For Your Eyes Only!
MQ Advanced Message Security

Jon Rumsey
IBM

Wednesday 10th August
Session # 9417
Agenda

• Message Level Security
• Digital Cryptography 101 (Alice & Bob)
• WebSphere MQ Advanced Message Security
• Architecture
• Administration
• Availability
Why Message Level Security?

- Messaging that does not involve humans
  - Command & control scenarios
  - Application to Application, no “human” checking

- Large MQ networks: difficult to prove security of messages
  - Against message injection / message modification / message viewing

- Data subject to standards compliance (PCI, HIPAA, etc)
  - Credit card data protected by PCI
  - Confidential government data
  - Personal information e.g. healthcare
  - Data at rest, administrative privileges, etc
Message Level Protection

• Assurance that messages have not been altered in transit
  • When issuing payment information messages, ensure the payment amount does not change before reaching the receiver

• Assurance that messages originated from the expected source
  • When processing control messages, validate the sender

• Assurance that messages can only be viewed by intended recipient(s)
  • When sending confidential information
Cryptography

- **Symmetric Keys**
  - Relatively fast
  - Poses key distribution challenges when faced with large numbers of senders/receivers
  - The key has to be known by the sender and receiver

- **Asymmetric Keys**
  - Message encrypted with one key can only be decrypted by the other one
  - Slower than symmetric key cryptography
  - Asymmetric Keys can be used to solve the key distribution challenges associated with symmetric keys
Symmetric Key Cryptography

Encryption

Decryption

plaintext → ciphertext → plaintext
Asymmetric Key Cryptography

- **Encryption**
  - Bob's Public Key
  - plaintext → ciphertext

- **Decryption**
  - Bob's Private Key
  - ciphertext → plaintext

**Bob's Public Key**

**Bob's Private Key**

plaintext → ciphertext → plaintext
Hash Functions

• Hash Function
  • Computes the message MAC (Message Authentication Code)
  • Easy to compute
  • Very difficult to reverse
  • Computationally infeasible to find two messages that hash to the same value
**Digital Signatures**

Alice hashes the plaintext to derive the hash \( h \).

Alice "signs" the hash (encrypts the hash with her private key).

Bob hashes the plaintext to derive the hash \( h \).

Bob decrypts the signed hash with Alice's public key.

**If hashes match:**
- Only Alice could have signed.
- Plaintext didn't change in transit.
WebSphere MQ Advanced Message Security

Sending App

MQ Msg

发送

接收

接收

MQ Msg

WebSphere MQ Advanced Message Security

SHARE: Technology - Connections - Results

SHARE in Orlando 2011
WebSphere MQ Advanced Message Security

• Provides additional security services over and above base MQ
• Application to Application protection for messages
  • Well suited to point to point, publish/subscribe limited
  • Have to know your authorized parties ahead of operation
• Asymmetric cryptography used to protect each message
• Non-invasive
  • No changes required to applications
• Administrative interfaces for policy management
  • Command line
  • MQ Explorer Plug-In (GUI)
WMQ vs WMQ AMS Security

- AMS is a complimentary offering, not a replacement to WMQ security

- WebSphere MQ
  - Authentication (Local OS user id, SSL peer for clients)
  - Authorization (OAM on distributed, RACF on z/OS)
  - Integrity (SSL for channels)
  - Privacy (SSL for channels)

- WebSphere MQ Advanced Message Security
  - Integrity (Digital signing of messages)
  - Privacy (Message content encryption)
Certificates, Interceptors and Policies

• AMS uses X.509 digital certificates for digital signing and encryption

• Interceptors installed in the application process to sign, encrypt and decrypt message data
  • No code changes to the application

• Policies are defined to control the interceptors
  • Matched against queue names
  • What level of protection, none, integrity or privacy
  • Which certificates are involved (DN)
    • Authorised signer(s)
    • Authorised recipient(s)
WMQ + AMS v7.0.1 Architecture
AMS Interceptors

**Server**
- API Exit

- MQ API (mqm lib)
- API Exit

- Application

**Client**
- Library Replacement

- Replacement mqic lib
- Renamed MQIC

- Application

- Channel Agent

- QMGR

**JMS**
- JMQI Intercept

- JMS Application

- JMS

- JMQI Intercept

- JMQI

- Channel Agent

- QMGR
AMS Policies

- Stored on SYSTEM.PROTECTION.POLICY.QUEUE

- Signature Algorithm
  - MD5 or SHA1

- Encryption Algorithm
  - RC2, DES, 3DES, AES128 or AES256

- Acceptable Signer(s)
  - Applicable when signing messages

- Message Recipient(s)
  - Applicable when signing and encrypting messages
Policy Administration

- Command line tools
  - `setmqsp1` : Set message protection policy
    - `-m QMGR`
    - `-p Policy_Name`
    - `-s Signing_Algorithm`
    - `-a Authorised_Signers`
    - `-e Encryption_Algorithm`
    - `-r Message_Recipients`
  - `dspmqsp1` : Display message protection policies
    - `-m QMGR`
    - `[-export]`
    - `[-p Policy_Name]`
Policy Administration
Securing an MQ Application

Alice
Sending App

AMS_QM
ALICE.Q

Bob
Receiving App
Securing an MQ Application

1. Install AMS Interceptor
Securing an MQ Application

1. Install AMS Interceptor
2. Create public / private key pairs
Securing an MQ Application

1. Install AMS Interceptor
2. Create public / private key pairs
3. Copy recipient's public key
Securing an MQ Application

1. Install AMS Interceptor
2. Create public/private key pairs
3. Copy recipient's public key
4. Define protection policy for the queue
WebSphere MQ AMS: Integrity Message Format

Original MQ Message

- Message Properties
- Message Data

AMS Signed Message

- Message Properties
- PDMQ Header
- PKCS #7 Envelope
  - Message Data
  - Signature
WebSphere MQ AMS: Privacy Message Format

Original MQ Message

<table>
<thead>
<tr>
<th>Message Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Data</td>
</tr>
</tbody>
</table>

AMS Encrypted Message

<table>
<thead>
<tr>
<th>Message Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDMQ Header</td>
</tr>
</tbody>
</table>

PKCS #7 Envelope

| Key encrypted with certificate |
| Data encrypted with key |

| Message Data |
| Signature    |
Availability

• MQ AMS dates :
  • Released : 8\textsuperscript{th} Oct 2010
  • 7.0.1.1 Released : 14\textsuperscript{th} April 2011
    • Added support for crypto hardware to store keys
  • 90 day Trial version available to download

• Platform support
  • Same as MQ 7.0.1 (except IBM i)
  • Works with MQ 6 & MQ 7 queue managers (JMS interceptor requires v7 jars)
Summary

- AMS provides message level security
  - Complements base MQ security, not a replacement
  - Can be applied selectively at a queue level
  - Each message protected with asymmetric key cryptography

- Application to application, end to end security
  - No code changes required
  - Well suited to point to point applications
# The rest of the week ……

<table>
<thead>
<tr>
<th>Time</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00</td>
<td>More than a buzzword: Extending the reach of your MQ messaging with Web 2.0</td>
<td>WebSphere MQ 101: Introduction to the world's leading messaging provider</td>
<td>Batch, local, remote, and traditional MVS - file processing in Message Broker</td>
<td>Lyn's Story Time - Avoiding the MQ Problems Others have Hit</td>
<td></td>
</tr>
<tr>
<td>09:30</td>
<td>WebSphere MQ 101: Introduction to the world's leading messaging provider</td>
<td>The Do's and Don'ts of Queue Manager Performance</td>
<td>So, what else can I do? - MQ API beyond the basics</td>
<td>MQ Project Planning Session</td>
<td></td>
</tr>
<tr>
<td>11:00</td>
<td>MQ Publish/Subscribe</td>
<td>The Do's and Don'ts of Message Broker Performance</td>
<td>Diagnosing problems for Message Broker</td>
<td>What's new for the MQ Family and Message Broker</td>
<td></td>
</tr>
<tr>
<td>12:15</td>
<td>MQ Freebies! Top 5 SupportPacs</td>
<td>The doctor is in. Hands-on lab and lots of help with the MQ family</td>
<td>Using the WMQ V7 Verbs in CICS Programs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>01:30</td>
<td>Diagnosing problems for MQ</td>
<td>WebSphere Message Broker 101: The Swiss army knife for application integration</td>
<td>The Dark Side of Monitoring MQ - SMF 115 and 116 record reading and interpretation</td>
<td>Getting your MQ JMS applications running, with or without WAS</td>
<td></td>
</tr>
<tr>
<td>03:00</td>
<td>Keeping your eye on it all - Queue Manager Monitoring &amp; Auditing</td>
<td>The MQ API for dummies - the basics</td>
<td>Under the hood of Message Broker on z/OS - WLM, SMF and more</td>
<td>Message Broker Patterns - Generate applications in an instant</td>
<td></td>
</tr>
<tr>
<td>04:30</td>
<td>Message Broker administration for dummies</td>
<td>All About WebSphere MQ File Transfer Edition</td>
<td>For your eyes only - WebSphere MQ Advanced Message Security</td>
<td>Keeping your MQ service up and running - Queue Manager clustering</td>
<td></td>
</tr>
<tr>
<td>06:00</td>
<td>Free MQ! - MQ Clients and what you can do with them</td>
<td>MQ Q-Box - Open Microphone to ask the experts questions</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Questions & Answers

Please fill out your evaluation forms
Session # 9417