

Safeguard your precious business data with the latest IBM i security enhancements

Thomas Barlen

barlen@de.ibm.com

**Consulting IT Specialist
Power Systems Security**



Agenda



- Observations & studies
- Base IBM i security enhancements
- Database security enhancements
- Cryptographic enhancements
- Network security enhancements



Agenda

- Observations & studies
- Base IBM i security enhancements
- Database security enhancements
- Cryptographic enhancements
- Network security enhancements

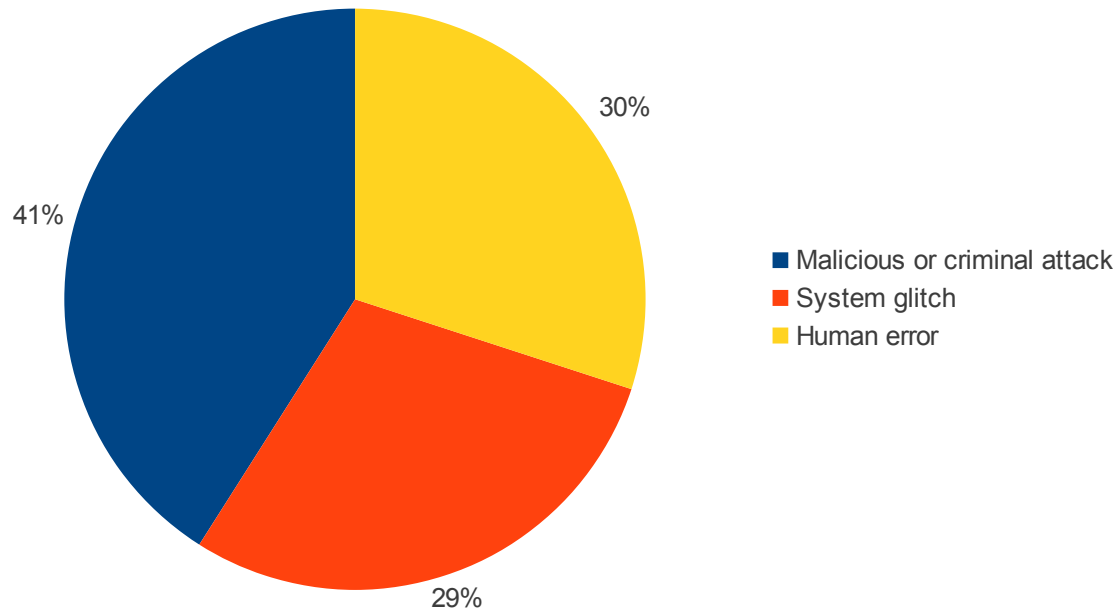
- Latest studies from the Ponemon Institute 2014 Cost of Data Breach: Global Analysis reveals:

- “Companies WW are finding that **data breaches have become as common** as a cold but far more expensive to treat”
- “Average cost of a data breach to a company was \$3.5 million in US dollars and 15 percent more than what it cost the previous year”
- “Research reveals that **reputation** and the **loss of customer loyalty** does the most damage”
- “In most countries, the primary root cause of the data breach is a **malicious insider** or criminal attack”
- “Having a strong security posture, incident response plan and CISO appointment reduced the cost per record

314 companies from 10 countries (United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India, United Arab Emirates, and Saudi Arabia) participated in the study. The number of compromised records range from 2,415 to slightly more than 100,000.

Observations & Studies (cont'd)

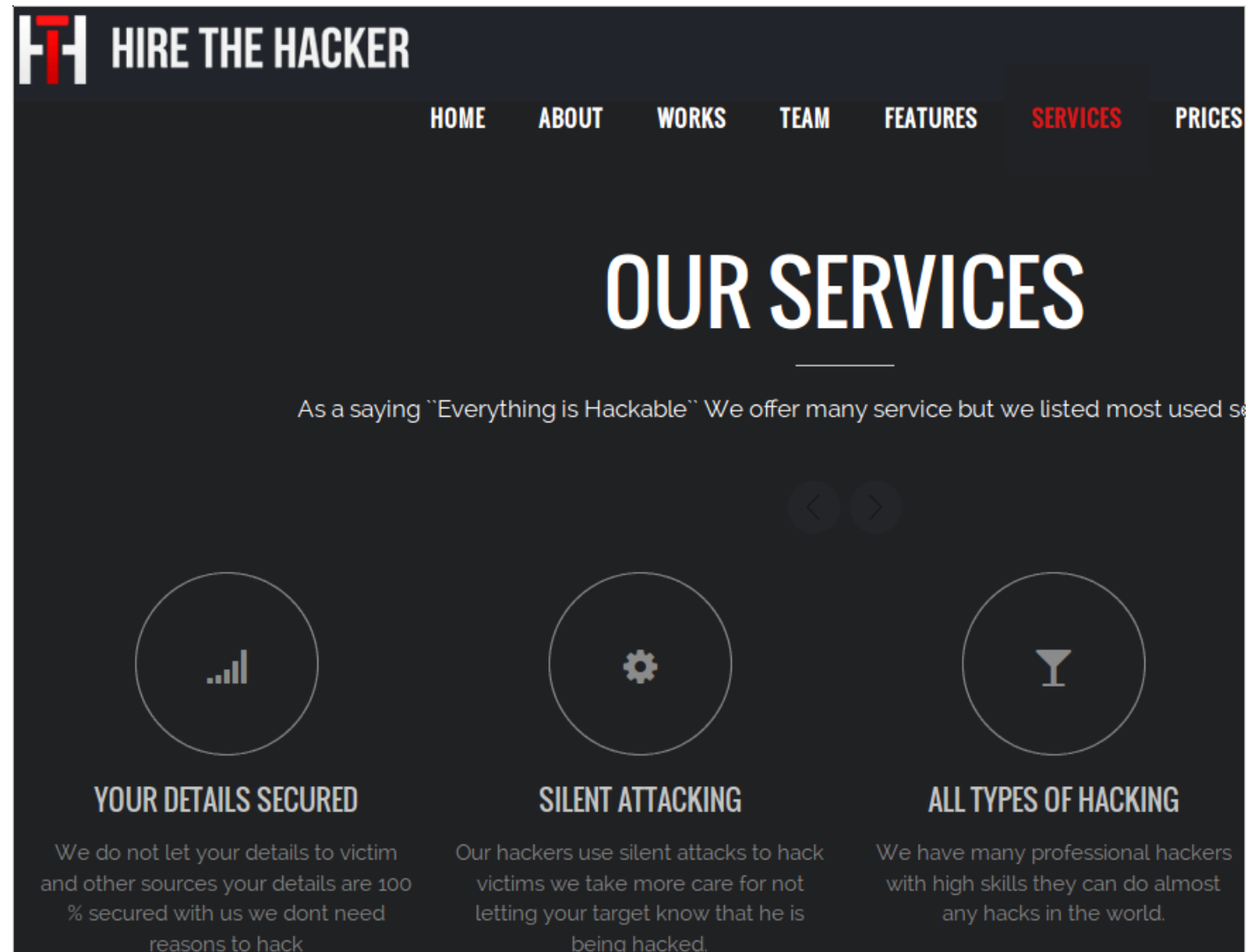
- Distribution of the root cause of the data breaches



- Companies are far more likely to have a small data breach than a mega breach

Your company could be the next target

- Many professional hacking services exist to hack into your company



The screenshot shows the 'HIRE THE HACKER' website. The navigation menu includes HOME, ABOUT, WORKS, TEAM, FEATURES, SERVICES (highlighted in red), and PRICES. The main heading is 'OUR SERVICES'. Below it, a quote reads: 'As a saying "Everything is Hackable" We offer many service but we listed most used services'. There are three service cards:

- YOUR DETAILS SECURED**: We do not let your details to victim and other sources your details are 100% secured with us we dont need reasons to hack
- SILENT ATTACKING**: Our hackers use silent attacks to hack victims we take more care for not letting your target know that he is being hacked.
- ALL TYPES OF HACKING**: We have many professional hackers with high skills they can do almost any hacks in the world.

Example:
<http://hirethehacker.com/>

Your company could be the next target (cont'd)



HIDDEN LYNX

PROFESSIONAL HACKERS FOR HIRE

WHO

- Hackers for hire
- Active since 2009
- Based in China
- Experts in breaching high security targets
- Proficient, innovative and methodical
- More capable than Comment Crew/APT1

KEY NUMBERS

- 50-100 Operatives
- 2 Teams - Team Naid and Team Moudoor
- 15 Regions impacted
- 100's Of organizations targeted
- 3 Zero-day exploits used since 2011
- >3 Years of operation

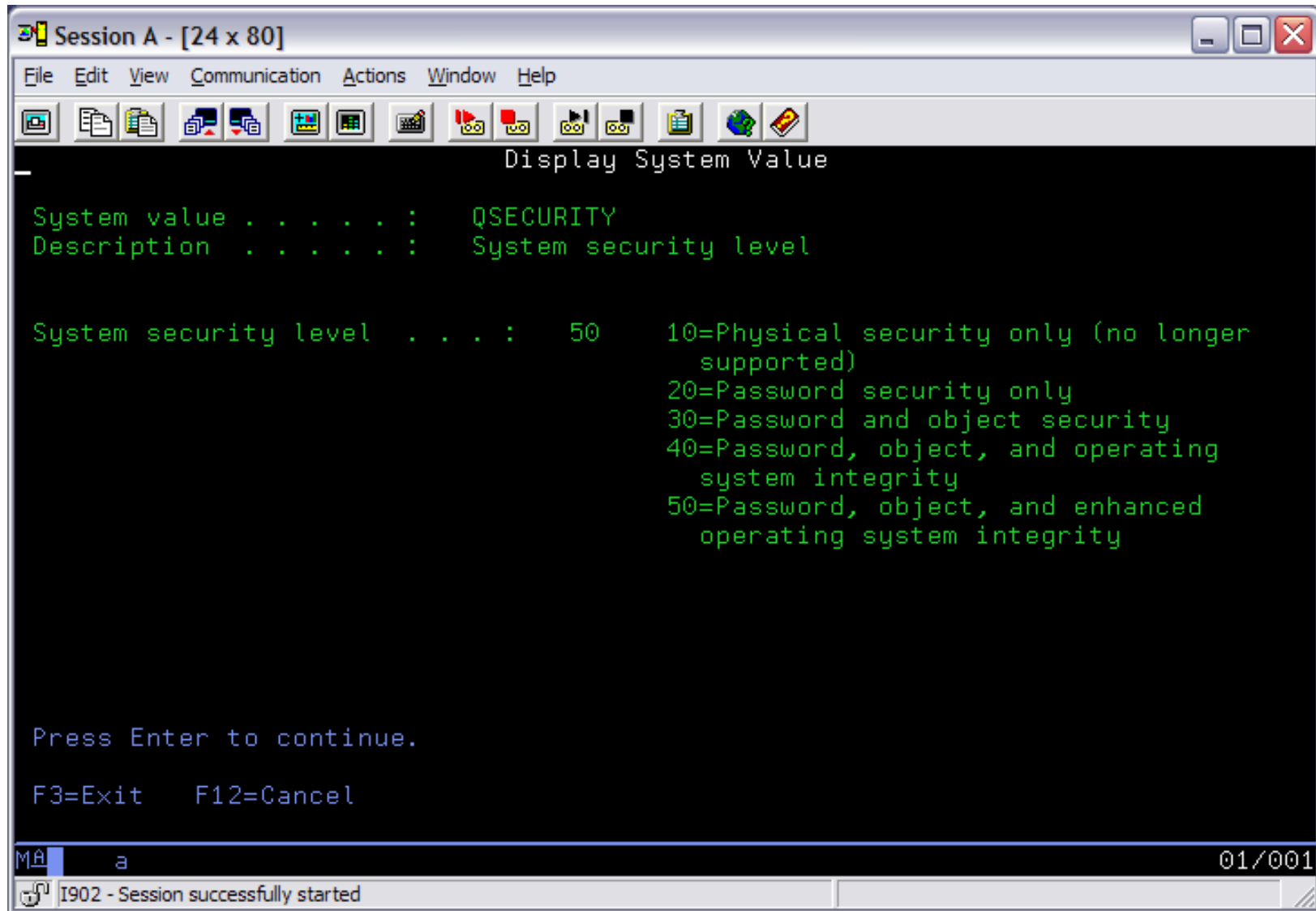




Agenda

- Observations & studies
- **Base IBM i security enhancements**
- Database security enhancements
- Cryptographic enhancements
- Network security enhancements

System Value: QSECURITY



The screenshot shows a terminal window titled "Session A - [24 x 80]". The window contains the following text:

```
Display System Value

System value . . . . . : QSECURITY
Description . . . . . : System security level

System security level . . . . : 50      10=Physical security only (no longer
                                         supported)
                                         20=Password security only
                                         30=Password and object security
                                         40=Password, object, and operating
                                         system integrity
                                         50=Password, object, and enhanced
                                         operating system integrity

Press Enter to continue.

F3=Exit   F12=Cancel
```

At the bottom of the terminal, the prompt "Mâ a" is visible, along with the page number "01/001" and a status bar that reads "I902 - Session successfully started".



Security Compliance – Password rule enhancements



- New system values supported ([more...](#))
 - **QPWDRULES**, define new pwd rules
 - **QPWDEXPWRN**, define pwd expired warning interval
 - **QPWDCHGBLK**, prevent passwords from being changed repeatedly
- Changed system value
 - **QLMTDEVSSN**, Limit device sessions (*NONE, 1-9 sessions)
- Changed/New user profile parameters
 - **LMTDEVSSN**, Limit device sessions (1-9 sessions)
 - **PWDCHGBLK** - Block password change (1-99 hours)



- Password syntax rules always apply when end users change their password (**CHGPWD** & **QSYCHGPW** API)
- Up to 7.1 System Administrators can use **CRT/CHGUSRPRF** to set a password to any value
- From 7.2
 - A new value ***ALLCRTCHG** for the QPWDRULES system value can also enforce password syntax rules for the **CRT/CHGUSRPRF** commands
 - 6.1: CP security audit record reflects a PWD that doesn't meet syntax rules



- QPWDRULES - System value to define password syntax
 - QPWDRULES, define password rules
 - Require special character
 - Require mixed case
 - Prevent all numeric password

 - Require x number of digits
 - Require x number of letters
 - Require x number of special characters

 - Require characters of any 3 classes

 - Other supported values as well....

QPWDRULES Password rules



NOTE: Validation tab 1 are the password rules pre 6.1

NOTE: Validation tab 2 are the combined password rules from 6.1 and higher

Password System Values - Localhost

General
Validation 1
Validation 2
Expiration

Password level (current):
Long passwords using an unlimited character set. (2)

Password validation options

Use the validation system values on the Validation 1 tab

Use the following validation rules. Certain corresponding system values on the Validation 1 tab will be ignored.

Password Lengths

Minimum Length (1-128): 1,2,3...128

Maximum Length (1-128): 1,2,3...128

Restrict repeating characters:

Letter Characters

Minimum Number (0-9): 0 - 9

Maximum Number (0-9): 0 - 9

Restrict consecutive letter characters

Digits

Minimum Number (0-9): 0 - 9

Maximum Number (0-9): 0 - 9

Restrict consecutive digits

Special Characters

Minimum Number (0-9): 0 - 9

Maximum Number (0-9): 0 - 9

Restrict consecutive special characters

First Character

Restrict from being a letter

Restrict from being a digit

Restrict from being a special character

Last Character

Restrict from being a letter

Restrict from being a digit

Restrict from being a special character

Require a new character in each position from previous password

Restrict user profile in password

Require a minimum number of lowercase and uppercase letters (0-9): 0 - 9

Require characters from at least 3 of the following types of characters:

uppercase letters, lowercase letters, digits, and special characters



- **QPWDCHGBLK** - System value to prevent reuse of “prior” password
 - **QPWDCHGDBLK**, Block Password Change
 - Prevent change of password for x hours
 - *NONE
 - 1 to 99 hours
 - Recommendation is 24 hours
 - Password change block not in effect if PWDEXP(*YES) has been specified by the system administrator
- **PWDCHGBLK** parameter added to the user profile

QPWDCHGBLK – Password Change Block



Password System Values - Localhost

General

Validation 1

Validation 2

Expiration

Password level (current):

Long passwords using an unlimited character set. (2)

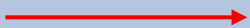
Password level (at next restart):

- Short passwords using a limited character set (0)
- Short passwords using a limited character set (1)
Disable IBM i NetServer passwords for Windows 95/98/ME clients
- Long passwords using an unlimited character set (2)
- Long passwords using an unlimited character set (3)
Disable IBM i NetServer passwords for Windows 95/98/ME clients

Minimum time between password changes:

- None
- Hours (1-99): 1,2,3...99

QPWDCHGBLK





- **QPWDEXPWRN** – Set password expiration warning interval
 - **QPWDEXPWRN**, Password Expiration Warning Interval
 - Warn user of expiring password
 - 7 is the Default
 - 1 to 99 days

QPWDEXPWRN – Password expiration warning



Password System Values - Localhost

General

Validation 1

Validation 2

Expiration

Password expiration:

Never expire

Days after last change (1-366): 1 - 366

Password expiration warning interval (1-99): 1,2,3...99 days

QPWDEXPWRN



- Additional information added to DSPUSRPRF
 - Password verifications not valid
 - Days before password expires
 - Creation Date
 - Change Date
 - Last used Date
 - Restore Date

New User Profile Parameters – 7.1



- New user profile “expiration” parameters in 7.1
 - **USREXPDATE**, User Expiration Date (Date when profile is *DISABLED)
 - **USREXPITV**, User Expiration interval (1-366 days)

```
Session A - [24 x 80]
File Edit View Communication Actions Window Help
Create User Profile (CRTUSRPRF)

Type choices, press Enter.

Home directory . . . . . HOMEDIR          *USRPRF
-----
EIM association:      EIMASSOC
EIM identifier . . . . .                *NOCHG
-----
Association type . . . . .                _____
Association action . . . . .              _____
Create EIM identifier . . . . .           _____
User expiration date . . . . . USREXPDATE *NONE
User expiration interval . . . . . USREXPITV
Authority . . . . . AUT                  *EXCLUDE

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

Mâ a 05/050
1902 - Session successfully started
```

Audit journal enhancements (5.4 / 6.1 / 7.1 / 7.2)



- CD entry format has been enhanced
 - CD entries are generated when command auditing is turned on
 - `CHGUSRAUD USRPRF(BARLEN) AUDLVL(*CMD)`
- CDCLP field in CD entry contains new values
 - N = Command run from a command line
 - Y = Command run within a compiled CL program
 - R = Command run from an interpreted REXX procedure **New**
 - E = Command run via Command Analyzer APIs (QCMDEXC, QCAPCMD, or QCAEXEC) **New**
 - B = Command is not being run from compiled CL or interpreted REXX or through a Command Analyzer API, and is in a batch job **New**
- Requires PTFs V5R4 (SI44854), 6.1 (SI44864), and 7.1 (SI44865)



Agenda

- Observations & studies
- Base IBM i security enhancements
- **Database security enhancements**
- Cryptographic enhancements
- Network security enhancements



Database Security Enhancements

- Business data is one of the most valuable assets in a company
- Sensitive data must be properly protected
 - Access control via object permissions
 - Encryption of sensitive data
 - Monitoring of unauthorized access attempts
 - Monitoring and control of read / write access over the network
 - Classification of data
- Most protection measures have been in IBM i for many years
- DB2 for IBM i provides new functions that can be used to implement
 - More granular access controls
 - Transparent encryption of data

Database Encryption

- IBM i provides several methods for encrypting data at rest
 - Common Cryptographic Architecture (CCA) APIs that use the 4765 cryptographic coprocessor
 - Cryptographic Services APIs
 - SQL encryption
- Using APIs to encrypt data within the business application requires changes to
 - Application code
 - Database column types and length
 - Interface changes for importing and exporting data
- New functions can be used to
 - Provide transparent encryption to applications
 - Data masking
 - Access control to data



7.1 IBM i DB2 Field Procedures

Column Level Encryption and Data Masking Enablement



- **DB2 Column Level (field) exit support**
 - Exit program (Field Procedure) called on insert/update/read of a column
 - Similar to “Triggers” but additional support to enable encryption
 - Exit added via SQL Alter Table
 - One exit per column
- **Enables Column Level Encryption**
 - Encrypt/Decrypt data in a DB2 column
 - No need to change column attributes like field length or data type
 - Encryption Key management must be implemented by the Exit Program (Field Procedure)



- **Data Masking support**

- Depending on FieldProc controls, data can be masked during decoding
- Example: User might just see last 4 digits of credit card PAN
PAN: **** * 1233
- Special considerations when updating or inserting rows
 - Special return code specified in sqlstate parameter Field Encoding function

- **Field Procedure is a user written program**

- Business partner solutions are available as well
- Example: Patrick Townsend, Linoma



- **Additional Security Checks within the Field Procedure**
 - To make the support meaningful, additional security checks should be implemented by the exit
 - Is the user listed on the Authorization list (*AUTL)?
 - If so, decrypt the SS# (data), otherwise return '-----' or '000000000'
- **DB2 handles all length and data type issues**
 - I/O buffer doesn't change but encrypted data length and data type can change
 - I/O buffer for SS# is 9 and type character
 - Result of encryption is, for example, length 16 and data type binary
 - Managed by DB2 internally



Row and Column Access Control

Row and Column Access Control (RCAC) - 7.2



- Provides more granular access control to columns or rows depending on user/group
- Implemented in DB
- Controls access for all interfaces, i.e. native SQL, ODBC, FTP, etc.
- Row access
 - Returns only rows where a user has access to
- Column access
 - Masks data that a user does not has access to
- High-level privileged users such as *ALLOBJ users are not exempt from these rules

Implementation

- RCAC can be used to complement the table privileges model
- Implemented via SQL commands
- Alters a table and adds access controls for rows and columns
- Enforced via database engine

Custno	Name	City	Country	Revenue
33123	Star hotels	Mainz	DE	*****
44541	Super hotels	Athens	GR	*****
45211	Bakery No 1	London	GB	32223.33
66541	Golden Pub	Manchester	GB	787611.32
76112	BBQ Joint	Raleigh	US	*****

Row access control

- Limit access to rows based on accessing user or group membership

```
CREATE PERMISSION SALARY_ROW_ACCESS ON EMPLOYEE
  FOR ROWS WHERE VERIFY_GROUP_FOR_USER (SESSION_USER,
    'MGR', 'ACCGRP') = 1
  ENFORCED FOR ALL ACCESS
  ENABLE;

COMMIT;

ALTER TABLE EMPLOYEE
  ACTIVATE ROW ACCESS CONTROL;

COMMIT;
```


Column access control

- Mask column values for users who do not have access

```
CREATE MASK SSN_MASK ON EMPLOYEE
  FOR COLUMN SSN RETURN
  CASE
    WHEN (VERIFY_GROUP_FOR_USER (SESSION_USER, 'PAYROLL')
          = 1)
      THEN SSN
    WHEN (VERIFY_GROUP_FOR_USER (SESSION_USER, 'MGR') = 1)
      THEN 'XXX-XX-' || SUBSTR (SSN, 8, 4)
    ELSE NULL
  END
  ENABLE;
COMMIT;

ALTER TABLE EMPLOYEE
  ACTIVATE COLUMN ACCESS CONTROL;
COMMIT;
```



Agenda

- Observations & studies
- Base IBM i security enhancements
- Database security enhancements
- **Cryptographic enhancements**
- Network security enhancements



IBM i **Software** Based Encryption

Encrypted ASP – Whole Disk Encryption

OS Option 45 (priced option)

Encryption of Data at Rest on disk (6.1)



- Meet **regulatory requirements** being imposed on our customers
- Reduce or eliminate the need for application providers to encrypt data
- Provide a more secure solution to help protect data
 - Key management done by the system

- **Encryption of data at rest**
 - Software solution
 - Both older, User ASPs, and newer, Independent ASPs are supported
 - Minimal key management requirements
- **Threats addressed by disk level encryption**
 - Protection of data in flight to SAN
 - Protection of data in flight in cross-site mirroring environment
 - Data Loss
 - Loss of disk drive
 - **Return drive to vendor (drive replacement of defective drive)**
 - **Single level store on IBM i does not eliminate the need to protect individual drives**

- **Provide the capability to encrypt all data residing on an ASP**
- Cryptographic keys will be stored in software but protected by “isolated” storage and master keys
 - **All data encryption keys are managed by the OS/LIC**
 - **The only key that needs to be managed by the customer is the ASP master key**
- **Minimal change required to an application**
 - ASP level changes may be required in the application to support independent ASPs (independent of encryption)

Create Master Key(s) via Navigator in 6.1



- Navigate to Security / Cryptographic Services Key Management / Master Keys

Manage Master Keys

Master keys are used to encrypt other keys. You can load, set, clear or display the properties of the selected master key.

<input type="checkbox"/>	Mater Key	Type	Current Key Verification Value
	No filter applied		
<input type="checkbox"/>	1	Not set	
<input type="checkbox"/>	2	Not set	
<input type="checkbox"/>	3	Not set	
<input type="checkbox"/>	4	Not set	
<input type="checkbox"/>	5	Set	21CFDCFB2EAB40F9FF214DEF45349DDBF67EC6FE
<input type="checkbox"/>	6	Set	052AA5DC2749D3D04BE8F3825194758EF1EFBBB2
<input type="checkbox"/>	7	Not set	
<input type="checkbox"/>	8	Not set	
<input type="checkbox"/>	SAVRST	Set	DD196A2A5466037C4FE67EC17CA38D152646EEAE
<input type="checkbox"/>	ASP	Set	DD196A2A5466037C4FE67EC17CA38D152646EEAE

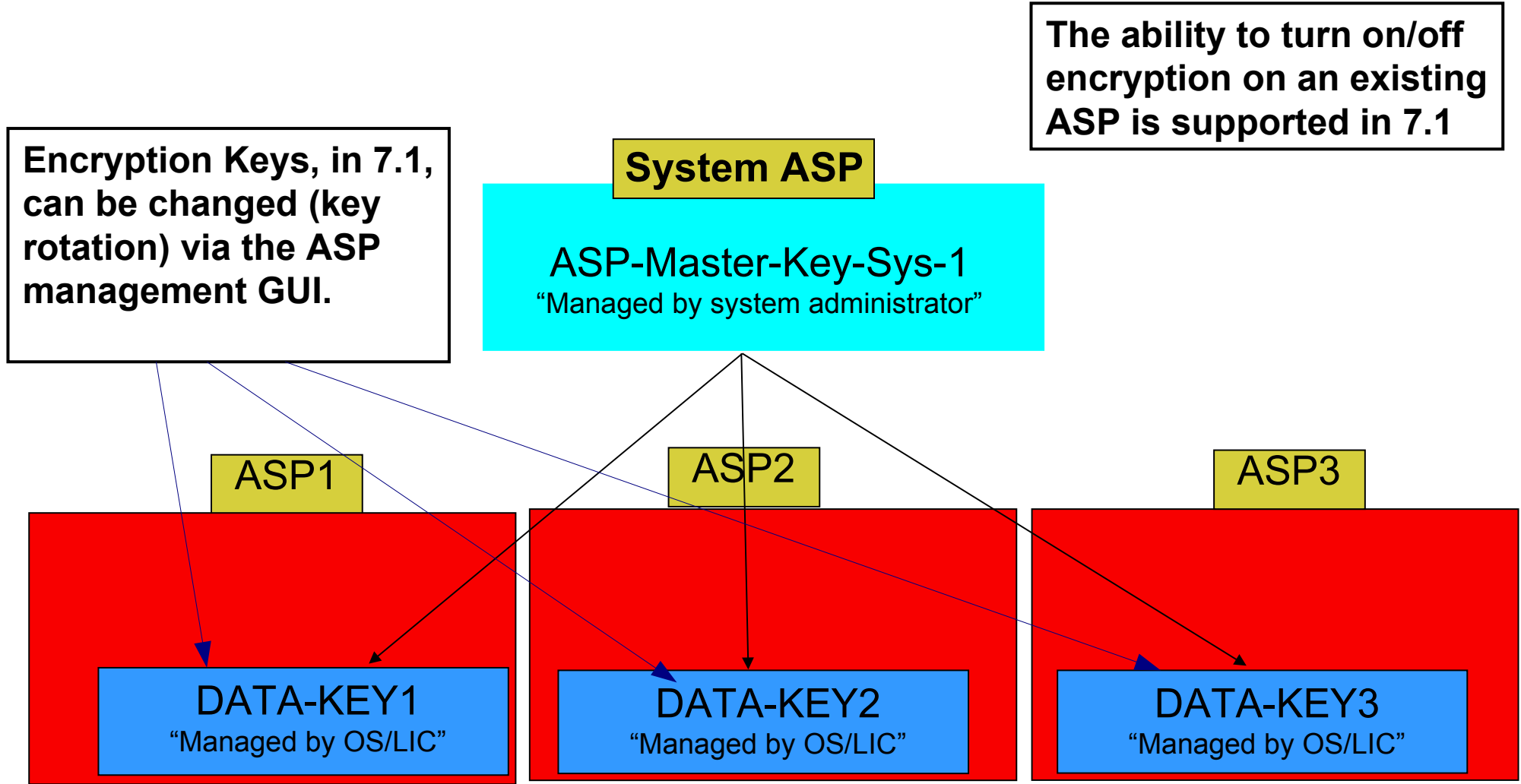
1 - 10 of 10 items 5 | 10 | 25 | 50 | **100** | All << < 1 > >>



SAVRST **Default** 16C1D3E3C073E77DB28F33E81EC165313318CE54

NOTE: The SAVRST Master Key is not yet set in the example above. A default key is in place to provide minimal protection until you set your key. This means that the master keys are not “in the clear” on your SAVSYS tape, but any IBM i system can decrypt them

ASP Key Management



The ability to turn on/off encryption on an existing ASP is supported in 7.1

Encryption Keys, in 7.1, can be changed (key rotation) via the ASP management GUI.

REQUIREMENT: ASP Master Key equal on all systems in cluster



Agenda

- Observations & studies
- Base IBM i security enhancements
- Database security enhancements
- Cryptographic enhancements
- **Network security enhancements**



Are you protected????

Don't worry ...

Simply plug in your IBM i
and it protects your data flawlessly
from any Network Access

As long as your 'network' only has these ...



For everyone else ...

Network Servers are likely to be your single biggest threat

Activities that come through the TCP servers are NOT audited – you cannot tell who is downloading (or uploading), running SQL statements, or even executing remote commands

Some servers allow command functions and IGNORE a profile's 5250 command line restriction





New CL Command to load and unload IP filter

- Load/Unload IP Filter (LODIPFTR)
- Prior to the new command, filter had to be loaded and unloaded via IBM i Navigator
- Requires PTF SI47941 in V7R1

```
Load/Unload IP Filter (LODIPFTR)
```

```
Type choices, press Enter.
```

```
Option . . . . . *LOAD, *UNLOAD  
Line description . . . . . Name, *ALL
```

Transport Layer Security (TLS) V1.1 and V1.2 support added

- Introduced with IBM i 7.1 TR6
- System-wide configuration via system value QSSLPCL

```
Change System Value

System value . . . . . : QSSLPCL
Description . . . . . : Secure sockets layer protocols

Type choices, press Enter.

Protocols
*SSLV3
*TLSV1
*TLSV1.1
*TLSV1.2
```

New values not listed in help text

TLS V1.1 & V1.2 defined per SSL-enabled application in DCM

- Application settings

Digital Certificate Manager

Work with Server Applications

Application Information

Application type: Server
Application ID: QIBM_QTV_TELNET_SERVER
Application description: IBM i TCP/IP Telnet Server

[View Application Definition](#) [Remove Application](#) [Validate](#)

SSL protocols	
<input checked="" type="radio"/>	*PGM
<input type="radio"/>	Define protocols supported:
<input type="checkbox"/>	TLS 1.2
<input type="checkbox"/>	TLS 1.1
<input type="checkbox"/>	TLS 1.0
<input type="checkbox"/>	SSL 3.0
<input type="checkbox"/>	SSL 2.0

7.1 Networking Enhancements



With TR6 cipher suites for SSL-enabled applications can also be defined in DCM

- Application settings

SSL cipher specification options		
<input checked="" type="radio"/>	*PGM	
<input type="radio"/>	Define cipher specification list:	Order
	RSA_AES_128_CBC_SHA256	1 ▼
	RSA_AES_128_CBC_SHA	2 ▼
	RSA_AES_256_CBC_SHA256	3 ▼
	RSA_AES_256_CBC_SHA	4 ▼
	RSA_3DES_EDE_CBC_SHA	5 ▼
	RSA_RC4_128_SHA	6 ▼
	RSA_RC4_128_MD5	Disable ▼
	RSA_DES_CBC_SHA	Disable ▼
	RSA_EXPORT_RC2_CBC_40_MD5	Disable ▼
	RSA_EXPORT_RC4_40_MD5	Disable ▼
	RSA_NULL_SHA256	Disable ▼
	RSA_NULL_SHA	Disable ▼
	RSA_NULL_MD5	Disable ▼
	RSA_RC2_CBC_128_MD5	Disable ▼
	RSA_3DES_EDE_CBC_MD5	Disable ▼
	RSA_DES_CBC_MD5	Disable ▼

7.1 Networking Enhancements



SSL enabled TELNET Client

- 7.1 release plus PTFs back to 5.4
- Enables secure TELNET connections

```
Start TCP/IP TELNET (TELNET)

Type choices, press Enter.

Remote system . . . . .

Internet address . . . . .

Port . . . . . *DFT 1-65534, *DFT
Secure connection . . . . . *ENVVAR *ENVVAR, *YES, *NO
```

Environment variable: QIBM_TELNET_CLIENT_SSL 'Y'



Transport Security Extensions

- Socket APIs - exit support
- Exit support on the accept, connect and listen APIs to enable additional network security capabilities

Work with Registration Information

Type options, press Enter.

5=Display exit point 8=Work with exit programs

Opt	Exit Point	Exit Point Format	Registered	Text
	QIBM_QSO_ACCEPT	ACPT0100	*YES	Exit point for APIs that accept
	QIBM_QSO_CONNECT	CONN0100	*YES	Exit point for sockets connect
	QIBM_QSO_LISTEN	LSTN0100	*YES	Exit point for sockets listen

Kerberos support for single sign-on

- Additional encryption algorithms supported
- RC4-HMAC, AES 128-bit, and AES 256-bit
 - Available via PTFs for V5R4, V6R1, and V7R1
- Steps to utilize new algorithms in an existing environment
 - Remove key table entries from IBM i key table and re-add them
 - Uncheck „DES Only“ option in Active Directory and change service account password
- IBM i Telnet client and FTP server/client have been enabled for SSO → V7R2



New Product - PRPQ (5799-SD1)

- Initialize DASD – Department of Defense standard algorithm
- Removes data from DASD
- Requirement – Drive must be in working order



This document was developed for IBM offerings in the United States as of the date of publication. IBM may not make these offerings available in other countries, and the information is subject to change without notice. Consult your local IBM business contact for information on the IBM offerings available in your area.

Information in this document concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this document has not been submitted to any formal IBM test and is provided "AS IS" with no warranties or guarantees either expressed or implied.

All examples cited or described in this document are presented as illustrations of the manner in which some IBM products can be used and the results that may be achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

IBM Global Financing offerings are provided through IBM Credit Corporation in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government clients. Rates are based on a client's credit rating, financing terms, offering type, equipment type and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.

IBM is not responsible for printing errors in this document that result in pricing or information inaccuracies.

All prices shown are IBM's United States suggested list prices and are subject to change without notice; reseller prices may vary.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this document may have been estimated through extrapolation. Users of this document should verify the applicable data for their specific environment.

Revised September 26, 2006

Special notices (cont.)



IBM, the IBM logo, ibm.com AIX, AIX (logo), AIX 5L, AIX 6 (logo), AS/400, BladeCenter, Blue Gene, ClusterProven, DB2, ESCON, i5/OS, i5/OS (logo), IBM Business Partner (logo), IntelliStation, LoadLeveler, Lotus, Lotus Notes, Notes, Operating System/400, OS/400, PartnerLink, PartnerWorld, PowerPC, pSeries, Rational, RISC System/6000, RS/6000, THINK, Tivoli, Tivoli (logo), Tivoli Management Environment, WebSphere, xSeries, z/OS, zSeries, Active Memory, Balanced Warehouse, CacheFlow, Cool Blue, IBM Watson, IBM Systems Director VMControl, pureScale, TurboCore, Chiphopper, Cloudscape, DB2 Universal Database, DS4000, DS6000, DS8000, EnergyScale, Enterprise Workload Manager, General Parallel File System, , GPFS, HACMP, HACMP/6000, HASM, IBM Systems Director Active Energy Manager, iSeries, Micro-Partitioning, POWER, PowerLinux, PowerExecutive, PowerVM, PowerVM (logo), PowerHA, Power Architecture, Power Everywhere, Power Family, POWER Hypervisor, Power Systems, Power Systems (logo), Power Systems Software, Power Systems Software (logo), POWER2, POWER3, POWER4, POWER4+, POWER5, POWER5+, POWER6, POWER6+, POWER7, POWER7+, Systems, System i, System p, System p5, System Storage, System z, TME 10, Workload Partitions Manager and X-Architecture are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries.

A full list of U.S. trademarks owned by IBM may be found at: <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

AltiVec is a trademark of Freescale Semiconductor, Inc.

AMD Opteron is a trademark of Advanced Micro Devices, Inc.

InfiniBand, InfiniBand Trade Association and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries or both.

PowerLinux™ uses the registered trademark Linux® pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the Linux® mark on a world-wide basis.

Microsoft, Windows and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries or both.

NetBench is a registered trademark of Ziff Davis Media in the United States, other countries or both.

SPECint, SPECfp, SPECjbb, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECapc, SPECchpc, SPECjvm, SPECmail, SPECimap and SPECsfs are trademarks of the Standard Performance Evaluation Corp (SPEC).

The Power Architecture and Power.org wordmarks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

TPC-C and TPC-H are trademarks of the Transaction Performance Processing Council (TPPC).

UNIX is a registered trademark of The Open Group in the United States, other countries or both.

Revised November 28, 2012

Other company, product and service names may be trademarks or service marks of others.

THANK YOU



IBM Systems Lab Services and Training

Our Mission and Profile

- Support the IBM Systems Agenda and accelerate the adoption of new products and solutions
- Maximize performance of our clients' existing IBM systems
- Deliver technical training, conferences, and other services tailored to meet client needs
- Team with IBM Service Providers to optimize the deployment of IBM solutions (GTS, GBS, SWG Lab Services and our IBM Business Partners)

Our Competitive Advantage

- Leverage relationships with the IBM development labs to build deep technical skills and exploit the expertise of our developers
- Combined expertise of Lab Services and the Training for Systems team
- Skills can be deployed worldwide to assure all client needs can be met

Europe Contacts

Virginie Cohen

VirginieCohen@fr.ibm.com

+33-4 -9211 41 33

Pierre Danze

pierre_danze@be.ibm.com

+32-2-339-5241