Automatic Encryption With V7R1

Townsend Security
THE ENCRYPTION COMPANY

Experience

25 years experience
data communication
and data security

Recognized industry
leaders in encryption

Trusted

Over 2000 customers
worldwide

Trusted by Fortune
500 Customers

Certified

NIST Certified Encryption

FIPS 140-2 Certified
Key Management

PCI-DSS Participating
Organization

Webinar Problems? Email webinar@townsendsecurity.com

www.townsendsecurity.com
Partners

- IBM
- Microsoft
- Symantec
- Quantum
- TriGeo Network Security
- help/systems
- SOLUTIONARY
- PGP
- BalaBit IT Security
- LogRhythm
- SDS
- ITChannel
Presenter: John Earl

- President & CEO of Townsend Security
- Leading IBM i (iSeries, AS/400) security expert
- Security Subject Matter Expert for COMMON
- Former Co-Founder & CTO of The PowerTech Group
- 30 years experience in IBM Midrange Security
• Data Gets Out.

• Loose data can easily fall into the wrong hands.

• Encryption and Key Management protect Loose Data by protecting the data – not the access.

• Townsend Security’s data privacy solutions protect data 24x7 – even when Data Gets Out.
What is Encryption?

- Encryption is a mathematical formula for protecting data
- Encryption is based on proven, well known algorithms
- Encryption is a system that uses “keys” to hide data

The best encryption algorithms are open, vetted, reviewed, and tested mercilessly by cryptographers.
What are the Major Types of Encryption?

Data in Motion

- SSL/TLS - Web browser sessions, host data connections, etc
- Virtual Privacy Networks
- Bulk file transfer - FTP, PGP
- XML/EDI - Record level data interchange

Every transfer of data from one system to another should consider the protection of that data.
What are the Major Types of Encryption?

Data at Rest

- Whole Disk Encryption - Including offline storage devices
- Flat File Encryption - PGP is a popular method
- Tape Encryption - Changes the way you do backups
- Data Base Encryption - The “Holy Grail” of encryption
  - Made even better in IBM i V7R1
What Encryption Should Be Used?

- AES encryption (FIPS-197)
- Recommend NIST certification
- NIST approved modes of encryption
- Watch out for non-standard AES
  - Incorrect data block sizes
  - Unrecognized encryption modes such as “CUSP” or “FFX”
- Know how your encryption performs. There are vast performance differences in encryption implementations.

Standards-based encryption is required by regulations such as PCI, HIPAA/HITECH, and State Privacy laws.
NIST Certification

- Regulators are increasingly calling for NIST certified encryption solutions.
- The 2009 HITECH Act makes specific reference to the NIST standards for Encryption – and Key Management.
- Most encryption vendors bypass NIST certification because it is easier and cheaper.
- Un-certified encryption solutions leaves data exposed to attacks, loss, and evolving regulations.

AES-256: Are you Secure?

NIST certified? No worries. NIST certified AES-256 requires 14-rounds and remains secure.
What are the Database Encryption Modes?

**Counter Mode (CTR)** - best mode for database encryption on IBM I

**Electronic Code Book Mode (ECB)** - The most basic mode - currently out of fashion

**Cypher Block Chaining Mode (CBC)** - Identical plain text gives you different cypher text

**Output Feed Back Mode (OFB)** - Similar to CBC

**Cypher Feed Back Mode (CFB)** - Can encrypt a single bit. Comes in 1,8, and 128 bit.

Avoid non-certified modes. Modes such as CUSP and the various FPE (Format Preserving Encryption) are less transportable or have known problems.
Which Encryption Modes Should Be Used?

- Block Ciphers (AES as FIPS-197)
- There are 9 NIST-recommended modes of encryption
- NIST Approved Database Modes: CTR, CBC, CFB, ECB, OFB, etc.

Modes are the engine

AES is the Vehicle

Webinar Problems? Email webinar@townsendsecurity.com
Key Management Is Crucial (continued)

- Key Management SP800-57
- Cryptographic Module Validation Program (CMVP)
- National Voluntary Laboratory Accreditation Program (NVLAP)
- FIPS-140

- AES is not a “secret”
- The key is the real “secret”

Data → AES encryption → Protected Data → Key

Webinar Problems? Email webinar@townsendsecurity.com
Encryption Key Types

Symmetric Keys

- A “secret” Encryption Key that can encrypt or decrypt the data
- Must be securely transmitted to the decryptor
- Should not be used for multiple purposes
- Most common Encryption Key for data at rest
Encryption Key Types

Asymmetric Keys

- You have a Public Key and a Private Key
- Everyone on the planet can know your Public Key
- Only you know your Private Key
- Data encrypted with your Public Key can only be decrypted with your Private Key
- Asymmetric Keys are best key data in motion.
How Do You Encrypt Data for a File Transfer?

It’s Easy!

1. Choose an approved encryption method (We like PGP encryption)
2. Acquire the Public Key of your intended recipient
3. Call your file encryption software and pass it to your file name and your intended recipient’s Public Key
4. Encrypt the entire file
5. Send the file to your recipient.
   • Or just post it in a public place for your recipient to retrieve!
How Do You Decrypt Data from a Bulk File Transfer?

It’s Still Easy!

1. Download the file to the intended computer
2. Call your file decryption software and pass it to your file name and your PRIVATE KEY
3. The file is decrypted
4. Move the data into the production application it was intended for
How Do You Do Database Encryption (At V6R1 or below)?

It’s Easy! (But it does take a little longer)

1. Choose an approved encryption method (AES256 is our choice)
2. Create a secret (symmetric) key to encrypt your data
3. Scan your source code for everywhere you do a record “Write” or an “Update” operation to the file in question
4. Add a call to your encryption API to encrypt the data fields before each “Write” or “Update” operation
5. Viola! The database fields you want are encrypted with AES256
How Do You Do Database Decryption (At V6R1 or below)?

A Little Tougher

1. Create business rules that define who can decrypt the data, and when.
2. Scan your source for every program that does a “Read” to the file that will be encrypted.
3. Add a call to your own unique program after every read operation.

Your program should:

1) Log the attempt to decrypt data
2) Decide if this person is allowed to decrypt the data
3) If yes, retrieve the secret key from the Key Store
4) Decrypt the data
What About Key Management?

Key Management is Critically Important to Encryption

- The keys are the secret - they must be protected and managed
- A good key management system will:
  1) Control access to keys
  2) Check keys in and out
  3) Log access to keys
  4) Back up keys
  5) Roll keys
  6) Expire keys,
  7) Etc.
Finally, Logging

Logging is an Important Part of Any Encryption Process

Things to log include:

1) Encryption actions
2) Key requests - Any action with keys should be logged
3) Decryption requests
4) Unauthorized decryption attempts
5) Program anomalies
Encryption at V7R1

It’s just a database change

➢ Identify all of the fields you want to encrypt
➢ Use the ALTER TABLE SQL command to add an encryption exit program to those fields
➢ Enter records in a control table that decides which users/programs can decrypt data
Your Encryption Project Just Got a Whole Lot Easier!

- No database changes required
  - No field size changes
  - Database conversion covered by the Encryption application

- Few (if any!) application changes required
  - Most applications can will run right out of the box
  - There are a few caveats that may require application modifications
Automatic Encryption: What Problem Does It Solve

- It is called FIELDPROC because it is a “Field Exit Procedure”
- FIELDPROC is not new - It has been around on the IBM System z Mainframe for a number of years
- It is slightly different on the IBM i platform due to differences in IBM architecture and DB2
- Attempts to use SQL Views and Triggers were disappointing due to the inability to update the view data on SELECT (read) operations
- The new transparent encryption API solves this problem by providing a way for a user application to modify data on read and write operations
Automatic Encryption: What Problem Does It Solve (continued)

OLD:

- DB2
- SQL View + Instead-of Trigger + UDF
- UDF

New:

- DB2
- Insert / Update
- Read
- FIELDPROC PGM

Webinar Problems? Email webinar@townsendsecurity.com
How Does It Work?

Like most exit points you must register your exit point program with the IBM i OS

A SQL statement used to do this:

```
ALTER TABLE ordmaster
ALTER COLUMN cardno
SET FIELDPROC prodlib/exit pgm
CONSTANT 'Unique-Value'
```

Now the DB will call your API program on every I/O operation
FIELDPROC Programs

What Can V7R1 Do?

Developers have freedom to implement virtually any column encoding & decoding scheme

- Encryption and/or Tokenization (from 3rd party provider)
- Change control / Audit logging
- Data Compression
- Text Normalization

FIELDPROC Program Requirements

- FIELDPROC program must be an ILE program object & contain no SQL
- Handle 3 different events:
  - FIELDPROC registration to define encoded attributes
  - Write operations encode data
  - Read operations decode data
FIELDPROC Programs

When Are They Used?

**FIELDPROC Write/Encode Events**
- SQL Insert, Update, & Merge statements
- Native record-level writes
- “Writing” CL Commands: CPYF, RGZPFM, STRDFU, ...
- Trigger Processing
  - FIELDPROC processing occurs after **BEFORE** triggers
  - FIELDPROC processing occurs **before** **AFTER** triggers

**FieldProc Read/Decode Events**
- SQL Select & Fetch
- Native record-level reads
- “Reading” CL commands: CPYF, RGZPFM, DSPPFM, DBU, FTP ...
- Trigger processing
FIELDPROC Programs

How Do They Get Called?

FIELDPROC Registration Interface - SQL !

CREATE TABLE ccstore (
    custid CHAR (5),
    cardnum CHAR(16) FIELDPROC mylib/ccpgm, cardexp DATE )

ALTER TABLE orders ALTER COLUMN cardnum
    SET FIELDPROC mylib/ccpgm

FIELDPROC Removal

ALTER TABLE orders ALTER COLUMN cardnum
    DROP FIELDPROC
Automatic Encryption: What It Is and Isn’t

What it does:
➤ Provides a column level exit for insert/read/update operations on a database

What it does not do:
➤ Does not provide encryption, tokenization, or key management
➤ You have to provide software for the Exit (an executable program) to handle encrypt/decrypt
➤ FIELDPROC does not provide security controls – that’s up to you!
➤ Doesn’t log actions – a compliance mandate!
New Security Concerns

The new FIELDPROC Exits expose new vulnerabilities! Once an exit point program is installed, it will be called regardless of the user application. Common utilities such as DFU, DBU, Display Physical File Member, and FTP can trigger automatic decryption of data.

Your APIs should implement:

- User access controls
- Application program controls
- Encryption key access controls
- Provide QAUDJRN logging of access
- Automatic masking of data by policy
Any Questions About Encryption, Compliance, etc?

Data Gets Out. Encrypt It.

AES & PGP Encryption, Key Management, Security Logging

Contact Townsend Security:
john.earl@townsendsecurity.com
www.townsendsecurity.com
800.357.1019
+1 360.359.4400