Db2 Security Best Practices Volume II

By Dave Beulke

Dave Beulke and Associates

Dave @ d a v e b e u l k e .com

Columbus, Detroit & Cleveland
Session code: September 11, 12 & 13, 2018
Platform: Cross Platform

Follow me on
Twitter: @DBeulke
&
LinkedIn
https://www.linkedin.com/in/davebeulke

I am honored and humbled to have been a presenter at all 30 years of IDUG

2018 – Philadelphia -**Best Design and Performance Practices for Analytics**
-Security Best Practices Volume II
2017 – Anaheim -Understand IDAA Performance and Justify an IDAA Appliance
2016 – Austin Performance Enterprise Architectures for Analytic Design Patterns
How to do your own Db2 Security Audit
2015 - Valley Forge Db2 Security Practices
Big Data Performance Analytics Insights
2014 – Phoenix Big Data SQL Considerations
2013 – Orlando Big Data Disaster Recovery Performance
2012 – Denver Agile Big Data Analytics
2011 – Anaheim Db2 Temporal Tables Performance Designs
2010 - Tampa - Java DB2 Developer Performance Best Practices
2009 – Denver -Java Db2 Perf with pureQuery and Data Studio
Improve Performance with Db2 Version 9 for z/OS
2008 – Dallas - Java pureQuery and Data Studio Performance
2007 - San Jose - Developing High Performance SOA Java Db2 Apps
Why I want Db2 Version 9
2006 - Tampa - Class - How to do a Db2 Performance Review
Db2 Data Sharing
Data Warehouse Designs for Performance
2005 – Denver - High Performance Data Warehousing
2004 – Orlando – Db2 V8 Performance
President of IDUG
2003 - Las Vegas - Db2 UDB Server for z/OS V8 Breaking all the Limits
Co-author IBM Business Intelligence Certification Exam
2002 - San Diego - Db2 UDB for LUW 8 - What is new in Db2 Version 8
Data Warehouse Performance
2001 – Orlando -Data Sharing Recovery Cookbook
Designing a Data Warehouse for High Performance
Co-authored the first IBM Db2 z/OS Certification Exam
2000 – Dallas - Db2 Data Warehouse Performance Part II
1999 – Orlando - Store Procedures & Multi-Tier Performance
Developing your Business Intelligence Strategy
Evaluating OLAP Tools
1998 - San Francisco - Db2 Version 6 Universal Solutions
Db2 Data Warehouse Performance
Db2 & the Internet Part II
1997 – Chicago - Db2 & the Internet
1996 – Dallas- Sysplex & Db2 Data Sharing
Best Speaker Award at CMG Conference Mullen Award
1995 – Orlando - Practical Performance Tips
Improving Application Development Efficiency
1994 - San Diego - Database Design for Time Sensitive Data &
Guidelines for Db2 Column Function Usage
1993 – Dallas - High Availability Systems: A Case Study &
Db2 V3: A First-Cut Analysis
1992 - New York -Db2 –CICS Interface Tuning
1991 - San Francisco - Pragmatic Db2 Capacity Planning for DBAs
1990 – Chicago - Performance Implication of Db2 Design Decisions
1989 – Chicago - Db2 Performance Considerations

Dave@davebeulke.com

- Member of the inaugural IBM Db2 Information Champions
- One of 40 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
- 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
  - ***Syspedia*** for data lineage and data dependencies since 2001 –
    - Find, understand and integrate your data faster!

Proven Performance Tips:
www.DaveBeulke.com

- **Consulting**
  - **Security Audit & Compliance**
  - **Db2 Performance Review**
  - **CPU MLC Demand Reduction**
  - **Analytics & Database Design Review**
  - **Db2 12 Migration Assistance**
  - **Java Application Development assistance**

- **Educational Seminars**
  - **Java Security for Application Developers**
  - **Db2 Version 12 Transition**
  - **Db2 Performance for Java Developers**
  - **Data Warehousing Designs for Performance**
  - **How to Do a Performance Review**

In my ***Security Volume I*** speech (found on my blog)

- 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
- **z/OS and LUW 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.

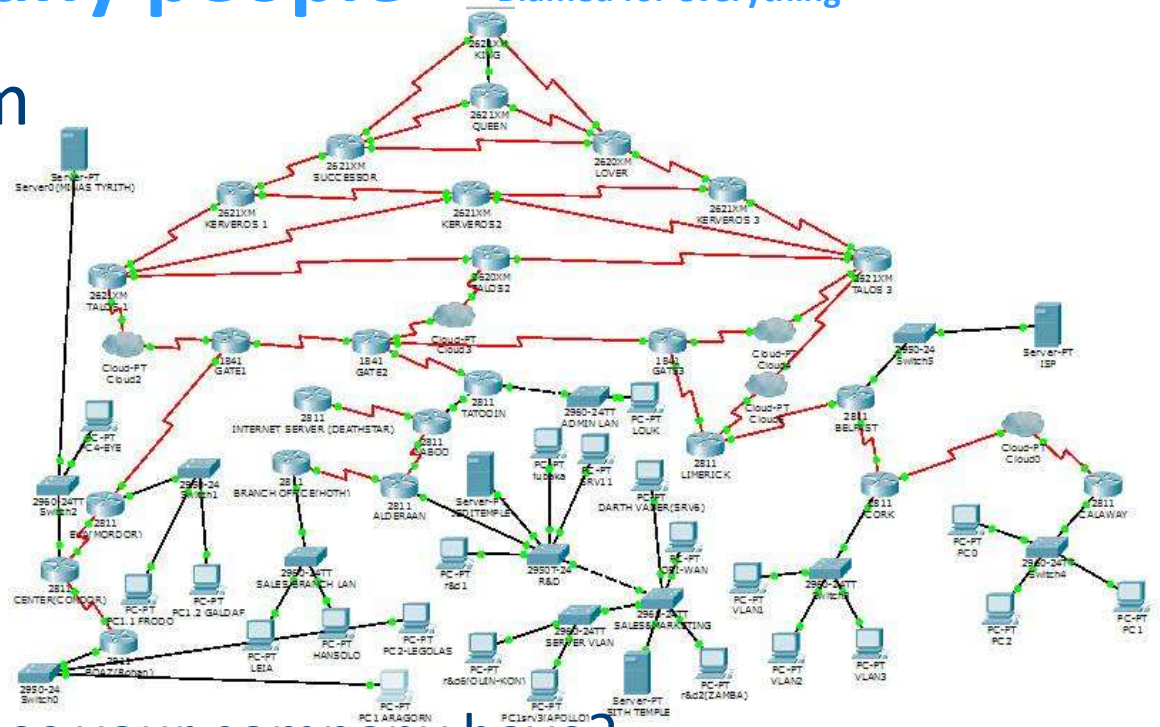
I'M NOT ALLOWED TO
SHOOT OFF STEAM
NOR EVEN CLANG THE BELL

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.

DBAs responsible for actions of many people - Blamed for everything



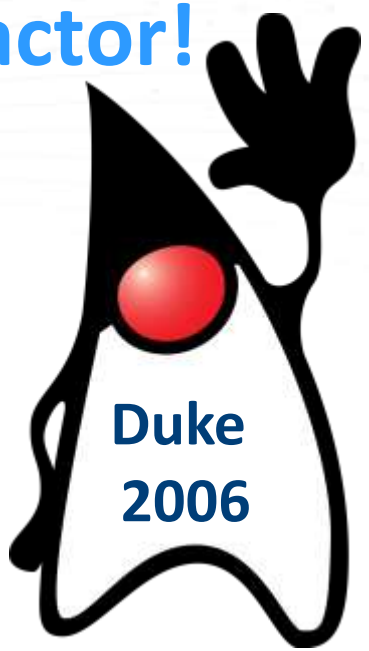
- Goes beyond a single operating system
  - System administrators – SYSADMs, SECADMs
  - DBAs – DBADMs
  - Operators – SYSOPR
- Goes beyond a single application
  - So many processes
  - Variety of programming languages
  - How many levels of authorized application does your company have?
- Welcome to the matrix of security complexity
  - Thousands/millions of security situations

DBA is the focus of different security procedures

- Security depends on *collective* of enterprise procedures
  - It is the *system owner's responsibility*
    - Require security risk evaluation to the enterprise
  - Start with all production environments/applications then development
- 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 Chief Information Security Officer - CISO?
- What new security holes are your developers implementing?
  - *Did the new implementation improve or diminish your security exposure?*

Technology updates are 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 stack security requirements and technology capabilities
  - According to Gartner 99% of hacks are because of outdated technology

DBAs collaborate with everyone-start documentation for (SOC)

- Partner with the system's owners for developing DBA procedures for SOC
  - **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 – **document security/interfaces handling for PII, HIPAA, GDPR data**
  - Document all the 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

- Evaluate risks of your configuration settings
  - Security conventions must be approved by your responsible management.
    - **Who signs off on security?**
- 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!
- Db2 z/OS zParms, Db2 LUW dbm cfg & db cfg
  - All interfaces – JDBC, ODBC, REST and IOT APIs

BoD☞CEO☞CISO☞CDO☞DBA - Cycle of engagement

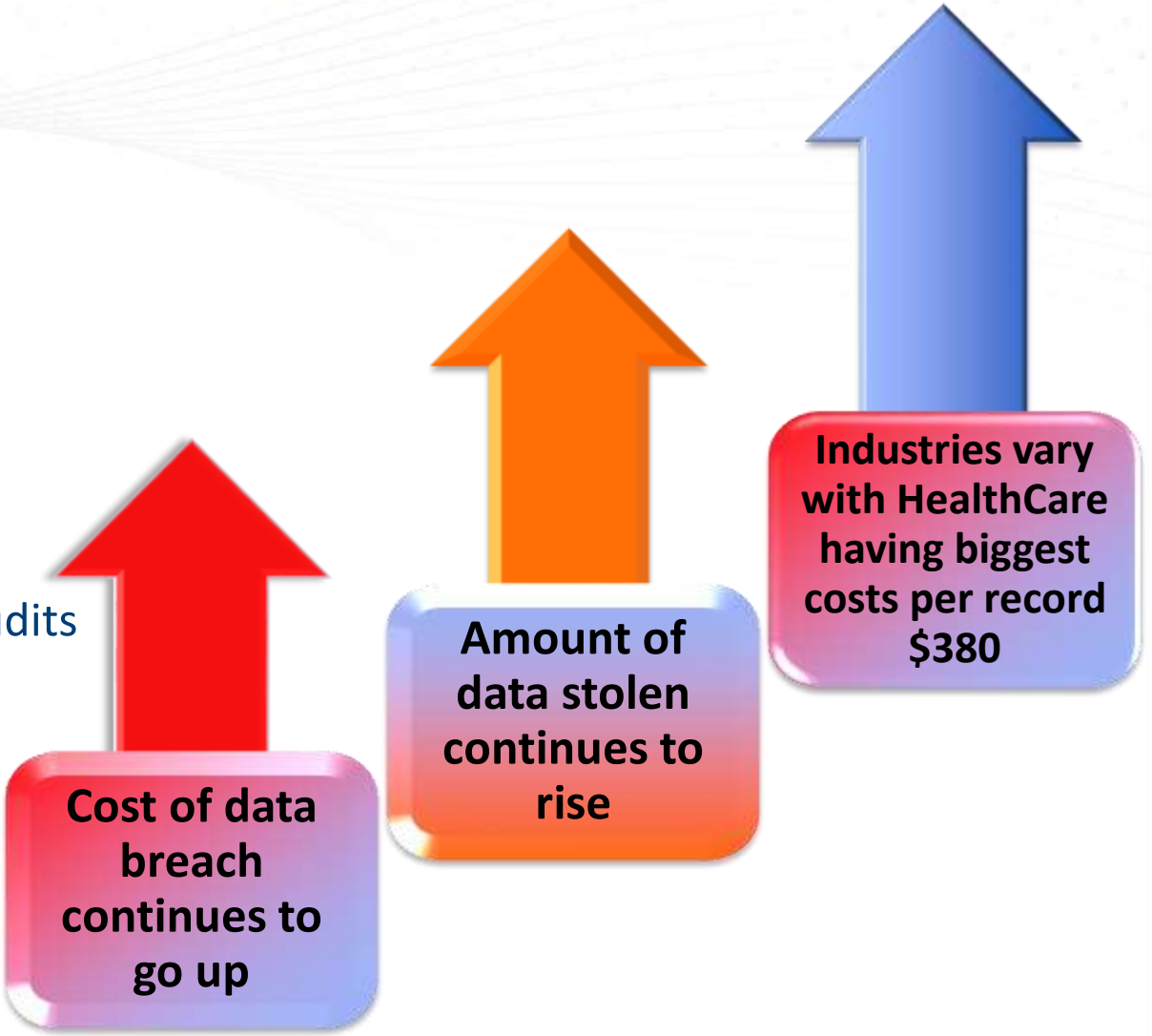
- SOC needs security audit baseline to manage the security evaluation of the existing and new applications
- The technology stack evaluation is the key to determining your security exposures
- SOC schedules regular security audits, drives the information baseline for upper management evaluation
- Do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

Establish SOC security summaries

- Establish DBA Security Operations Center (SOC).
  - 48% of companies 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 for z/OS and Db2 LUW

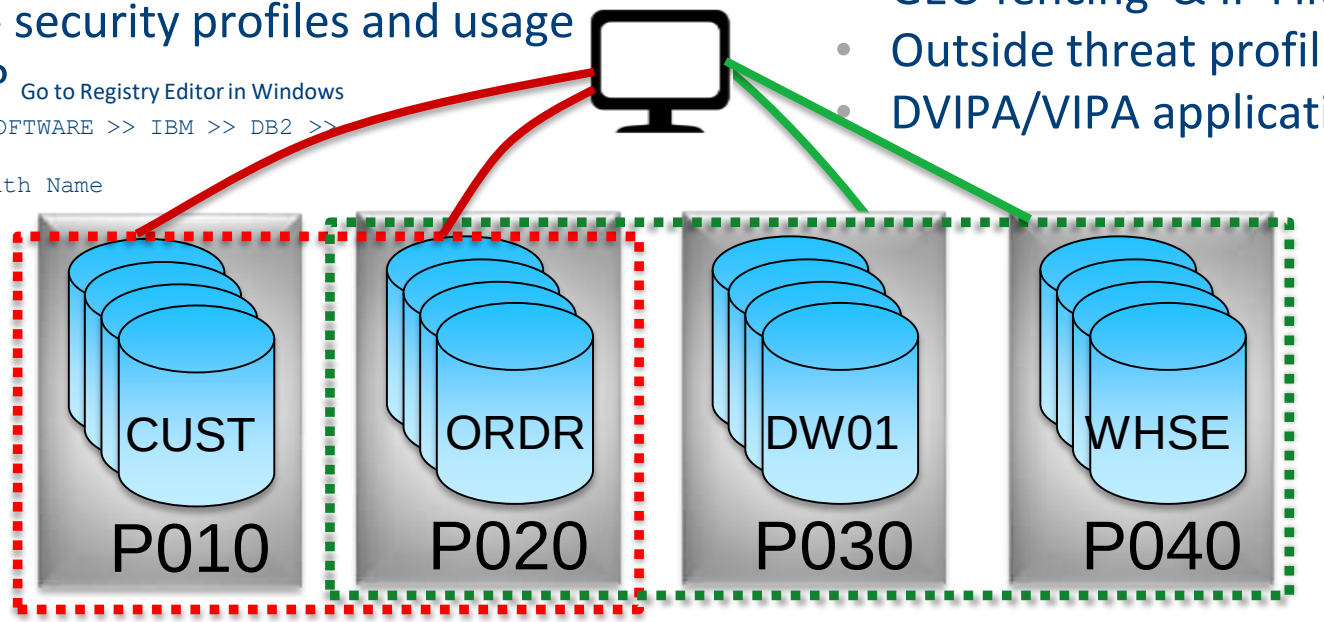
- Best practices for systems
  - Multi-layered protection
    - Multi-Tiered system access inventoried
    - Multiple logon authentication - 2-factor authorization
    - Almost all trusted devices and clients (>99%)
    - Monitoring Tools standard for PII HIPAA
  - SOC established with known active procedures
  - Development lifecycle system & application security audits
- Techniques for systems
  - Security & configurations standardized – UNIX & z/OS
  - Monitoring auditing tools utilized
  - Automated Security breach response/tools
    - z/OS RACF 3-strikes



System security perimeter assessment

- System application usage profile
  - **"PUBLIC" access revoked everywhere**
  - Who are the Insider threats?
  - Risk assessment of systems activity access auditing
  - System versus storage/apps - duties segregated?
  - Version Maintenance - independence agility
  - 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
  - **Intrusion Detection Services/Tools**
  - Public versus private access segregation
  - Network App PII segmentation
  - 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
    - SEARCH Keywords: **`Flashes, alerts and bulletins for DB2 Tools for z/OS`**
- Db2 LUW FixPaks and PTFs frequency
  - Operating system updates
  - SEARCH Keywords: **`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
    - Data at rest storage encryption key store protection
    - `CREATE DATABASE BEULKE ENCRYPT CIPHER AES KEY LENGTH 192 MASTER KEY LABEL mylabel.mydb.myinstance.myserver;`
  - Design your database with steganography features
    - Table splits/naming
    - Column splits/naming
    - Data Procedures secured for data access
  - Design/improve with 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 everywhere your system can control!

Security practices for Db2 database definition

- Techniques for fortifying databases
  - Secure and minimize all **authorizations** for DBA, DML, DDL, SQL, tools & **utilities**
    - Your environment provides 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 - REVOKE access *from* PUBLIC
    - Restrict access to configuration and underlying file system resources
    - CREATE DATABASE *BEULKE* RESTRICTIVE ENCRYPT
    - Protect and **restrict** access to Db2 Logs and SQL Auditing history
      - Make sure **audit is always active!**
- After goes to production revoke-tighten security authorizations!

Validate NIST FIPS 140-2 compliance

- Validate your DB2 Cryptographic configuration through the Db2 database manager configuration and Db2 registry
  - Get the Db2 manager configuration – >$**db2 get dbm cfg**
    - SSL_VERSIONS needs to be set to TLSV12
    - SSL_CIPHERSPECS needs to name an algorithm w/key length => 112 bytes
    - SSL_SVC_LABEL needs to name a RSA key length certificate => 2048 bytes
  - Next use the db2 command - > $**db2 set all** to discover the DB2COMM setting
    - Needs to include the SSL

  - Use SQL query to validate the database level encryption used for your encrypting your data at rest
    - **SELECT SUBSTR(object_name,1,8) AS NAME, SUBSTR(object_type,1,8) AS TYPE, SUBSTR(algorithm,1,8) AS ALGORITHM, SUBSTR(algorithm_mode, 1,8) AS ALGORITHM_MODE, KEY_LENGTH, SUBSTR(master_key_label, 1,8) AS MASTER_KEY_LABEL, SUBSTR(keystore_name,1,8) as KEYSTORE_NAME FROM TABLE(sysproc.admin_get_encryption_info())**
  - These settings ensure encrypted communication, encrypted data at rest and that all connections over SSL in any CLP or Java application strictly adhere to encrypted NIST SP 800-131A standard.

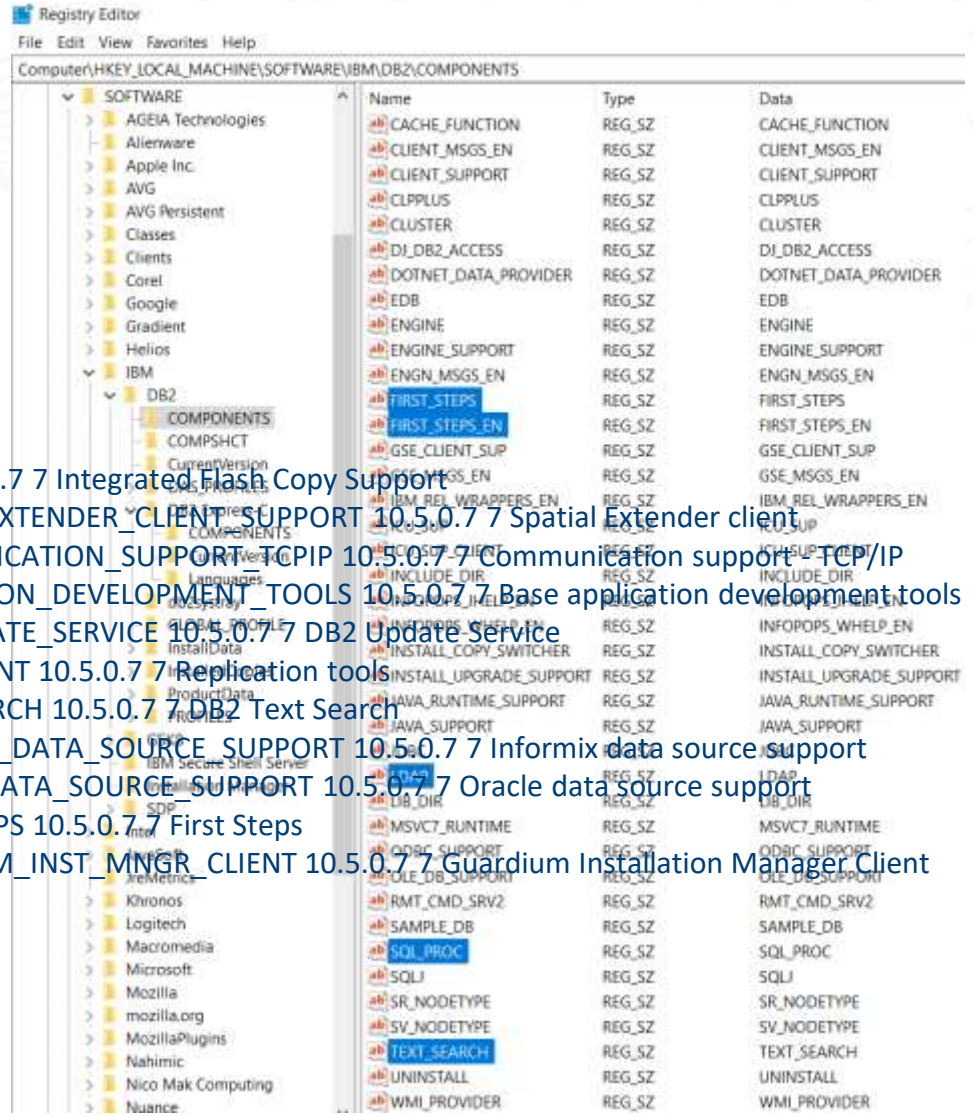
Assess and tighten production security perimeter

- 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
    - Not just Db2 ids but also all the Linux/UNIX/Window user ids with access to those directories
  - **Encrypt** ***all*** data at rest!
- 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?

What Db2 components are required?

- Database (LUW)
  - Go to Registry Editor in Windows

    HKEY_LOCAL_MACHINE >> SOFTWARE >> IBM >> DB2 >> COMPONENTS
    - Lists all the possible Db2 related installed components
      - BASE_CLIENT 10.5.0.7 7 Base client support
      - JAVA_SUPPORT 10.5.0.7 7 Java support
      - SQL_PROCEDURES 10.5.0.7 7 SQL procedures
      - BASE_DB2_ENGINE 10.5.0.7 7 Base server support
      - CONNECT_SUPPORT 10.5.0.7 7 Connect support
      - DB2_DATA_SOURCE_SUPPORT 10.5.0.7 7 DB2 data source support
      - SPATIAL_EXTENDER_SERVER_SUPPORT 10.5.0.7 7 Spatial Extender server support
      - JDK 10.5.0.7 7 IBM Software Development Kit (SDK) for Java(TM)
      - LDAP_EXPLOITATION 10.5.0.7 7 DB2 LDAP support
      - INSTANCE_SETUP_SUPPORT 10.5.0.7 7 DB2 Instance Setup wizard
    - There can be many components installed that are not needed
  - Remove any components not needed for the processing
    - They can be used to attack your system, database and data



- ACS 10.5.0.7 7 Integrated Flash Copy Support
- SPATIAL_EXTENDER_CLIENT_SUPPORT 10.5.0.7 7 Spatial Extender client
- COMMUNICATION_SUPPORT_TCPIP 10.5.0.7 7 Communication support - TCP/IP
- APPLICATION_DEVELOPMENT_TOOLS 10.5.0.7 7 Base application development tools
- DB2_UPDATE_SERVICE 10.5.0.7 7 DB2 Update Service
- REPL_CLIENT 10.5.0.7 7 Replication tools
- TEXT_SEARCH 10.5.0.7 7 DB2 Text Search
- INFORMIX_DATA_SOURCE_SUPPORT 10.5.0.7 7 Informix data source support
- ORACLE_DATA_SOURCE_SUPPORT 10.5.0.7 7 Oracle data source support
- FIRST_STEPS 10.5.0.7 7 First Steps
- GUARDIUM_INST_MNGR_CLIENT 10.5.0.7 7 Guardium Installation Manager Client

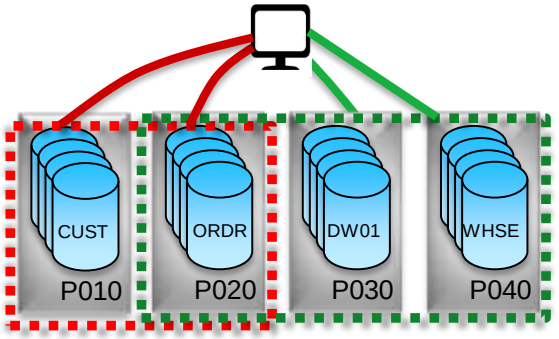
Framework liability?

- 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 ***very*** 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 and risky

- Framework is only secure if…
  - **Programming is done with the latest APIs, certificates are used correctly and interfaces security 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 different methods
  - Are each of your applications 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?

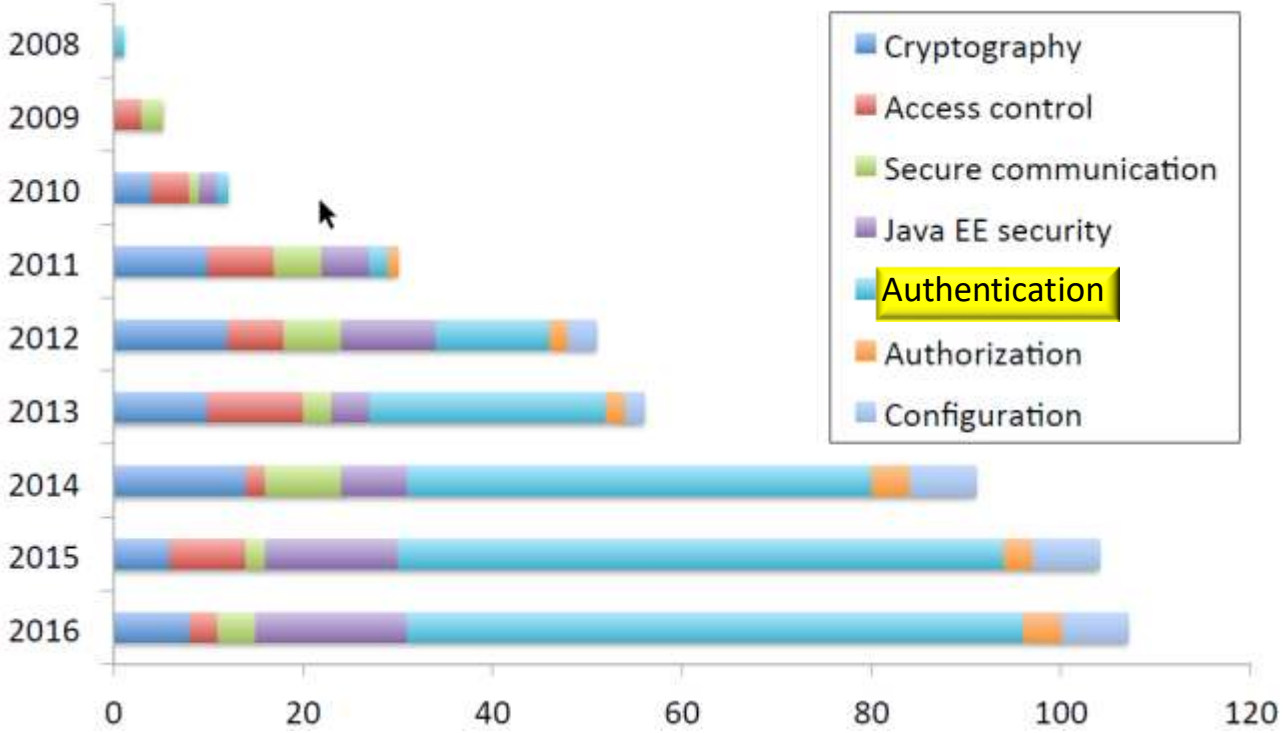
- Applications security best practices
  - Eliminate or upgraded old software versions
    - Frameworks – Spring, Ruby Groovy etc.
    - Old Java and supporting software libraries
    - Especially **Open Source code** with *known* issues
  - Old Application (JUNIT) testing reviews
    - JavaScript security execution
    - XSS Cross-Site Scripting
    - Research app for indirect site references
  - All types of ***injection*** possibilities that need inspection
    - R, Python, JS, XML, SQL, NoSQL, LDAP etc..
      - Anywhere a value is passed to a program

Does each application have a security risk rating?

- Techniques for applications
  - Insufficient logging and monitoring
    - Securing system and application logs and all debugging/audit information
      - Too much access to the logging within all the systems
  - Standard application error handling procedures and practices
    - Coding reviews for standard security 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

Older versions of software

- Research your framework, application libraries and special situations
  - Older or Community version of JBoss, Spring, etc.…
  - 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

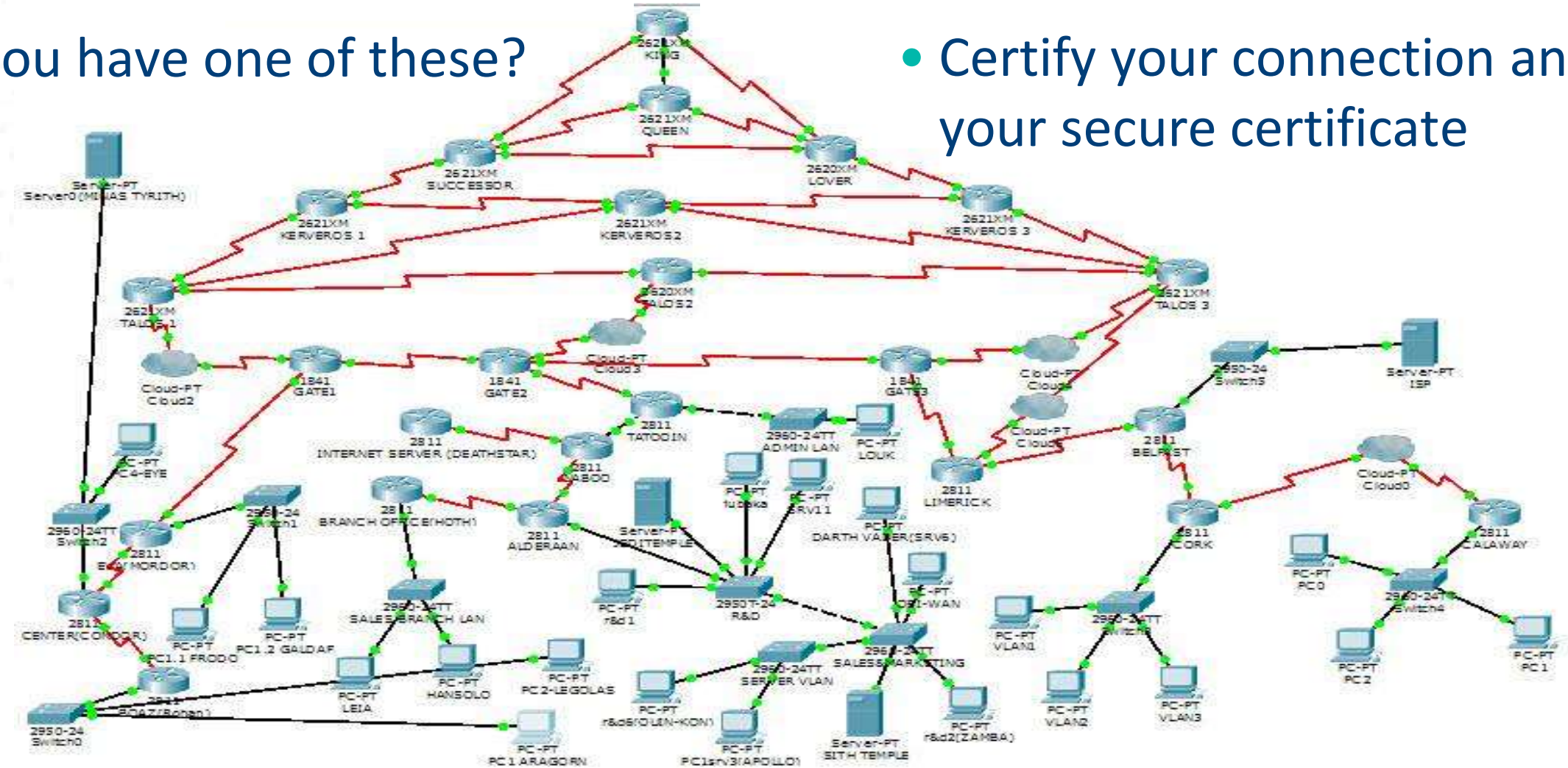
- Threat scenario for each application?
- Where are your companies PII valuables?
- Email exposures
  - Attachment scanning
  - Link validation
  - Email training
- Cloud provider risk
  - Our cloud is move secure than theirs

The threat landscape

	Common attacks	Advanced attacks	Emerging attacks
What is it?	These are attacks that exploit known vulnerabilities using freely available hacking tools, with little expertise required to be successful	Advanced attacks exploit complex and sometimes unknown ("zero-day") vulnerabilities using sophisticated tools and methodologies	These attacks focus on new attack vectors and vulnerabilities enabled by emerging technologies, based on specific research to identify and exploit vulnerabilities
Typical threat actors	Unsophisticated attackers, such as disgruntled insiders, business competitors, hacktivists and some organized crime groups	Sophisticated attackers such as organized crime groups, industrial espionage teams, cyber terrorists and nation states	Sophisticated attackers such as organized crime groups, industrial espionage teams, cyber terrorists and nation states
Examples	▸ Unpatched vulnerability on a website, exploited using a freely available exploit kit ▸ Generic malware delivered through a phishing campaign, enabling remote access to an endpoint ▸ Distributed Denial of Service (DDoS) attack for hire with a basic random demand	▸ Spear phishing attacks using custom malware ▸ "Zero-day" vulnerabilities exploited using custom-built exploit code ▸ Rogue employees "planted" to undertake deep reconnaissance/espionage ▸ Vendors/suppliers exploited as a way to gain access to ultimate target organization	▸ Exploiting vulnerabilities on "smart" devices to gain access to data and/or control systems ▸ Leveraging security gaps created with the convergence of personal and corporate devices into one network ▸ Using advanced techniques to avoid detection and/or bypass defenses

Security diagram

- Do you have one of these?



- Certify your connection and your secure certificate

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.

Audit Research - SQL

- PUBLIC is not your friend - REVOKE

1. DB2 Trusted Communications
2. Authorities over/usage privileges
   - Databases, plans, packages, Distinct Types, usage of BPs, SGs & TSs

```
--- CONTAINS ONE ROW FOR EACH TRUSTED CONTEXT.
SELECT *
FROM SYSIBM.SYSCONTEXT
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- CONTAINS ONE ROW FOR EACH TRUSTED CONTEXT.
SELECT *
FROM SYSIBM.SYSCTXTTRUSTATTRS
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- ONE ROW FOR EACH AUTHORIZATION
-- ID WITH WHICH THE TRUSTED CONTEXT CAN BE USED.
SELECT *
FROM SYSIBM.SYSCONTEXTAUTHIDS
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- RECORDS THE PRIVILEGES THAT ARE
---HELD BY USER OVER DATABASE
SELECT *
FROM SYSIBM.SYSDBAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--RECORDS THE PRIVILEGES THAT
--ARE HELD BY USERS OVER PLAN.
SELECT *
FROM SYSIBM.SYSPLANAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--RECORDS THE PRIVILEGES THAT ARE
--- HELD BY USERS OVER PACKAGES.
SELECT *
FROM SYSIBM.SYSPACKAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- PACKAGE OWNER CAN BE A ROLE
-- ALSO IN DOWNERTYPE
SELECT *
FROM SYSIBM.SYSPACKDEP
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- PLAN OWNER CAN BE A ROLE
-- ALSO IN DOWNERTYPE
SELECT *
FROM SYSIBM.SYSPLANDEP
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
---SYSIBM.SYSRESAUTH RECORDS
-- CREATE IN AND PACKADM  ON
-- PRIVILEGES FOR COL; USE PRIVILEGES
--- FOR DISTINCT TYPES,  BPs, SGs & TSs
SELECT *
FROM SYSIBM.SYSRESAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

Audit Research - SQL

- Run time executables within your environment
  3. AUDIT Policies & Executable modules
  4. ROLES, Ids

```
---SECADM -- CONTAINS ONE ROW FOR
--- EACH AUDIT POLICY.
SELECT *
FROM SYSIBM.SYSAUDITPOLICIES
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- CONTAINS AUDITING OPTION COLUMN
--- AUDIT ALL/CHANGE/NONE
SELECT *
FROM SYSIBM.SYSTABLES
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- CONTAINS SECURITY DETAILS ON
--- SPs, UDFs & CAST FUNCTIONs
SELECT *
FROM SYSIBM.SYSROUTINEAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- CONTAINS EXTERNAL_SECURITY
--- COLUMN DB2/SESSION_USER/DEFINER
SELECT *
FROM SYSIBM.SYSROUTINES
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
-- THE SYSIBM.SYSROLES TABLE
-- CONTAINS ONE ROW FOR EACH ROLE.
SELECT *
FROM SYSIBM.SYSROLES
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
---CONTAINS A ROW FOR EACH PARAMETER
-- OF A ROUTINE OR MULTIPLE ROWS FOR
---TABLE PARAMETERS (ONE FOR EACH
---COLUMN OF THE TABLE).
--- ROUTINE CAN HAVE A ROLE IN OWNERTYPE
SELECT *
FROM SYSIBM.SYSPARMS
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
-- THE SYSIBM.SYSSCHEMAAUTH TABLE
-- CONTAINS ONE OR MORE ROWS FOR EACH
-- USER THAT IS GRANTED A PRIVILEGE ON A
-- PARTICULAR SCHEMA IN THE DATABASE.
SELECT *
FROM SYSIBM.SYSSCHEMAAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
-- SYSIBM.SYSSEQUENCEAUTH TABLE
-- RECORDS THE PRIVILEGES THAT ARE HELD
-- BY USERS OVER SEQUENCES
SELECT *
FROM SYSIBM.SYSSEQUENCEAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

Audit Research - SQL

5 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

```
-- THE SYSIBM.SYSUSERAUTH TABLE RECORDS THE
-- SYSTEM PRIVILEGES THAT ARE HELD BY USERS
SELECT *
FROM SYSIBM.SYSUSERAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
-- THE SYSIBM.SYSTABAUTH TABLE RECORDS THE
-- PRIVILEGES THAT USERS HOLD ON AND VIEWS
SELECT *
FROM SYSIBM.SYSTABAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- SECADM - ONE ROW FOR EACH ROW PERMISSION
--- AND COLUMN MASK
 SELECT *
 FROM SYSIBM.SYSCONTROLS
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
--- LISTS THE DEPENDENT OBJECTS FOR EACH ROLE
SELECT *
FROM SYSIBM.SYSOBJROLEDEP
FETCH FIRST 10 ROWS ONLY WITH UR;
```

```
-- THE SYSIBM.SYSCOLAUTH TABLE RECORDS THE
-- UPDATE OR REFERENCES PRIVILEGES  THAT ARE
--- HELD BY USERS ON INDIVIDUAL
--- COLUMNS OF A TABLE OR VIEW.
SELECT *
FROM SYSIBM.SYSCOLAUTH
FETCH FIRST 10 ROWS ONLY WITH UR;
```

Default Access Cleaned Up? – DB2 LUW

- REVOKE PUBLIC Access
  - Limit discovery of your metadata
  - Start with TABSCHEMA
    - SYSCAT, SYSIBM, SYSIBMADM, and SYSTOOLS

```
SELECT 'REVOKE SELECT ON '|| TABSCHEMA||'.'
||TABNAME||' FROM PUBLIC; '
FROM SYSCAT.TABLES
-- Start with SYSCAT%, SYSIBM%, SYSIBMADM%, SYSTOOLS% for your TABSCHEMA
WHERE TABSCHEMA LIKE 'table schema name'
ORDER BY TABSCHEMA, TABNAME
WITH UR;
```

- REVOKE miscellaneous user access
  - Change TABSCHEMA to your databases' schema name
  - Eliminate all extra access authorities to your databases

Db2 Security procedures

- Plan your DBA security profile for every interface
  - Cross reference the security profile for every piece of data especially PII
  - Document your procedures for the SOC
- Build a baseline security audit of your..
  - Systems security profiles
  - Applications security public and private ids
  - Application interfaces
    - Encrypted communication usage
  - Application Certificate handling
  - Confirm DBA documentation, 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 reviews, 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 .com

Proven Performance Tips:
www.DaveBeulke.com

Session code: G16

Thank you!

Please fill out your session evaluation before leaving!

Thank you! Here is some light reading

- **IBM Security Guide**
  https://www.ibm.com/support/knowledgecenter/en/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/security-overview.html
- **2017 Internet Security Threat Report**
  https://www.symantec.com/security-center/threat-report
- **Building and Operating an effective Security Operations Center**
  http://www.ciscopress.com/articles/article.asp?p=2460771
- **Secure Coding Practices in Java Challenges and Vulnerabilities**
  https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&cad=rja&uact=8&ved=0ahUKEwjah_f9paPZAhVkUt8KHW3gC-IQFghpMAU&url=https%3A%2F%2Farxiv.org%2Fpdf%2F1709.09970&usg=AOvVaw3KvqqXrhYFSc DYG65BU0vp
- **iKeyman - GUI tool for managing Java keystores**
  https://www.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/ikeyman.html?view=kc
- **NIST Cryptographic Key Management systems (CKMS)**
  https://csrc.nist.gov/projects/key-management/cryptographic-key-management-systems
- **Android Developer**
  https://developer.android.com/training/articles/security-ssl.html
- **Java Authentication and Authorization Service (JAAS)**
  https://www.ibm.com/support/knowledgecenter/en/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/introduction.html
- **JAAS HelloWorld Example –**
  https://www.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/samples.html#samples__jsse2
- **5 Steps to Building and Operating an Effective Security Operations Center (SOC)**
  http://www.ciscopress.com/articles/article.asp?p=2460771
- **TCP/IP configuration statements DVIPA networking adressing**
  https://www.ibm.com/support/knowledgecenter/en/SSEPEK_11.0.0/dshare/src/tpc/db2z_exampletcpipconfig.html

Connections and Services – DB2 LUW-12

- Db2 dbm and db cfg
- Defaults everywhere
  - Default TCP/IP within your environment
    - Where behind the company firewall is your database
  - Default Port used for the DB2 Instance
    - Production available
  - Shared DB2 Instance for Test and Production
    - Asking for trouble

- Default Discovery Parameters
  - Database Manager Configuration
    - Discovery mode (DISCOVER) = SEARCH
    - Discover server instance (DISCOVER_INST) = ENABLE
  - Database Configuration
    - Discovery support for this database (DISCOVER_DB) = ENABLE

Connections and Services – DB2 LUW-13

- Is encryption used within your connections?
  - DB2 Connect Version?
    - How up to date is your middleware?
  - Use AES encrypted DB2 Connect "DATA_ENCRYPT" settings
    - Encrypt ALL data on the wire between the Client and the Host database
  - Are your connections using the Transport Layer Security (TLS)?
    - Provides security certificates on each end of your processing
- Is encryption used within your databases?

What Connections and Services – DB2 LUW-19

- Take care of default Instance Discovery Mode
  - Discovery Mode Let DB2 Instance to be discovered
    - "Hack Me" sign on your DB2 Instance

- Database Discovery Parameters

- **DB2 "GET DBM CFG"**
  - **Database Manager Configuration**

```
Discovery mode                      (DISCOVER) = SEARCH
Discover server instance       (DISCOVER_INST) = ENABLE
```

- **DB2 "GET DB CFG"**
  - **Database Configuration**

```
Discovery support for this database (DISCOVER_DB) = ENABLE
```

- **Disable** all of these Discovery Mode parameters!

What Connections and Services – DB2 LUW-18

- To take care of existing old databases to encryption
  - Take a non encrypted backup
    - Reduces encryption overhead on the backup and the restore
  - Restore from the backup and use the new “Encrypt” clause
    - Take your database from exposed to encrypted
    - Legacy Is encryption used
    - There is a performance overhead for encryption
    - Some Server chips have encryption algorithms burned into the chips
      - Hardware assist
  - Encryption protects data at rest

What Connections and Services – DB2 LUW-17

- Is encryption used within your databases?
  - If your databases are already created
    - Make sure to Encrypt backup also.
    - Encrypt with a specific key command is:

```
BACKUP DATABASE database_name
    ENCRYPT ENCRLIB 'libdb2encr.dll'
    ENCROPTS 'BEULKEKey=theBestEncryption';
```

    - Compress and Encrypt command is:
      - `BACKUP DATABASE database_name ENCRYPT ENCRLIB db2encr_compr.dll;`

Default Access Cleaned Up? – DB2 LUW-23

- ***NOTE*** Analysis and testing should be done to determine the impact of any DB2 security REVOKE within your DB2 environment prior to implementation.**

Remember authorizations cascade and so do the REVOKE authorities within your system.

Before revoking access *make sure to analyze and test the operations of your system*, its databases, the various utilities, and your application operations. DB2 security is very complex and inter-dependent.

One of the best ways to analyze the REVOKE impacts is by using a Redirected Restore of your DB2 system to a test environment where all the REVOKE statement cascades and impacts can be thoroughly tested and realized.

Another DB2 security REVOKE testing scenario can be analyzed and started in your test environment. Once the full impact of your DB2 Security REVOKEs are realized, they can be migrated into your other environments and finally your production environments. Be careful! Properly managed DB2 security is critical to protect your environment and to maintain an operational environment that is critical to your company's bottom line.

Default Access Cleaned Up? – DB2 LUW-24

- Default database creation gives PUBLIC too much

```
REVOKE BINDADD ON DATABASE FROM PUBLIC;
REVOKE CREATETAB ON DATABASE FROM PUBLIC;
REVOKE CONNECT ON DATABASE FROM PUBLIC;
REVOKE IMPLICIT_SCHEMA ON DATABASE FROM PUBLIC;
REVOKE ACCESSCTRL ON DATABASE FROM GROUP PUBLIC;
REVOKE DATAACCESS ON DATABASE FROM GROUP PUBLIC;
REVOKE DBADM ON DATABASE FROM GROUP PUBLIC;
```

```
REVOKE ALTERIN ON SCHEMA <my schema name> FROM PUBLIC;
REVOKE CREATEIN ON SCHEMA <my schema name> FROM PUBLIC;
REVOKE DROPIN ON SCHEMA <my schema name> FROM PUBLIC;
```

```
REVOKE EXTERNALROUTINE ON DATABASE FROM GROUP PUBLIC ;
REVOKE LOAD ON DATABASE FROM GROUP PUBLIC ;
REVOKE NOFENCE ON DATABASE FROM GROUP PUBLIC ;
REVOKE QUIESCECONNECT ON DATABASE FROM GROUP PUBLIC ;
REVOKE LIBRARYADM ON DATABASE FROM GROUP PUBLIC ;
REVOKE SECURITYADM ON DATABASE FROM GROUP PUBLIC ;
REVOKE SQLADM ON DATABASE FROM GROUP PUBLIC ;
REVOKE WLMADM ON DATABASE FROM GROUP PUBLIC ;
REVOKE EXPLAIN ON DATABASE FROM GROUP PUBLIC ;
REVOKE CREATESECURE ON DATABASE FROM GROUP PUBLIC;
```

```
REVOKE USE OF TABLESPACE USERSPACE1 FROM PUBLIC;
```

Default Access Cleaned Up? – DB2 LUW-25

- REVOKE PUBLIC Access
  - Limit discovery of your metadata
  - Start with TABSCHEMA
    - SYSCAT, SYSIBM, SYSIBMADM, and SYSTOOLS

```
SELECT 'REVOKE SELECT ON '|| TABSCHEMA||'.'
||TABNAME||' FROM PUBLIC; '
FROM SYSCAT.TABLES
-- Start with SYSCAT%, SYSIBM%, SYSIBMADM%, SYSTOOLS% for your TABSCHEMA
WHERE TABSCHEMA LIKE 'table schema name'
ORDER BY TABSCHEMA, TABNAME
WITH UR;
```

- REVOKE miscellaneous user access
  - Change TABSCHEMA to your databases' schema name
  - Eliminate all extra access authorities to your databases

Default Access Cleaned Up? – DB2 LUW-26

- REVOKE Monitoring Tables access
  - Limit discovery of your metadata
  - Start with TABSCHEMA
    - SYSCAT, SYSIBM, SYSIBMADM, and SYSTOOLS

```
REVOKE SELECT ON MON_DB_SUMMARY from public
REVOKE SELECT ON MON_CONNECTION_SUMMARY from public
REVOKE SELECT ON MON_WORKLOAD_SUMMARY from public
REVOKE SELECT ON MON_SERVICE_SUBCLASS_SUMMARY from public
REVOKE SELECT ON MON_CURRENT_UOW from public
REVOKE SELECT ON MON_CURRENT_SQL from public
REVOKE SELECT ON MON_PKG_CACHE_SUMMARY from public
REVOKE SELECT ON MON_LOCKWAITS from public
REVOKE SELECT ON MON_TBSP_UTILIZATION from public
REVOKE SELECT ON MON_BP_UTILIZATION from public;
```