Db2 Security Best Practices Volume II

By Dave Beulke

Dave Beulke and Associates

Dave @ d a v e b e u l k e . c o m

Session code: G16
Thursday, May 3, 2018 - 9:20am

Cross Platform
Dave@davebeulke.com

- Member of the inaugural IBM DB2 Information Champions
- One of 35 IBM DB2 Gold Consultant Worldwide
- President of DAMA-NCR, Past President of International DB2 Users Group - IDUG
- Best speaker at CMG conference & former TDWI instructor

- Former Co-Author of certification tests
  - DB2 DBA Certification tests
  - IBM Business Intelligence certification test
- Former Columnist for IBM Data Management Magazine

Consulting
- Security & Compliance Audits
- Adding ML and AI to systems and applications
- AI Analytics application integration
- DB2 12 Performance Reviews
- DB2 10 Performance IBM White Paper & Redbook

Teaching Educational Seminars
- Security Practices for Java Developers
- AI and ML Analytical Designs for Performance
- How to Do a Performance Review
- DB2 Performance for Java Developers
- DB2 Version 12 Transition

- Extensive experience in Big Data systems, DW design and performance
  - Working with DB2 on z/OS since V1.2
  - Working with DB2 on LUW since OS/2 Extended Edition
  - Designed/implemented first data warehouse in 1988 for E.F. Hutton
  - Working with Java for Syspedia since 2001 – Syspedia - Find, understand and integrate your data faster!
In case you missed my *Security Volume I* speech

- 4 Aspects of security
- Physical infrastructure
- System infrastructure
- Database infrastructure connections
- Application infrastructure
- Understand your connections
- Secure the network connections
- Secure servers
- Encryption protocols, practices and options
- FIPS-140 Compliance
- Achieving FIPS 140 standards
- Protecting data at rest
- IDs used through your services
- Connection governance
- Standard and exception protocols
- Risk Assessment and Access Realization
- Security encryption long term commitment
- Defining a secure database
- Using database steganography
- Table steganography
- Column steganography
- Audit discovery for Db2 z/OS and Db2 LUW
- SQL for discovery of user permissions
- Audit SQL Db2 LUW
- Audit Research – SQL for z/OS
- User Ids research
- Understand the extend of the Ids in your system
- Determine risk of each user id
- Begin list to eliminate obsolete ids
- Ids by database and application cross reference
- Ideas for auditing your environment security
- Tighten up your infrastructure system definitions
- Governance Risk assessments are integrated into lifecycle
- >250 Audit SQL Security queries
My Job

I’M NOT ALLOWED TO RUN THE TRAIN
THE WHISTLE I CAN’T BLOW

I’M NOT ALLOWED TO SAY HOW FAST
THE RAILROAD TRAIN CAN GO.

I’M NOT ALLOWED TO
SHOOT OFF STEAM
NOR EVEN CLANG THE BELL

BUT LET THE DAMNED TRAIN
JUMP THE TRACK
AND SEE WHO CATCHES HELL!!!
Security is only as good as the weakest link in the chain

- **Database security depends on many supporting technologies:**
  - The *host operating system(s)* – provides protection of the database, its configuration and data.
  
  - The **networks** – provides protections via network devices and applications.
  
  - **Cloud, Web and application servers** – provide the security framework for all the cloud interfaces, hosted web applications;
    - Connected world-These servers control access to other servers and applications that control others etc..
  
  - The **applications** – provides access to the data. If the application does not contribute to the security model, it can provide fully-privileged, un-audited access to the database and any data it connects to.
Security depends on many people

• Goes beyond a single operating system
  • System administrators – SYSADMs, SECADMs
  • DBAs – DBADMs
  • Operators – SYSOPR

• Goes beyond a single application
  • So many processes
  • Variety of programming languages
  • What is an authorized application anymore?

• Welcome to the matrix of security complexity
  • Thousands of security situations
Security depends on many different area procedures

- Security depends on collective of enterprise procedures
  - It is the system owner’s responsibility
    - They must be required to evaluate the security risks to the enterprise
    - For all environments/applications especially production environments

- Security goes to the lowest level implemented anywhere!
  - Do all the procedures - trace back to Security Ops Center(SOC) controls?
  - Does your BoD have a new CISO?

- What new security holes are your developers implementing?
  - Did the new implementation improve or diminish your security exposure?
Technology is most important security factor!

- Technology security factors
  - Vendor viability
  - Version overall age
  - Patch level
  - Patch frequency
  - Open source support contract

- Early identification of the security vulnerability and misconfigurations

- Evaluate and audit shared security services and shared controls

- Understand technology stack security requirements and capabilities
  - According to Gartner 99% of hacks are because of outdated technology
DBAs need to collaborate with the everyone (SOC)

• Partner with the system’s owners for developing SOC DBA procedures
  • Application technology base inventory
    • Risk profile of technology – version and patch history

• System data security -
  • GDPR, PII profile requirements/exposure
    • Application Interface inventory
    • Security profiles unique and shared within the application
    • Shared application access point requirements

• DBAs works with the SOC to socialize the important aspects:
  • Systems architecture – cloud, hybrid, HTAP, outsourced, cross-platform, database operational profile
  • Database design characteristics – secure handling for PII, HIPAA, GDPR impacts etc.
  • Interfaces available to the application users, administrators and operations

Danger increases!
In 2018, average probability is 27.7% that organizations in the study will have a data breach in the next 2 years.
Last year, the average probability was only 25.6%!
SOC needs to evaluate/test the exposure

- The evaluated risks resulting from not applying specified configuration settings
  - Security conventions must be approved by your responsible management. Who?

- Failure to test before implementation may lead to a loss of required security and functionality.

- There are no do overs – once the data is exposed no going back!
BoD, CEO, CISO, CDO, DBA - Cycle of engagement

- SOC needs security audit baseline to manage the security evaluation of the existing and new applications
- The technology stack evaluation is the key to determining your security exposures
- SOC schedules regular security audits, drives the information baseline for upper management evaluation
- Do you have something to cover your procedures?
Establish SOC security summaries

• Establish DBA Security Operations Center (SOC).
  • 48% do not have a SOC
  • detect, protect and react are not enough
  • cyber breach response plan (CBRP) developed

• Understand your legal liabilities of a data breach
  • Ready – GDPR=$, $$$, $$$ -Good for budget allocation

• Inventory all hard and soft targets
  • Talent, audit security tools, PII data, home grown or packaged software etc.

• CDO/DBAs need to raise their profile of interaction
  • Drive the process or be driven by the security issues – your choice

• Board of Directors commitment reported twice monthly/yearly
Db2

• Best practices for systems
  • Multi-layered protection
    • Multi-Tiered system access inventoried
    • Multiple logon authentication
    • Majority trusted devices and clients
    • Monitoring Tools standard for PII HIPAA
  • SOC established with known active procedures
  • Regularly scheduled system & application security audits

• Techniques for systems
  • Security & configurations standardized - UNIX
  • Monitoring auditing tools utilized
  • Automated Security breach response/tools

Cost of data breach continues to go up
Amount of data stolen continues to rise
Industries vary with HealthCare having biggest costs per record $380

The cost of data breach continues to go up, while the amount of data stolen continues to rise. Industries vary, with Healthcare having the biggest costs per record at $380.
System security perimeter assessment

**System application usage profile**
- Who are the Insider threats?
- Risk assessment of systems activity access auditing
- System versus storage/apps - duties segregated?
- Version Maintenance - independence agility
- “PUBLIC” revoked everywhere
- Inventoried interface - security profiles and usage
- How many Db2 LUWs? Go to Registry Editor in Windows
  
  Computer >> HKEY_LOCAL_MACHINE >> SOFTWARE >> IBM >> DB2 >> installedCopies >> DB2COPY1 Then find the value of the DB2 Path Name

**Network**
- Public versus private access segregation
- Network App PII segmentation
- Intrusion Detection Services/Tools
- FIPS-140 Access Only
- AT-TLS
- GEO fencing & IP Filtering
- Outside threat profiling
- DVIPA/VIPA application affinity definition
Db2 System Security - Maintenance methods

• Maintenance, maintenance and more maintenance
• Most shops have a rhythm of maintenance
  • Db2 has recently had some RED ALERTS – How were those handled?
  • How quickly can a PTF be applied across your Db2 systems
  • Are you keeping up with the Db2 agile development? Db2 V12 is almost ? years old
    • Google: Flashes, alerts and bulletins for DB2 Tools for z/OS

• Db2 LUW FixPaks and PTFs frequency
  • Operating system updates
  • Google: Db2 Linux, Unix and Windows APAR list
    • http://www-01.ibm.com/support/docview.wss?uid=swg21321001

• Research interactions between applications
Security practices for Db2 database definition

• Best practices for databases
  • Broad encryption protection
    • Storage layer encrypt key store protection
  • Database steganography
    • Table splits/naming
    • Column splits/naming
    • Data Procedures
  • GDPR, PII and HIPAA granular security layer
    • Table special auditing
    • Columnar security
    • Element access control
    • Column masking/encryption
    • Column Obfuscation

• Verify trusted and encrypted communication
Security practices for Db2 database definition

- Techniques for fortifying databases
  - Secure and minimize all DBA, DML, DDL, SQL, tool and utility authorizations
    - Your environment has too much access, especially production!
  - Schema, database, tablespace, table, index, view, function, procedure, package, method BINDADD, CREATE xxxx etc.
    - Monitor all GRANTs
    - Secure Db2 Catalog from PUBLIC
    - Restrict access to configuration and underlying file system resources
    - CREATE DATABASE <dbname> RESTRICTIVE
    - Protect and restrict access to Logs and SQL Auditing history

- After goes to production revoke-tighten security authorizations!
Assess and tighten production security perimeter

• **Database (LUW)**
  - Go to Registry Editor in Windows
    Computer >> HKEY_LOCAL_MACHINE >> SOFTWARE >> IBM >> DB2 >> installedCopies >> DB2COPY1
    Then find the value of the DB2 Path Name
  - Repurposed, split or moved machine

• **Data**
  - Understand your storage configuration to realize shared device exposures
  - Map out the channel connections used within your environment
  - Verify the security ids that have access to your Db2 databases and their HLQs

• **Security ids**
  - Where in your systems or connections can your user id be changed or *grouped* into another id?
  - What services or operational authorities are there over your Db2 systems, applications or tools?
Framework liability?

- Picture says it all
  - How secure is your framework?
  - How many releases are your applications behind?
  - Java 10 coming which version are you on?
  - Old Spring releases are vulnerable!
  - POJO security is achievable needs verification!
    - Also needs to stay up with software fixes

https://www.slideshare.net/kunalashar/the-2014-decision-makers-guide-to-java-web-frameworks
Frameworks can be the most vulnerable

- Framework is only secure if...
  - Programming is done with the latest APIs, certificates are used correctly and peer reviewed
  - Configurations is confirmed to be controlled properly
  - Change control and implementation is secured with good procedures

- Spring can use several configurations to secure the environment
  - Are you using the XML based or Java based Spring security classes, configuration and procedures
    - Have you migrated from the old one to the new one?
    - Did you update the security?

- HttpSecurity has 10 methods
  - Are yours set up correctly? Reviewed lately?
  - The security `antMatcher("/api/**")` needs to be invoked before `addFilterAfter(...)`
  - So `filter is only applied to URLs matching the pattern "*/api/**"`. 
Framework in production reviewed/updated lately?

• Applications security best practices
  • Eliminate or upgraded old software versions
    • Frameworks – Spring, Ruby Groovy etc.
    • Old Java and supporting software libraries
    • Especially Open Source code with known issues
  
• Old Application (JUNIT) testing reviews
  • JavaScript security execution
  • XSS Cross-Site Scripting
  • Research app for indirect site references

• All types of injection possibilities that need inspection
  • XML, SQL, NoSQL, LDAP etc.
Does each application have a security risk rating?

- Techniques for applications
  - Insufficient logging and monitoring
    - Securing Logs and audit information
    - Too much access to the logs
  - Standard application error handling procedures and practices
    - Coding reviews for standard secure techniques and practices
  - Poor connection, trust manager and certificate management controls
    - Architecture for always secure and encrypted communications
    - Stick with reference MVC architecture
- Establish application security baseline
  - Establish Security Audit Risk Rating for each application!
7 phases of security

• Security roles, access control, and authentication requirement
  • Authentication is most important and popular of the three

• Problems caused by wrong versions of software libraries and version conflicts between dependent processes
Security Audit Application Risk Rating

- Develop an application liability rating
- Annual application evaluation
  - Threat agent factors
    - Individual, Group, Company or Nation-state
    - Motive, Opportunity, Size and Skill
  - Vulnerabilities rating
    - Discovery, exploitability, awareness, intrusion detection
  - Technical Factors
    - Software, Interfaces, data integrity, confidentiality, accountability
  - Business Impacts
    - Compliance, GDPR, HIPAA, PII
- Access techniques
  - Column protections, procedures and column steganography
- Encryption techniques
  - Keystore, disk and backup encryption
Db2 system application usage profiles

- SECADM, DBA, Application Security profiles
  - How are these set up differently within your RACF/Other security profiles
  - Within Db2 LUW are different ids used for administration

- User interactions with PII/HIPAA data
  - Special handing for the review, update and auditing of the special data?
  - Auditing is special requirements for every PII data element.
  - What provisions are put in place for
    - Government regulations
    - Audit reporting
    - GDPR requirements
Older versions of software

• Research your framework, application libraries and special situations
  • Older or Community version of JBoss
  • Redhat has its own CVE

• National Vulnerability Database – https://nvd.nist.gov/

• NIST is the national standard – national crisis
  • Mitre also - https://cve.mitre.org/

• Research your exposures and endpoint’s status
  • iOS and Android rogue apps
  • Chinese phones send data back
  • Google tracks every Android phone movement!
    https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/
Understand your security threat landscape

- Threat scenario for each application?
- Where are your companies PII valuables?
- Email exposures
  - Attachment scanning
  - Link validation
  - Email training
- Cloud provider risk
  - Our cloud is move secure than theirs
How will you be attacked?

• How much risk is acceptable?
  • Within a system
  • Within an application
    • Example: Olympic snow boarder

• Where can your limit resources or efforts be most effective?

• Where can get the most benefit for reviewing security?
Security diagram

• Do you have one of these?

• Certify your connection and your secure certificate
Audit results: Application problems with Certificates

- Self Signed certificates should **not** be used.
- TrustManagers should also be **avoided!**
  - Does not avoid DNS or MIM attacks

- Problems with the Diffie-Hellman (DH) and Menezes-Qu-Vanstone (MQV) key establishment schemes
  - Because the establishment scheme is know there are routines that can crack encryption in real time

- Parameter-size set FA is no longer approved for use, FB and FC are now referred to as “FIPS 136 186-type” parameter-size sets.
TLS/SSL Configuration

• Are your using TSL/SSL
  • Are your connections TSL/SSL by default?
  • Are you on the latest version of TSL for your platform?

• Software errors handling of user credentials
  • Including hard-coded password and plaintext passwords in configuration files

• Java Credentials Certification Path
  • Defines a set of classes and interfaces to create, build, and validate digital certification paths

• Are you FIPS certifiable?
  • IBM FIPS-approved providers IBMJSSEFIPSProvider and IBMJCEFIPS
How safe are your certificates?

• The default certificate is not intended for production use
• The reason most are automatically generated and self-signed.
  • Self-signed certificates are not recommended for use in production.
  • The auto-generation of the certificate is intended for developer convenience only.
  • The duration is 1 year, which is too short for a trusted certificate.
  • What certificates do you use?

• Certificates used in production should be properly chained certificates issued or signed by a trusted authority such as Verisign or Entrust.
  • If you want to use a self-signed certificate (not recommended) with a longer duration, one can be created using the bin/securityUtility createSSLCertificate task.
How up to date are your practices?

• Who recommended what when?
  • The usage of MD5 and SHA-1 algorithms were repetitively suggested since 2012, although these algorithms are notoriously insecure and should not be used anymore!
  
  • Does your enterprise trust all incoming SSL/TLS certificates from servers as a workaround to certificate verification errors. Such practice completely disables the security checks of SSL!

• SSLSocket does not perform hostname verification
• Beware that HostnameVerifier.verify() doesn't throw an exception on error but instead returns a boolean result
Db2 Security procedures

- Plan your SOC security profile for every interface
  - Cross reference the security profile for every piece of data especially PII

- Build a baseline security audit of your..
  - Systems security profiles
  - Applications security public and private ids
  - Application interfaces
    - Encrypted communication usage
  - Certificate handling
  - Procedures and understanding with SOC

- Prioritize your security plan of action
- Monitor, Monitor, Monitor
- Automate Actions prevention
- Remediate, Response and Repeat
Assume the worst will happen

• Establish SOC or start the discussions with BoD, CEO, CDO or ?
• Has your company done a database security audit?
  • There is no excuse for not doing security audits, develop risk ratings for each system & application
• According to Gartner - Greg Young
  • “Through 2020, 99% of vulnerabilities exploited will continue to be the ones known by security and IT professionals for at least one year.”
  • Identifying and closing off known vulnerabilities before they are exploited is crucial.
  • Good comprehensive cybersecurity procedures (SOC?) to identify infrastructure where majority of simple attacks can take place
• Save the company’s reputation, address risk and save big money$$!
Db2 Security Best Practices Volume II
By Dave Beulke
Dave Beulke and Associates
Dave @ d a v e b e u l k e . c o m

Thank you!

Please fill out your session evaluation before leaving!