

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



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.

Highly varied needs for



- ✓ Security
- ✓ Flexibility
- ✓ Ease of safe use
- ✓ Integration
- ✓ Assurance



The logo for "e-business" features a red '@' symbol followed by the word "business" in a black, sans-serif font.

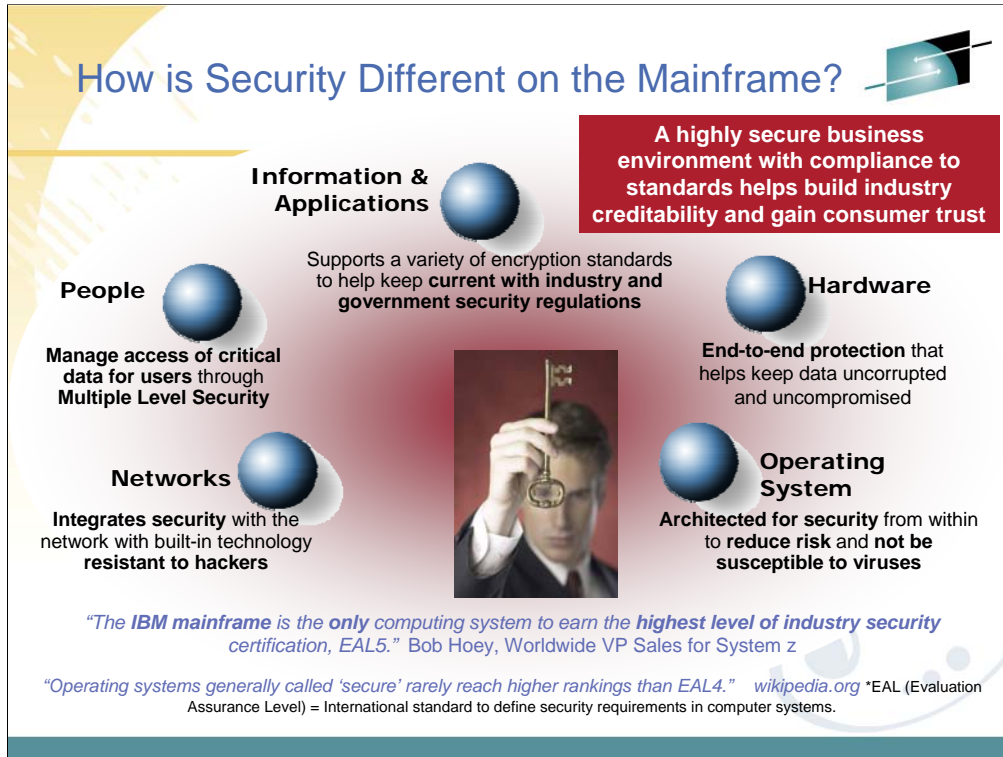


Everyone seems to be more aware of security today. Improving integration and making security more robust and easier to manage are very important.

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, but generally less secure, that we'll call application security.

Finally, it will be helpful to see what assurance can be provided, such as Common Criteria certification.



As we all know, security is one of the hottest topics in the industry these days. You may have heard in the news about data cartridges being lost in transit and legislation demanding higher levels of accountability. Because of unfortunate events like these, security has become a front and center topic in every IT shop. Not surprisingly, there is no better platform to handle the challenges of keeping your data secure than the System z.

System z has a history of ensuring that any and all data residing on it is safe and secure. This goes far beyond the usual measures of other platforms. System z takes a holistic approach to security and is designed so that every component works flawlessly. Each component cooperates with the system as a whole to guarantee the safety of your most important revenue generating items. Everything -- from the data coming through your network to the people allowed to access that data -- is closely monitored, thus providing end-to-end protection of your critical business information.

But how secure is it, really? System z has been certified at EAL level 5. EAL, or Evaluation Assurance Level, is an industry security certification ranging from level 1 through 7. Only 3 systems have reached EAL 5... and they're all IBM machines. That has to give you an idea of the strength of System z security. z/OS has achieved EAL4 certification and DB2 V8 is currently in evaluation at EAL3 for two profiles, CAPP and LSPP.

Layered security



Application code
Web servers
Database servers
Directory and authentication devices
Firewalls
Network and enclave configuration
Operating systems and platforms

Since we know that systems are built and used in layers, the security also needs to be implemented in each layer. The operating systems and platforms are the foundation for security. If the foundation is not secure and strong, then the other layers cannot protect themselves. If security is not stringent, then access to the operating system facilities must be restricted. The network can be the focus for an attack and for defense. Data on a LAN is often very vulnerable unless encryption is used. Firewalls can prevent some problems, but do not address many others. Database servers provide a wide variety of protection mechanisms. The lower levels have stronger defenses. If application code uses the security mechanisms, then the need for assurance is much less. If the application implements security, then much stronger assurance is required. If the application does not pass through the security information, then the ability to use database and operating system security can be compromised.

Security Objectives & Needs



I'll try to go quickly through the introduction to security. I think this is important to make sure we start from the same point.

The needs for security are diverse – in several dimensions. The degree of security needed and the specific concerns differ. The needs and the environment should drive the security policy, which, in turn, drives the security controls. The objective is to match the controls as closely as possible with the security policy, filling in the details.

What are your concerns?
Level of concern?



Destruction of data

Changing data

Reading, confidentiality, disclosure or privacy

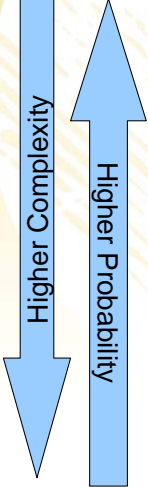

Denial of service

Audit trail

Here are some of the diverse dimensions and concerns for security. The needs will be driven by the type of business, the kinds of data and the business and legal issues for your enterprise. Financial information, health care data and defense have very different statements of security objectives, but some of the same principles apply. More commercial concerns for read access are arising from the need for privacy.

Still, the key concern for most commercial enterprises is being able to do the business, rather than the confidentiality of the information.

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?

SHARE
Technology • Connections • Results

VIEW NOW COMPUTERWORLD Security IDG

SEARCH Google™ Custom Search GO

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 2.3 million 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

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

Managing encrypted data doesn't have to be frustrating.

Simplify with centralized key management

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=EWKLNNAV070507STR1>

<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

Security principles



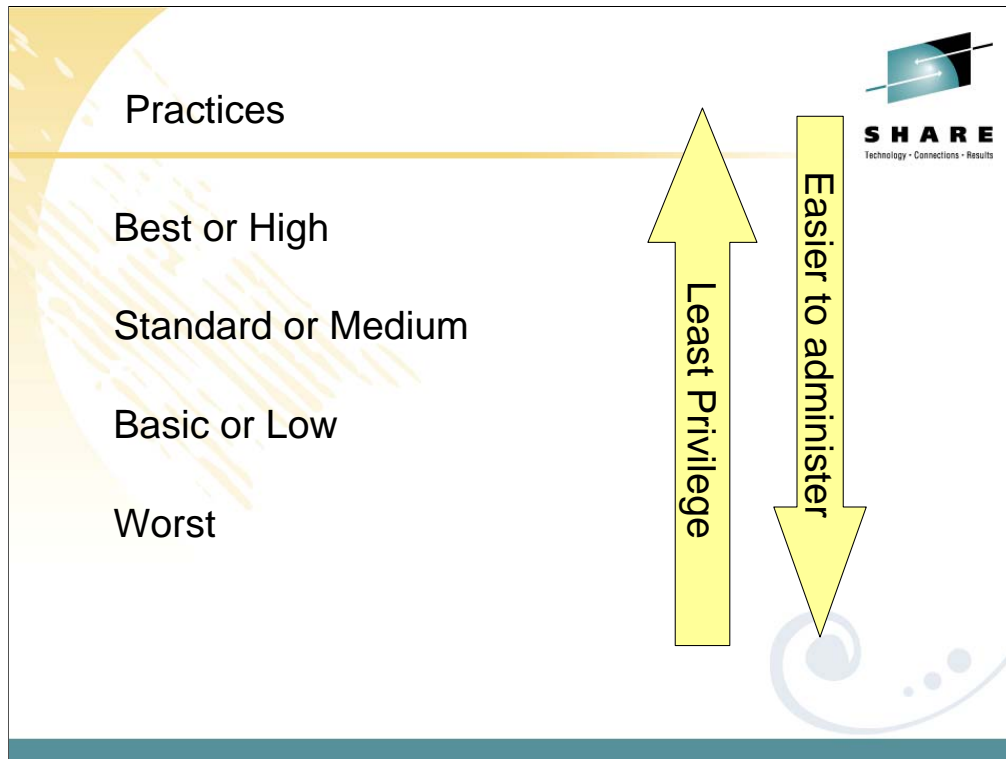
- Layered security
- Individual accountability
- Group & role authorization & ownership
- Least privilege
- Ease of safe use

Since we know that systems are built and used in layers, the security also needs to be implemented in each layer.

Whenever possible, the authorization and ownership should be to or by a group or a role, but the individual who requests information needs to be understood to provide accountability.

“Least Privilege – This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.”

One of the primary concepts in security is giving the individuals only the privileges needed to do the job. That often means using more granular controls. Another key principle is ease of safe use. We want individuals to have all of the privileges they need to do the full job, but no more. If there is less complexity in the security controls, that means less cost and generally results in better compliance.



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



Information Management software

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.

Who do you trust? How much?



No one?	Security officer?
Administrators?	Auditors?
Application programmers?	End users?

What software do you trust?

Operating system?	Security Monitor?
DB2?	Other monitor?
Applications?	Web or PC applications?

The primary job of identification and authentication in DB2 is assigned to the security subsystem. That technique means that access for many resources can be more consistent, whether the resource is a file, a printer, communications or database access. Another way of distinguishing the level of security is the software layer used for the access control. The tightest security would use a single security monitor. Using system controls and subsystems will allow tighter security than having application programs provide the security.

Primary areas to address for all



z/OS

system integrity

security settings

Security monitor: RACF, ACF2, Top Secret

DB2 configuration

Encryption

Auditing

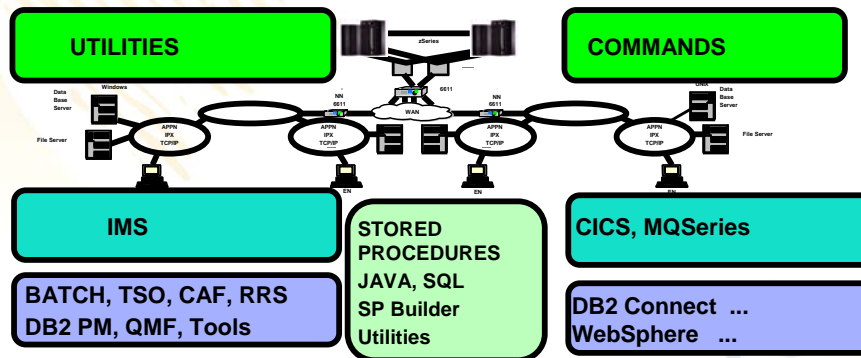
Here are the primary areas for security. I will skip over the sections on the operating system and security monitor. For an example of configuration restriction, see chapter 7, Evaluated Configuration of the Common Criteria in the book, *Planning for Multilevel Security and the Common Criteria*, GA22-7509.

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

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



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.

DB2 configuration



- Subsystem parameters
- Security exits and interfaces
- Encryption options
- Protecting data sets
- Protecting subsystem connection
- Service levels or maintenance

The DB2 configuration has a few parameters with required settings for security, but many other parameters are important to consider. The options, exits and interfaces can make a big difference. Data set protection is provided by the security subsystem. Software currency can also be important for security.

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.

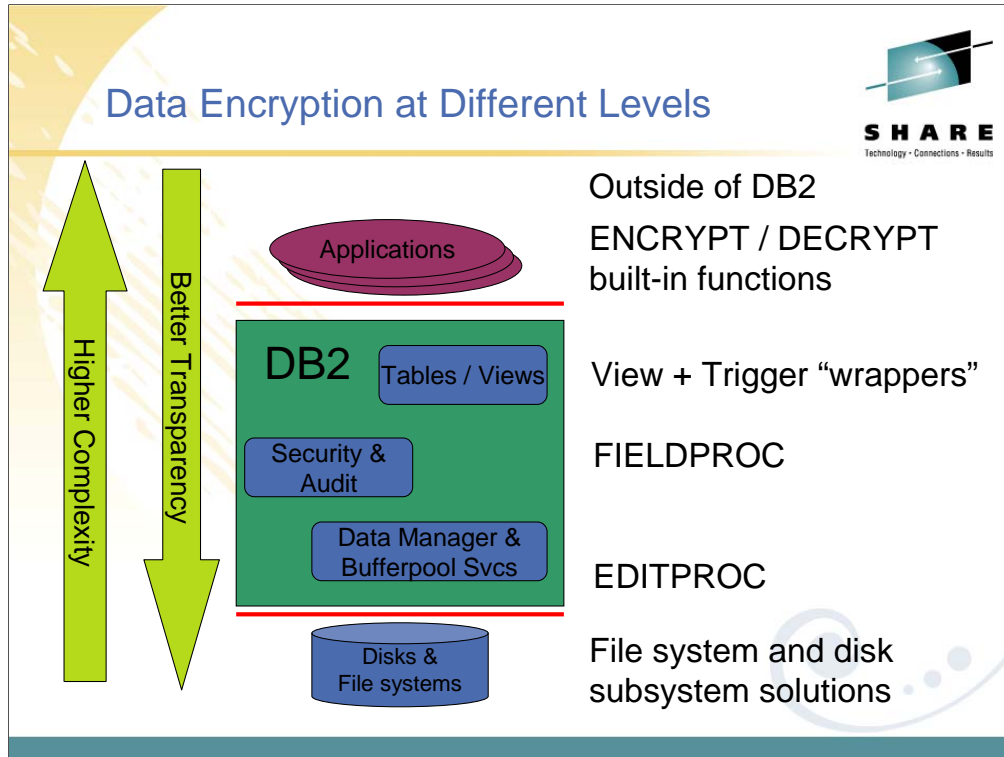
Cryptography and DB2: options



What do you want to protect? From whom? Effort?
Techniques, where to encrypt / decrypt

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
SQL functions (DB2 V8)	General, flexible, invocation needed, no relational range comparisons
On the wire (DRDA V8, SSL V9, IPsec)	General, flexible
Tape Backup (z/OS, TS1130)	General, flexible, IBM hardware & software

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>



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>

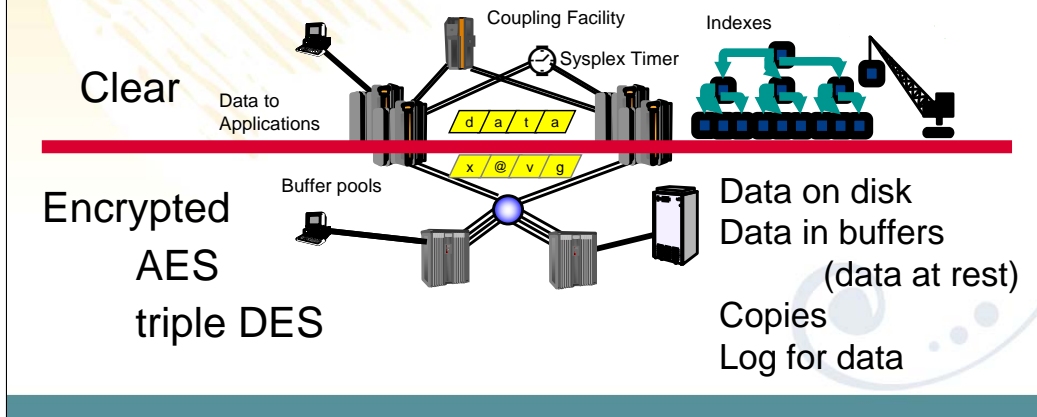
<http://www.redbooks.ibm.com/redbooks/pdfs/sq247111.pdf>

sections 1.1.13 & 1.1.14

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



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.

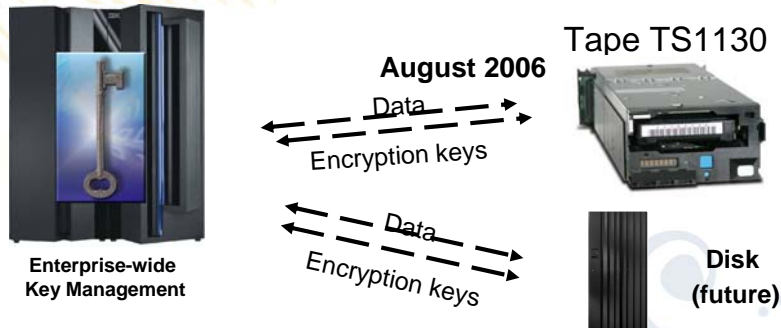
<http://www.ibm.com/software/data/db2imstools/db2tools/ibmencrypt.html>

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

Future Directions – Extending Encryption to IBM TotalStorage



- Statement of Direction: To address customers' growing concern with data security, IBM is announcing a statement of direction for the development, enhancement and support of encryption capabilities within storage environments such that the capability does not require the use of host server resources.
- This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage® portfolio to support outboard encryption and to leverage the centralized key management functions planned for z/OS ICSF.



Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only

Statement of Direction: To address customers' growing concern with data security, IBM is announcing a statement of direction for the development, enhancement and support of encryption capabilities within storage environments such that the capability does not require the use of host server resources.

This includes the intent to offer, among other things, capabilities for products within the IBM TotalStorage® portfolio to support outboard encryption and to leverage the centralized key management functions planned for z/OS ICSF. The first part of this statement of direction is delivered in the TS1120 announced in August 2006 and also in the TS1130.

The rest of the statement of direction is beyond currently announced products, including DB2 9, but a launch has begun.

<http://www.ibm.com/systems/storage/solutions/>

<http://www.ibm.com/systems/storage/solutions/security/index.html>

IBM Information Infrastructure Self-encrypting Tape and Disk Storage



- **Client value**
 - Encrypt data with virtually no input/output performance impact
 - Scale linearly, automatically, and transparently to applications, system administrators, and end-users
 - Secures data less disruptively, more manageably and cost effectively than other alternatives.
- **Reasons to buy**
 - U.S. National Security Agency (NSA) has qualified self-encrypting hard drives for computers deployed by U.S. government agencies and contractors for national security purposes¹
 - Standards-based software encryption key manager to support tape and disk systems
 - Device-level encryption enables compression, de-duplication, and other advanced functions to be performed first, saving space.

Encrypt *all* the data with virtually no performance degradation!



Information Security

http://www.ibm.com/systems/storage/solutions/data_encryption/index.html

Leading the Industry in Self-encrypting Tape and Disk Storage

IBM pioneered tape drives with encryption capability, and announced its 3rd tape drive with encryption in September. IBM has grown tape market share to over 40%, in part, because of this technology.

IBM plans to introduce 2 disk systems with encryption and key management in Q1'09, which we expect to be another first.

IBM's expertise with encryption and key management delivers a highly scalable solution. Nobody else has this capability.

IBM's ability to provide end-to-end encryption (database, TSM, disk, and tape), management with Tivoli Key Lifecycle Manager, and GTS implementation services; could be a game changing value proposition for enterprise clients in 2009.

Content by Allen Marin,

Tape Drive Encryption TS1120 TS1130



- High performance tape drive encryption
 - Cost effectively encrypt large quantities of tape data
 - Avoid Host MIPS encryption overhead
 - Minimize impact to existing processes and applications
- Variety of implementation methods
 - System managed**
 - Library managed TS3500 Tape Library
 - Application managed IBM Tivoli® Storage Manager



The IBM System Storage TS1120 and TS1130 tape drives have been enhanced to provide the customer the option of using drive based data encryption. This encryption capability is now standard on all new TS1120 Tape Drives and is a chargeable upgrade feature for existing installed TS1120 Tape Drives. The encryption capability includes drive hardware as well as microcode additions and changes. Also being introduced is a new, separate IBM Encryption Key Manager component for the Java Platform(TM) program that supports the generation and communication of encryption keys for the tape drives across the enterprise.

The TS1120 based encryption and associated Encryption Key Manager component are supported in a wide variety of operating system environments including z/OS, i5/OS, AIX, HP, Sun, Linux and Windows. In addition, three different encryption management methods are supported: Application, System, or Library Managed. This encryption capability is supported when the TS1120 Tape Drive is integrated or attaches in the IBM System Storage TS3500 Tape Library, IBM System Storage TS1120 Tape Controller Model C06, IBM TotalStorage 3592 Tape Controller Model J70, IBM TotalStorage 3494 Tape Libraries, IBM TotalStorage C20 Silo Attach frame, and standalone environments. For more information on encryption please see:

http://www.ibm.com/servers/eserver/zseries/zos/pdf/White_Paper_ESG_System_z_final.pdf

Is your data encrypted?

SHARE
Technology • Connections • Results

TECH DISPENSER
Tech blogs filtered by humans, not bots

COMPUTERWORLD
Security

JUMP TO More Resources

SEARCH Google™ Cust

Home
News
E-mail Newsletters
Tech Dispenser
+ Shark Bait
- Knowledge Centers
+ Operating Systems
+ Networking & Internet
+ Mobile & Wireless
- Security
Cybercrime & Hacking
Spam, Malware & Vulnerabilities
Security Hardware & Software
Standards & Legal Issues
Privacy
Intellectual Property & DRM
Disaster Recovery
+ Storage
+ Business Intelligence
+ Servers & Data Center
+ Hardware

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.

IS YOUR DATA SECURED RELIABLY?

MORE RELAT

- Ultramobiles hungry, AMT
- Parallels Det released
- Computex: Ir graphics chi

TODAY'S TO

- Microsoft s for next wi
- Beyond iPh gadget tren
- Offshore fi settle H-1B

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.

Protecting data sets Basic



Use RACF, ACF2, Top Secret, etc.

Must be done to prevent direct access

DSN1* usage permitted as required

Protecting subsystem connection Standard

DSNR access profiles

Any program running on z/OS can access the DB2 data sets, unless they are protected. Define userids for the started tasks and prevent almost every other id from accessing the DB2 data sets. There are some exceptions for administrators who must manage the logs or work with the DSN1* utilities. Having separate ids for each subsystem is the standard recommendation.

Access control for the subsystem can be used for some separation, for example of test from production.

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, and 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

SHARE
Technology • Connections • Results

100 BEST PLACES TO WORK IN IT 2007 VIEW NOW

COMPUTERWORLD
Security

IDG

JUMP TO More Resources

SEARCH Google Custom Search

Home
News
E-mail Newsletters
Tech Dispenser
Shark Bait
Knowledge Centers
Operating Systems
Networking & Internet
Mobile & Wireless
Security
Cybercrime & Hacking
Spam, Malware & Vulnerabilities
Security Hardware & Software
Standards & Legal Issues
Privacy
Intellectual Property & DRM
Disaster Recovery
Storage
Business Intelligence
Servers & Data Center
Hardware
Software

Oracle ships critical update for database, applications

Fifty-one holes plugged, including one that maxes out the CVSS vuln scale

Sumner Lemon Today's Top Stories • or Other Security Stories •

October 17, 2007 (IDG News Service) – Oracle Corp. released its latest critical patch update on Wednesday, fixing 51 vulnerabilities in a range of products, including its flagship database line.

Oracle's critical patch update fixes holes in Oracle Database Server, Oracle Application Server, Oracle Enterprise Manager, Oracle E-Business Suite, and Oracle PeopleSoft Enterprise. Twenty-seven of the patched vulnerabilities are found in Oracle Database Server, including the most serious vulnerability fixed.

"The most critical, rating 6.5 with the new CVSS 2.0 metric, is a problem in the import utility," said Alexander Kornbrust, managing director of Red Database Security GmbH, which found 13 of the 27 vulnerabilities in Oracle Database Server that are patched with this update.

CVSS 2.0, or Common Vulnerability Scoring System version 2.0, is a rating system developed by the Forum of Incident Response and Security Teams as a way of measuring the severity and urgency of IT vulnerabilities. The vulnerabilities patched by Oracle's latest critical update have CVSS 2.0 ratings from 4.0 to 6.5.

The vulnerability in the import utility could allow an attacker to run code on a database as the user SYS, Kornbrust said. SYS is the most powerful user in an Oracle database, and is able

so consumers have another way to verify their security.

With Extended Validation

MORE RELATED CONTENT

- Critical Oracle patches come next week
- Oracle posts big gains for quarter
- BNSF Railway to upgrade back office with SAP software

TODAY'S TOP STORIES

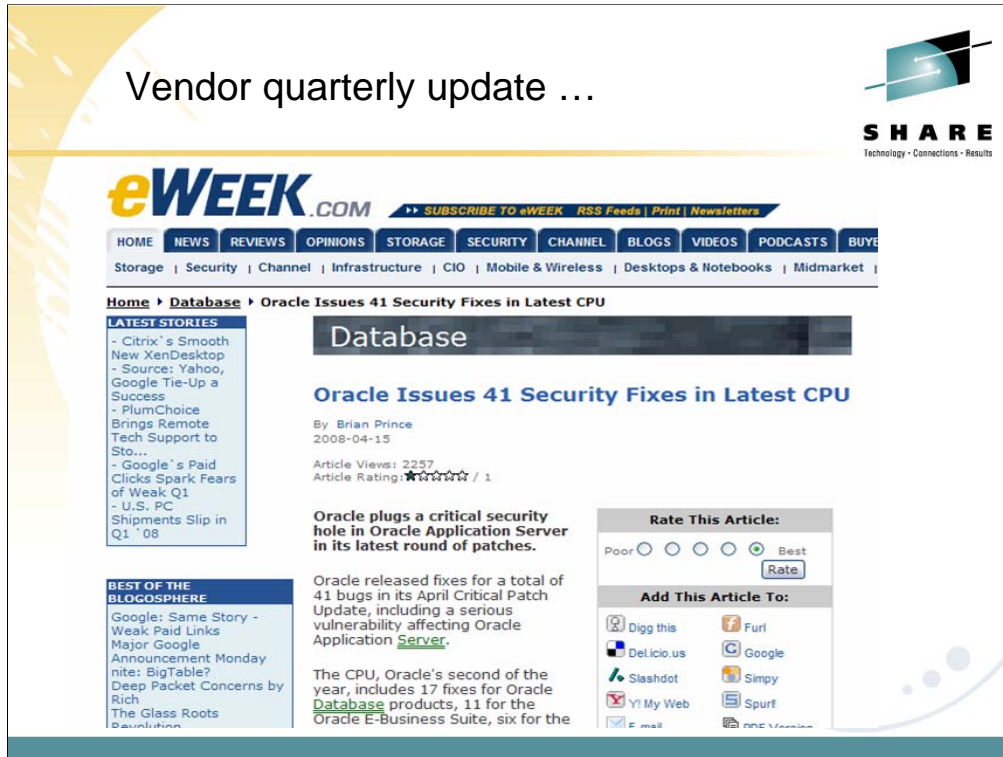
- HD Moore takes iPhone exploits public
- Oracle ships critical update for database, applications
- SAP buys BPM vendor boost NetWeaver

More top stories •

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9042942&source=rss_topic17

The patch situation is not exactly the same on some other platforms. System z, z/OS and DB2 for z/OS are not perfect, but this level of problems was addressed many years ago with system integrity, security design and a more conservative approach.

The IBM System z commitment to system integrity and security was made in 1970s and 1980s, then reiterated and improved in the past 30 years. A bad quarter on DB2 for z/OS would be to have one update that might be usable. A critical update would mean a bad decade.



eWeek Oracle Issues 41 Security Fixes in Latest CPU

By Brian Prince 2008-04-15

Oracle plugs a critical security hole in Oracle Application Server in its latest round of patches.

Oracle released fixes for a total of 41 bugs in its April Critical Patch Update, including a serious vulnerability affecting Oracle Application Server.

The CPU, Oracle's second of the year, includes 17 fixes for Oracle Database products, 11 for the Oracle E-Business Suite, six for the Oracle Siebel Enterprise Suite, three for Oracle Application Server, three for the PeopleSoft-JD Edwards Suite and one for Oracle Enterprise Manager.

...

January's CPU featured 26 security fixes for Oracle products. The next CPU is slated to be released July 15.

<http://www.eweek.com/c/a/Database/Oracle-Issues-41-Security-Fixes-in-Latest-CPU/>

Vendor quarterly update ...

SHARE
Technology • Connections • Results

COMPUTERWORLD
Security

SEARCH Google Custom Search GO

[Corporate Network Safety at Employees' Homes](#) |
 [Case Study - Simplifying Network Infrastructure and Reducing Costs](#) |
 [Video - Drive-By Download](#) |
 [Secure Remote Access Anytime, Anywhere](#)

Oracle issues 36 patches, but is anyone applying them?

DBAs face quarterly conundrum: To patch or not to patch

By Jaikumar Vijayan

October 15, 2008 (Computerworld) Many database administrators don't always apply security patches to their environments in a speedy fashion, but that's not stopping Oracle Corp. from releasing dozens of them on a quarterly basis.

The latest batch was released yesterday and includes fixes for 36 newly discovered vulnerabilities across a wide range of Oracle products.

The update was smaller than usual for Oracle and included fixes for 15 vulnerabilities in its database products, six in its application server products, and five in its e-business suite of products. The patches were released as part of the company's quarterly critical patch update schedule which it introduced in November 2004.

The most severe of the flaws, according to a post in an Oracle company blog, is a vulnerability that affects an Apache plug-in for the Oracle WebLogic Server that the company inherited in its purchase of BEA Systems Inc. earlier this year.

Oracle said the flaw can be exploited remotely and gave it a rating of 10, the highest level on the company's severity scale. A total of 11 of the flaws disclosed yesterday can be exploited remotely and therefore pose a greater danger than vulnerabilities that require an attacker to be authenticated on a system, according to Oracle.

The latest update is smaller than most of Oracle's typical quarterly updates and appears to present less serious threats than usual, said Amichai Shulman, chief technology officer at database security firm Imperva Inc., which discovered two of the vulnerabilities that were patched this week. But what continues to be surprising is that some of the patches appear to be addressing issues for which patches had been issued previously, he said.

INTRODUCING THE NEW
SonicWALL E-CLASS
SO MUCH FOR THE STATUS QUO.

SONICWALL
PROTECTION AT THE SPEED OF BUSINESS

SEE E-CLASS DEMO NOW >

RESOURCE ALERTS

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9117266&source=NLT_SEC&nid=38

Oracle issues 36 patches, but is anyone applying them?

DBAs face quarterly conundrum: To patch or not to patch

By Jaikumar

October 15, 2008 (Computerworld) Many database administrators don't always apply security patches to their environments in a speedy fashion, but that's not stopping Oracle Corp. from releasing dozens of them on a quarterly basis. The latest batch was released yesterday and includes fixes for 36 newly discovered vulnerabilities across a wide range of Oracle products.

The update was smaller than usual for Oracle and included fixes for 15 vulnerabilities in its database products, six in its application server products, and five in its e-business suite of products. The patches were released as part of the company's quarterly critical patch update schedule which it introduced in November 2004.

The most severe of the flaws, according to a post in an Oracle company blog, is a vulnerability that affects an Apache plug-in for the Oracle WebLogic Server that the company inherited in its purchase of BEA Systems Inc. earlier this year.

Oracle said the flaw can be exploited remotely and gave it a rating of 10, the highest level on the company's severity scale. A total of 11 of the flaws disclosed yesterday can be exploited remotely and therefore pose a greater danger than vulnerabilities that require an attacker to be authenticated on a system, according to Oracle.

The latest update is smaller than most of Oracle's typical quarterly updates and appears to present less serious threats than usual, said Amichai Shulman, chief technology officer at database security firm Imperva Inc., which discovered two of the vulnerabilities that were patched this week. But what continues to be surprising is that some of the patches appear to be addressing issues for which patches had been issued previously, he said.



<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.

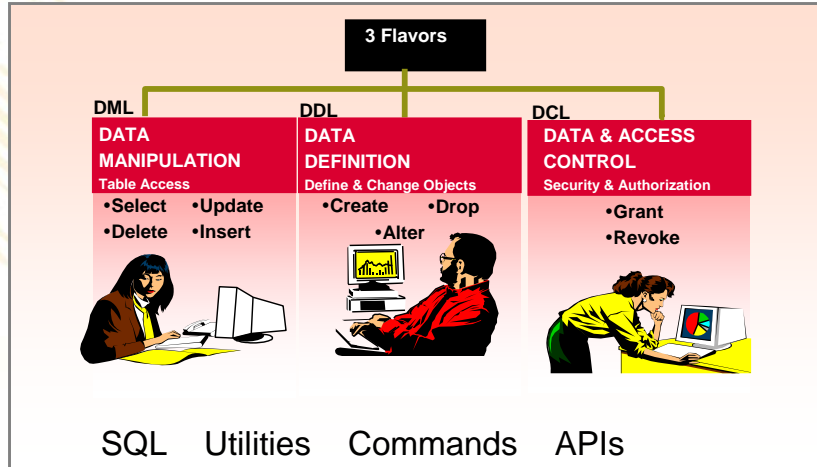
You must plan to use RACF facilities more, like groups and patterns. The implementation team needs both DB2 and RACF knowledge for implementation.

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>

Structured Query Language (SQL)



SQL or the Structured Query Language is generally separated into the ability to

- manipulate data: get information via SELECT or modify via INSERT, UPDATE and DELETE
- define data: CREATE new objects, ALTER them or DROP them
- data access and control: GRANT and REVOKE provide the built-in security.

There are many other interfaces into DB2: utilities, commands, and other Application Programming Interfaces (API). Security and authorization are included in GRANT and REVOKE for all of the interfaces.

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.

Using a VIEW Basic to Standard



Retrieve from CUSTOMER table
using SW_CUSTOMER view

```
SELECT CUST_NBR, CUST_NAME,  
       CUST_REGION  
FROM SW_CUSTOMER  
WHERE CUST_CREDIT = 'AAA'
```

or without the SW_CUSTOMER view

```
SELECT CUST_NBR, CUST_NAME,  
       CUST_REGION  
FROM CUSTOMER  
WHERE CUST_REGION = 'SW'  
AND CUST_CREDIT = 'AAA'
```

Join to remove information

This example shows the ability to simplify. Using the view, only the additional qualification is needed. Often a view can be used to handle more complex logic, such as a multiple table join or UNION (in Version 7). The person who uses the view does not need to be concerned with the join, UNION or authorization concerns, if those are addressed in the view.

Session Variables: Standard to Best



- Variables set by DB2, connection or signon exit
- Built in function to retrieve value for a variable
 - Use function in views, triggers, stored procedures & constraints to enforce security policy
- Can have more general, flexible access checks
 - Multiple columns, AND/OR logic, ...
- Complements other security mechanisms

```
CREATE VIEW V1 AS SELECT * FROM T1 WHERE  
COL5 = GETVARIABLE('SYSIBM.SECLABEL');
```

Session Variables provide another way to provide information to applications. Some variables will be set by DB2. Others can be set in the connection and signon exits to set these session variables

A new built-in function **GETVARIABLE** is added to retrieve the values of a session variable. This function can be used in views, triggers, stored procedures and constraints to help enforce a security policy. If your primary security need is more general, flexible controls, this information complements other security mechanisms.

For example, you can have a view which provides data that is at the user's current security label.

Session Variables ...



Set by DB2 SYSIBM.varname

- PLAN_NAME
- PACKAGE_NAME
- PACKAGE_SCHEMA
- PACKAGE_VERSION
- SECLABEL
- SYSTEM_NAME
- VERSION
- DATA_SHARING_GROUP_NAME
- SYSTEM_ASCII_CCSID
- EBCDIC
- UNICODE

Set by connection & signon exits

- Up to 10 variables SESSION.varname

The session variables set by DB2 are qualified by SYSIBM. You can get the plan name, package name (schema, name and version), the user's seclabel, DB2 subsystem name, data sharing group name, version and CCSID information. This information is useful for security controls, but programmers have other needs for this information as well.

Customers can add up to ten variables, with the qualifier SESSION, by setting the name and value in the connection and signon exits. Both the name and the value allow up to 128 characters. Session variables can be accessed, but not changed, in applications.

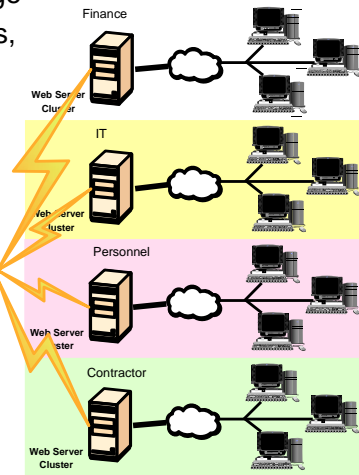
Multilevel Security and DB2 Best



- 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	46	Canada	29%

Data
Single Data Store



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>




Network security:	
Use Kerberos, Passticket	Best
Enterprise Identity Manager	Best
Encryption of passwords web and on disk	Basic
Better to encrypt session	Standard or High
DRDA	Standard
SSL	Best
IPSec	Best
Do NOT use already verified	Basic
Do not trust a client	Basic

Network security is a very important area. The Kerberos and Passticket techniques provide the best security for identification and authentication. If the data is sensitive and uses a network, then protecting or encrypting the network communication is required. If you need to use passwords, then encrypt `SYSIBM.SYSUSERNAMES`. APAR PQ95205 for V8 adds the ability to encrypt the user and password in the `SYSIBM.USERNAMES` catalog table.

In any case, if you use already verified or trust a client, then the server can be compromised whenever a client is compromised. These are generally unacceptable choices with today's understanding of security.

See the DB2 Administration Guide for much more on this topic.

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.

IBM Information Infrastructure Auditability

IBM Tivoli zSecure Suite: Administration, Audit, Alert Management



Client value

- Improves efficiency of mainframe administration and provisioning
- Enables enterprise wide, cross-platform visibility into the organization's security and compliance posture.*

Reasons to Buy

- Provides capability to report all transactions, detect exposures, and execute status audit
 - Creates a transparency of the definitions that control the system security
 - Raises awareness of violations and intrusions
 - Monitors user activity
 - Improves security and incident handling
- * via integration with Tivoli Security Information and Event Manager

Extend auditability Best Practices to the mainframe environment, improving security posture



Information Security



Information Compliance

<http://www.ibm.com/software/tivoli/products/zsecure/>

New version 1.10 available Q4 2008

New version expected in Fall 08 (December)

Audit & Admin are cornerstone solutions, and others extend the functionality & capabilities

Content by Kelly Schupp

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.

Audit data sources



- DB2 catalog
- audit, accounting and performance traces
- recovery log, current & historical data
- RACF audit facility, other SMF data, ...

Audit tools and techniques

- SQL queries on catalog, other data
- tracing: audit, performance, accounting, monitor
- formatting the traces: Omegamon, DB2 PE or PM,
- Consul, DB2 Audit Management Expert, DSN1SMFP, others
- log formatting: tools, DSN1LOGP, Log Analyzer
- various recovery and cloning techniques
 - REPORT RECOVERY
 - RACF print, unload

Notes on audit data sources, information, tools & techniques

- DB2 catalog: SQL Reference, some queries in Admin book
 - audit, accounting and performance traces - Audit chapter of Admin, details in Admin; traces in Command Reference & DSNWMSGs
 - recovery log – Admin appendix, DSNDQJ00
 - RACF audit facility, other SMF data, ... RACF Access Control Module Guide, RACF books, z/OS SMF book
- audit tools and techniques:
- SQL queries on catalog, other data Some in Admin
 - tracing: Command Reference, Admin. Audit chapter, DSNWMSGs
 - formatting traces: Omegamon, DB2 PE, DB2 PM, DB2 Audit Management Expert, See Omegamon books, Report Reference
 - Consul audit tool, DSN1SMFP (if you don't have products)
 - log formatting: tool, DSN1LOGP, Admin, Utility Guide
 - various recovery and cloning techniques: REPORT RECOVERY: Utility Guide and Administration Guide
 - RACF print, unload: RACF documentation

DB2 Instrumentation Records IFCIDs for Audit



Accounting Audit	0003	successful access
	0140:	Audit all authorization failures
	0141:	Audit all grants & revokes
	0142:	Audit DDL Create / Alter / Drop
	0143:	Audit First Write
	0144:	Audit First Read
	0145:	Audit DML Statement
	0314:	Authorization Exit Parameters
Performance	0004:	Trace Start
	0005:	Trace Stop
	0023:	Utility Start
	0024:	Utility Change
	0025:	Utility End
	0106:	System Parameters
	0247:	input host variables
	0350:	SQL Statement
	...	

Here are some suggested audit traces and other traces. These traces were chosen for a DB2 V8 Common Criteria audit. Most of the audit products will format all of them. The instrumentation has information about the performance, resources, and processes, as well as security and specific sensitive data audits. If more detailed information is required, you can also examine the individual SQL statements (IFCID 0350), input host variables (IFCID 0247), record accesses and locking. Other detailed trace data allows full accounting by user or transaction, with detailed data written every plan deallocation or change of user and fully detailed tracing down to individual call / IO / component level.

If you are using DB2 9, then add Audit class 10 IFCIDs 269 and 270.

DB2 security audit suggestion: catalog table queries



Audit class 1, 2, 3

0140: audit all authorization failures
0141: audit all grants & revokes

DB2 9 audit class 10: audit trusted context

0269: establish trusted connection and switch user
0270: CREATE & ALTER TRUSTED CONTEXT statements

Performance

0004: Trace Start
0005: Trace Stop
0106: System Parameters

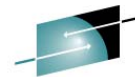
Here is a minimal audit trace intended to cover only auditing for security – not the specific auditing for changes or access to data. The performance overhead for these traces should be much smaller than 0.01% unless you have severe security problems. The primary records are IFCIDs 0140 and 0141. Authorization failures need to be understood. Finding and correcting authorization errors is important to avoid widening exposures. IFCIDs 0004, 0005, and 0106 ensure that system security is functioning and that the audit trace data is complete.

The primary cost of these audit classes is writing the data to a monitor (1X), GTF (2X), or SMF (4X). Context switch can occur frequently, but all others should have negligible performance and space concerns, as they should be very infrequent.

Also use queries on the DB2 catalog tables to answer most authorization questions.

If you are running DB2 9, then these trusted context audit records should be added to the prior page and used whenever trusted contexts exist.

Streamlined Compliance in DB2 9 for z/OS



SHARE
Technology • Connections • Results

- DB2 9 built on security of V8 and provides even greater control, flexibility and audit
- DB2 9 provides more flexible authorization and control
 - Database Roles
 - Trusted Context
 - Audit: Improved audit selectivity improves security performance, problem isolation and performance monitoring
- Extend encryption to tape controller (now) and disk storage (future direction)



Common Criteria security certification: DB2 for z/OS V8 evaluated at EAL3+ level.

DB2 for z/OS V8 provides many enhancements for security, DB2 9 builds on that base and improves control, flexibility and ability to audit. DB2 9 roles are used to provide a more flexible technique than groups or users in assigning and controlling authorization, while improving consistency with the industry. A network trusted context provides a technique to work with other environments more easily, improving flexibility. The instead of trigger is an SQL technique that allows a trigger to be used in place of a view update, consistent with DB2 for LUW. Improved audit selectivity is needed for being able to see that security is functioning. Secure Socket Layer or SSL implementation provides encryption of data on the wire. Some additional techniques for data encryption will help protect data at rest and in backups – now for tapes and in the future for disks.

Common Criteria: z/OS V1.7 with the RACF optional feature has achieved EAL4+ for Controlled Access Protection Profile (CAPP) and Labeled Security Protection Profile (LSPP). DB2 for z/OS Version 8 is evaluated under the Common Criteria for CAPP and LSPP with a conformance claim of EAL3+, earning the service mark above.

See:

<http://www.ibm.com/systems/z/security/>

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

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

http://www.ibm.com/security/standards/st_evaluations.shtml

<http://www.ibm.com/software/tivoli/governance/action/08162007.html>



BSI-DSZ-CC-0286-2008

IBM DB2 Universal Data Base for z/OS Version 8 (DB2 UDB V8) and the IBM z/OS Version 1 Release 6 operating system (z/OS V1R6) from International Business Machines (IBM) Inc.

PP Conformance: Labeled Security Protection Profile (LSPP), Version 1.b, 8 October 1999, and the Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999

Functionality: PP conformant plus product specific extensions, Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant EAL 3 augmented by ADV_SPM.1, ALC_FLR.1

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using *the Common Methodology for IT Security Evaluation, Version 2.3* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)*.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

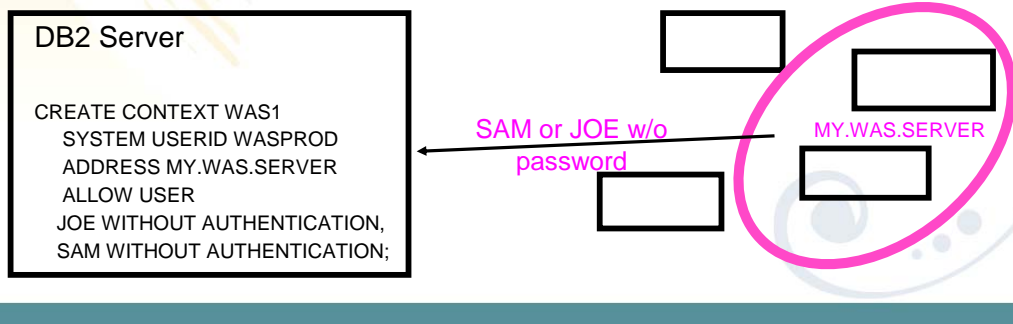
This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 25. January 2008

Network Trusted Security Context



- Identifies “trusted” DDF, RRS Attach, or DSN application servers
- Allows selected DB2 authids on connections without passwords
 - reduces complexity of password management
 - reduces need for an all-inclusive “system authid” in app servers
 - more visibility/auditability of which user is current running
 - enables mixed security capabilities from a single app server



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 ROLES



ROLE is a “virtual authid”

- Assigned via TRUSTED CONTEXT
- Provides additional privileges only when in a trusted environment using existing primary AUTHID.
- Can optionally be the OWNER of DB2 objects

```
CREATE ROLE PROD_DBA;  
GRANT DBADM ... TO PROD_DBA;  
  
CREATE TRUSTED CONTEXT DBA1 ...  
  DEFAULT ROLE PROD_DBA OWNER(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.

Improved audit: DB2 Trace Filtering

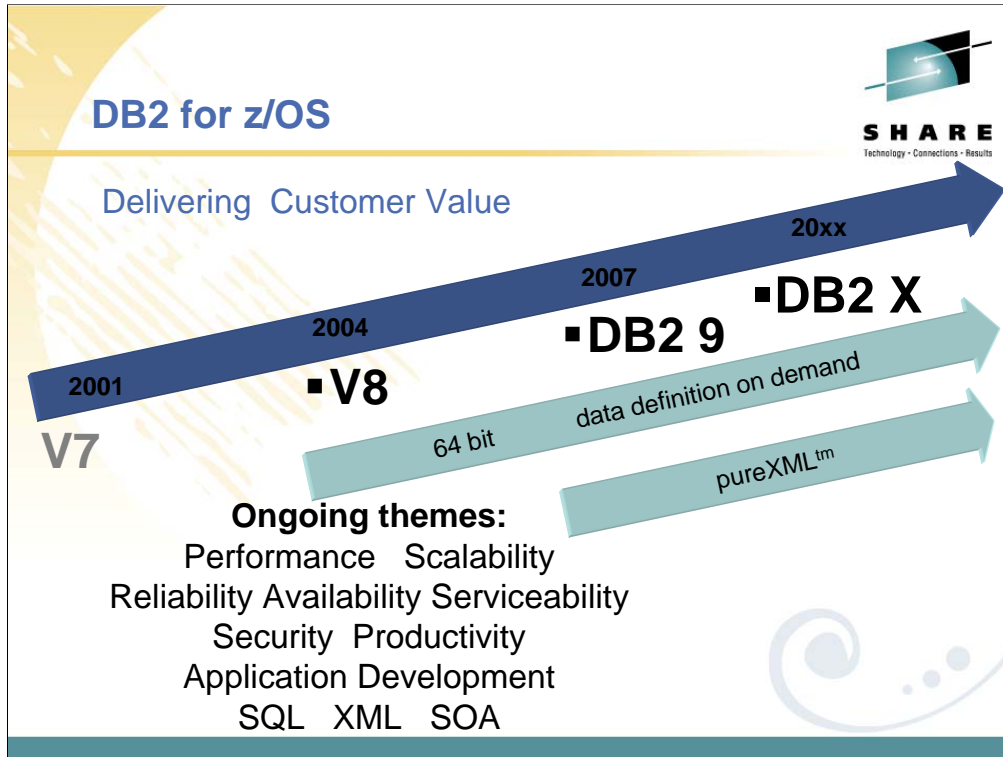


New filtering capabilities for `–START TRACE` that `INCLUDE` or `EXCLUDE` based on these keywords:

- USERID -- client userid
- WRKSTN -- client workstation name
- APPNAME -- client application name
- PKGLOC -- package LOCATION name
- PKGCOL -- package COLLECTION name
- PKGPROG -- PACKAGE name
- CONNID -- connection ID
- CORRID -- correlation ID
- ROLE – end user’s database ROLE

Improved trace filtering makes the jobs of auditing and of performance management easier. Many more options can be used to minimize the amount of data collected, so the overhead is reduced and the extraneous data does not need to be processed.

Wild cards can be used to trace generics, rather than needing a full list of names.



DB2 for z/OS V7 became generally available (GA) March 2001, and V8 delivered three years later. DB2 9 became generally available in March 2007, three more years. We expect the next version will be 2.5 roughly 3 years from DB2 9 GA to GA of DB2 10 or DB2 X or whatever the name becomes.

The themes for future versions will continue to focus on core platform strengths of performance, scalability, reliability, stability, availability, resilience, and security. PureXML and Schema evolution or data definition on demand will be ongoing for a long time. In contrast, most of the 64 bit evolution should be completed in DB2 X.

The key interfaces for customers and vendors expand for both XML and for SQL. Information is a key leg of the SOA platform, and DB2 for z/OS provides many advantages for data management in SOA.

Standards, interoperability, portability and security along with secure access using the latest technologies are key touch points. Productivity improvements for application developers and for database administrators are very important as data grows in scale and complexity.

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** 
- ✓ **Integration**
- ✓ **Ease of use for safe security**
- ✓ **Assurance**

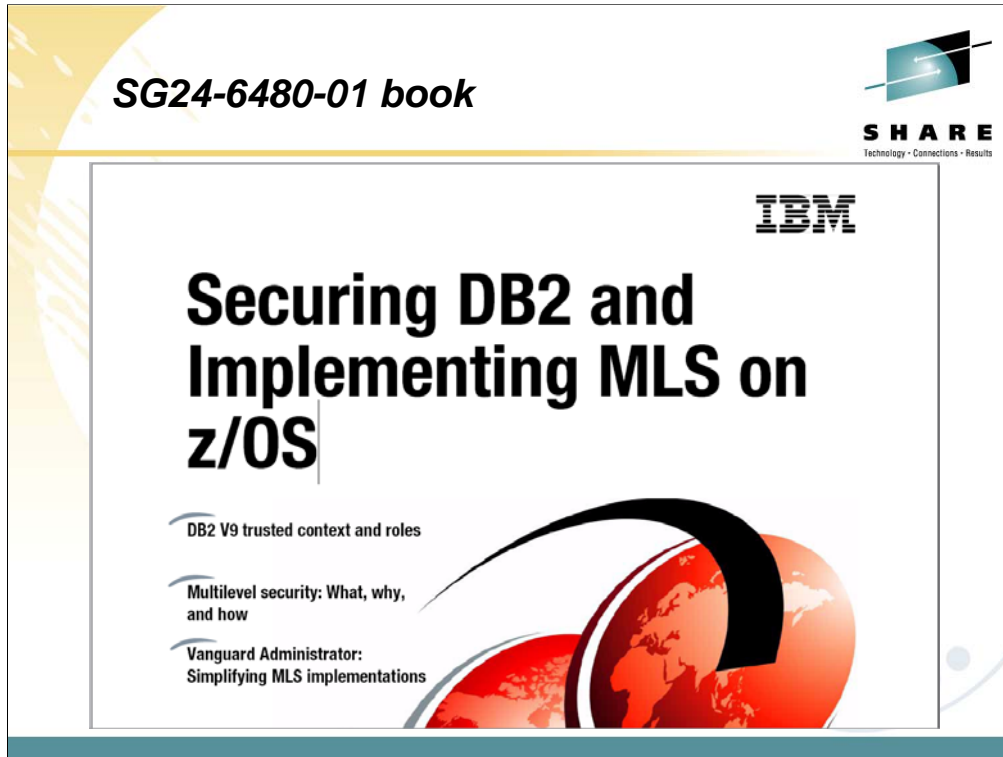


Everyone seems to be more aware of security today. Improving integration and making security more robust and easier to manage are very important.

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.



This is the recently updated redbook, SG24-6480-01, describing DB2 9 security enhancements. It discusses use of multi-level security and the new DB2 9 security enhancements.

The DB2 9 for z/OS Technical Overview, SG24-7330, chapter on security, chapter 10, also provides a description of the DB2 improvements in security.

Other books: DB2 9 in **IBM Redbooks**


- DB2 9 Technical Overview SG24-7330
- DB2 9 Performance Topics SG24-7473
- DB2 9 Stored Procedures SG24-7604
- Index Compression with DB2 9 for z/OS paper
- SQL Reference for Cross-Platform Development
- DB2 9 Optimization Service Center SG24-7421
- LOBs with DB2 for z/OS SG24-7270
- Powering SOA with IBM Data Servers SG24-7259
- Enhancing SAP - DB2 9 SG24-7239
- Best practices SAP BI - DB2 9 SG24-6489-01
- Data Sharing in a Nutshell, SG24-7322
- Securing DB2 & MLS z/OS SG24-6480-01



DB2 library more information <http://www.ibm.com/software/data/db2/zos/library.html>

Ten IBM Redbooks publications, one Redpaper and one cross-platform book on DB2 9 are published, in addition to the standard library, with more in the works. Check for updates.

- DB2 9 Technical Overview, SG24-7330, <http://www.redbooks.ibm.com/abstracts/SG247330.html>
- DB2 9 Performance Topics, SG24-7473, <http://www.redbooks.ibm.com/abstracts/SG247473.html>
- DB2 for z/OS Stored Procedures: CALL & Beyond, SG24-7604, <http://www.redbooks.ibm.com/abstracts/SG247604.html>
- Index Compression with DB2 9 for z/OS, redpaper REDP4345, <http://www.redbooks.ibm.com/abstracts/redp4345.html>
- Cross-Platform Development Version 3, <http://www.ibm.com/developerworks/db2/library/techarticle/0206sqlref/0206sqlref.html>
ftp://ftp.software.ibm.com/ps/products/db2/info/xplatsql/pdf/en_US/cpsqlrv3.pdf
- Powering SOA with IBM Data Servers, SG24-7259, <http://www.redbooks.ibm.com/abstracts/SG247259.html>
- LOBs with DB2 for z/OS: Stronger & Faster, SG24-7270, <http://www.redbooks.ibm.com/abstracts/SG247270.html>
- Securing DB2 & MLS z/OS, SG24-6480-01, <http://www.redbooks.ibm.com/abstracts/sg246480.html>
- Enhancing SAP - DB2 9, SG24-7239, <http://www.redbooks.ibm.com/abstracts/SG247239.html>
- Best practices SAP BI - DB2 9, SG24-6489-01, <http://www.redbooks.ibm.com/abstracts/sg246489.html>
- DB2 9 Optimization Service Center, SG24-7421, <http://www.redbooks.ibm.com/abstracts/sg247421.html>
- Data Sharing in a Nutshell, SG24-7322, <http://www.redbooks.ibm.com/abstracts/sg247421.html>



DB2 for z/OS and tools information: ibm.com/software/data/

Webcast tools <http://www.ibm.com/software/os/zseries/telecon/14sep/>
<https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=27252&sessionId=1&key=0F949E721ACA599ECA97D7811BF61143&referrer=&sourcepage=register>

System z cryptography
<http://www.ibm.com/systems/z/security/cryptography.html>
<http://www.ibm.com/systems/z/security/features.html>
<http://www.ibm.com/systems/z/security/>
<http://www.ibm.com/systems/systemz9/feature092705/>
http://www.ibm.com/servers/eserver/zseries/zos/encryption_facility/

DB2 presentations
<http://www.ibm.com/software/swnews/swnews.nsf/n/cres6t5k2m?OpenDocument&Site=software>
<http://www.ibm.com/support/docview.wss?uid=swg27007842&aid=1>
<http://www.ibm.com/support/docview.wss?uid=swg27007843&aid=1>
<http://www.ibm.com/support/docview.wss?uid=swg27007844&aid=1>

tape cryptography
http://www.ibm.com/servers/eserver/zseries/zos/pdf/White_Paper_ESG_System_z_final.pdf

Here are some additional pointers for information about DB2, security and compliance. Planning for Multilevel Security is on the web under z/OS library, System level books, or

ibm.com/servers/eserver/zseries/zos/bkserv/r5pdf/zsys.html

DB2 V8 books including the RACF Access Control Module Guide are located at

<http://www.ibm.com/software/data/db2/os390/v8books.html>

ICSF and key management:

<ftp://ftp.software.ibm.com/software/mktsupport/techdocs/keymgmt.pdf>

[http://www.ibm.com/support/techdocs/atmastr.nsf/fe582a1e48331b5585256de50062ae1c/eb1b01f317fa015786256dd400020e85/\\$FILE/zoscrypto-techdocs.pdf](http://www.ibm.com/support/techdocs/atmastr.nsf/fe582a1e48331b5585256de50062ae1c/eb1b01f317fa015786256dd400020e85/$FILE/zoscrypto-techdocs.pdf)

<http://www.ibm.com/support/techdocs/atmastr.nsf/WebIndex/PRS1880>

[http://www.ibm.com/support/techdocs/atmastr.nsf/032f6e163324983085256b79007f5aec/09ae5cfe8c313657862570850058afa4/\\$FILE/Clear%20Key%20Secure%20Key%20Primer.pdf](http://www.ibm.com/support/techdocs/atmastr.nsf/032f6e163324983085256b79007f5aec/09ae5cfe8c313657862570850058afa4/$FILE/Clear%20Key%20Secure%20Key%20Primer.pdf)

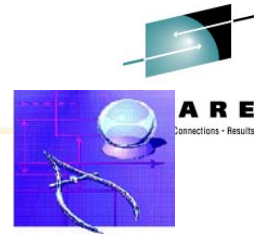
Disclaimers & Trademarks*

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.