MQ Jumping

. . . . Or, move to the front of the queue, pass go and collect £200

Martyn Ruks

DEFCON 15
2007-08-03

MWR InfoSecurity

One Year Ago

- Last year I talked about IBM Networking attacks and said I was going to continue with my research.
- But like any penetration tester I had other client work to do and that led to me looking at Websphere MQ.
- It was so interesting I decided to do some more research and hence the reason I'm here again.
- It wasn't a conscious decision to look at IBM technology, it should be seen as an indication of the level of adoption of IBM technology in the marketplace.

MWR INFOSECURITY

Introduction

MWR InfoSecurity

Who am I ?

- My name is Martyn Ruks and I am a Security Consultant with MWR InfoSecurity in the UK.
- I have approached this subject from the perspective of a penetration tester and then as a security researcher. I do not have a formal background in IBM computing.
- I chose the subject of the presentation based on a number of interesting client engagements.

MWR InfoSecurity

Intended Audience

This talk is aimed at the following people:

- Security Managers
- Penetration Testers
- Application Developers

There are no pre-requisites for the contents of this presentation.

MWR InfoSecurity

What will I talk about

- Websphere MQ is a Middleware application for Messaging
- MQ is a huge topic so I will focus on a number of specific areas today
- I will talk about a TCP/IP environment
- All the research has been conducted against Windows and UNIX platforms

MWR INFOSECURITY

Why study Websphere MQ?

- The systems that communicate using it are usually business critical.
- Tools for testing the software are not currently in the public domain.
- The lack of security testing knowledge means that users of the software are potentially exposed to risk.
- If you own the Middleware you usually own the business process.

MWR INFOSECURITY

Technical Background

MWR InfoSecurity

MQ Series – A brief history

- In 1993 IBM bought IP rights to ezBridge from SSI Systems
- IBM produced a Mainframe version and SSI for other platforms
- In 1994/5 IBM produced versions for AIX, OS/2 and AS/400
- MQSeries was renamed Websphere MQ at version 5.3
- The new and improved version 6.0 was revealed in April 2005

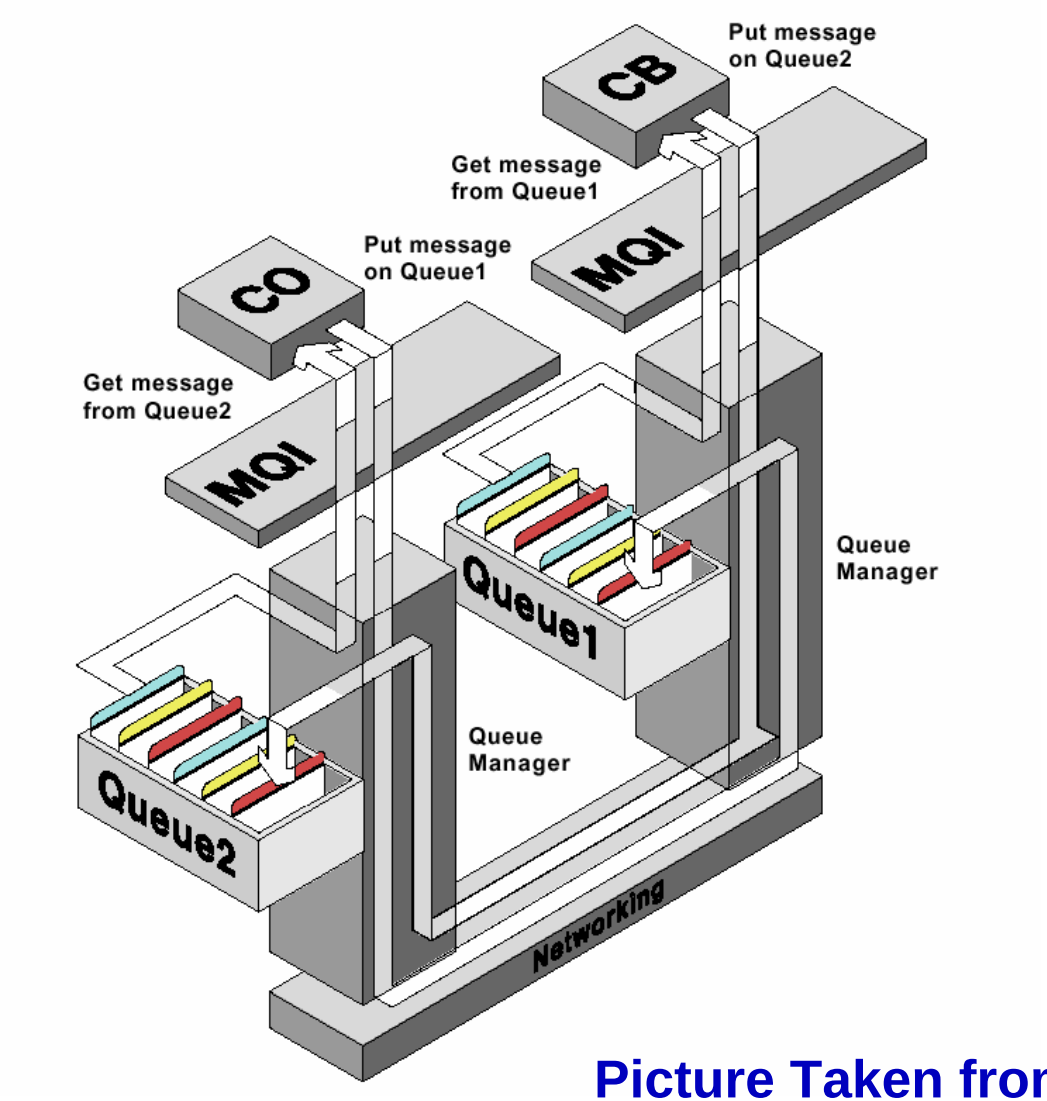
MWR INFOSECURITY

Why do Businesses use MQ ?

- A unified messaging solution is vital for a business that relies on reliable data communication.
- Websphere MQ is solid and stable Enterprise technology
- It runs on lots of platforms (Windows, Unix, Mainframes)
- It has lots of feature rich APIs (C, Java, PERL)
- It has accounting and lots of other Enterprise functionality

MWR InfoSecurity

A Typical Environment



Picture Taken from document by Joe Conron

MWR InfoSecurity

Terminology

A number of key terms are used within the MQ world

- Queue Managers
- Channels
- Queues
- Triggers and monitors

We will cover these in more detail as we go along

MWR InfoSecurity

What is a Queue Manager ?

- A Queue Manager is an application that is responsible for managing the message queues.
- One instance of a Queue Manager can exist on any one TCP port.
- Each Queue Manager is an independent entity but they can be linked.
- You often find multiple Queue Managers on a system (Production, Development etc).

MWR InfoSecurity

What is a Channel ?

- A channel is a logical connection between a client and a server or two servers.
- Essentially a channel is a conduit to get to the message queues
- There are several types of channel and each can be used in a different way.

MWR InfoSecurity

What is a Queue ?

- A queue is a storage container for messages (data)
- Everything in MQ is based on using Queues for moving data around
- They are usually a FIFO structure
  (except when using priorities)
- Queues can be opened and then GET or PUT operations used to move the data around

MWR InfoSecurity

The WebSphere MQ Protocol

- Information about the protocol is not public but is in Ethereal/Wireshark
- Each packet contains a series of discreet sections
- The layers in each packet depend on the type of operation it is performing
- All packets contain a Transmission Segment Header (TSH)

MWR INFOSECURITY

A Typical Packet

- WebSphere MQ (MQGET_REPLY)
  - Transmission Segment Header
  - API Header
  - Message Descriptor
  - Get Message Options
  - MQPUT/MQGET
- WebSphere MQ Programmable Command Formats (INQUIRE_Q_MGR)
  - MQ Command Format Header

```
0000  54 53 48 20 00 00 0b 44  01 95 30 00 00 00 00 00   TSH ...D ..0.....
0010  00 00 00 00 00 00 01 11  04 b8 00 00 00 00 0b 44   ........ .......D
0020  00 00 00 00 00 00 00 00  00 64 f8 c8 4d 44 20 20   ........ .d..MD
0030  00 00 00 02 00 00 00 00  00 00 00 02 ff ff ff ff   ........ ........
0040  00 00 00 00 00 00 01 11  00 00 04 b8 4d 51 41 44   ........ ....MQAD
0050  4d 49 4e 20 00 00 00 00  00 00 00 00 41 4d 51 20   MIN .... ....AMQ
0060  71 6d 5f 76 75 6c 6e 33  20 20 20 20 ef 83 13 46   qm_vuln3     ...F
0070  20 00 1c 0f 41 4d 51 20  71 6d 5f 76 75 6c 6e 33    ...AMQ  qm_vuln3
0080  20 20 20 20 ef 83 13 46  20 00 1d 06 00 00 00 00       ...F  .......
0090  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00a0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00b0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00c0  71 6d 5f 76 75 6c 6e 33  20 20 20 20 20 20 20 20   qm_vuln3
00d0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00e0  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
00f0  61 64 6d 69 6e 69 73 74  72 61 74 6f 16 01 05 15   administ rato....
0100  00 00 00 93 e3 62 48 e1  92 24 75 07 e5 3b 2b f4   .....bH. .$u..;+.
0110  01 00 00 00 00 00 00 00  00 00 00 0b 20 20 20 20   ........ ....
0120  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
0130  20 20 20 20 20 20 20 20  20 20 20 20 00 00 00 0b                ....
0140  65 62 53 70 68 65 72 65  20 4d 51 5c 62 69 6e 5c   ebSphere  MQ\bin\
0150  61 6d 71 70 63 73 65 61  2e 65 78 65 32 30 30 37   amqpcsea .exe2007
0160  30 34 30 34 31 30 35 39  33 37 33 35 20 20 20 20   04041059 3735
```

MWR InfoSecurity

PCF Commands

- Programmable Command Format (PCF) can be used to manage the Queue Manager itself.
- They are passed to the Queue Manager as a data section within a normal GET or PUT message
- A PCF data structure has a header and a number of parameters in a number of well defined format

MWR InfoSecurity

Issuing PCF Commands

A number of steps are required to execute a PCF command: -

1. Connect to the Queue Manager
2. Open the System's Admin queue
3. Open a Dynamic (Model) queue for the data
4. Use MQ PUT onto the Admin queue
5. Use MQ GET on the Dynamic queue

MWR INFOSECURITY

Security Features

MWR InfoSecurity

Security Features

There are essentially three types of security feature

- MCAUSER – A tag within the packet that identifies the locally logged on user.
- Security Exit – An external program that can be used for access control.
- SSL/TLS – Transport security and access control using certificates and DN based user filtering.

MWR INFOSECURITY

MCAUSER – The Basics

- It is a parameter that is passed in parts of the message packets.
- There are lots of rules about how the MCAUSER works.
- The MCAUSER parameter on the Server Connection channel basically tells MQ which user to run under.
- In simple terms it’s a method of controlling access based on the user running a process which accesses a queue.

MWR INFOSECURITY

MCAUSER - Limitations

- By default a blank MCAUSER will be present on SYSTEM channels.
- The MCAUSER data in packets is a client side security control only.
- There is lots of confusion about what MCAUSER security actually means.
- Never rely on MCAUSER settings to protect your installation.

MWR InfoSecurity

Security Exits – The Basics

- A security exit is an external program that can be executed before an MQ connection is established.
- The exit can technically be written to perform any operation.
- Usually the exit checks a username and password.
- Protecting a channel with a security exit enforces access control.

MWR InfoSecurity

Security Exits – Limitations

- A security exit on a cleartext channel can be just as bad as Telnet
- Insecure code could get your system compromised
- MQ has to make sure the security exit actually gets called

MWR InfoSecurity

SSL Support – The Basics

- MQ can support SSL and TLS connections on a per channel basis
- The Queue Manager can communicate using both cleartext and encryption on the same TCP port
- Only one cipher suite is supported on a channel
- Version 0.9.8a of OpenSSL supports all of MQ's SSL versions
- FIPS Compliance can be achieved using just the software or with hardware accelerators

MWR InfoSecurity

SSL Support - Limitations

- Cycling through the ciphers lets you see which one is supported on a channel
- Supporting SSL does not enforce any authentication control by default
- The tools I have written work just as well over SSL as they do over Cleartext
- Remote host authentication is based on the trusted CAs in the key repository

MWR InfoSecurity

SSL Client Authentication – The Basics

- The Queue Manager can be configured to accept connections only from clients with certificates from authorised CAs
- Filtering of users can be achieved based on the values in the DN of the client's certificate.
- Both ends of the connection can be authenticated based on the data held within the key repository at each side.

MWR InfoSecurity

SSL Client Authentication – Limitations

- By default a large number of trusted CAs are included in a key repository
- An attacker with a certificate signed by a trusted CA can still gain access
- This attack is easy to accomplish using the OpenSSL based tools discussed earlier
- SSL DN filtering pattern matches from the start of the string but doesn't care about trailing characters

MWR INFOSECURITY

Testing Websphere MQ

MWR InfoSecurity

Connecting to MQ

The success of connection will depend on a number of things

- Finding the correct port to connect to
- Knowing a channel name to communicate with
- The MCAUSER of the channels on the system
- The use of a security exit on the channels
- The use of SSL and certificate based authentication

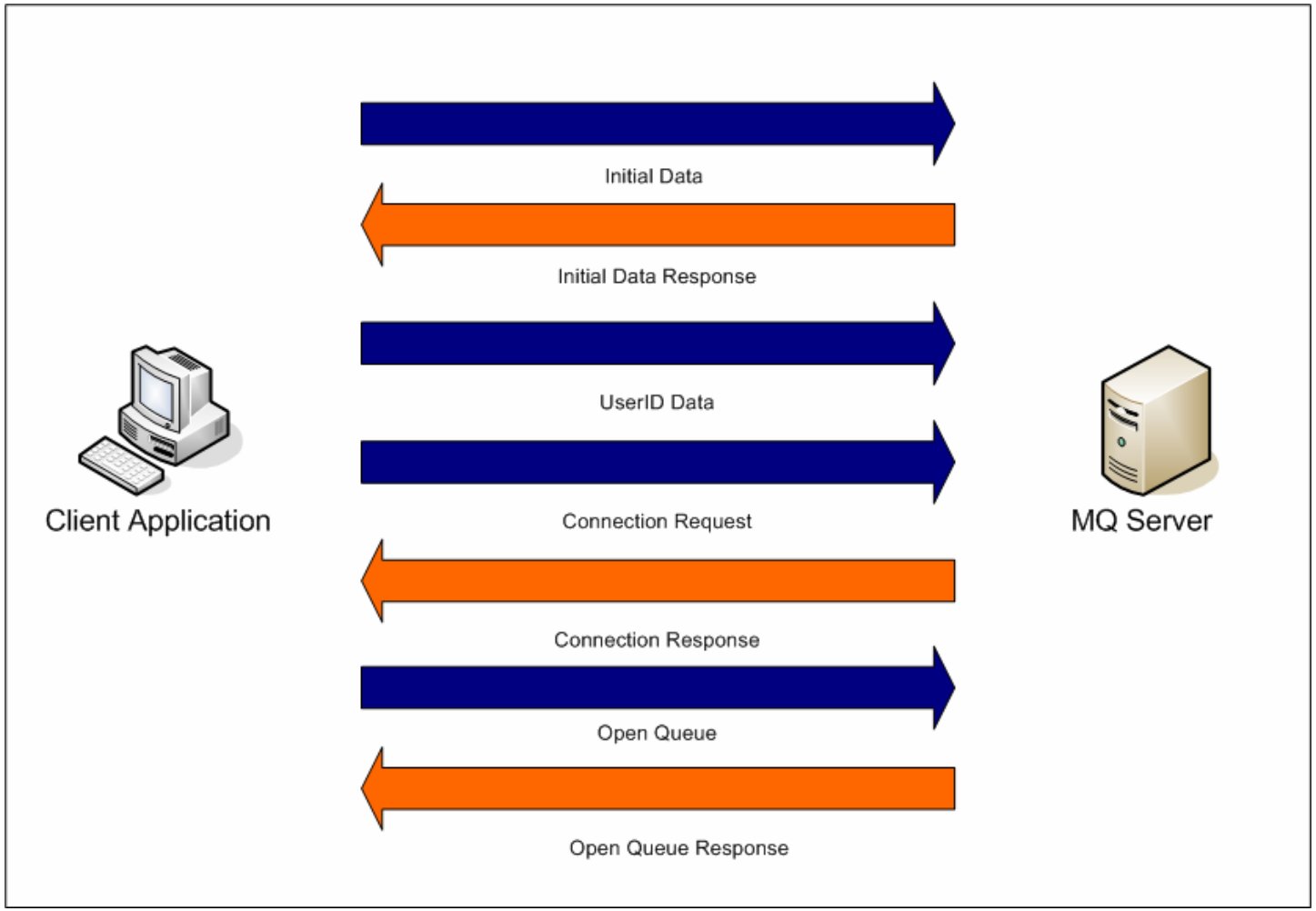
MWR InfoSecurity

Finding Websphere MQ

- By default a Queue Manager will listen on TCP port 1414
- We can attempt the MQ Initial Data handshake against the ports on our target
- If we get a response we have found MQ and we get the name of the Queue Manager returned as well
- We will see this in the demo later in the talk

MWR INFOSECURITY

How to Connect



MWR InfoSecurity

Channel Auto Definition

- Channel Auto definition is a feature that allows the automatic creation of a channel.
- At connection time if the specified channel doesn’t exist it will be automatically created.
- If Auto definition is enabled and a poorly secured template is used you might get lucky.

MWR InfoSecurity

Once Connected

Once connected your actions are dependent on the MCAUSER permissions on the channel but you could: -

- Issue PCF commands
- Open and browse queues
- GET and PUT data
- Execute OS Commands

MWR INFOSECURITY

Useful PCF Commands

If you can execute PCF in reality its game over, but there are still useful things to try

- Version Enumeration
- Channel discovery
- Queue Discovery
- Permission data

MWR INFOSECURITY

Executing Commands – Method 1

- Websphere Version 6.0 supports “Services”
- PCF can be used to Create, Delete, Start, Stop, Inquire them
- A service defines an external application that can be run
- If PCF can be executed so can Operating System commands

MWR InfoSecurity

Executing Commands – Method 2

- Triggers can be defined which fire when messages are placed on a given queue
- PCF commands need to be executed to set up the process and the queue

  1. Create a new process for our command
  2. Alter a queue or create a new one with trigger control on
  3. Place a message onto the relevant queue

- If a trigger monitor is running it will execute the process using the privileges it is started with

MWR InfoSecurity

Executing Commands – Method 2.1

- Rather than setting all the queues up its easier just to put the data onto the initiation queue
- If the correct format of data is used in the PUT the command will be executed
- If a message is left on the initiation queue when the trigger monitor is not running it will execute when it is next started

MWR INFOSECURITY

I’m Not Scared Yet !!

- In the process of testing client installations I discovered two new vulnerabilities
- These vulnerabilities were reported to IBM in January and May 2007.
- I spoke directly to the MQ development team and used CPNI in the UK to report these issues

STATUS OF ISSUE FROM IBM TO BE UPDATED

MWR InfoSecurity

Security Exit Bypass

- A vulnerability was discovered that enabled a security exit to be bypassed
- This allows access to a protected channel
- Versions 5.1 – 5.3 on Solaris are vulnerable
- Version 6 on Windows was not vulnerable

STATUS OF ISSUE FROM IBM TO BE UPDATED

MWR InfoSecurity

Invalid MCAUSER Bypass

- A vulnerability was discovered that enabled a channel set to an MCAUSER of nobody to be accessed
- Versions 5.1 – 5.3 and 6.0 on Solaris and Windows are known to be vulnerable
- Of the versions I have tested all have been affected by the issue

STATUS OF ISSUE FROM IBM TO BE UPDATED

MWR INFOSECURITY

How to exploit the vulnerabilities

DETAILS TO BE RELEASED ON THE DAY

MWR InfoSecurity

Our Toolkit – Part 1

- Find MQ services on hosts on the network
- Confirm a list of channels on the system
- Test SSL settings on each channel
- Recover Information about the Queue Manager, Channels, Queues, Triggers, Processes

MWR InfoSecurity

Our Toolkit – Part 2

- Read data from a Queue
- Write data to a Queue
- Execute commands using a previously created trigger monitor
- Execute commands using the Create Service command

MWR InfoSecurity

The Tools

- I have written a set of classes for defining MQ traffic and various useful payloads
- It is written in Python and is still in active development
- The generic classes and one sample tool are now available
- If you look closely at the code you can build your own interesting packets

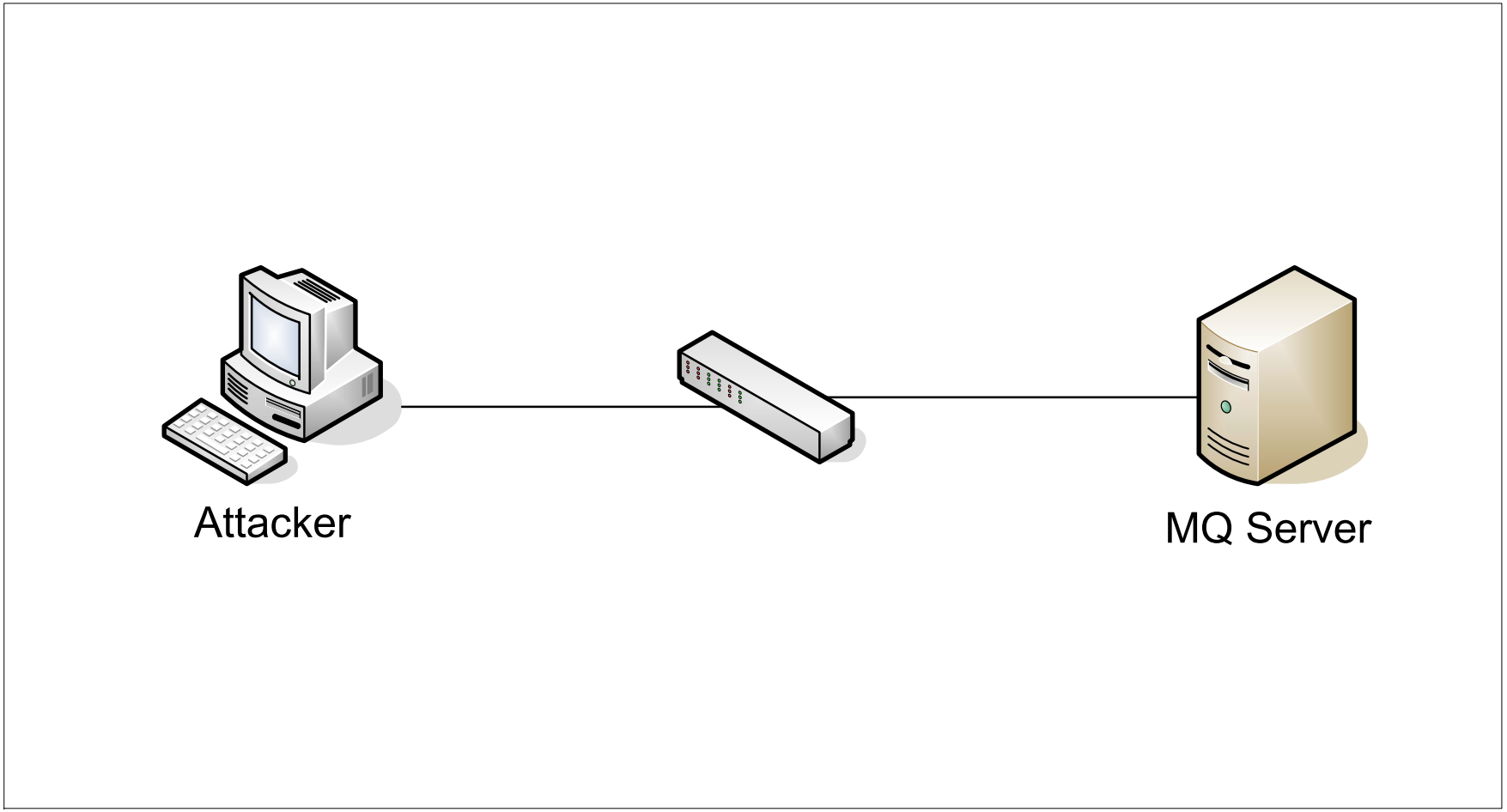
MWR INFOSECURITY

More Information

- I am in the process of writing a white paper on MQ security
- It will have lots of detail about the areas I have talked about plus some others
- This will be published within the next month
- You will be able top find it at: - http://www.mwrinfosecurity.com

MWR InfoSecurity

Demo – The Setup



MWR InfoSecurity

Demo – The Objectives

- Examine a box for MQ Services
- Work out the SSL support on a default channel
- Recover some information using the Command Server
- Execute commands to start netcat running

MWR INFOSECURITY

Recommendations

MWR INFOSECURITY

Technical Recommendations

- Protect the default and admin channels and restrict the permissions on the others.
- Never rely on the MCAUSER parameter for security
- Always use security exits on channels and make sure you have the code audited.
- Don’t have the command server turned on if you don’t need it
- Don’t use Channel Auto Definition

MWR InfoSecurity

Technical Recommendations – Part 2

- Use an appropriate strength of SSL on all channels
- Remove all non-required CAs from the Key Repository
- Be specific with the User Filtering strings
- Clear the initiation queue before starting a trigger monitor
- Trigger monitor accounts should use lowest privileges

MWR INFOSECURITY

High Level Recommendations – Part 1

Middleware security is just as important as the front-end application and the back-end database

- Test Middleware properly
- Don’t rely on “vulnerability scans”

Follow best practice and use all the security features

- Use access control
- Use encryption
- Apply all security fixes

MWR InfoSecurity

High Level Recommendations – Part 2

Ensure security testing is thorough

- Make sure pen testers know about the application
- The entire environment needs testing

Each environment needs securing

- Development shouldn’t impact on Live
- Understand the security of remote queues
- Each component of a cluster must be secured

MWR INFOSECURITY

So are we safe now ?

Maybe not! There is still lots more work to be done

- Clustered Environments need more research
- Always more fuzzing to be done
- MQ on iSeries and z/OS
- Tivoli is recommended for administration
- How does Sun MQ compare

MWR INFOSECURITY

Summary

- If you don’t get the basics right you will get burnt and by default MQ is not secure.
- New vulnerabilities can expose the security of any installation.
- Using multiple layers of defence will always help to lower the risk.

MWR INFOSECURITY

References and Further Reading

Websphere MQ Information Centre

http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp

IBM Redbooks

http://www.redbooks.ibm.com/abstracts/sg247128.html

IBM Downloads

http://www-128.ibm.com/developerworks/downloads/ws/wmq/

MWR InfoSecurity

References and Further Reading – Part 2

QFlex product

http://www.netflexity.com/qflex/index.shtml

MQ PERL Modules

http://search.cpan.org/dist/MQSeries/

MWR InfoSecurity White Paper (Available Soon)

http://www.mwrinfosecurity.com

Contact Me

martyn.ruks@mwrinfosecurity.com

MWR INFOSECURITY

Questions ?