Encryption on IBM i

Mark Flora – Ciber

MRMUG – 2/2014

ciber®

Encryption on IBM i

- Threats
  - Credit card information
    - Inside and outside your organization
  - Personnel data like SSN or phone number
    - Inside and outside your organization
  - Key business information
    - Competitors
    - Disgruntled employees
    - News organizations
  - General privacy principles
    - Government and hacker snooping

ciber®

Encryption on IBM i

- Considerations
  - Performance
    - Encryption/decryption takes horsepower
      - External storage systems
      - Dedicated Cryptographic processor available
    - Encryption/decryption takes time
      - Response time issues
      - Batch job execution windows
  - Management
    - Keys
      - Cost of certificates
      - Key vault software on DR systems
      - Keys available as part of DR process

ciber®

Encryption on IBM i

- Exposures
  - Data in flight
    - Data outside your organization
  - Data at rest
    - Data inside your organization

ciber®

Encryption on IBM i

- Data in flight
  - Threat: Intercepting passwords or data from HTTP users to IBM i acting as web server
  - Protection: Use Secure HTTP (https://)
  - Consideration: Requires certificate but generally no programming changes

ciber®

Encryption on IBM i

- Data in flight
  - Threat: Intercepting passwords or data from TN5250 users to IBM i
  - Protection: Use Secure Sockets Layer (SSL)
    - Properly called Transport Layer Security (TLS)
  - Consideration:
    - Requires certificate but generally no programming changes
    - Requires SSL client setup

ciber®

Encryption on IBM i

- Data in flight
  - Threat: Intercepting passwords or data from IBM i Access 5250 or file transfer users to IBM i
  - Protection: Use Secure Sockets Layer (SSL)
  - Consideration:
    - Requires certificate but generally no programming changes
    - Requires SSL client setup; standard IBM i Access support
  - Protection: Virtual Private Network
  - Consideration:
    - Often need client code installed
    - Use firewall VPN or IBM i VPN

ciber®

Encryption on IBM i

- Data in flight
  - Threat: Intercepting passwords or data FTP users to IBM i
  - Protection: Use Secure Sockets Layer (SSL) or Secure FTP
    - SFTP usually means Simple FTP
  - Consideration:
    - Requires certificate but generally no programming changes
    - Requires SSL client setup; special Windows FTP client
  - Protection: Virtual Private Network
  - Consideration:
    - Often need client code installed
    - Use firewall VPN or IBM i VPN

ciber®

Encryption on IBM i

- Data in flight
  - Threat: Intercepting data during replication to Disaster Recovery site
    - Tough to gather usable data from remote journal data stream
  - Protection: External VPN
  - Protection: SSL protection of TCP links

Encryption on IBM i

- Data in flight
  - Threat: Theft of backup tapes
  - Protection: Tape encryption
  - Consideration:
    - Most modern IBM tape drives offer hardware-based encryption
    - Encryption key will be required to restore to DR system
    - BRMS offers software-based encryption
    - Encrypted data doesn't compress well
  - BRMS is recommended to keep encrypted / non-encrypted tapes separate

ciber®

Encryption on IBM i

- Data at rest
  - Threat: Disk or entire SAN removed and examined
  - Protection: Encrypt entire User ASP via IBM i OS
    - Considerations:
      - Both original and independent ASPs
      - May meet your regulatory requirements
      - Protects data in flight to SAN
  - Protection: Encrypt just sensitive columns
  - Protection: SAN hardware encryption
    - Considerations:
      - Data in flight to SAN unprotected
  - Protection: DASD Scrub 5799-SD1

ciber®

Encryption on IBM i

- Data at rest
  - Threat: Someone has access to OS and/or Utilities
  - Protection: Encrypt at SQL level
  - Considerations:
    - Applications may need to use SQL DB access
    - Application SQL statements need to be modified
      - Individual columns secured
    - Applications need access to the key

ciber®

Encryption on IBM i

- Data at rest
  - Threat: Someone has access to SQL
  - Protection: Encrypt at SQL level
  - Considerations:
    - Applications may need to use SQL DB access
    - Application SQL statements may need to be modified
      - Individual columns secured
    - Applications need access to the key

ciber®

Encryption on IBM i

- Data at rest
  - Threat: Someone has access to the application
  - Protection: Encryption doesn’t help here

ciber®

Encryption on IBM i

- SQL encryption

```
CREATE TABLE empTDES (
        employeeId CHAR(7),
        ssn CHAR(64) FOR BIT DATA
        name VARCHAR(40),
        salary CHAR(64) FOR BIT DATA

SET ENCRYPTION PASSWORD='enig1942ma'
INSERT INTO empTDES VALUES(
        '1000001',
        ENCRYPT_TDES('111223333'),
        'ROBERT',
        ENCRYPT_TDES(4000000))
```

ciber®

Encryption on IBM i

- SQL decryption

```
SET ENCRYPTION PASSWORD=:passwordvar
SELECT
        employeeId,
        char(DECRYPT_CHAR(ssn), 9 ),
        name,
        char(DECRYPT_CHAR(salary), 13)
    FROM empTDES
```

ciber®

Encryption on IBM i

- SQL decryption with a view

```
SET ENCRYPTION PASSWORD=:passwordvar
CREATE VIEW empview(employeeId, ssn, name, salary) AS
   SELECT
         employeeId,
         char(DECRYPT_CHAR(ssn), 9 ),
         name,
         char(DECRYPT_CHAR(salary), 13)
      FROM empTDES
```

ciber®

Encryption on IBM i

- SQL encryption with a trigger

```
CREATE TRIGGER insert_empTDES
        BEFORE INSERT ON empTDES
REFERENCING NEW ROW AS n
FOR EACH ROW
        BEGIN
        DECLARE encrypt_passwd VARCHAR(127);
        SET encrypt_passwd = GET_PASSWD(:hintvar);
        SET n.ssn = ENCRYPT_TDES(n.ssn, encrypt_passwd);
        SET n.salary = ENCRYPT_TDES(n.salary, encrypt_passwd);
        END
```

Encryption on IBM i

- SQL decryption with a trigger
  - Every application & utility automatically decrypts
    - Regardless of SQL or native access
    - So, why have encryption?
    - If this meets your requirements, it might be a low-impact change

Encryption on IBM i

- Version 7.1 field trigger
  - Similar to regular trigger but at the column level
  - Only active when the column is accessed
  - Easier field length handling

ciber®

Encryption on IBM i

- Resources
  - Security Guide for IBM i V6.1 - SG24-7680
  - IBM System i Security: Protecting i5/OS Data with Encryption - SG24-7399
  - IBM i Virtual Users Group http://ibm.biz/IBMiVUG
    - **What's New in 6.1 & 7.1 Security**

ciber®

Encryption on IBM i

Thank you!