Database Security Or Leave it to the Hackers

Rob Bestgen
bestgen@us.ibm.com
IBM - Db2 for i Consultant

NHMUG
New Hampshire Midrange User Group

Power Systems

Concerns over data security continue to haunt organizations, with the vast majority of global companies indicating they feel vulnerable to data threats.

The worry is justified, according to a new study, as too many organizations focus on compliance ahead of breach prevention; and invest in technologies that do not prevent data breaches.

Information Management article “Majority of Global Organizations Feel Vulnerable to Data Threats” by David Weldon February 16, 2016
http://www.information-management.com/news/security/majority-of-global-organizations-feel-vulnerable-to-data-threats-10028266-1.html

Among the study's findings:

63% of U.S. respondents believe privileged users are the most dangerous insiders

Information Management article "Majority of Global Organizations Feel Vulnerable to Data Threats" by David Weldon February 16, 2016
http://www.information-management.com/news/security/majority-of-global-organizations-feel-vulnerable-to-data-threats-10028266-1.html

Securing Data

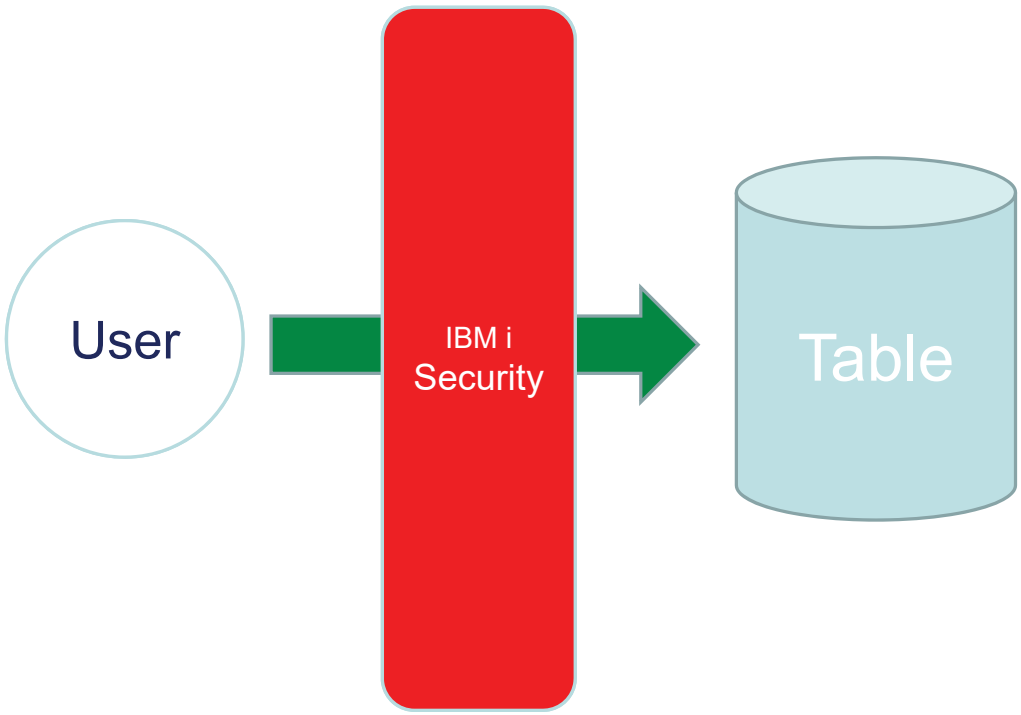
Power Systems

PII – Personal Identifiable Information

Power Systems

1. Do not carry (private) data elements unnecessarily
   - Normalize private data into (very) few tables
   - Proper relational modeling accomplishes this

2. Protect data element(s) first with object level authority
   - Avoid application or menu based security schemes
   - Adoption approach possible via data access layer



Question:

Who has *ALLOBJ special authority?

Power Systems

- Determine how data needs to be protected
  - Everyone can update?!
  - Some can read, authorized users can update
  - No one can access by default, authorized users given access
- Approaches
  - Private Authorities
  - Adopted Authorities
  - Separation of Duties

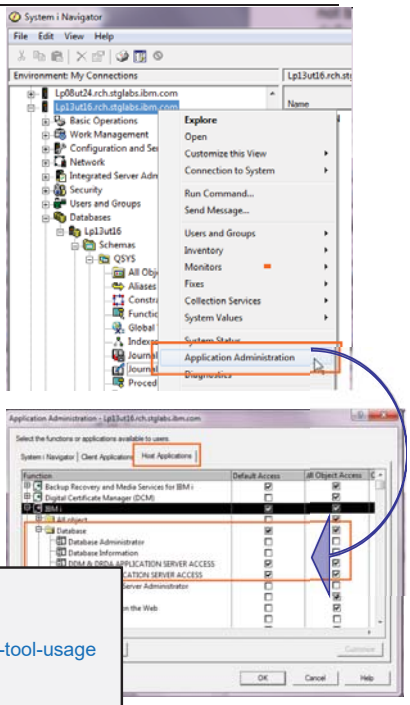
Power Systems

- Step #1 – Limit number of *ALLOBJ special authority users
  - No direct control to prevent *ALLOBJ user from accessing object
- Step #2 – Tighten down *PUBLIC authority
  - QCRTAUT System Value controls default behavior
  - SQL interfaces can have different behavior
    - *SQL Naming – *PUBLIC given *EXCLUDE
    - *SYS Naming – follows QCRTAUT model
- Step #3 – Consider granularity of private authorities
  - Individual user profiles
  - Group profiles
  - Authorization lists
  - Adopted authority
  - Separation of Duties

Power Systems

Database Function Usage Identifiers:

- **QIBM_DB_DDMDRDA** (ability to lock down DRDA and DDM application server access)
- **QIBM_DB_SQLADM** (enable use of OnDemand Performance Center tools and more)
- **QIBM_DB_SYSMON** (SQL Details for jobs)
- **QIBM_DB_ZDA** (restrict ODBC and JDBC Toolbox from the server side, including Run SQL Scripts, System i Navigator and others)
- **QIBM_DB_SECADM**
  Alternative to *SECOFR, administer security



Articles:

Improved Security Controls Open Door to DB2 for i Tool Usage

http://iprodeveloper.com/database/improved-security-controls-open-door-db2-i-tool-usage

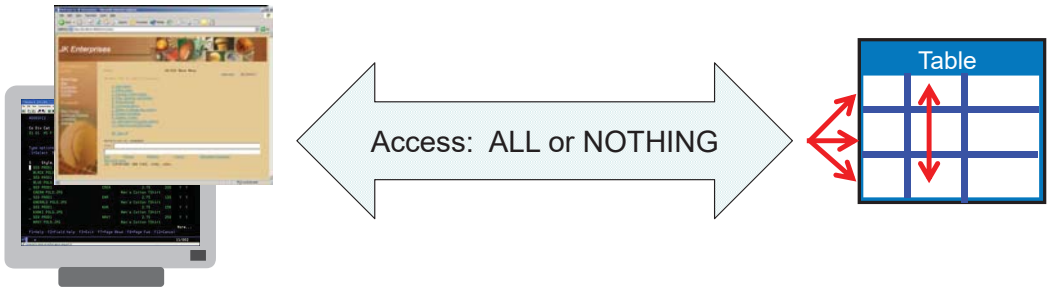
Granular security control with function usage

https://www.ibm.com/developerworks/ibmi/library/i-granular-security/

Power Systems

More Granular Security

Power Systems



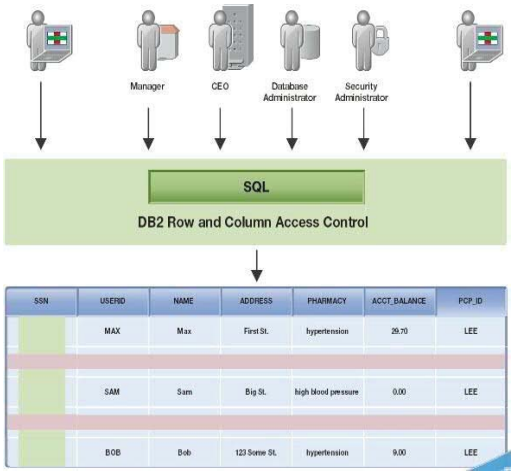
- No easy way to restrict access to a specific set of rows or values within a column
- Government regulations and corporate policies aggressively pushing IT to restrict user/application access to sensitive data

A Solution….

Row and Column Access Control (RCAC)

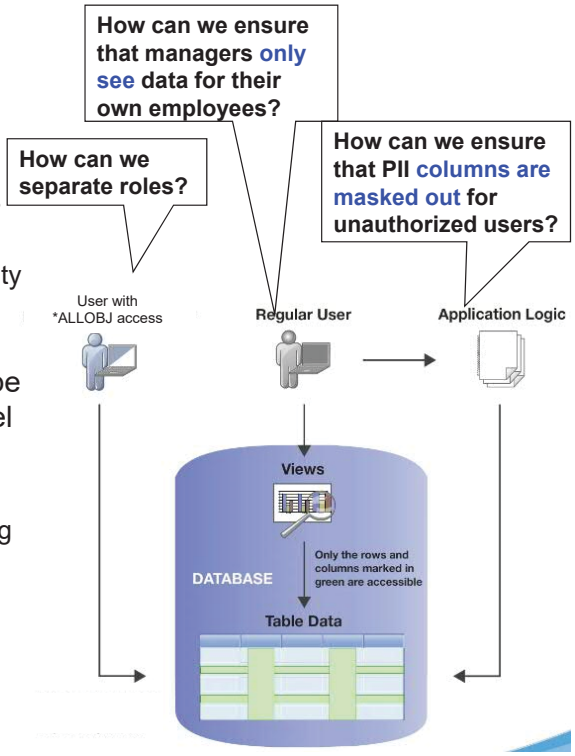
Power Systems

- Additional layer of data security available with Db2 complementary to table level security
  - Available since V7R2
- Includes separation of duties
- Controls access to only “need to know” rows and hides data in columns
- Two sets of rules
  - Permissions for rows
  - Masks for columns
- Delivered with IBM Advanced Data Security for i feature
  - No-charge feature, option 47
  - Required on development & production systems



Power Systems

- Currently, data access is restricted with application logic or logical views
- Users with direct access to DB2 objects can bypass these layers
  - Example: Users with *ALLOBJ authority can still view all data
- DB2 RCAC enables all data access to be controlled at the row and/or column level
  - Set up rich security policies
  - Prevents security administrators (*ALLOBJ or *SECADM) from accessing data in a database
  - No dependency on application logic
  - Restrict rows and mask columns
    - PERMISSION – row filtering
    - MASK – column masking



Power Systems

- Scenario has the following permissions attached
  - Patients
    - 1 Can only access their own data
  - Physicians
    - 2 Can only access their own patients' data
  - Membership officers, Accounting, and Drug researchers
    - 3 Can access all data
  - Nobody else sees any data

```
CREATE PERMISSION access_to_row ON patient
FOR ROWS WHERE
(
  VERIFY_GROUP_FOR_USER(SESSION_USER,'PATIENT') = 1
  AND patient.userid = SESSION_USER
)
OR
(
  VERIFY_GROUP_FOR_USER (SESSION_USER,'PCP') = 1
  AND patient.pcp_id = SESSION_USER
)
OR
(
  VERIFY_GROUP_FOR_USER (SESSION_USER,'MEMBERSHIP') = 1
OR
  VERIFY_GROUP_FOR_USER (SESSION_USER,'ACCOUNTING') = 1
OR
  VERIFY_GROUP_FOR_USER(SESSION_USER,'RESEARCH')=1
)
ENFORCED FOR ALL ACCESS
ENABLE;

ALTER TABLE patient ACTIVATE ROW ACCESS CONTROL;
```

1

2

3


```
SELECT * FROM patient
```

PID	USERID	NAME	ADDRESS	PHARMACY	ACCT_BALANCE	PCP_ID
123 551 234	MAX	Max	First St.	hypertension	89.70	LEE
123 119 856	SAM	Sam	Big St.	codeine	12.50	LEE
123 456 789	BOB	Bob	123 Some St.	hypertension	9.00	LEE

- Row Access Control
  - Doctors can only see the data of their own patients


```
UPDATE patient SET pharmacy = 'codeine' WHERE name='DOUG'
```

PID	USERID	NAME	ADDRESS	PHARMACY	ACCT_BALANCE	PCP_ID
123 551 234	MAX	Max	First St.	hypertension	89.70	LEE
123 589 812	MIKE	Mike	Long St.	diabetics	8.30	JAMES
123 119 856	SAM	Sam	Big St.	codeine	12.50	LEE
123 191 454	DOUG	Doug	Good St.	influenza	7.68	JAMES
123 456 789	BOB	Bob	123 Some St.	hypertension	9.00	LEE

- Unsuccessful UPDATE statement
  - *Row not found for UPDATE*
  - *SQLSTATE=02000, SQLCODE=100*
- If you cannot view a row, you cannot update (or add) the row either

- Scenario has the following permission attached
  - PID number column
    - Patients can see full Patient ID number
    - Everyone else sees 'XXX XXX ' + last three digits of PID

```
CREATE MASK pid_mask ON patient FOR
COLUMN pid RETURN
   CASE
     WHEN
       VERIFY_GROUP_FOR_USER(SESSION_USER,'PATIENT') = 1
         THEN pid
       ELSE
         'XXX XXX ' || SUBSTR(pid, 8, 3)
   END
ENABLE;

ALTER TABLE patient ACTIVATE COLUMN ACCESS CONTROL;
```

Power Systems


```
SELECT * FROM patient
```

PID	USERID	NAME	ADDRESS	PHARMACY	ACCT_BALANCE	PCP_ID
XXX XXX 234	MAX	Max	First St.	hypertension	89.70	LEE
XXX XXX 856	SAM	Sam	Big St.	codeine	12.50	LEE
XXX XXX 789	BOB	Bob	123 Some St.	hypertension	9.00	LEE

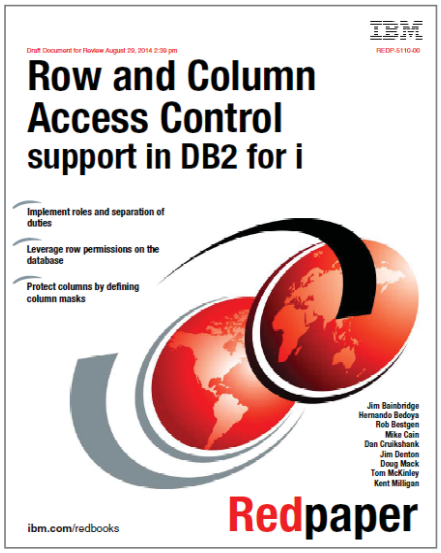
- Column Access Control
  - Doctors cannot see PID numbers
- Row Access Control
  - Doctors can only see the rows of their own patients

Power Systems


```
SELECT * FROM patient
```

PID	USERID	NAME	ADDRESS	PHARMACY	ACCT_BALANCE	PCP_ID
123 456 789	BOB	Bob	123 Some St.	hypertension	9.00	LEE

- Column Access Control
  - Patients can see PID numbers
- Row Access Control
  - Patients can only see their own data



www.redbooks.ibm.com/redpieces/abstracts/redp5110.html

- **Offering from the Systems Lab Services DB2 for IBM i team**
- **Multi-day facilitated workshop including the following:**
  - Review of the current state, current requirements, and future requirements for managing data access
  - Education on possible solutions and related best practices for their implementation
  - Discussion and formulation of a strategic roadmap for implementation
- **For more information, contact mcain@us.ibm.com**

Defining and Measuring Compliance

Data governance, control and security

…is the domain of Business, not IT.

Business defines the rules.

IT implements the rules.

- Security Policy
  - No policy, no plan for securing data
  - No policy, no measurement
  - No policy, expensive audits

- Resource Security
  - Prevents data breaches from internal & external intrusions
  - Closely tied to Security Policy definition

A Measured Solution

Power Systems

Compliance Assessment and Reporting Tool (CART) aka IBM PowerSC for i

System and Security Reporting Solution by IBM Lab Services

- Automated collection, analysis, and reporting tool on over 1000 system and security related risks, information, statistics and demographics.
- Centralized collection and reporting. Easy to use!
- Event monitoring – capture actions as they happen.
- Enables compliance officer to demonstrate adherence to pre-defined or customer-defined security polices.

"I just want to arrive in the morning, get a cup of coffee, and have a view of what systems are in compliance and which are not."

http://ibm.biz/IBMiSecurity

or

Terry – taford@us.ibm.com

Doug – mackd@us.ibm.com

Power Systems

CART

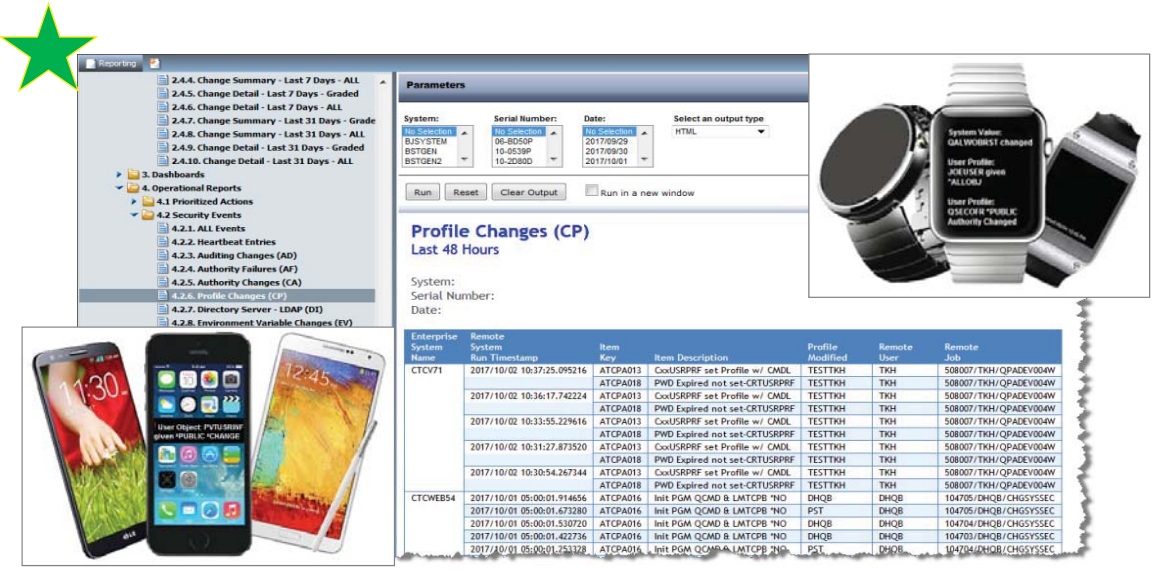
http://ibm.biz/IBMiSecurity

- Daily compliance dashboard reports from LPAR to enterprise level
  - Multiple, different security policy perspectives
  - Including cross system analysis
  - Traffic lighting for easier problem identification
- Covers all aspects of system security
  - Operational security
  - Profile administration and Password management
  - Special authorities and group inheritance
  - Network configuration
  - NetServer attributes
  - PTF currency
  - Event monitoring
  - Highlights Security risks
  - ….
- Extensible
  - Add custom defined items
  - Collect/consolidates files you specify!
  - 'Push' changes*

* Optional and under your control

Power Systems

CART



http://ibm.biz/IBMiSecurity

Power Systems

CART – Single Server/LPAR Edition

http://ibm.biz/IBMiSecurity

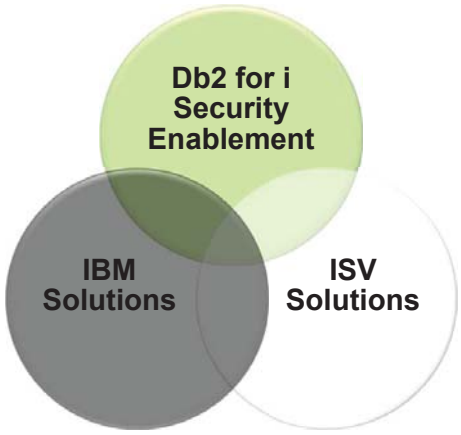
- An automated collection, analysis, and reporting tool on over 1000 system and security related risks, information, statistics and demographics. All in one location and easy to use!

- **Covers:**
  - Password management
  - Profile administration
  - Special authorities
  - Group inheritance
  - Network configuration
  - NetServer attributes
  - Operational security
  - PTF currency
  - Event monitoring
  - Custom defined items
  - Highlight security risks

- Enables compliance officer to demonstrate adherence to pre-defined or customer-defined security polices.
- System and Security reporting made easy!

Area Reviewed	Risk Potential	Value Retrieved
Profiles with *ALLOBJ Special Authority	*YES	25
Profiles with *JOBCTL Special Authority	*YES	70
Profiles with *SPLCTL Special Authority	*YES	62
Profiles with Default Passwords	*YES	1
Profiles with Passwords that Never Expire (*NOMAX)	*YES	35
Group Profiles with Passwords	*NO	0
*ALLOBJ Special Authority through Group Profile	*NO	0
*JOBCTL Special Authority through Group Profile	*YES	5
*SPLCTL Special Authority through Group Profile	*NO	0
Profile objects that are *PUBLICly Authorized	*YES	5
Profile objects that are Privately Authorized	*YES	6
Audit Journal	*YES	Yes
DDM Password Requirements	*YES	*USRIDPWD
Does the *SYSTEM Store Exist	*EXCLUDE	*EXCLUDE
ROOT (/) is Shared	*YES	Yes
ROOT (/) *PUBLIC Authority is *RWX	*YES	*RWX
Subsystems with *PUBLIC not *USE or *EXCLUDE	*YES	13
Job Descriptions with *PUBLIC not *USE or *EXCLUDE	*YES	78
Job Queues with *PUBLIC not *USE or *EXCLUDE	*YES	13
*IBM Libraries with *PUBLIC not *USE or *EXCLUDE	*YES	3
USER Libraries with *PUBLIC not *USE or *EXCLUDE	*YES	426
QSECOFR Adoption in USER Libraries	*YES	544
AUTH Lists with *PUBLIC not *USE or *EXCLUDE	*YES	9
Allow Change to System Values	*YES	Yes
QSECURITY - System security level	*LOW	40

- **Securing personal data is an absolute necessity.**
- **IBM i object based security is a good start but is not enough.**
- **IBM i and Db2 for i provide many additional tools to protect your data.**
- **Monitoring and Compliance support is available.**
- **Let us help you protect your data!**



Thank You!

www.ibm.com/developerworks/ibmi/techupdates/db2