Security
- Information Retention
- Information Compliance

•What do we mean by Information Infrastructure? This is the overall infrastructure of integrated and optimized storage HW and SW, application servers, applications and middleware, networks, and endpoint devices that combine to deliver information across the extended enterprise.

The IBM Information Infrastructure aims to help businesses get the right information to the right people when they need it… in a secure manner.



The IBM Security Framework

IBM Security Solutions

SHARE
Technology • Connections • Results

The IBM Security Framework

Security Governance, Risk Management and Compliance

People and Identity

Data and Information

Application and Process

Network, Server, and End-point

Physical Infrastructure

Common Policy, Event Handling and Reporting

- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)
- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **INFORMATION SECURITY**
  - Protect and secure your information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points

Within this security framework, we have segmented our offerings into five solution areas… Security Compliance, Identity and Access Management, Information Security, Application Security, and Infrastructure Security. For the purposes of this presentation, we will focus our attention on Information Security, which addresses the challenges of protecting and securing an organization's information assets.

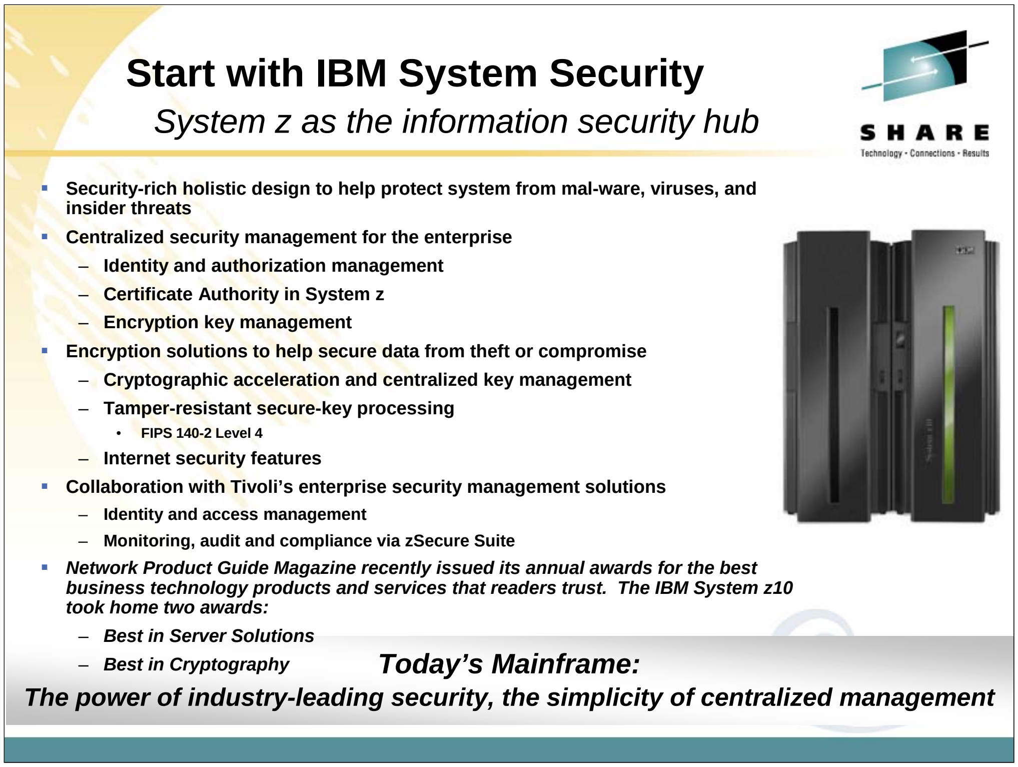
•People and Identity – Tivoli Identity Manager, Tivoli Federated Identity Manager, Tivoli Access Manager, Trusted Identity, Identity Provisioning, Identity Proofing, access control capabilities inherent in our server and storage platforms

•Data and Information - Database/Content Management, Content Monitoring, Data Governance, Data Encryption Solutions, Storage Management

•Application and Process - Secure Development Tools, Security Method Enforcement, Web Application Scanning, Application Firewall, SOA & XML Security

•Network, Server, and Endpoint - Intrusion Detection, Vulnerability Mgmt., Event Correlation, Change & Configuration Mgmt, Security Compliance Scan

•Physical Infrastructure - Digital Video Surveillance, Smart Surveillance Solutions, RFID solutions, Enterprise Asset Mgmt, Physical Security



Start with IBM System Security

System z as the information security hub

- Security-rich holistic design to help protect system from mal-ware, viruses, and insider threats
- Centralized security management for the enterprise
  - Identity and authorization management
  - Certificate Authority in System z
  - Encryption key management
- Encryption solutions to help secure data from theft or compromise
  - Cryptographic acceleration and centralized key management
  - Tamper-resistant secure-key processing
    - FIPS 140-2 Level 4
  - Internet security features
- Collaboration with Tivoli’s enterprise security management solutions
  - Identity and access management
  - Monitoring, audit and compliance via zSecure Suite
- *Network Product Guide Magazine recently issued its annual awards for the best business technology products and services that readers trust. The IBM System z10 took home two awards:*
  - *Best in Server Solutions*
  - *Best in Cryptography*

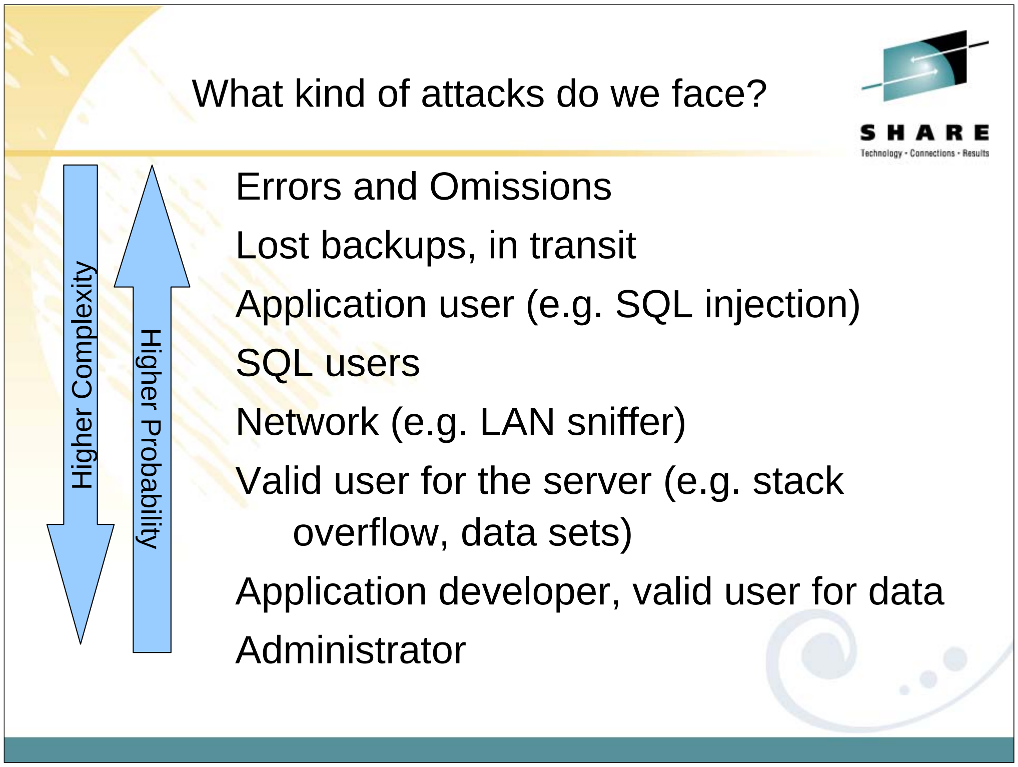
Today’s Mainframe:

The power of industry-leading security, the simplicity of centralized management

When you’re talking about securing your information infrastructure, it’s difficult to not mention the mainframe. For years, the IBM mainframe has been satisfying the most demanding customers with the highest levels of performance, availability, and security. Originally designed to be shared by thousands of users, the mainframe has security built into nearly every level of the system - from the processor level, to the operating system to the application level. This design helps protect it from malware, viruses and threats from both within and from outside the organization.

By providing the ability to enforce, monitor and manage security, System z is the logical central management point for enterprise-wide security. From user identification and authentication, access control and auditing to distributed directory, networking security and security administration, the mainframe is designed to provide integrity, process isolation and cryptographic capabilities to help keep information secure. On top of this solid hardware foundation, System z operating systems offer a variety of customizable security elements within the Security Server and Communication Server components.

And of course along with the inherent security built into the mainframe, there are additional security management offerings from Tivoli, like Identify and Access Management and the Tivoli zSecure suite, that can provide even more security to help protect the information infrastructure. Clients with mainframes already know all this.   But it’s helpful to understand why customers consider System z as the information security hub for their businesses. System z security technologies include high-performance cryptography, multilevel security, large-scale digital certificate authority and lifecycle management, improved Secure Sockets Layer (SSL) performance and advanced Resource Access Control Facility function. And with the addition of z/OS Intrusion Detection Services, System z has enhanced the system's ability to resist network-based attacks.



Higher Complexity
Higher Probability

What kind of attacks do we face?

Errors and Omissions

Lost backups, in transit

Application user (e.g. SQL injection)

SQL users

Network (e.g. LAN sniffer)

Valid user for the server (e.g. stack overflow, data sets)

Application developer, valid user for data

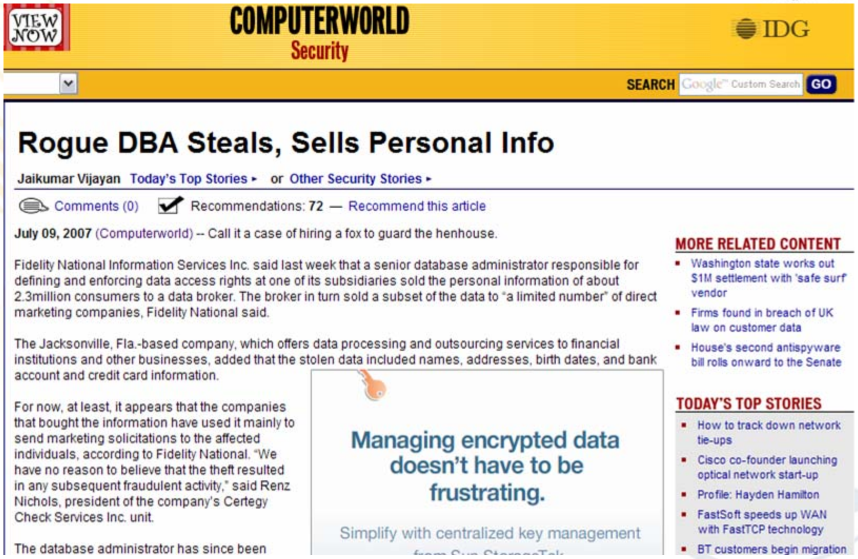
Administrator

See the next few slides and the operational environment slide for more potential of places which need to be addressed, including application code, web servers, database servers, directory and authentication devices, firewalls, network and enclave configuration and operating system platforms.

It’s important to understand the other security techniques and the controls to be sure there are no gaps in the fences.

In general, we find more business losses from errors and omissions than from any other category. This area is a gateway to bigger problems, and one that can have a very positive return on investment.

Administrators?



Rogue DBA Steals, Sells Personal Info

Jaikumar Vijayan Today's Top Stories ▸ or Other Security Stories ▸

Comments (0) Recommendations: 72 — Recommend this article

July 09, 2007 (Computerworld) -- Call it a case of hiring a fox to guard the henhouse.

Fidelity National Information Services Inc. said last week that a senior database administrator responsible for defining and enforcing data access rights at one of its subsidiaries sold the personal information of about 2.3million consumers to a data broker. The broker in turn sold a subset of the data to "a limited number" of direct marketing companies, Fidelity National said.

The Jacksonville, Fla.-based company, which offers data processing and outsourcing services to financial institutions and other businesses, added that the stolen data included names, addresses, birth dates, and bank account and credit card information.

For now, at least, it appears that the companies that bought the information have used it mainly to send marketing solicitations to the affected individuals, according to Fidelity National. "We have no reason to believe that the theft resulted in any subsequent fraudulent activity," said Renz Nichols, president of the company's Certegy Check Services Inc. unit.

The database administrator has since been

Managing encrypted data doesn't have to be frustrating.

Simplify with centralized key management from Sun StorageTek

MORE RELATED CONTENT

- Washington state works out $1M settlement with 'safe surf' vendor
- Firms found in breach of UK law on customer data
- House's second antispyware bill rolls onward to the Senate

TODAY'S TOP STORIES

- How to track down network tie-ups
- Cisco co-founder launching optical network start-up
- Profile: Hayden Hamilton
- FastSoft speeds up WAN with FastTCP technology
- BT customers begin migration

This is the headline on eWeek, but the financial loss information is sent broadly. One blog states "DBA is weakest link at processing firm." While the database administrators are difficult to control, they still cannot have access to all of the information without controls. Here is a recent headline and the sources on the web from the July 3, 2007 disclosure.

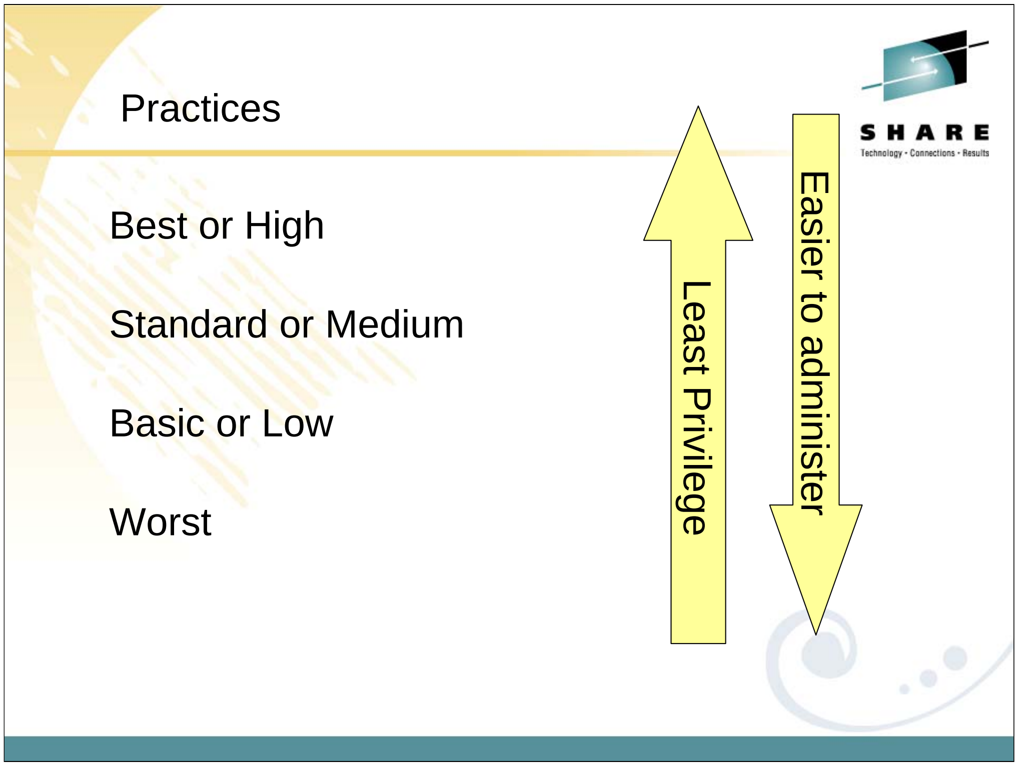
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=298312&taxonomyId=17&intsrc=kc_top

http://www.eweek.com/article2/0,1895,2154837,00.asp?kc=EWKNLNAV070507STR1

http://authentium.blogspot.com/2007/07/dba-is-weakest-link-at-processing-firms.html

http://www.forbes.com/feeds/ap/2007/07/03/ap3882026.html

http://www.forbes.com/prnewswire/feeds/prnewswire/2007/07/03/prnewswire200707030830PR_NEWS_B_MWT_CL_CLTU026.html



Practices

Best or High

Standard or Medium

Basic or Low

Worst

Least Privilege
Easier to administer

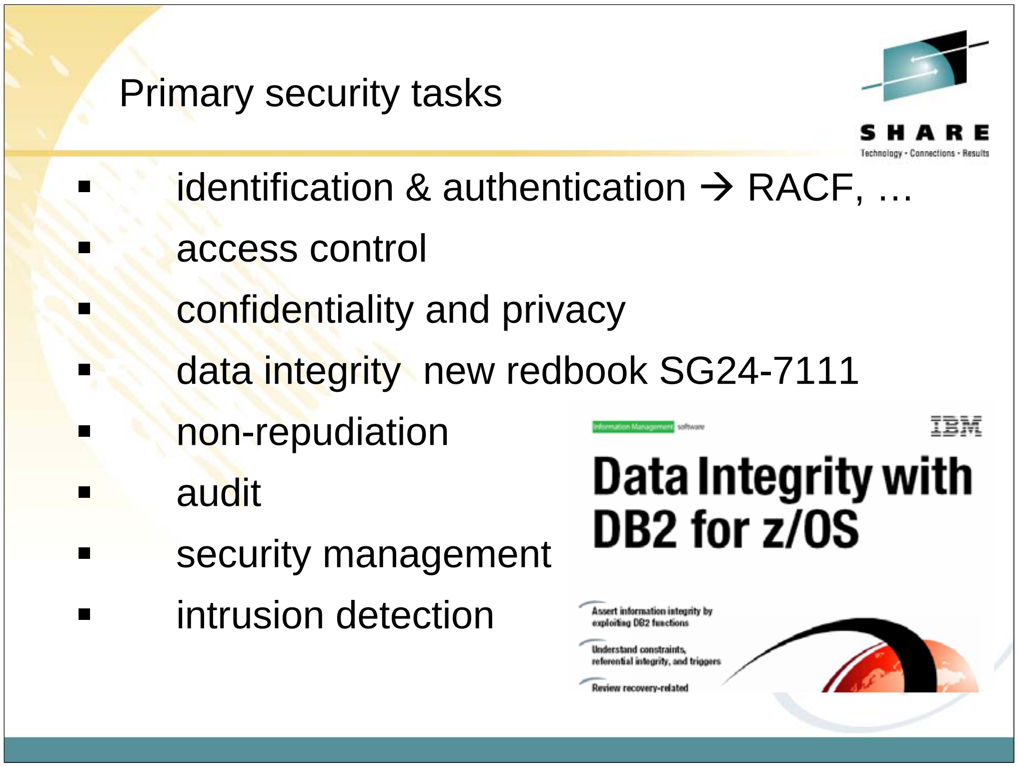
Security needs, dimensions and concerns for security vary widely. Some of the information needs best security practices, while other information can use standard or basic security to reduce the administration.

Best practice or high security will prohibit user access to a wide range of resources and require intensive access level checking. This mode may disable some less secure function and might reduce system performance. Access control is strict, with stringent audit and comprehensive protection.

Standard practice or medium security provides a balance of security with administration cost and system performance. The access control is moderately strict, with selective auditing. This level provides protection of resources that will be adequate for much of the information.

Basic practice or low security provides basic or minimal protection, with few constraints.. Minimal auditing is done. Protection is provided for some resources and a higher degree of risk is accepted for the lower cost of administration.

Worst practice provides essentially no security. One example is GRANT SYSADM TO PUBLIC or to groups that are broadly permitted, such as all data base administrators. Another example would be no use of audit.



Primary security tasks

- identification & authentication → RACF, …
- access control
- confidentiality and privacy
- data integrity new redbook SG24-7111
- non-repudiation
- audit
- security management
- intrusion detection

SHARE
Technology • Connections • Results
Information Management software
IBM
Data Integrity with DB2 for z/OS
Assert information integrity by exploiting DB2 functions
Understand constraints, referential integrity, and triggers
Review recovery-related

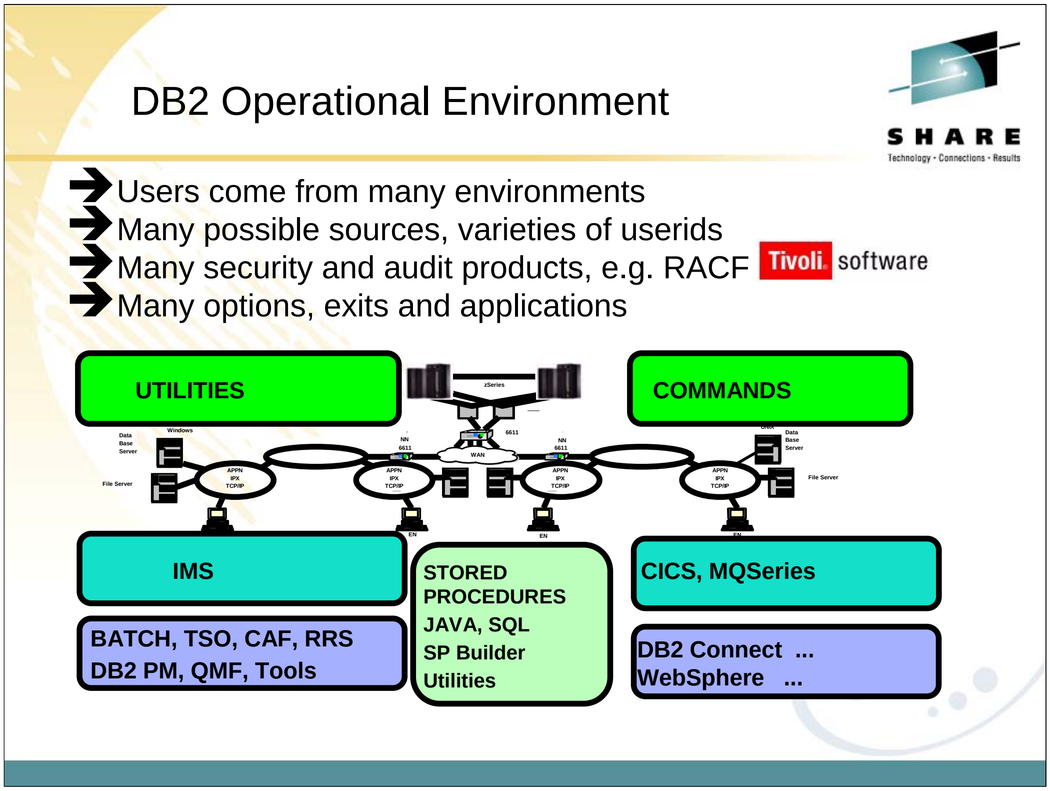
Security control components are often categorized: Identification and authentication determine who the user is. Access control uses that identification to determine what resources can be used. Confidentiality and privacy controls help ensure that the access is allowable and monitored.

Data integrity controls are the basis for every database management system, with the ACID properties (atomicity, consistency, isolation and durability).

Non-repudiation assures that authorized users are not denied access.

Audit is the step of assuring that the access controls are working as intended. This step lets us correct the inevitable mistakes and find attacks.

Security management is the process of setting up the controls.



DB2 Operational Environment

- Users come from many environments
- Many possible sources, varieties of userids
- Many security and audit products, e.g. RACF Tivoli. software
- Many options, exits and applications

UTILITIES

COMMANDS

IMS

BATCH, TSO, CAF, RRS
DB2 PM, QMF, Tools

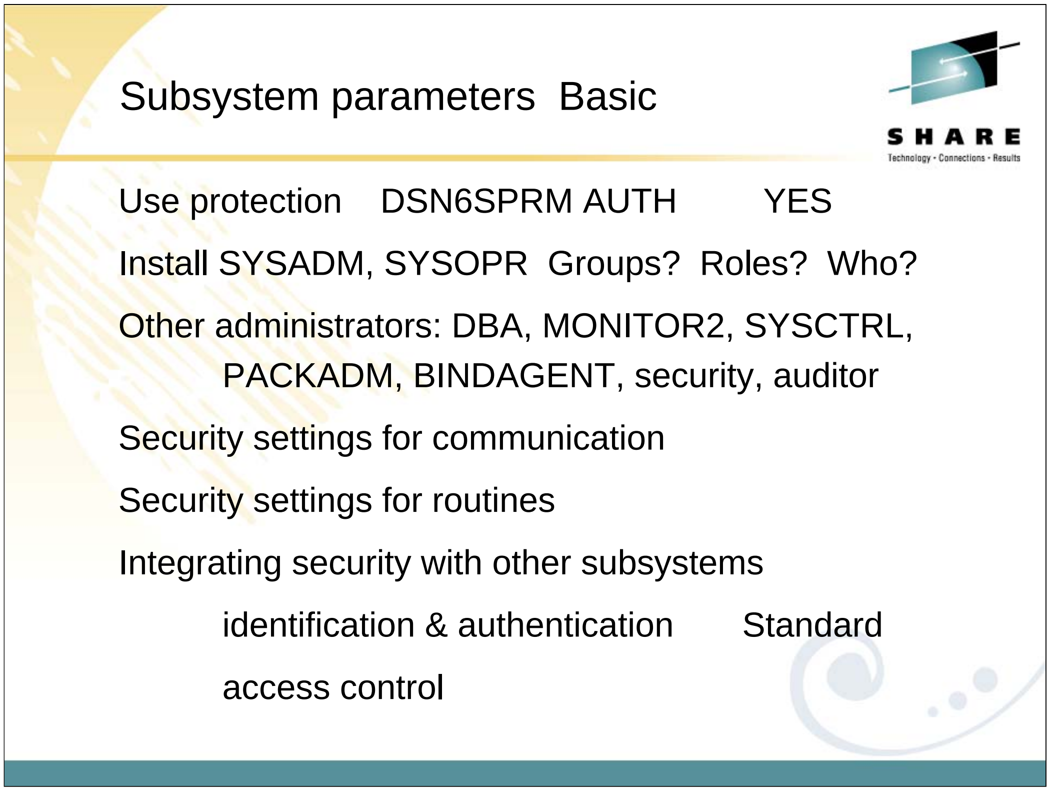
STORED PROCEDURES
JAVA, SQL
SP Builder
Utilities

CICS, MQSeries

DB2 Connect ...
WebSphere ...

There are many different environments for DB2, with different connections and security. DB2 uses the security context when possible, so batch jobs, TSO users, IMS and CICS transactions have security that uses a consistent identification and authentication. This is true for stored procedures from these environments as well. The large number of options, exits, environments and asynchronous or parallel work provide challenges for security. Some key applications manage security at the application level.

For some work, such as distributed database serving, DB2 is the initial point on this platform. For this work (DRDA distributed access, remote stored procedures), DB2 establishes the security context and manages the work.



Subsystem parameters Basic

Use protection   DSN6SPRM AUTH   YES

Install SYSADM, SYSOPR Groups? Roles? Who?

Other administrators: DBA, MONITOR2, SYSCTRL,
PACKADM, BINDAGENT, security, auditor

Security settings for communication

Security settings for routines

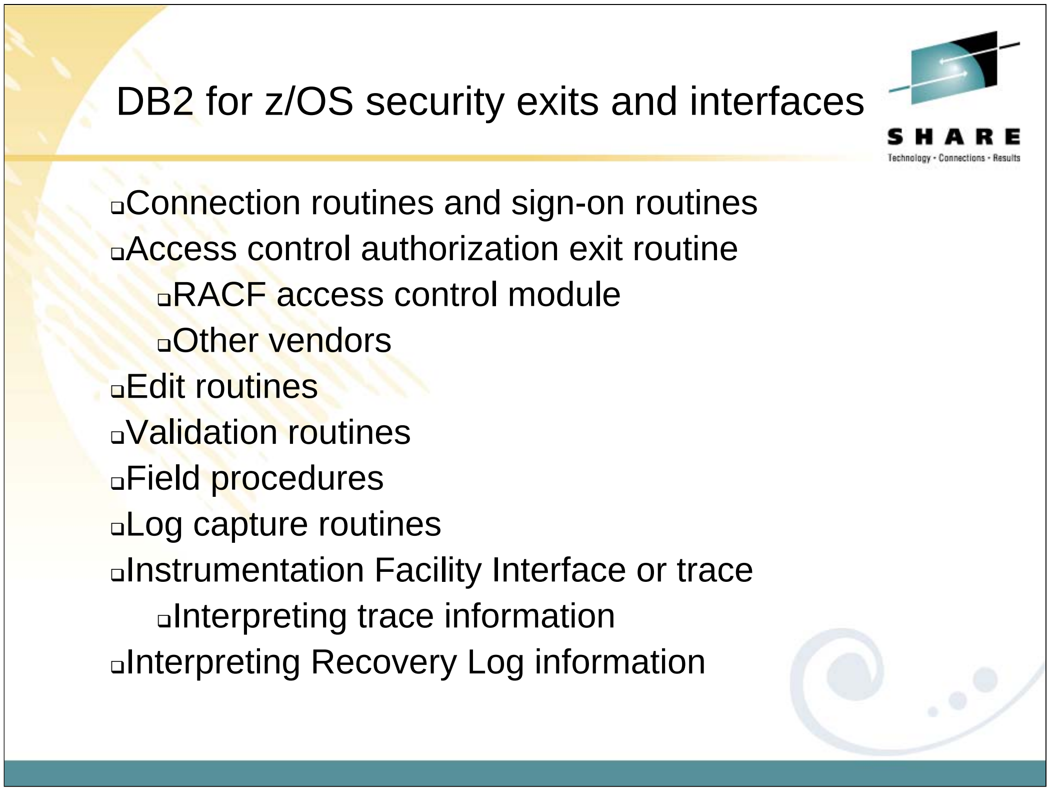
Integrating security with other subsystems

identification & authentication   Standard

access control

There are a few requirements for basic DB2 security. One is that authorization should always be used. The number of people who can be install SYSADM, SYSADM or SYSCTRL should be small. These names should be groups or roles, and the number of people able to use those groups or roles should be small. My rule of thumb would be 10 people, most of whom do not use this authority for their normal work.   Access with SYSADM authority should be audited. Other administrative users should be restricted to the access needed. Where the work is sensitive, auditing is required.

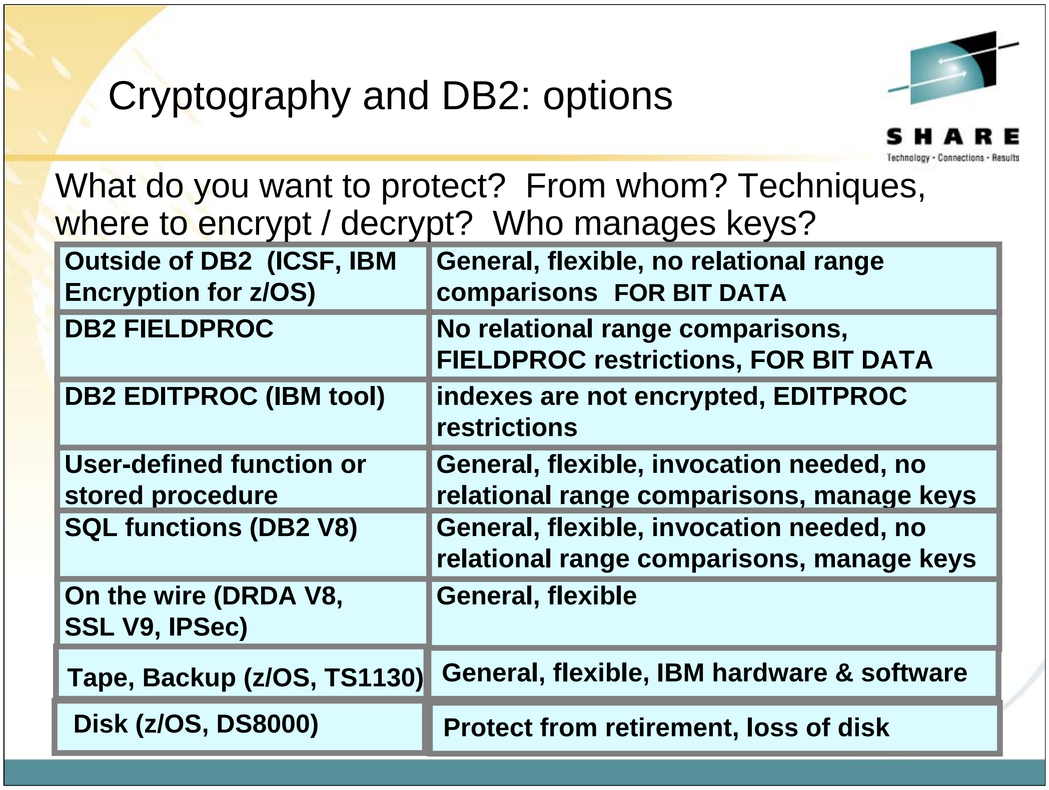
BINDAGENT and SYSCTRL are relatively weak security. The BINDAGENT privilege is intended for separation of function, not for strict security. A bind agent with the EXECUTE privilege might be able to gain all the authority of the grantor of BINDAGENT.



DB2 for z/OS security exits and interfaces

- Connection routines and sign-on routines
- Access control authorization exit routine
  - RACF access control module
  - Other vendors
- Edit routines
- Validation routines
- Field procedures
- Log capture routines
- Instrumentation Facility Interface or trace
  - Interpreting trace information
- Interpreting Recovery Log information

DB2 exit routines can make significant changes in identification, authentication, access control and auditing. Most of the information about these routines is in Appendix B, Writing Exit Routines, of the Administration Guide. Other appendices document tracing, instrumentation interfaces, and recovery log data used for audit.

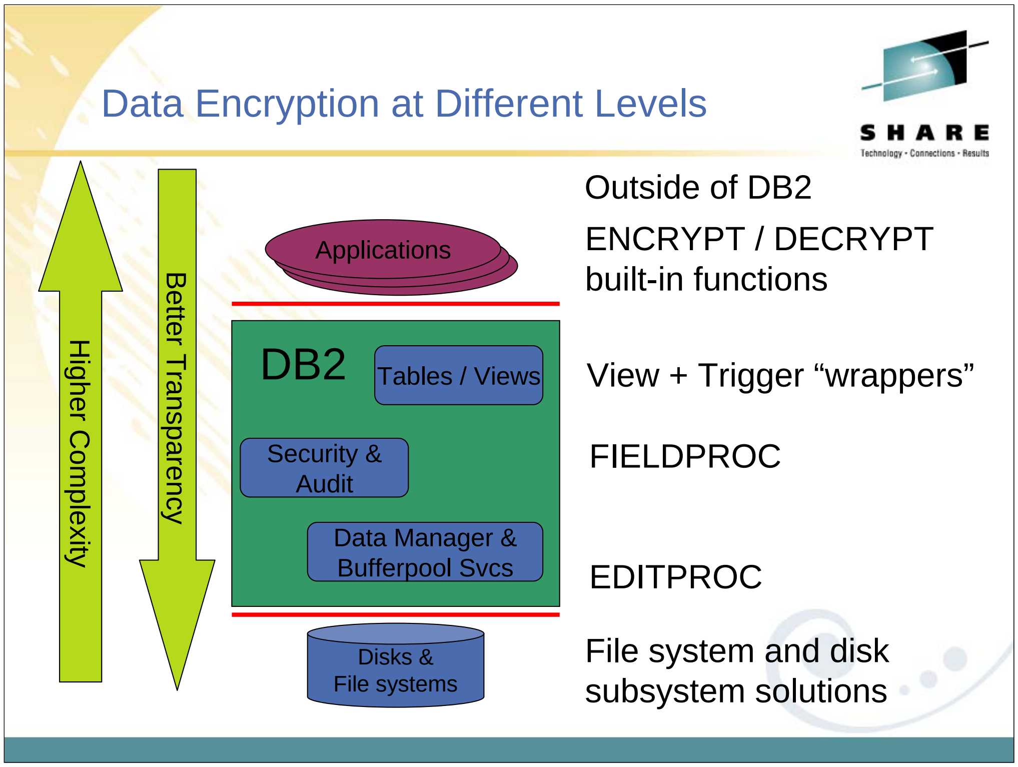


Cryptography and DB2: options

What do you want to protect? From whom? Techniques, where to encrypt / decrypt? Who manages keys?

Outside of DB2 (ICSF, IBM Encryption for z/OS)	**General, flexible, no relational range comparisons FOR BIT DATA**
DB2 FIELDPROC	**No relational range comparisons, FIELDPROC restrictions, FOR BIT DATA**
DB2 EDITPROC (IBM tool)	**indexes are not encrypted, EDITPROC restrictions**
User-defined function or stored procedure	**General, flexible, invocation needed, no relational range comparisons, manage keys**
SQL functions (DB2 V8)	**General, flexible, invocation needed, no relational range comparisons, manage keys**
On the wire (DRDA V8, SSL V9, IPSec)	**General, flexible**
Tape, Backup (z/OS, TS1130)	**General, flexible, IBM hardware & software**
Disk (z/OS, DS8000)	**Protect from retirement, loss of disk**

There are many ways to encrypt data in DB2. The answers to the questions, "What do you want to protect and from whom?" and “How much effort can be used?” are generally needed to determine which technique to use and where to encrypt and decrypt. Encryption does mean some tradeoffs in function, usability and performance. Either the indexes are not encrypted or encrypted data will not give correct results for comparisons other than equals or not equals. All greater than, less than and range predicates are not usable. An EDITPROC is the most used technique, and one is provided to use cryptography hardware with an IBM Tool. The CMOS Cryptographic Coprocessors feature and ICRF hardware were designed to address high volume cryptographic transaction rates and bulk security requirements on z/OS. The Integrated Cryptographic Service Facility (ICSF) and the IBM Encryption Facility for z/OS provide the interfaces to service routines supported by the hardware, such as key management. http://www.ibm.com/servers/eserver/zseries/security/cryptography.html



Data Encryption at Different Levels

Outside of DB2

ENCRYPT / DECRYPT built-in functions

View + Trigger “wrappers”

FIELDPROC

EDITPROC

File system and disk subsystem solutions

This diagram shows the range of places where data encryption can be performed. It is complementary to the prior page, which indicates some of the specific challenges.

If the applications are already written, then there is generally a very high need for transparency. But transparency means that some kinds of protection are not provided.

Some vendors address encryption as well.

Here are the primary references for encryption in DB2.

http://www.ibm.com/support/docview.wss?uid=swg21168217

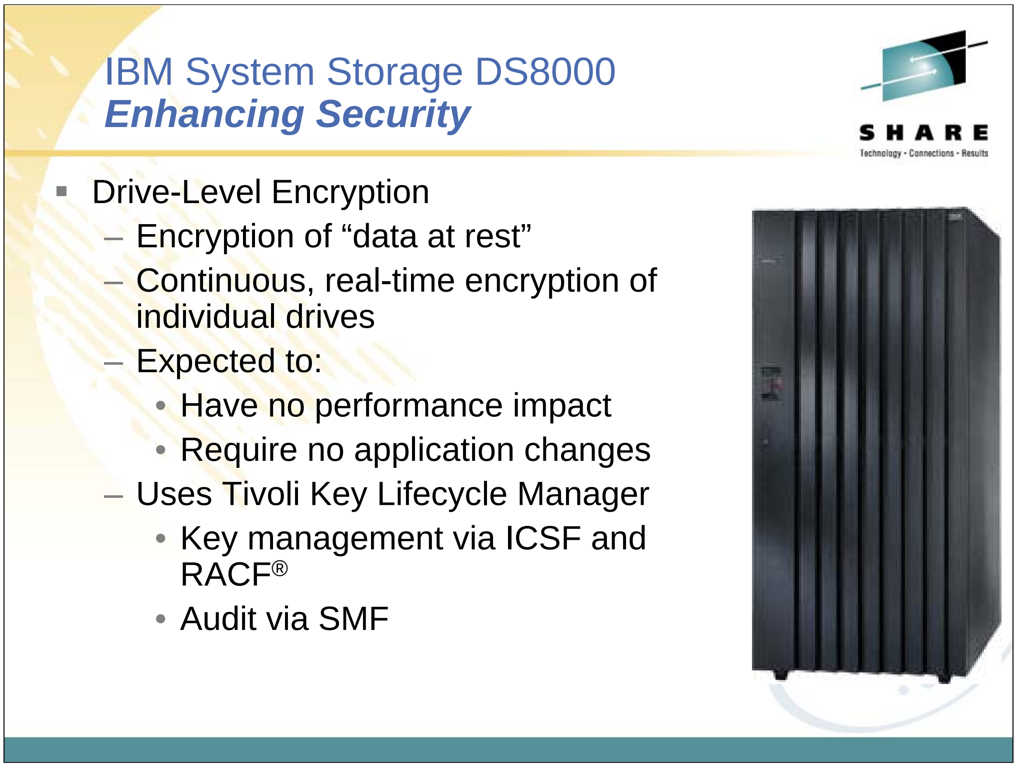
http://www.ibm.com/support/docview.wss?uid=swg27007844&aid=1

http://www.ibm.com/support/docview.wss?uid=swg27007842&aid=1

http://www.ibm.com/developerworks/db2/library/techarticle/benfield/0108benfield.html

http://www.redbooks.ibm.com/redbooks/pdfs/sg247111.pdf

sections 1.1.13 & 1.1.14



IBM System Storage DS8000
Enhancing Security

- Drive-Level Encryption
  - Encryption of “data at rest”
  - Continuous, real-time encryption of individual drives
  - Expected to:
    - Have no performance impact
    - Require no application changes
  - Uses Tivoli Key Lifecycle Manager
    - Key management via ICSF and RACF®
    - Audit via SMF

Drive-Level Encryption

New DS8000 feature supports encryption of “data at rest”

Continuous, real-time encryption of the individual drives

Expected to:

Have no performance impact

Require no application changes

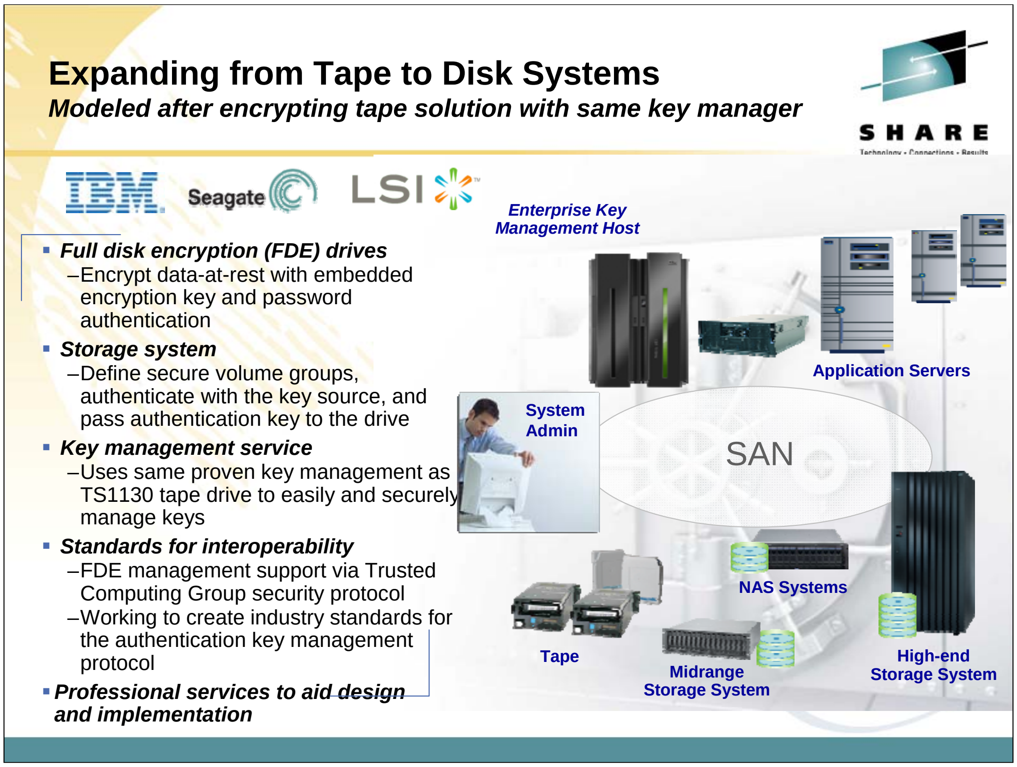
Uses Tivoli Key Lifecycle Manager (5608-A91)

Key management via ICSF and RACF®

Auditability via SMF

TKLM availability planned for March 2009

Supported on z/OS R9 R10 with the PTF
for APAR OA27393



Expanding from Tape to Disk Systems

Modeled after encrypting tape solution with same key manager

- ***Full disk encryption (FDE) drives***
  - –Encrypt data-at-rest with embedded encryption key and password authentication
- ***Storage system***
  - –Define secure volume groups, authenticate with the key source, and pass authentication key to the drive
- ***Key management service***
  - –Uses same proven key management as TS1130 tape drive to easily and securely manage keys
- ***Standards for interoperability***
  - –FDE management support via Trusted Computing Group security protocol
  - –Working to create industry standards for the authentication key management protocol
- ***Professional services to aid design and implementation***

Last fall, IBM, Seagate, and LSI made a technology announcement that will bring drive-level encryption to disk storage systems in the data center, which is the next logical step to the existing encrypting tape solution. Customers and industry observers have shown great interest, and we're excited about extending storage encryption leadership to further protect our customers from the security threat of losing sensitive information when both tapes and disks are removed from the data center. At a high level, the solution aims to address key IT requirements for simplicity and manageability for data-at-rest encryption:

•Simplified and proven key management system, operational in the largest banks in the world. Unified key management will handle all forms of storage – The encrypting disk solution will use TKLM (formerly EKM), the same key manager used for IBM's tape encrypting solution. As with the encrypting tape solution, the encrypting disk solution will be transparent to the OS, applications, databases, system administrators, and end-users, which will make deployment much simpler than deploying specialized encryption appliances.

•Designed for standard-based manageability - Every one of the hard drive vendors is active in the Trusted Computing Group, the organization writing the standards for these self-encrypting drives. Standards drive interoperability, which drives volume and creates competition. Volume and competition drive cost. We expect the other HDD vendors to closely follow us with products.

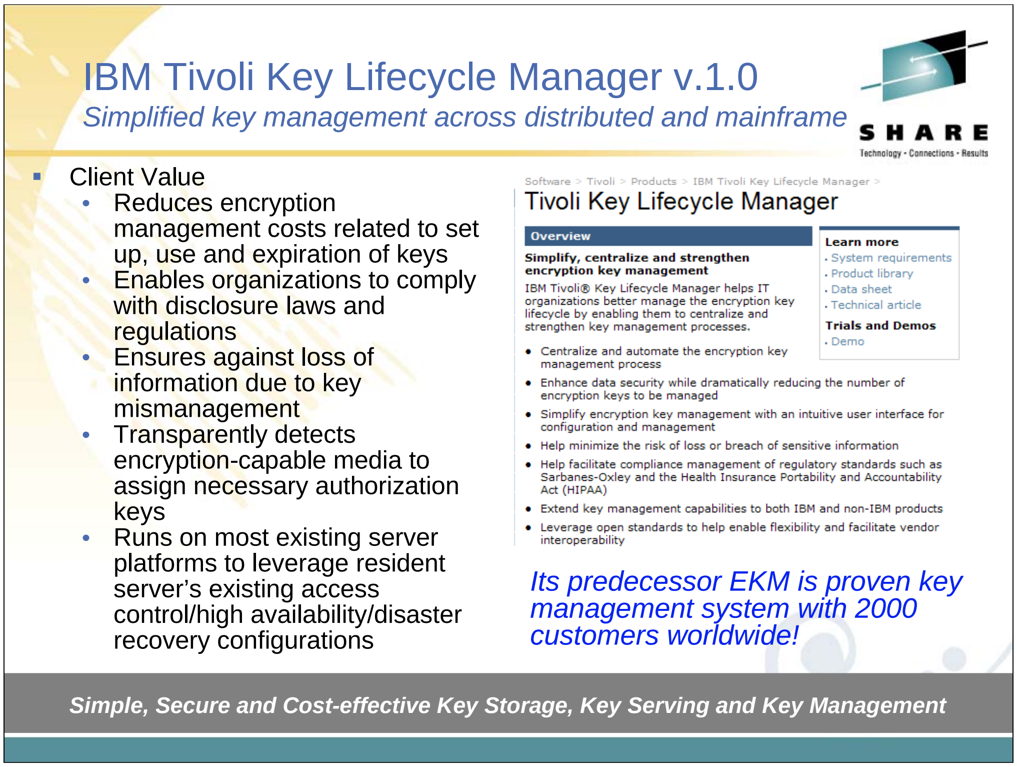
•Maintains performance and linear scalability – The Seagate Secure drives include ASICs, which maintain I/O speeds, and since encryption is done within each drive, the system scales linearly without additional hardware accelerators necessary with specialized encryption appliances.

At its core, the self-encrypting disk solution will consist of Seagate Secure full-disk encrypting drives. Each Seagate Secure drive will have an ASIC, which encrypts data as in enters the drive and decrypts data as in leaves the drive.

The role of the Storage System is that it owns the disk drives, formats them and manages the data on them to ensure the appropriate DATA PROTECTION, DATA AVAILABILITY, PERFORMANCE, COPY SERVICES, PARTITIONING, and ZONING. In our encryption model, the storage system is the connection and management point between the disk drives and the key server, so as data is written or read from the encrypting drives, the storage system manages the interaction between the drives, the applications, and the key manager.

The role of the key management service is to manage the keys associated with encrypting an decrypting the data. The Tivoli Key Lifecycle Manager (previewed in April and scheduled to be available in Q4) will transparently detect encryption-capable media and assign the authorization keys necessary to lock and unlock individual drives. The key manager includes backup and synchronization for high availability and long-term retention, as well as auditing capabilities for both internal and external compliance purposes. Since it is a Java-based application, TKLM can run on most existing server platforms to leverage the resident server's existing access control and high availability/disaster recovery configurations, which greatly simplifies implementation of this model. For the various security reasons mentioned earlier, we recommend deploying TKLM on the mainframe if customers have one.

Lastly, this is intended to be a standards-based solution. Every one of the hard drive vendors is active in the Trusted Computing Group, the organization writing the standards for these self-encrypting drives. Standards drive interoperability, which, in turn, drives volume and competition. With volume and competition comes lower prices. IBM, Seagate, and LSI are actively involved in the development and ratification of these standards, and the whole storage industry is moving aggressively to bring these standards to market.



IBM Tivoli Key Lifecycle Manager v.1.0

Simplified key management across distributed and mainframe

SHARE Technology • Connections • Results

- Client Value
  - Reduces encryption management costs related to set up, use and expiration of keys
  - Enables organizations to comply with disclosure laws and regulations
  - Ensures against loss of information due to key mismanagement
  - Transparently detects encryption-capable media to assign necessary authorization keys
  - Runs on most existing server platforms to leverage resident server's existing access control/high availability/disaster recovery configurations

Software > Tivoli > Products > IBM Tivoli Key Lifecycle Manager >

Tivoli Key Lifecycle Manager

Overview

Simplify, centralize and strengthen encryption key management

IBM Tivoli® Key Lifecycle Manager helps IT organizations better manage the encryption key lifecycle by enabling them to centralize and strengthen key management processes.

- Centralize and automate the encryption key management process
- Enhance data security while dramatically reducing the number of encryption keys to be managed
- Simplify encryption key management with an intuitive user interface for configuration and management
- Help minimize the risk of loss or breach of sensitive information
- Help facilitate compliance management of regulatory standards such as Sarbanes-Oxley and the Health Insurance Portability and Accountability Act (HIPAA)
- Extend key management capabilities to both IBM and non-IBM products
- Leverage open standards to help enable flexibility and facilitate vendor interoperability

Learn more
- System requirements
- Product library
- Data sheet
- Technical article

Trials and Demos
- Demo

Its predecessor EKM is proven key management system with 2000 customers worldwide!

Simple, Secure and Cost-effective Key Storage, Key Serving and Key Management

Brand new offering! GA in 2H08 http://www-01.ibm.com/software/tivoli/products/key-lifecycle-mgr/

Transparently detects encryption-capable media and assigns the authorization keys necessary to lock and unlock individual drives

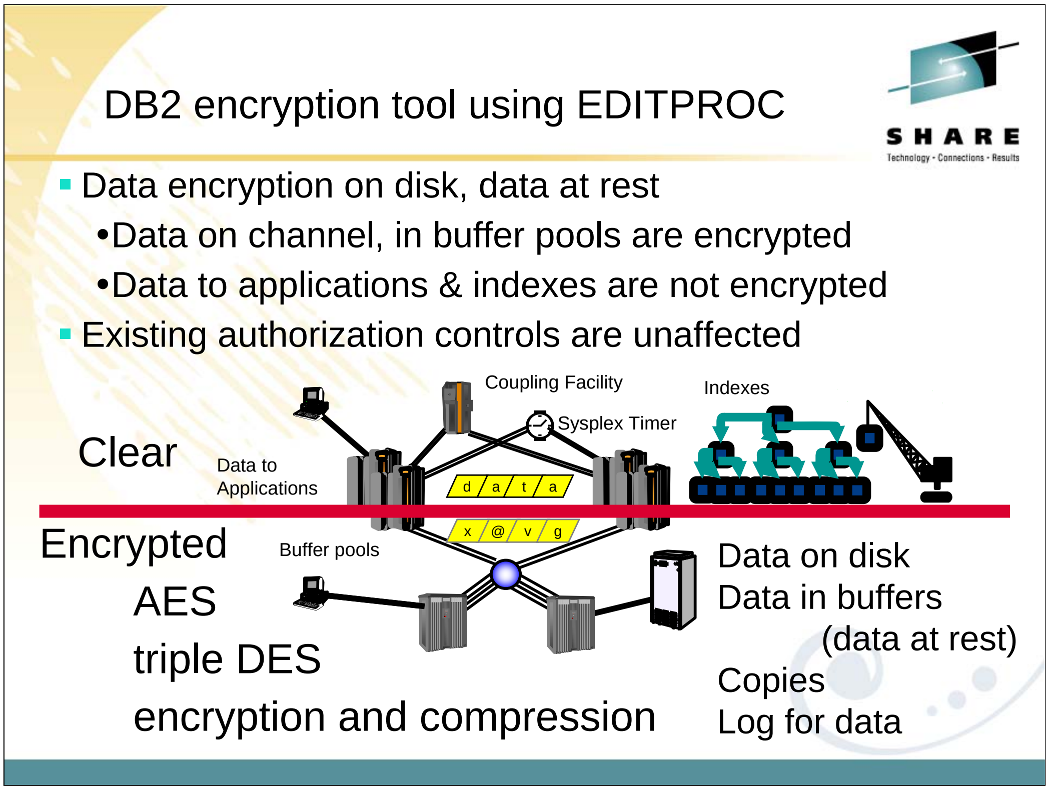
Greatly simplifies implementation: Can run on most existing server platforms to leverage the resident server's existing access control and high availability/disaster recovery configurations

Notes on Tivoli Key Lifecycle Manager (formerly TKLM)… TKLM is part of the IBM Java environment and uses the IBM Java Security components for its cryptographic capabilities. TKLM has three main functions that are used to control its behavior:

1. **Keystore** – customers have a choice of using key stores they've already deployed or installing new key stores, including the TKLM one.
   - SW-based keystore type: JCEKS (file-based)
   - HW-based keystore type: PKCS11IMPLKS (PKCS11 cryptographic device), System z, System i
   - In total about 40 3rd-party keystores are supported by TKLM's key serving engine (see below)
2. **Key serving** (Cryptographic services provider) – this is the most valuable component of the TKLM today, which transparently detects storage (tape) media, assigns unique encryption keys to each tape cartridge, and automatically serves the keys when a tape cartridge is mounted into the drive. The key serving mechanism supports about 40 3rd-party key stores and uses standard APIs, like PKCS11 and T10, to access 3rd-party key stores. In addition to the 40 3rd-party key stores supported, TKLM also supports 6 different *types* of key stores for additional implementation flexibility.
3. **Key management** – maintains policies to perform cryptographic services, like what data gets encrypted, which keys to use, synchronization of key stores, audit capabilities. These policies are stored in different places according to the encryption model the customer deploys (i.e., the tape library or the application itself). [Note: Future versions could include automatic rotation/deletion of keys and other automated policy functions.]

Tape Systems supporting encrypting tape drives: Enterprise: TS3400 TS3500 TS7700, TS7500 (no attach to System z); LTO: TS3500, TS3310, TS3100 TS3200, and DR550

Another option is the System z ability to encrypt data written to tape with its (Encryption Facility for z/OS).



DB2 encryption tool using EDITPROC

- Data encryption on disk, data at rest
  - •Data on channel, in buffer pools are encrypted
  - •Data to applications & indexes are not encrypted
- Existing authorization controls are unaffected

Coupling Facility

Indexes

Sysplex Timer

Clear

Data to Applications

d / a / t / a

x / @ / v / g

Encrypted

Buffer pools

AES

triple DES

encryption and compression

Data on disk

Data in buffers

(data at rest)

Copies

Log for data

On this slide, data above the middle line is not encrypted and data below the line is encrypted.

In this example, the encryption is not providing an additional level of security for your DB2 or IMS applications. It is providing encryption of the data on the disk.

Once the data is brought, for example, into DBMS working storage, you are using the existing DB2 and IMS authorizations to secure data. As the data is written out to disk, that is once it leaves the channel and enters the network to move to the disk, the data is encrypted.

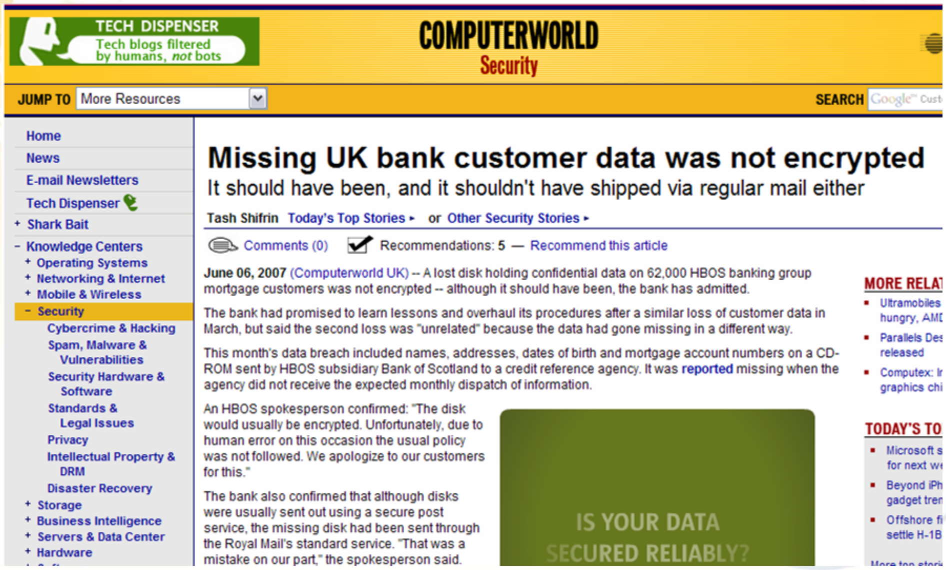
The example on this slide shows two subsystems with disks. The circle on the bottom half of the picture might be what we have known as an ESCON director in the past. The processor on the right hand side, below the line, might also be attached to that same I/O device; however, if the processor is a System z that does not have the encryption key it will not be able to interpret the data.

See the DB2 tools web pages for more about this.

http://www.ibm.com/software/data/db2imstools/db2tools/ibmencrypt.html

http://www.ibm.com/software/os/zseries/telecon/14sep/

Is your data encrypted?



Missing UK bank customer data was not encrypted

It should have been, and it shouldn't have shipped via regular mail either

Tash Shifrin Today's Top Stories ▸ or Other Security Stories ▸

Comments (0) Recommendations: 5 — Recommend this article

June 06, 2007 (Computerworld UK) -- A lost disk holding confidential data on 62,000 HBOS banking group mortgage customers was not encrypted -- although it should have been, the bank has admitted.

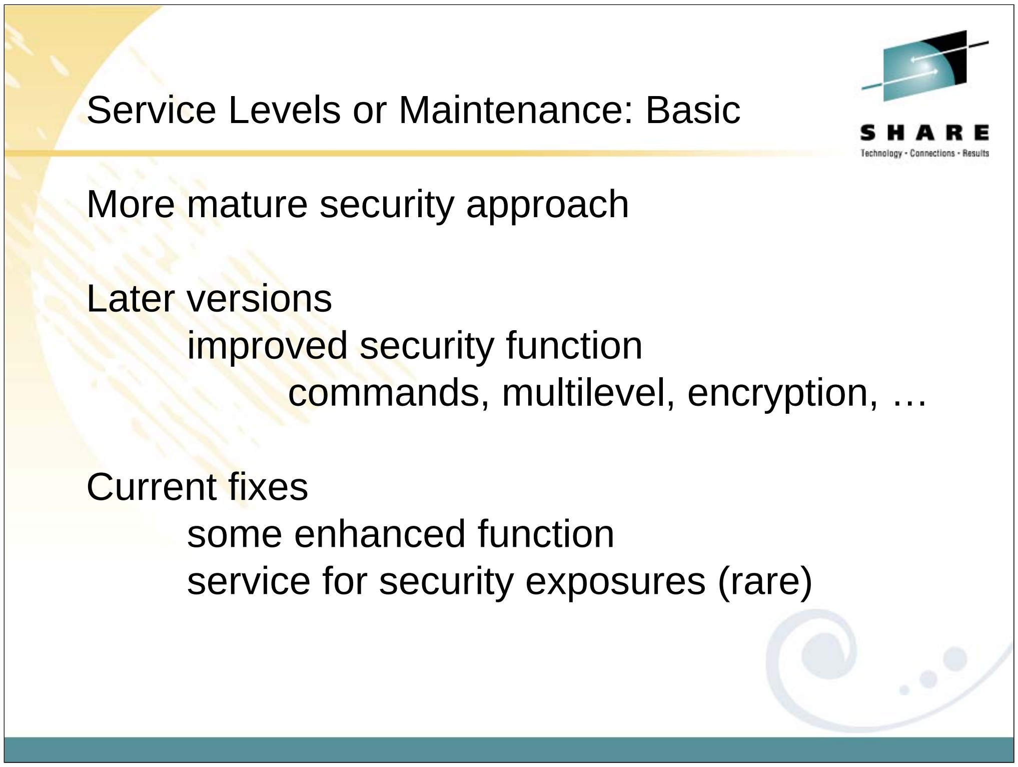
The bank had promised to learn lessons and overhaul its procedures after a similar loss of customer data in March, but said the second loss was "unrelated" because the data had gone missing in a different way.

This month's data breach included names, addresses, dates of birth and mortgage account numbers on a CD-ROM sent by HBOS subsidiary Bank of Scotland to a credit reference agency. It was reported missing when the agency did not receive the expected monthly dispatch of information.

An HBOS spokesperson confirmed: "The disk would usually be encrypted. Unfortunately, due to human error on this occasion the usual policy was not followed. We apologize to our customers for this."

The bank also confirmed that although disks were usually sent out using a secure post service, the missing disk had been sent through the Royal Mail's standard service. "That was a mistake on our part," the spokesperson said.

You don’t want the next headline to be yours. The costs are simply too high in terms of disclosure and lost customers. The costs are too low to encrypt anything which might be sent outside the secure vault.



Service Levels or Maintenance: Basic

More mature security approach

Later versions

- improved security function
  - commands, multilevel, encryption, …

Current fixes

- some enhanced function
- service for security exposures (rare)

Service levels for z/OS are generally a bit less critical for security fixes than Unix, Linux or Windows, since there are very few security fixes needed, any many fewer significant security exposures. The security was driven by commitments for system integrity and system security on System z in the 1970s and 1980s.

Still, later levels and service do provide some improvements in security function. Some examples are improved security in DB2 for z/OS V8 with command security, multilevel security and encryption options.

On the Unix, Windows and Linux platforms, be sure to install the needed service.

Vendor quarterly update
January 13, 2009…

Security - eWeek
SEARCH
Google Custom Search
eWEEK.COM
SUBSCRIBE TO eWEEK RSS Feeds | Print | Newsletters
enterprise
HOME
NEWS
REVIEWS
DATA STORAGE
SECURITY
DESKTOPS/NOTEBOOKS
MOBILE/WIRELESS
APP DEV
BLOGS
VIDEOS
THE CHANNEL
BUYERS GUIDE
Security News | Security Reviews | Security Blogs | IT Infrastructure | Government IT | Linux & Open Source | Enterprise Networking | Applications | All eWeek Topics
Microsoft SQL Server 2008
Harness the power of the data explosion
ADVERTISEMENT
Storage eSeminar: De-Mystifying NAS Clusters February 3, 2009
» LEARN MORE
eseminars
Home ▸ Security ▸ Oracle Releases Critical Patch Update with 41 Fixes
Microsoft
30 Days Most Popular
7 Days Most Popular
Rate This Article:
Poor ○ ○ ○ ○ ● Best
Rate

LATEST STORIES

- Enterprise Network Outlook
- United Airlines to Offer In-Flight Wi-Fi
- Rethinking Storage in the Data Center
- Toshiba Says in Talks to Buy Fujitsu's Hard ...
- Analysts Take Heart in Selection of New Yaho...

Security

Oracle Releases Critical Patch Update with 41 Fixes

By Brian Prince
2009-01-13

Article Views: 2461
Article Rating:☆☆☆☆☆ / 0

Resource Library:
· What Do Customers Really Think About Scalable NAS?

Oracle releases 41 security fixes in its first critical patch update of 2009. The CPU includes fixes for a number of flaws with the highest possible severity rating.

MOST READ SECURITY STORIES
PAST 7 DAYS

1 - Euro-Police Hacking Goes Out of Control (8984)
2 - Microsoft Plans Small Patch Tuesday (4710)
3 - List of Most Dangerous Programming Errors Changes IT Security Discussion (3028)
4 - Data Breaches Exposed More Than 35 Million Records in 2008 (2824)
5 - Oracle Releases Critical Patch Update with 41 Fixes (2440)
6 - MeriTalk Cyber-security Survey Highlights Work Ahead for Obama (2427)
7 - Microsoft Patch Tuesday Fixes Vulnerabilities in SMB Protocol (2219)
8 - Novell Looks to Ease Access to Microsoft SharePoint (1903)

http://www.eweek.com/c/a/Security/Oracle-Releases-Critical-Patch-Update-With-41-Fixes/?kc=EWKNLNAV01142009STR3

Oracle Releases Critical Patch Update with 41 Fixes

By Brian Prince
2009-01-13

Oracle releases 41 security fixes in its first critical patch update of 2009. The CPU includes fixes for a number of flaws with the highest possible severity rating.

Oracle delivered 41 security fixes to its customers in its first CPU (Critical Patch Update) of 2009.

Among those fixes are patches for serious flaws affecting Oracle WebLogic Server and Windows versions of Oracle Secure Backup. According to Oracle, a vulnerability in the WebLogic Server plug-ins for Apache, Sun Microsystems and IIS (Internet Information Services) Web servers received a CVSS (Common Vulnerability Scoring System) rating of 10 and can be exploited remotely without authentication.

There are also three other vulnerabilities affecting WebLogic Server and an additional vulnerability in WebLogic Portal. The highest CVSS rating among them is 6.8.

Four of the nine vulnerabilities affecting Oracle Secure Backup received a CVSS score of 10. All nine of these flaws, however, can be exploited remotely without authentication.

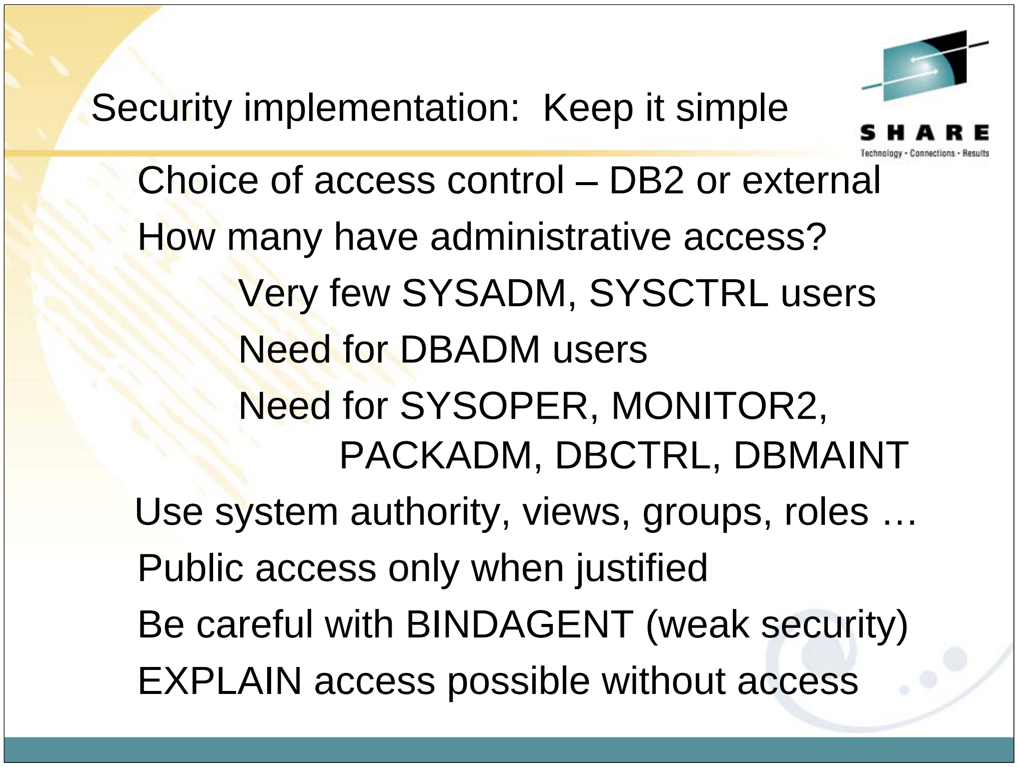
Amichai Shulman, CTO of Imperva, said the lack of technical details provided by Oracle—particularly for the vulnerabilities rated 10—makes it difficult for customers to assess their exposure.

"What we know is the vulnerabilities rated 10 for Secure Backup are important because they allow an attacker to take control of the databases being backed up," Shulman said. "Also, the WebLogic vulnerability rated 10 allows an attacker to take over a Web application without authentication. These are both serious flaws."

There are a total of 10 vulnerabilities for the Oracle Database, and one for the Oracle TimesTen Data Server. None of the 10 database vulnerabilities can be exploited without authentication, but the TimesTen flaw can.

Oracle is supplying additional fixes for four flaws affecting Oracle Application Server, one for the Oracle Collaboration Suite, four for the Application suite and one for Oracle Enterprise Manager. Another six security fixes are for the PeopleSoft and JD Edwards Suite.

The next CPU is scheduled to be released April 14.



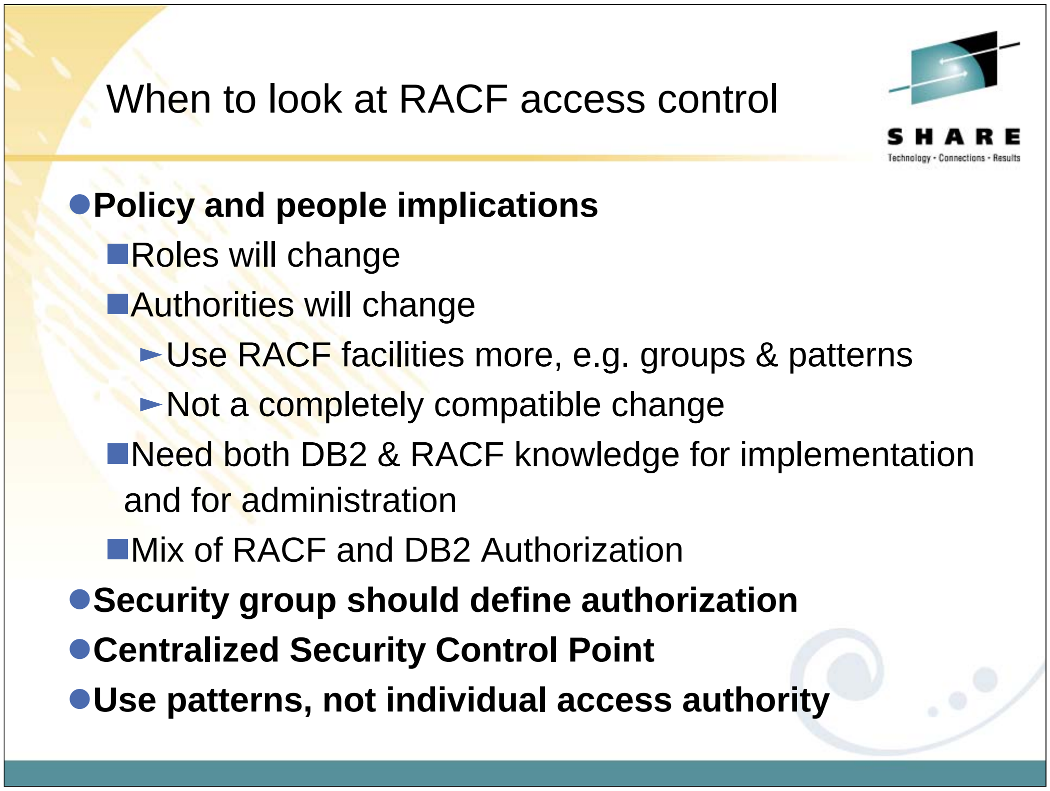
Security implementation: Keep it simple

- Choice of access control – DB2 or external
- How many have administrative access?
  - Very few SYSADM, SYSCTRL users
  - Need for DBADM users
  - Need for SYSOPER, MONITOR2, PACKADM, DBCTRL, DBMAINT
- Use system authority, views, groups, roles …
- Public access only when justified
- Be careful with BINDAGENT (weak security)
- EXPLAIN access possible without access

One of the keys to success is keeping the security as simple as possible. Having as direct as possible a mapping from the security policy to the implementation will keep mistakes to a minimum, but we must allow for mistakes and for correcting those mistakes.

The number of people who can be install SYSADM, SYSADM or SYSCTRL should be small. These names should all be groups or roles, and the number of people able to use those groups or roles should be small. My rule of thumb would be 10 people, most of whom do not use this authority for their normal work.   All access with SYSADM or SYSCTRL authority should be audited. Other administrative users should be restricted to the access needed and also be groups or roles. Where the work is sensitive, auditing is required. SYSOPER can be controlled. MONITOR2 should only be provided to those who can view all work on the DBMS. Public access should be avoided without careful justification and understanding of the security policy.

The BINDAGENT privilege is relatively weak security. Grant BINDAGENT from an id with only the needed authority, not SYSADM in general. There is a fairly new example of how to provide EXPLAIN access when the individuals do not have direct access to the data. An example showing how to have EXPLAIN authorization without direct access to the tables is provided with the V8 Visual Explain and APARs PQ90022 and PQ93821. For this example, you may want to have the binder not have SYSADM, and will not want to grant access to public.
http://www.ibm.com/software/data/db2/zos/osc/ve/index.html



When to look at RACF access control

- **Policy and people implications**
  - Roles will change
  - Authorities will change
    - Use RACF facilities more, e.g. groups & patterns
    - Not a completely compatible change
  - Need both DB2 & RACF knowledge for implementation and for administration
  - Mix of RACF and DB2 Authorization
- **Security group should define authorization**
- **Centralized Security Control Point**
- **Use patterns, not individual access authority**

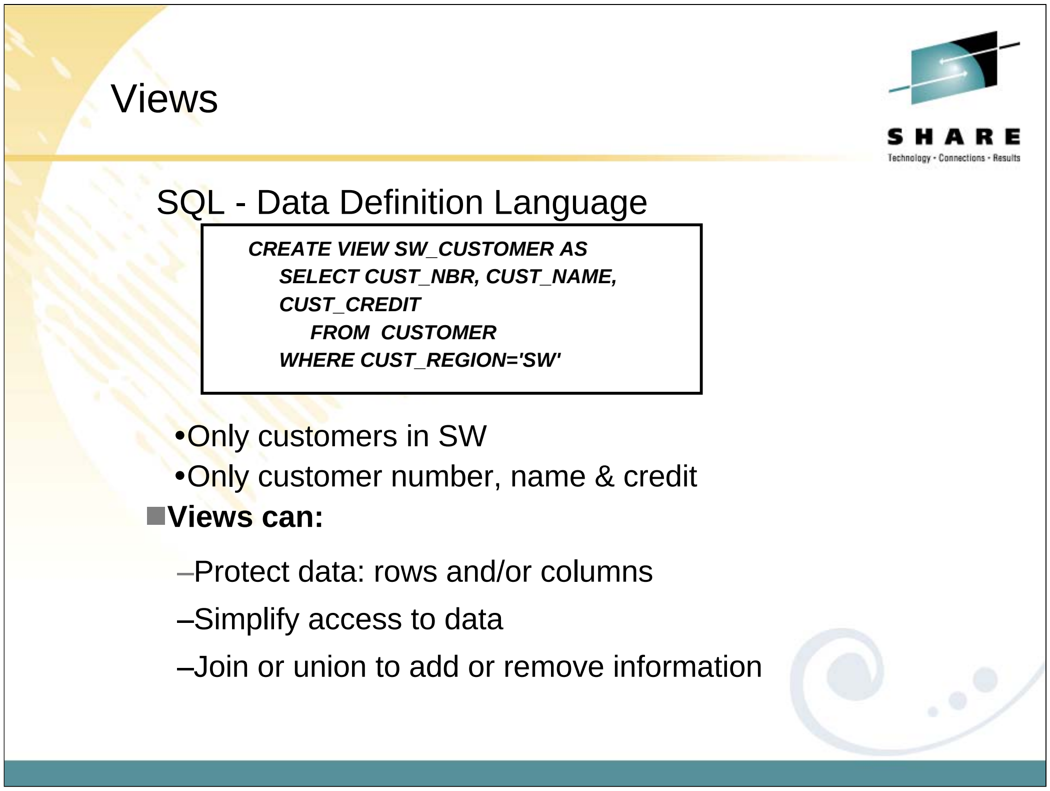
The choice of using RACF for access control is not for everyone. There are significant policy and people implications. If you want the database administrators to manage security, then integration with DB2 is very important. If you want security administrators to manage security, then integration with the security server is more important. As you make this change, note that roles will change and authorities will change. This is not a compatible change.

You must plan to use RACF facilities more, like groups and patterns. The implementation team needs both DB2 and RACF knowledge for implementation.

If you want a security group to define authorization and a centralized security control point, then this is a match for your needs. As you implement, plan to use patterns instead of individual item access authorities.

See the Protect Your Assets presentation for more on this topic:

http://www.ibm.com/support/docview.wss?rs=64&uid=swg27001877



Views

SQL - Data Definition Language

```
CREATE VIEW SW_CUSTOMER AS
    SELECT CUST_NBR, CUST_NAME,
    CUST_CREDIT
        FROM  CUSTOMER
    WHERE CUST_REGION='SW'
```

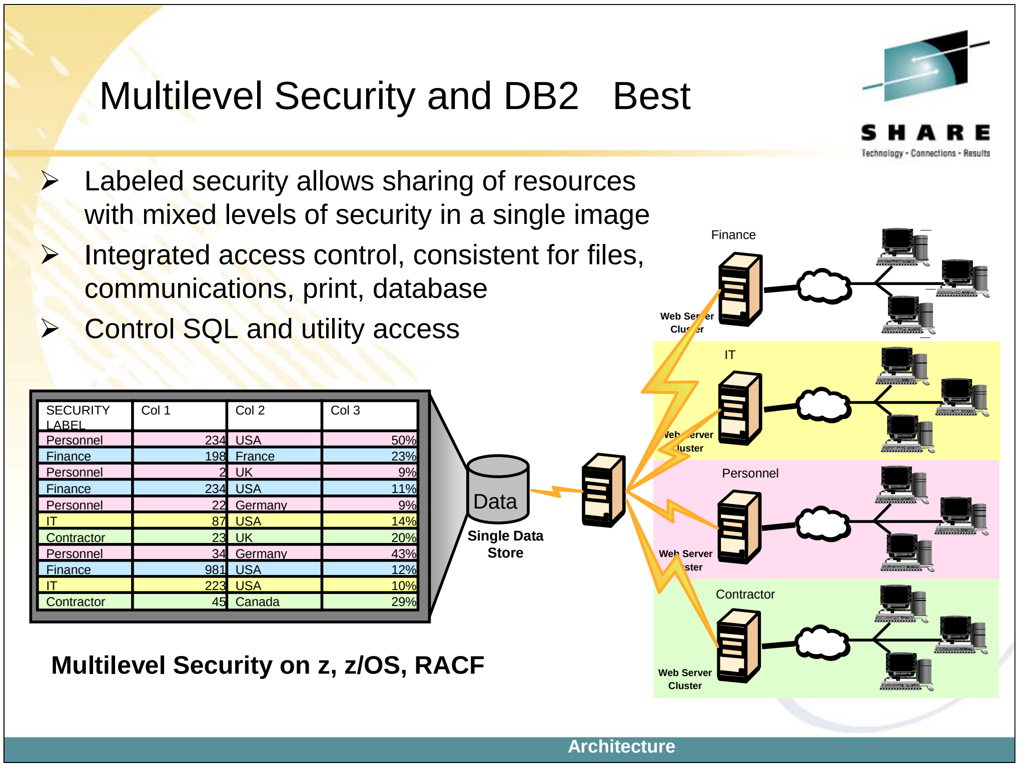
- Only customers in SW
- Only customer number, name & credit

Views can:

- Protect data: rows and/or columns
- Simplify access to data
- Join or union to add or remove information

Views can be used to hide data. They can provide only certain fields, as noted. Views are often used to simplify access to data by being able to define the view once and use it many times.

Table privileges DELETE, INSERT, SELECT, UPDATE, or ALL can be granted individually on a view. By creating a view and granting privileges on it, you can give someone access only to a specific combination of data. This capability is sometimes called field-level access control or field-level sensitivity.



Multilevel Security and DB2 Best

- Labeled security allows sharing of resources with mixed levels of security in a single image
- Integrated access control, consistent for files, communications, print, database
- Control SQL and utility access

SECURITY LABEL	Col 1	Col 2	Col 3
Personnel	234	USA	50%
Finance	198	France	23%
Personnel	2	UK	9%
Finance	234	USA	11%
Personnel	22	Germany	9%
IT	87	USA	14%
Contractor	23	UK	20%
Personnel	34	Germany	43%
Finance	981	USA	12%
IT	223	USA	10%
Contractor	45	Canada	29%

Multilevel Security on z, z/OS, RACF

Architecture

z/OS 1.5 and RACF or Security Server 1.5 (improved in 1.6) add another type of security, called multilevel security, labeled security or mandatory access control (MAC). The only option in the past with a high degree of separation has been physical separation. In the database world that might mean another machine or LPAR or perhaps another subsystem, another database or another table. With multilevel security, we still have a high degree of security even with data in the same table.

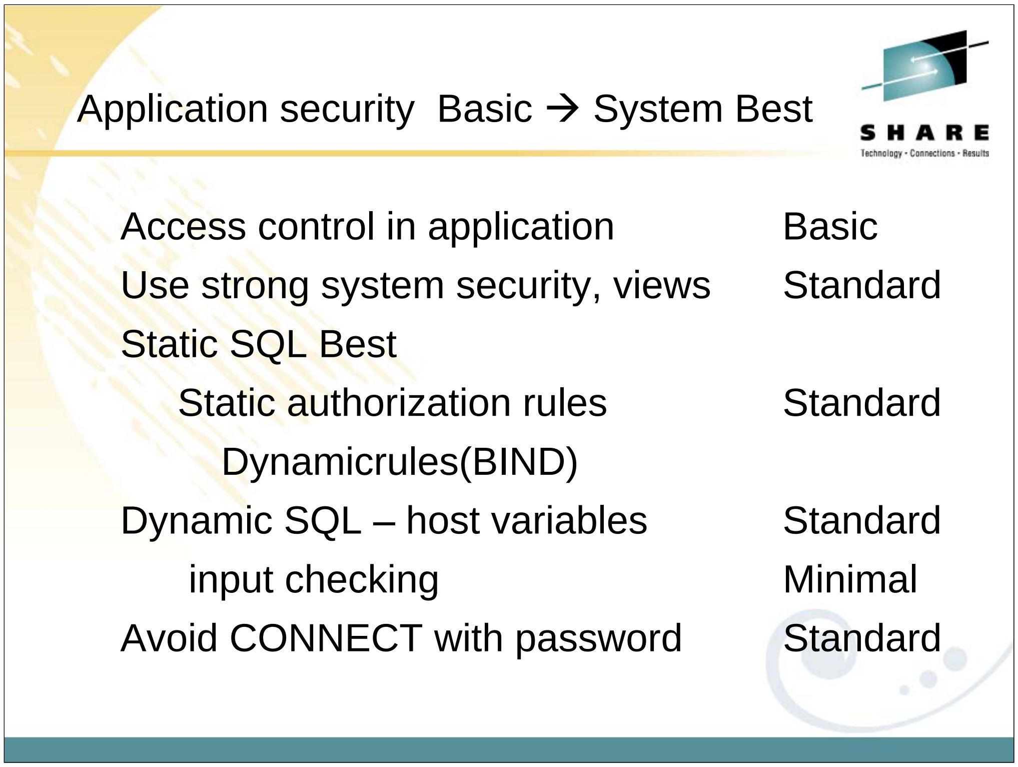
Access control is consistent across many types of resources using RACF, so that multilevel controls apply for data sets, for communications, for print and for database access – both objects and now with row level granularity. The DB2 controls are for both SQL access and for utility access.

For more on multilevel security, see **Planning for Multilevel Security and Common Criteria (GA22-7509)**

http://publibz.boulder.ibm.com/epubs/pdf/e0z2e121.pdf

Securing DB2 and Implementing MLS on z/OS, SG24-6480-01
http://www.redbooks.ibm.com/abstracts/sg246480.html

http://www.ibm.com/systems/z/security/mls.html

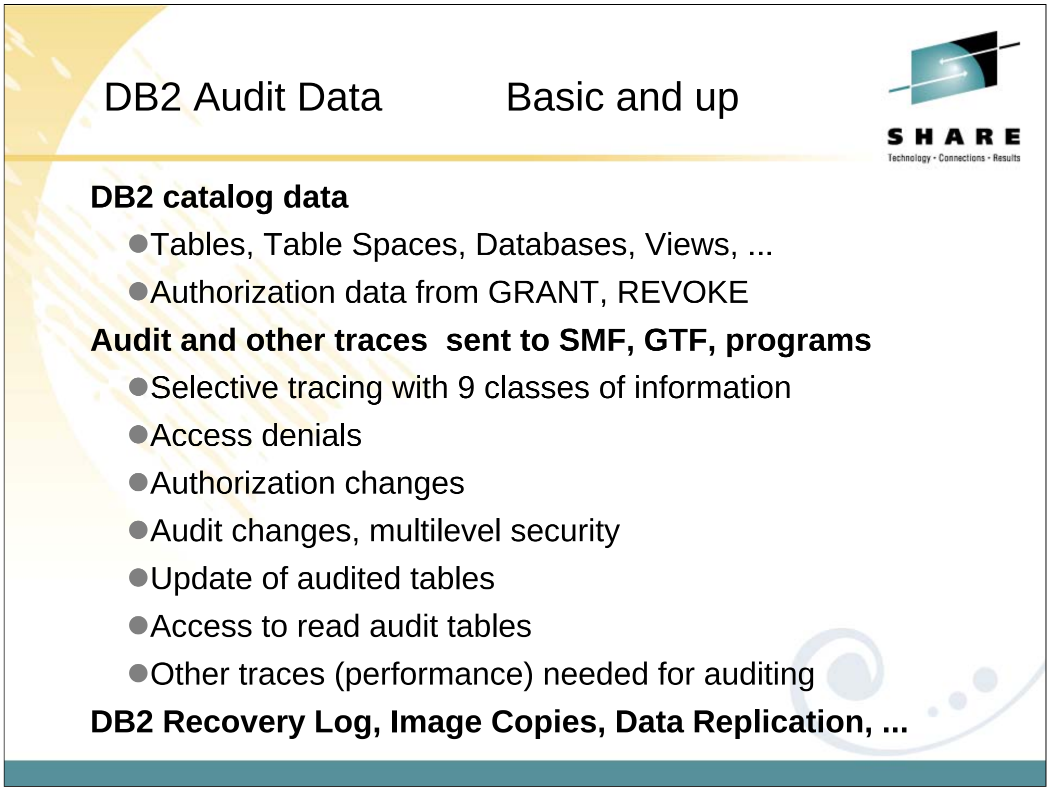


Application security Basic → System Best

Access control in application	Basic
Use strong system security, views	Standard
Static SQL Best	
Static authorization rules	Standard
Dynamicrules(BIND)	
Dynamic SQL – host variables	Standard
input checking	Minimal
Avoid CONNECT with password	Standard

Applications do not have some of the protection mechanisms or the level of assurance provided by system security, so use the stronger system techniques whenever possible. Static SQL prevents a number of problems, including SQL injection, while improving performance. Static SQL authorization techniques can be used to avoid granting wide access to tables. If dynamic SQL is used, then use of parameter markers and host variables for input can also avoid SQL injection. Checking the input must be performed. Use of CONNECT with a password provides a shared technique and userid that will make management more difficult. Use system identification and authentication. Changing the password is needed more if you have passwords in programs.

There are several vendors for application security function.



DB2 Audit Data Basic and up

DB2 catalog data

- Tables, Table Spaces, Databases, Views, ...
- Authorization data from GRANT, REVOKE

Audit and other traces sent to SMF, GTF, programs

- Selective tracing with 9 classes of information
- Access denials
- Authorization changes
- Audit changes, multilevel security
- Update of audited tables
- Access to read audit tables
- Other traces (performance) needed for auditing

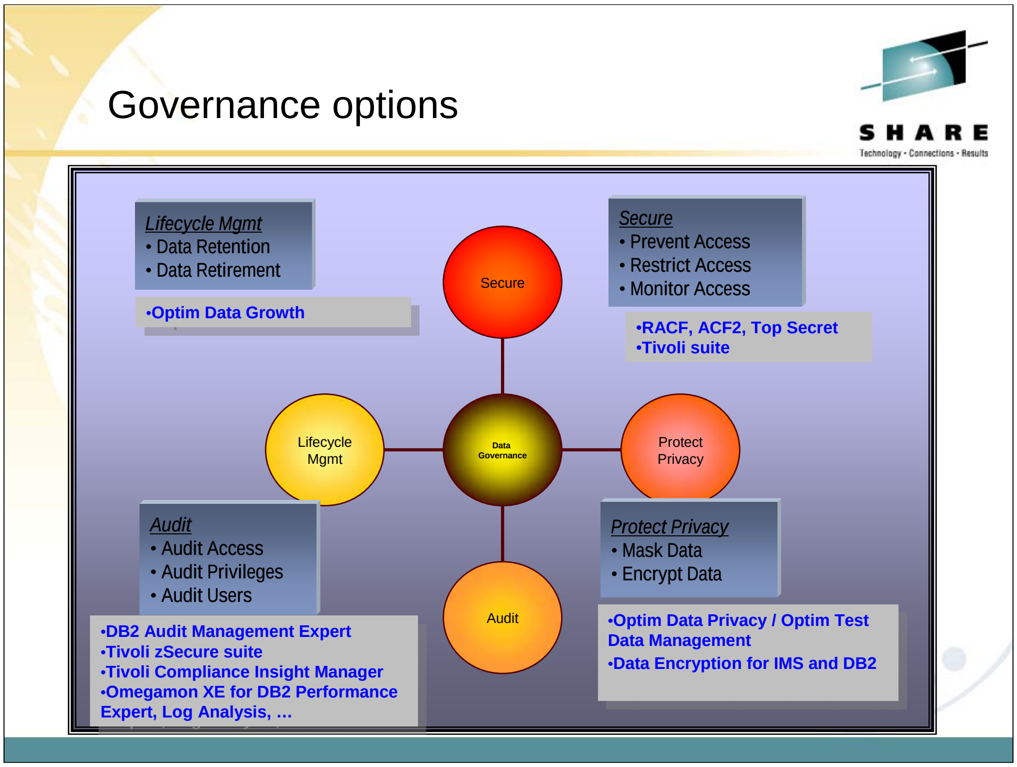
DB2 Recovery Log, Image Copies, Data Replication, ...

There are many kinds of audit information available in DB2. The DB2 catalog stores the definitions of all the objects and the authorization. Users who are allowed to access these tables can use the power of SQL to audit and manage security. RACF has an unload facility that allows its security definitions to be loaded into DB2, so that broader auditing can be performed.

One of the primary audit sources is an audit trace that can provide very selective information. Other trace information can also be used in auditing.

The DB2 recovery log and utilities are also helpful in finding out how and when some data was modified.

Please read the Audit section of the Security and Auditing chapter of the DB2 Administration Guide.



Governance options

Lifecycle Mgmt
- Data Retention
- Data Retirement

•Optim Data Growth

Secure
- Prevent Access
- Restrict Access
- Monitor Access

•RACF, ACF2, Top Secret
•Tivoli suite

Audit
- Audit Access
- Audit Privileges
- Audit Users

•DB2 Audit Management Expert
•Tivoli zSecure suite
•Tivoli Compliance Insight Manager
•Omegamon XE for DB2 Performance Expert, Log Analysis, ...

Protect Privacy
- Mask Data
- Encrypt Data

•Optim Data Privacy / Optim Test Data Management
•Data Encryption for IMS and DB2

With data compliance and privacy regulations on the rise, many IT organizations are experiencing new levels of complexity around data management. The DB2 and IMS Tools offer a data governance solution that responds to ongoing requirements related to the auditing, retention and privacy of your data. The tools provide the capabilities IT organizations need to more confidently comply with regulations while saving time and expense in the data center.

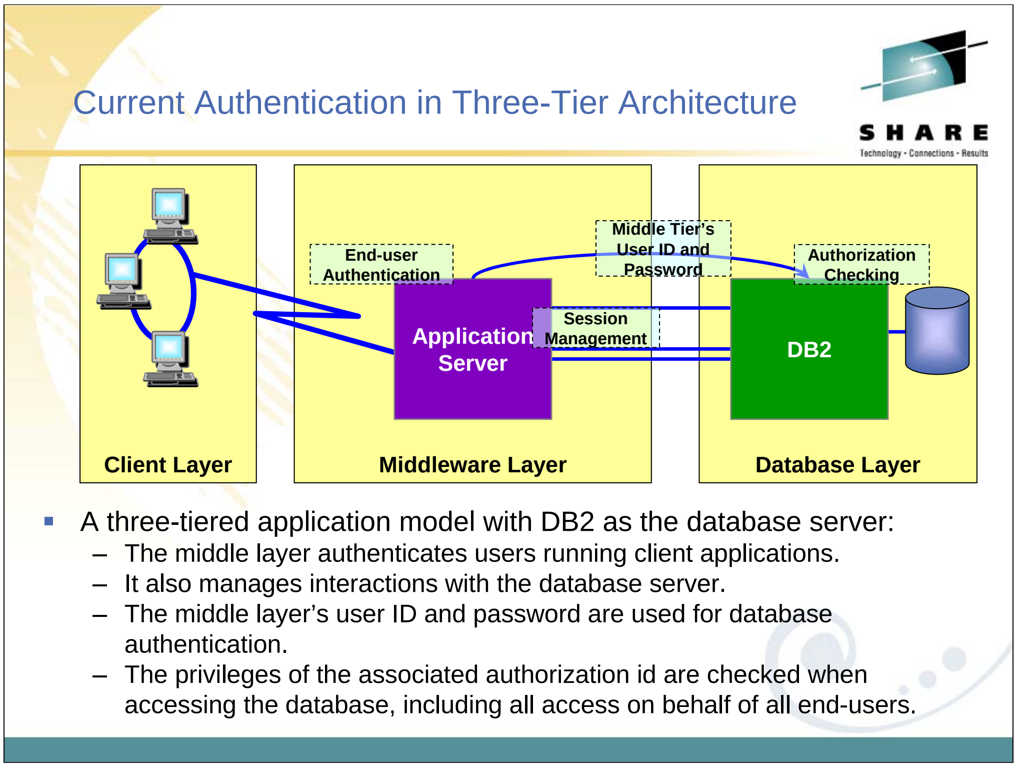
Is your DB2 audit reporting strategy lacking institutional controls, or perhaps even nonexistent? Are you using "live" production data for unit testing, with no masking of sensitive data values? Are you wasting resources storing large amounts of unreferenced and inactive data on your operational databases? Is sensitive data potentially being exposed to theft while at rest or in transit between you and your business partners?

Many products from IBM and others can help with parts of the challenge, from security management to detailed auditing.

http://www.ibm.com/software/data/db2imstools/solutions/compliance.html

http://www.ibm.com/software/tivoli/solutions/security/

http://www.ibm.com/servers/eserver/zseries/zos/racf/



Current Authentication in Three-Tier Architecture

- A three-tiered application model with DB2 as the database server:
  - The middle layer authenticates users running client applications.
  - It also manages interactions with the database server.
  - The middle layer's user ID and password are used for database authentication.
  - The privileges of the associated authorization id are checked when accessing the database, including all access on behalf of all end-users.

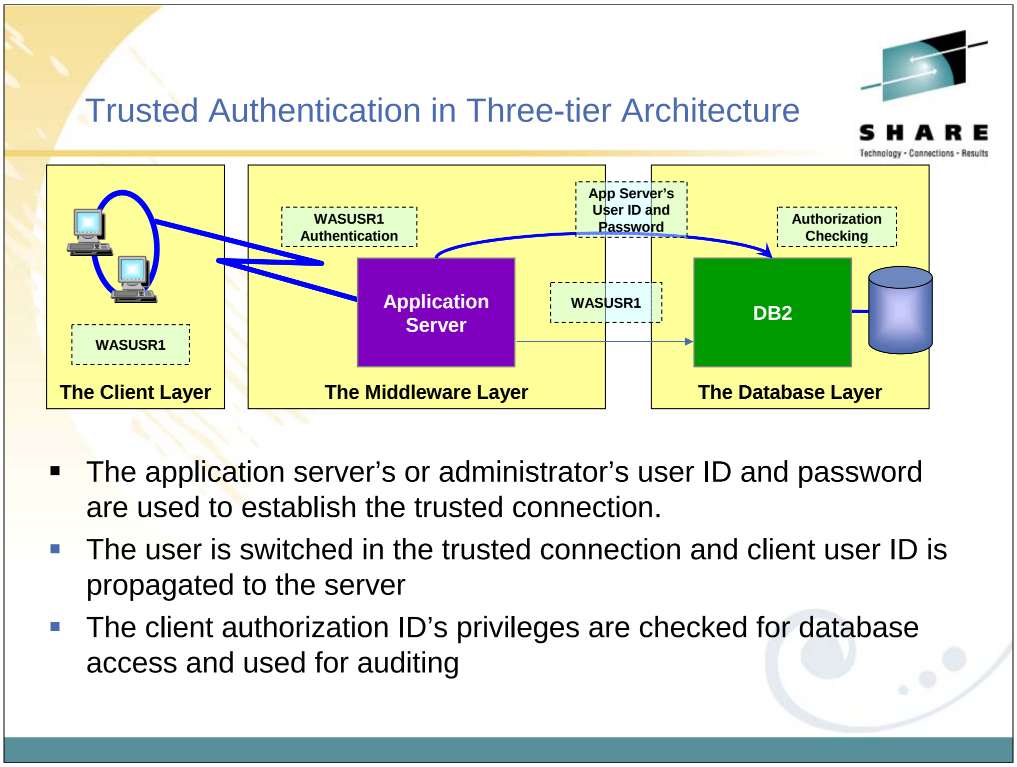
In a typical three-tiered application model with DB2 as the database server:

The middle layer (sometimes called the middleware layer) authenticates users running client applications.

The middle layer also manages interactions with the database server (DB2).

The middle tier's user ID and password are used for authentication purposes.

The database privileges associated with that authorization ID are checked when accessing the database, including all access on behalf of all end-users.



Trusted Authentication in Three-tier Architecture

WASUSR1

The Client Layer

WASUSR1 Authentication

Application Server

The Middleware Layer

App Server's User ID and Password

WASUSR1

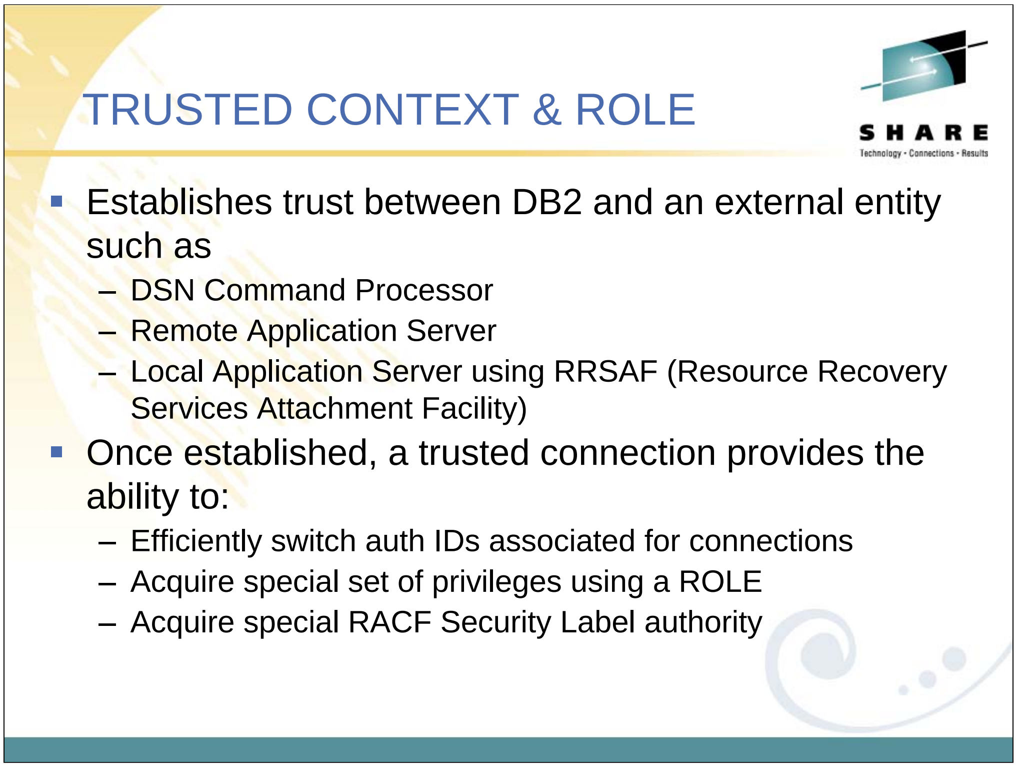
Authorization Checking

DB2

The Database Layer

- The application server's or administrator's user ID and password are used to establish the trusted connection.
- The user is switched in the trusted connection and client user ID is propagated to the server
- The client authorization ID's privileges are checked for database access and used for auditing

Trusted context addresses the problem of establishing a trusted relationship between DB2 and an external entity, such as a middleware server.
A series of trust attributes are evaluated at connect time to determine if a specific context is to be trusted.
The relationship between a connection and a trusted context is established when a connection to the server is first created.
Once established, a trusted connection provides the ability to:
-Use the trusted connection for a different user without authentication.
-Acquire special set of privileges by an authorization ID, that are not available to it outside the trusted context. This is accomplished by associating a role with the trusted context.
-Allow a role to own objects, if objects are created in a trusted context with role defined as the owner.
-Acquire security label (RACF SECLABEL) to be used for multi-level security verification. Multi-level security restricts access to an object or a row based on the security label of the object or row and the security label of the user.



TRUSTED CONTEXT & ROLE

- Establishes trust between DB2 and an external entity such as
  - DSN Command Processor
  - Remote Application Server
  - Local Application Server using RRSAF (Resource Recovery Services Attachment Facility)
- Once established, a trusted connection provides the ability to:
  - Efficiently switch auth IDs associated for connections
  - Acquire special set of privileges using a ROLE
  - Acquire special RACF Security Label authority

Trusted security context: Today, you have the option to set a system parameter which indicates to DB2 that all connections are to be trusted. It is unlikely that all connection types, such as DRDA, RRS, TSO, and batch, from all sources will fit into this category. It is likely that only a subset of connection requests for any type and source may be trusted or that you want to restrict trusted connections to a specific server. More granular flexibility will allow for the definition of *trusted connection objects*.

Once defined, connections from specific users via defined attachments and source servers will allow trusted connections to DB2. The users defined in this context can also be defined to obtain a *database role*.

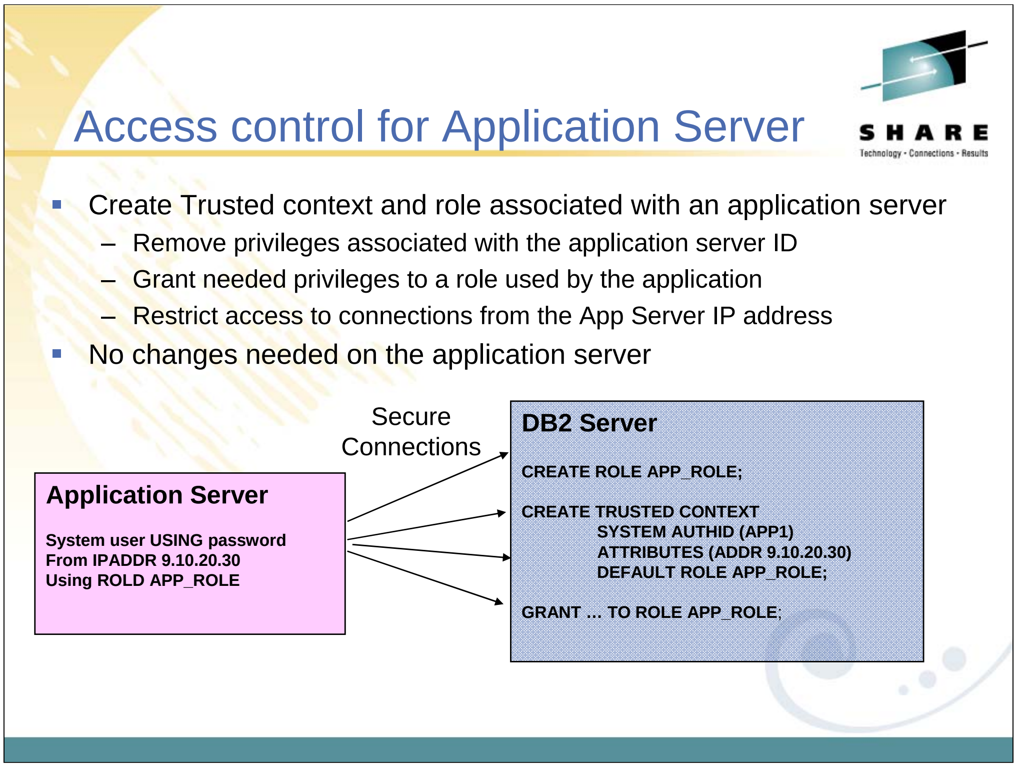
Database role: A database role is a virtual authorization ID that is assigned to the user via the context mentioned next. DB2 privileges are assigned to the defined role.

The role exists as an object independent of its creator, so creation of the role does not produce a dependency on its creator.

This capability can allow a DBA to have privileges to create objects and manage them for a time, even though ownership is to be another id.

The role can be assigned and removed from individuals via the trusted authorization context as needed. This allows a DBA to perform object maintenance during a change control window on a Saturday night, for example. But when Monday arrives, they do not have the authority to do this same work.

Auditing trails of the work completed during the maintenance window are available for verification by a security administrator or auditor.



Access control for Application Server

- Create Trusted context and role associated with an application server
  - Remove privileges associated with the application server ID
  - Grant needed privileges to a role used by the application
  - Restrict access to connections from the App Server IP address
- No changes needed on the application server

Application Server

System user USING password
From IPADDR 9.10.20.30
Using ROLD APP_ROLE

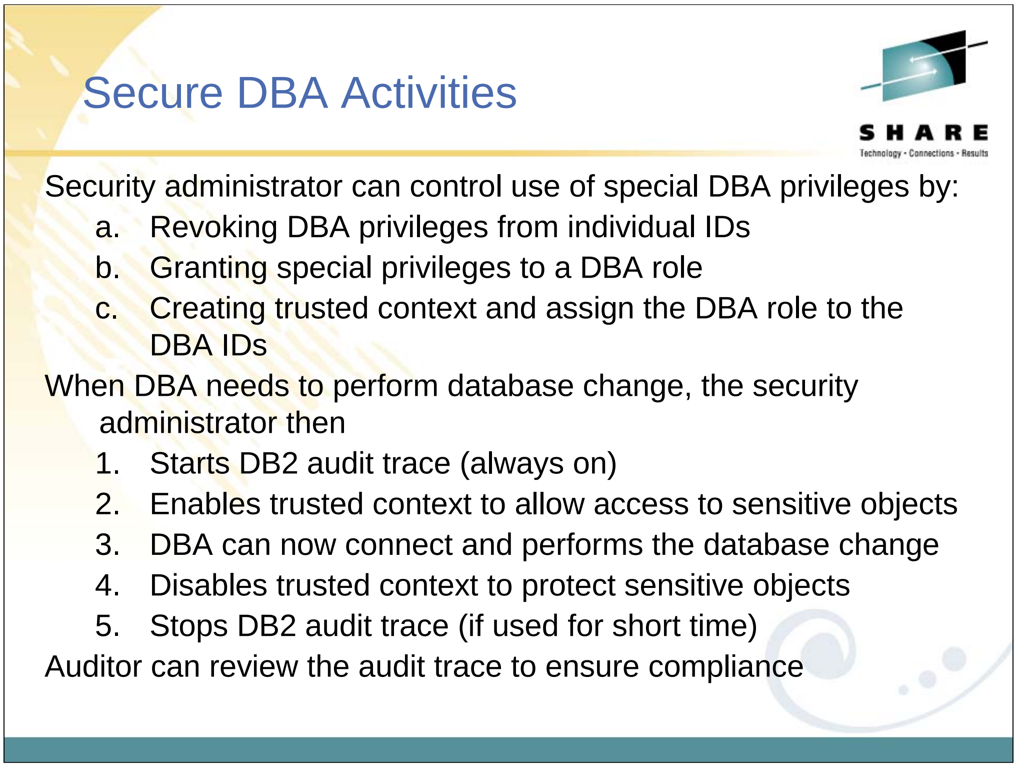
DB2 Server

```
CREATE ROLE APP_ROLE;

CREATE TRUSTED CONTEXT
        SYSTEM AUTHID (APP1)
        ATTRIBUTES (ADDR 9.10.20.30)
        DEFAULT ROLE APP_ROLE;

GRANT ... TO ROLE APP_ROLE;
```

ROLEs and Trusted Context can be used to provide added security for your network-attached application servers. These new capabilities allow the DBA to make GRANT statements conditional, so that they can only be used from a specified list of IP addresses. If someone steals the application server's userid / password, they won't be able to access the database unless they are also able to execute the SQL statement on one of the approved application servers.



Secure DBA Activities

Security administrator can control use of special DBA privileges by:

a. Revoking DBA privileges from individual IDs
b. Granting special privileges to a DBA role
c. Creating trusted context and assign the DBA role to the DBA IDs

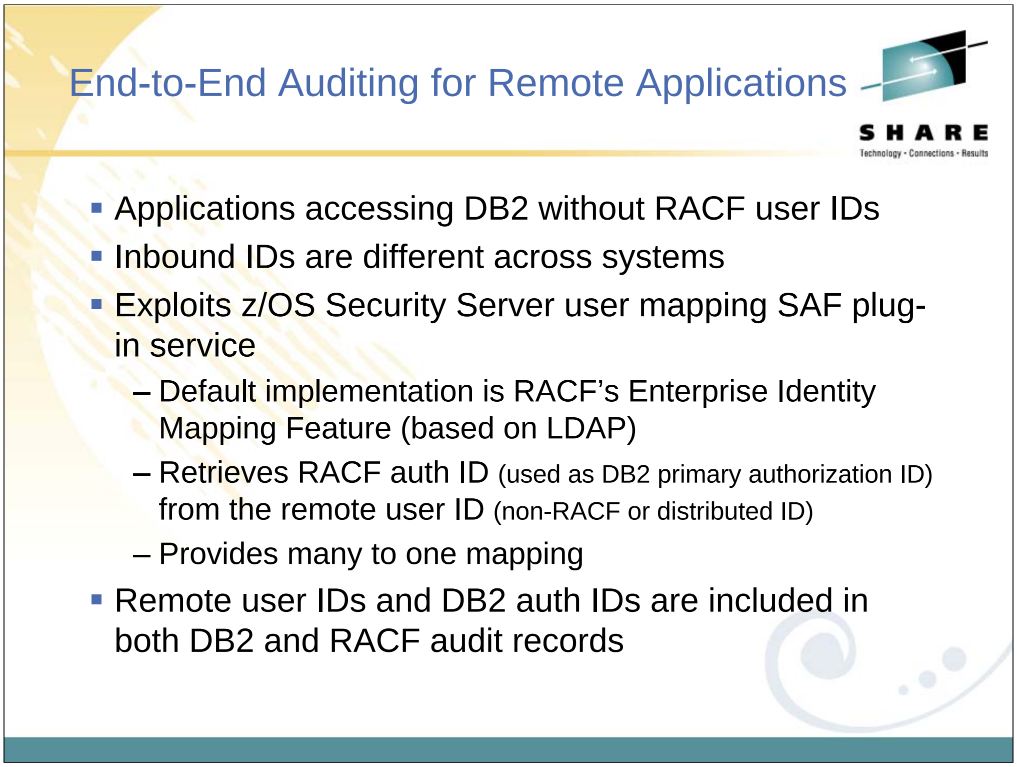
When DBA needs to perform database change, the security administrator then

1. Starts DB2 audit trace (always on)
2. Enables trusted context to allow access to sensitive objects
3. DBA can now connect and performs the database change
4. Disables trusted context to protect sensitive objects
5. Stops DB2 audit trace (if used for short time)

Auditor can review the audit trace to ensure compliance

The Trusted Context and ROLE support can be used to implement DBA privileges that can easily be disconnected and reconnected to individual employees. This provides function similar to shared SYSADM or DBADM userids, but avoids the audit compliance problems associated with shared userids. The ROLEs have the ability to “own” DB2 objects, so that revoking a person’s ROLE does not cause the objects to be cascade deleted.

With these capabilities, customers are able to create DBA procedures that can be audited and protected so that one individual cannot violate the established rules without being detected during the audit review.



End-to-End Auditing for Remote Applications

- Applications accessing DB2 without RACF user IDs
- Inbound IDs are different across systems
- Exploits z/OS Security Server user mapping SAF plug-in service
  - Default implementation is RACF’s Enterprise Identity Mapping Feature (based on LDAP)
  - Retrieves RACF auth ID (used as DB2 primary authorization ID) from the remote user ID (non-RACF or distributed ID)
  - Provides many to one mapping
- Remote user IDs and DB2 auth IDs are included in both DB2 and RACF audit records

The default implementation of the z/OS Security Server RACF (SAF) user mapping plug-in makes use of EIM domain on z/OS. EIM is a LDAP server, which acts as a repository of mappings between an authenticated user registry name and a z/OS user ID.

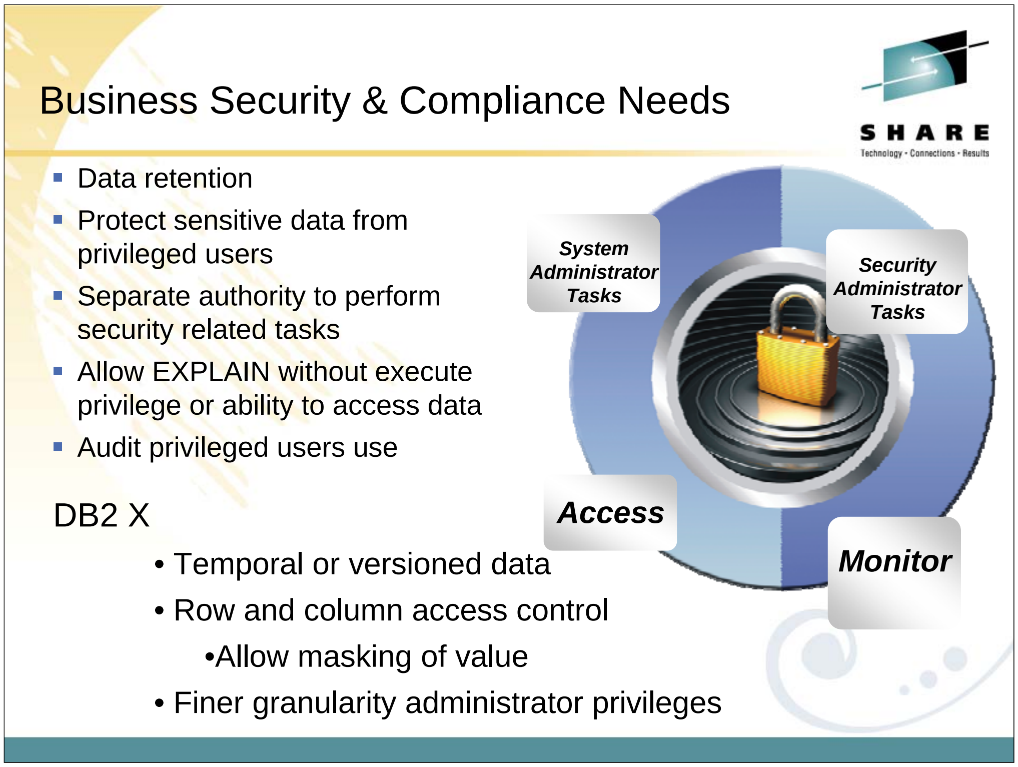
For DB2 to use the SAF user mapping plug-in, you need to set up and configure an EIM domain with user registries and user ID mappings on the z/OS system

To enhance the auditing of user identities who authenticate themselves in a distributed security domain and then access resources on a z/OS system, DB2 provides the original end user identity and the authenticated source registry name (Identity Context) to be included in RACF audit records. z/OS V1.8 or later is required for EIM. More details about EIM can be found at:

http://www.ibm.com/servers/eserver/security/eim/

Trusted connection is established using application server’s user id and password. The user is switched in the trusted connection and client id and registry name are sent to the DB2 server. DB2 maps the registry name and client id to obtain DB2 authorization id. DB2 authorization id is used to determine if the user is allowed to switch in the trusted connection.

See chapter 9 and appendix B in the Securing DB2 and Implementing MLS on z/OS (SG24-6480-01) IBM Redbooks publication for more information on EIM scenario.



Business Security & Compliance Needs

- Data retention
- Protect sensitive data from privileged users
- Separate authority to perform security related tasks
- Allow EXPLAIN without execute privilege or ability to access data
- Audit privileged users use

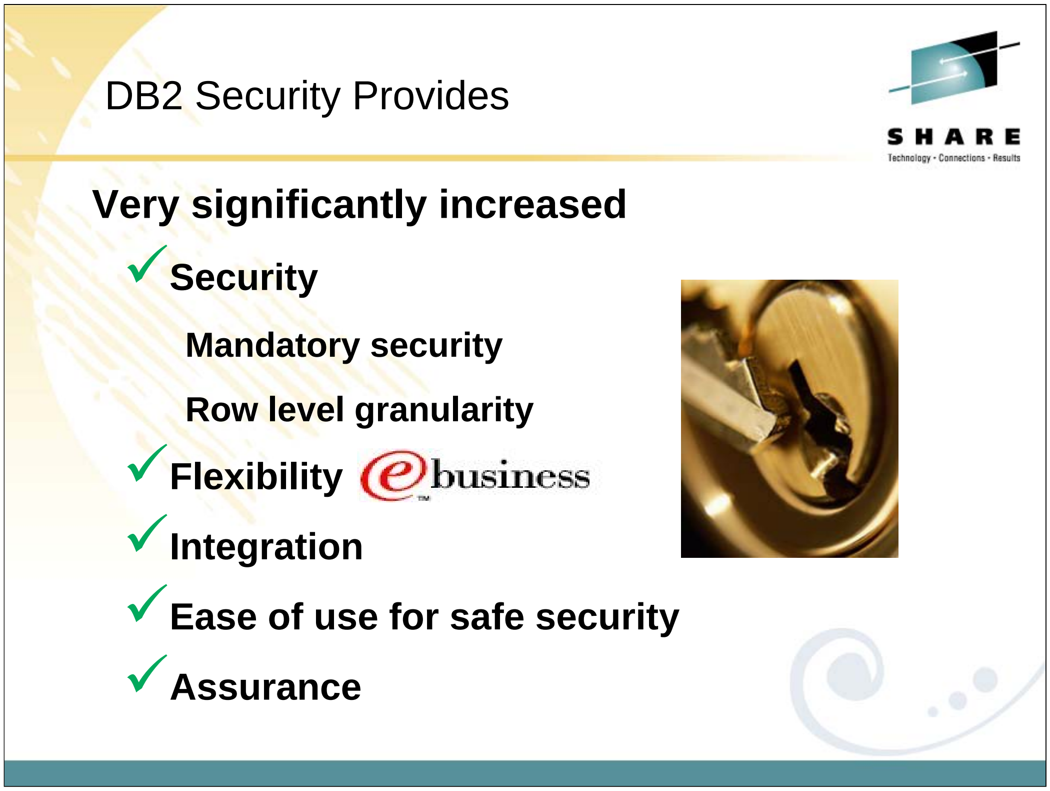
DB2 X

- Temporal or versioned data
- Row and column access control
  - Allow masking of value
- Finer granularity administrator privileges

Customers are being pressed for a wide range of improved security and compliance. Data retention is a growing need. Protecting sensitive data from the privileged users and administrators is required. Separation of authority for security, access, and some common tasks, like EXPLAIN will help. Auditing for privileged users can also make compliance simpler.

In DB2 X, we expect to have a form or temporal data or the ability for a table to contain both current and historical data, and to query the information as of a specific point in time.

Access control is refined in several ways with better granularity for the administrative privileges and with finer grained access control at the row and column level, including the ability to mask access to some fields. Auditing is also enhanced.



DB2 Security Provides

Very significantly increased

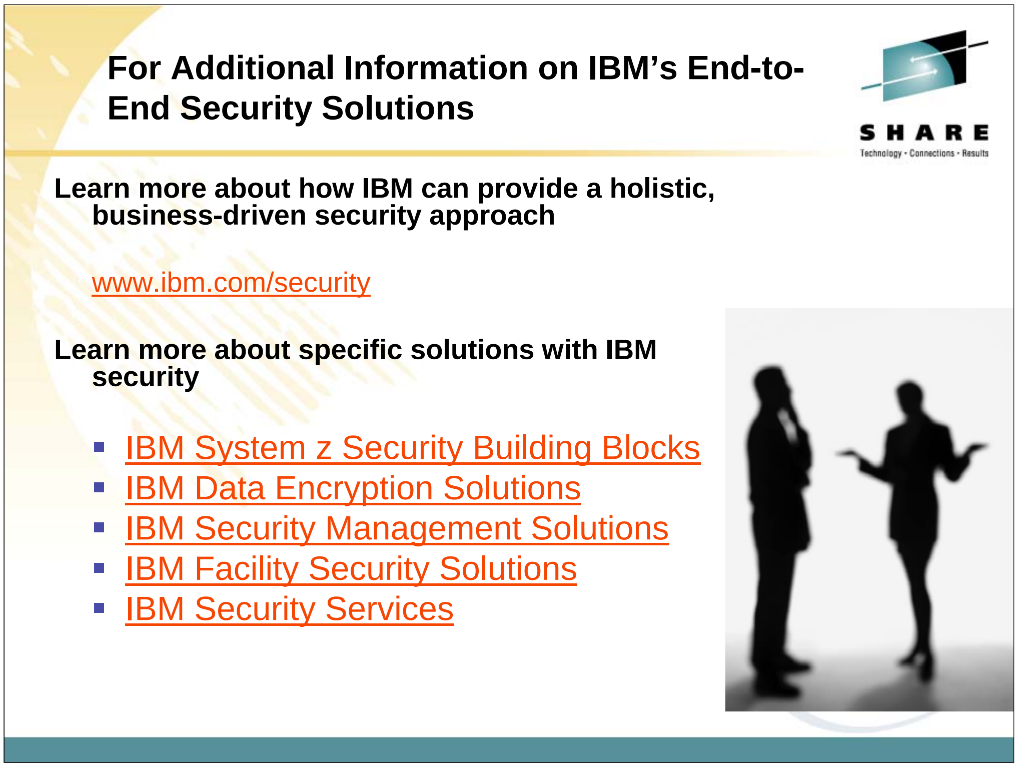
- ✓ **Security**
  - **Mandatory security**
  - **Row level granularity**
- ✓ **Flexibility** *e*business
- ✓ **Integration**
- ✓ **Ease of use for safe security**
- ✓ **Assurance**

Everyone seems to be more aware of security today. Improving integration and making security more robust and easier to manage are very important.

Customers asked for a wide range of enhancements for security. New options for tighter security, more granularity, and more information for additional flexibility in applications and SQL are needed. Improved integration with the hardware and software platform provide a better end-to-end solution.

The design point for DB2 security is being easy to use for safe security, with solid system security and some security that is more flexible, that we'll call application security.

Finally, it will be helpful to see what assurance can be provided, such as certification. DB2 V8 is in evaluation for Common Criteria certification.



For Additional Information on IBM's End-to-End Security Solutions

Learn more about how IBM can provide a holistic, business-driven security approach

www.ibm.com/security

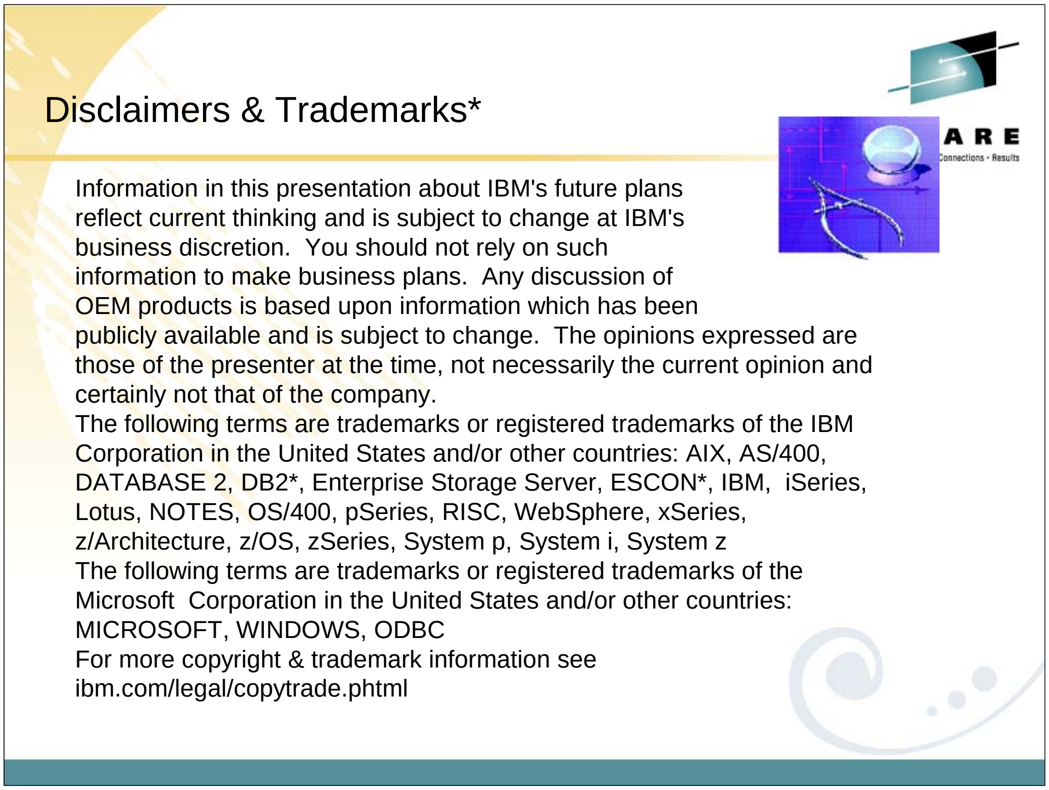
Learn more about specific solutions with IBM security

- IBM System z Security Building Blocks
- IBM Data Encryption Solutions
- IBM Security Management Solutions
- IBM Facility Security Solutions
- IBM Security Services

http://www.ibm.com/security/
http://www.ibm.com/systems/z/advantages/security/features.html
http://www.ibm.com/systems/storage/solutions/data_encryption/index.html
http://www.ibm.com/software/tivoli/solutions/security/
http://www.ibm.com/services/us/index.wss/offerfamily/gts/a1027703
http://www.ibm.com/services/us/index.wss/itservice/iss/a1030786

http://www.ibm.com/security/outlook.html
http://memphistn.rchland.ibm.com/wps/wcm/connect/content_en_US/systems/systems/dynamicinfrastructure
ftp://ftp.software.ibm.com/software/tivoli/whitepapers/outlook_emerging_security_technology_trends.pdf

Disk encryption announcement,
http://www.ibm.com/common/ssi/rep_ca/0/897/ENUS109-120/ENUS109-120.PDF
http://www.ibm.com/systems/storage/
http://www.ibm.com/systems/storage/disk/ds8000/index.html
http://www.ibm.com/systems/storage/solutions/security/



Disclaimers & Trademarks*

Information in this presentation about IBM's future plans reflect current thinking and is subject to change at IBM's business discretion. You should not rely on such information to make business plans. Any discussion of OEM products is based upon information which has been publicly available and is subject to change. The opinions expressed are those of the presenter at the time, not necessarily the current opinion and certainly not that of the company.

The following terms are trademarks or registered trademarks of the IBM Corporation in the United States and/or other countries: AIX, AS/400, DATABASE 2, DB2*, Enterprise Storage Server, ESCON*, IBM, iSeries, Lotus, NOTES, OS/400, pSeries, RISC, WebSphere, xSeries, z/Architecture, z/OS, zSeries, System p, System i, System z

The following terms are trademarks or registered trademarks of the Microsoft Corporation in the United States and/or other countries: MICROSOFT, WINDOWS, ODBC

For more copyright & trademark information see ibm.com/legal/copytrade.phtml

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in the operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only. This information may contain examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.