A Business Case for MQ Security

Business Case Overview

Security is a business issue and it competes with other business issues for resources and budget money. But since most people do not see a return on investment (ROI) for security, they relegate it to the bottom of the list of items that need to be purchased or funded.

Background and Problem Statement

Did you know the default install and creation of a IBM MQ (aka WebSphere MQ & MQSeries) queue manager on Unix, IBM i (OS/400), Windows, Linux and even z/OS leaves the queue manager totally exposed to hackers or over zealous employees? Anyone with a simple program can view, insert, update or delete messages in a queue of a queue manager and not only would you not know they have done so but there would be no record of the event! This is a major security risk.

MQ client applications running on servers or PCs access remote queue managers via a 'SVRCONN' (Server Connection) channel. If the client application uses a blank UserID and the MCAUSER field of the SVRCONN is blank then the MQ Listener process uses its own UserID for the connecting application. Since the MQ Listener process is usually running under the UserID of 'mqm' for UNIX, 'MUSR_MQADMIN' for Windows, 'QMQM' for OS/400, etc., the connecting application will therefore, have full access to any message in any queue within the queue manager! This is a major security risk.

Most MQ Administrators use IBM and third party MQ software tools for the configuration and the administration of the queue managers queues, channels, processes, etc. These MQ Tools use a SVRCONN channel (generally 'SYSTEM.ADMIN.SVRCONN') to connect to the remote queue manager to do their work. Once this SVRCONN channel is defined (or any other SVRCONN channel), it can be used by any application that knows the name of the channel. This is a major security risk.

MQ Security Solution Options

There are three solutions to avoid this problem:

1. Disable all SVRCONN channels so that MQ client applications or MQ administration tools cannot connect to a remote queue manager. This is an effective solution but it is not practical.

2. Secure the SVRCONN channels with SSL. This is a viable solution. The server and client exchange SSL certificates for identification purposes. However it has the following drawbacks:
   - SSL Certificates must be purchased.
   - SSL Certificates expire, requiring regular repurchase and renewal.
   - There is no logging capability to see who accessed which Queue Manager.
   - This form of security is only as secure as the integrity of the client side certificates. Anyone that possesses a copy of the certificate has full access.
   - SSL is dangerous on a Windows PC because you can boot from floppy and copy the 'keystore' file to diskette. The malicious user can then copy the 'keystore' file to another PC and successfully connect to the queue manager from the other PC!

3. Secure the SVRCONN channels with Capitalware's ***MQ Standard Security Exit*** solution. This solution validates the incoming UserId and/or IP address of the connection against a predefined list of UserIds and/or IP addresses. The security solution is comprised of a server-side security exit.

The server-side security exit is available in 3 forms:

- Windows DLL
- Shared library for AIX, HP-UX, Linux, and Solaris
- IBM i exit module

Operating System	MQ v7.0, v7.1, v7.5, v8.0, v9.0, v9.1 & v9.2
AIX v6.1 or higher	64-bit
HP-UX IA64 v11.23 or higher	64-bit
IBM i (OS/400)	64-bit
Linux x86	32-bit
Linux x86_64	64-bit
Linux on POWER	64-bit
Linux on zSeries	64-bit
Raspberry Pi ARM	32-bit
Solaris SPARC v10 & v11	64-bit
Solaris x86_64 v10 & v11	64-bit
Windows 2008, 2012, 2016, 7, 8, 8.1 & 10	32-bit & 64-bit

The server-side security exit major features are:

- Allow or restrict the incoming UserID against a regular expression pattern
- Allows or restricts the incoming UserID against a Group
- Support for Proxy UserIDs
- Allow or restrict the incoming IP address against a regular expression pattern
- Allow or restrict the incoming hostname against a regular expression pattern
- Allow or restrict the incoming SSL DN against a regular expression pattern
- Limit the number of incoming channel connections on a SVRCONN channel.
- Allow or restrict the use of 'mqm' or 'MUSER_MQADMIN' UserIDs
- Provides monitoring tool tie-in by using custom MQ event messages
- Provides logging capability for all connecting client applications regardless if they were successful or not.

Recommendation

We recommended that your company pursue the third option. Capitalware Inc. has a commercially available product called ***MQ Standard Security Exit*** that was specifically created for the purpose of securing SVRCONN channels via allowing or restricting connections to the channel. This security solution will work with any MQ client application or MQ software tool for the configuration and the administration.

Benefits

- All connections from MQ client applications and MQ Administration tools remotely accessing MQ queue managers will be examined to see if they match the given criteria.
- All logon attempts, regardless if successful or not, will be logged.
- Future MQ client applications can be set up to create secure channel connections to the queue manager.

Solution Cost

The server-side security exits are provided in the format of a native DLL / shared library and are currently available for AIX, HP-UX, IBM i (OS/400), Linux, Solaris and Windows. The pricing of Capitalware's ***MQ Standard Security Exit*** solution is on a 'per queue manager' basis.

Retail Pricing is as follows:

Units from	Up to	Price per Queue Manager * (USD)
1	9	$249.00
10	49	$225.00
50	99	$199.00
100	249	$175.00
250	Unlimited	$149.00
Enterprise License **		$45,000.00

* Yearly maintenance is 15% of the purchase price.
** Unlimited number of queue managers in any company location worldwide.

Capitalware Inc.
Unit 11, 1673 Richmond Street, PMB524
London, Ontario N6G2N3
Canada
sales@capitalware.com
https://www.capitalware.com