IBM WebSphere MQ Security

Martyn Ruks

martyn.ruks@mwrinfosecurity.com

EUSecWest 08
2008-05-22

Introduction to MQ

Why study WebSphere MQ?

- The environments in which it is used are usually business critical.
- A methodology for testing the software has not previously been available.
- Our company's clients are using this technology so we need to understand it.
- If an attacker owns the Middleware they usually own the business process.

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
- Version 7.0 is now in Beta !

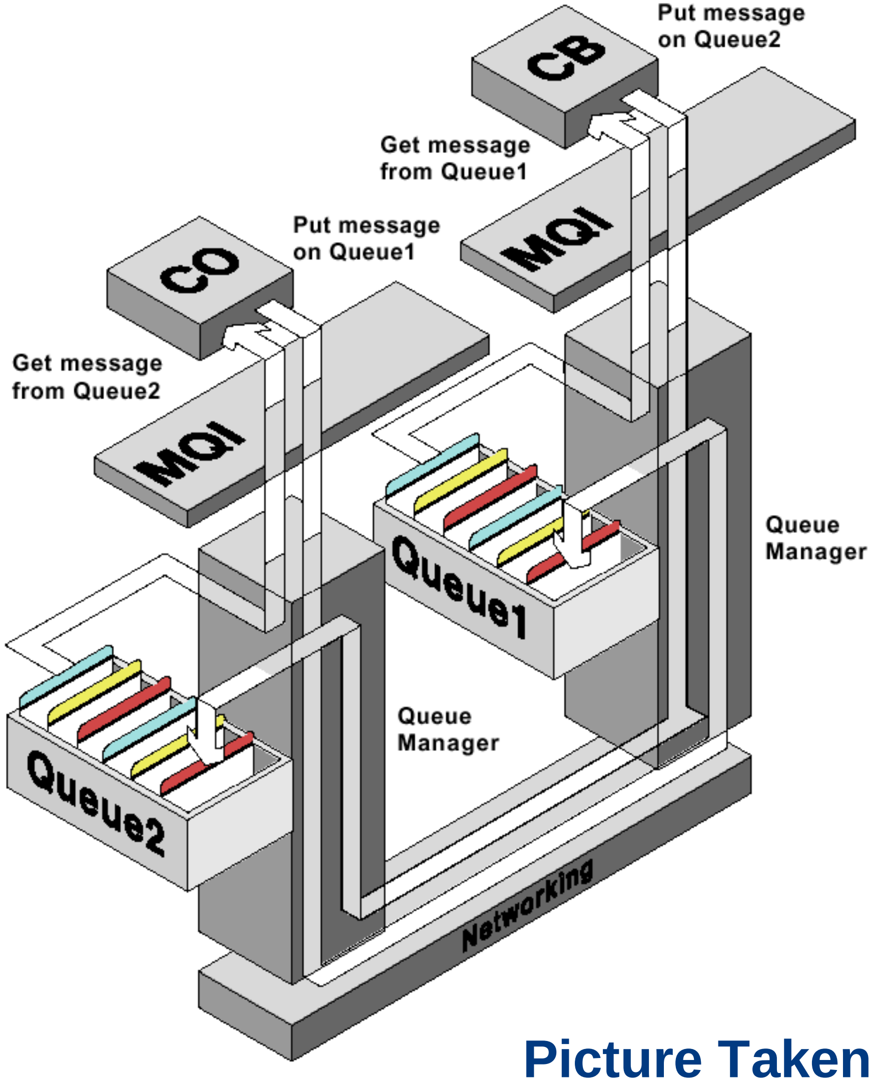
Why do Businesses use MQ ?

- 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

What are the Risks ?

- Breach of data confidentiality
- Adding, altering or deleting messages (integrity)
- Affecting availability
- Gaining access to the Operating System (impact on other applications)

A Typical Environment



Picture Taken from document by Joe Conron

Terminology

A number of key terms are used within the MQ world

- Queue Managers
- Channels
- Queues
- Object Authority Manager
- Triggers and monitors

We will cover these in more detail as we go along

What is a Queue Manager ?

- A Queue Manager is an application that is responsible for managing the message queues
- Only 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 across a network
- You often find multiple Queue Managers on a system (Production, Development etc)

What is a Channel ?

- Channels are used to facilitate connections between a client and a server or two servers.

- A channel can be thought of as a conduit through which to access the message queues

- There are several types of channel and each can be used in a different way.

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

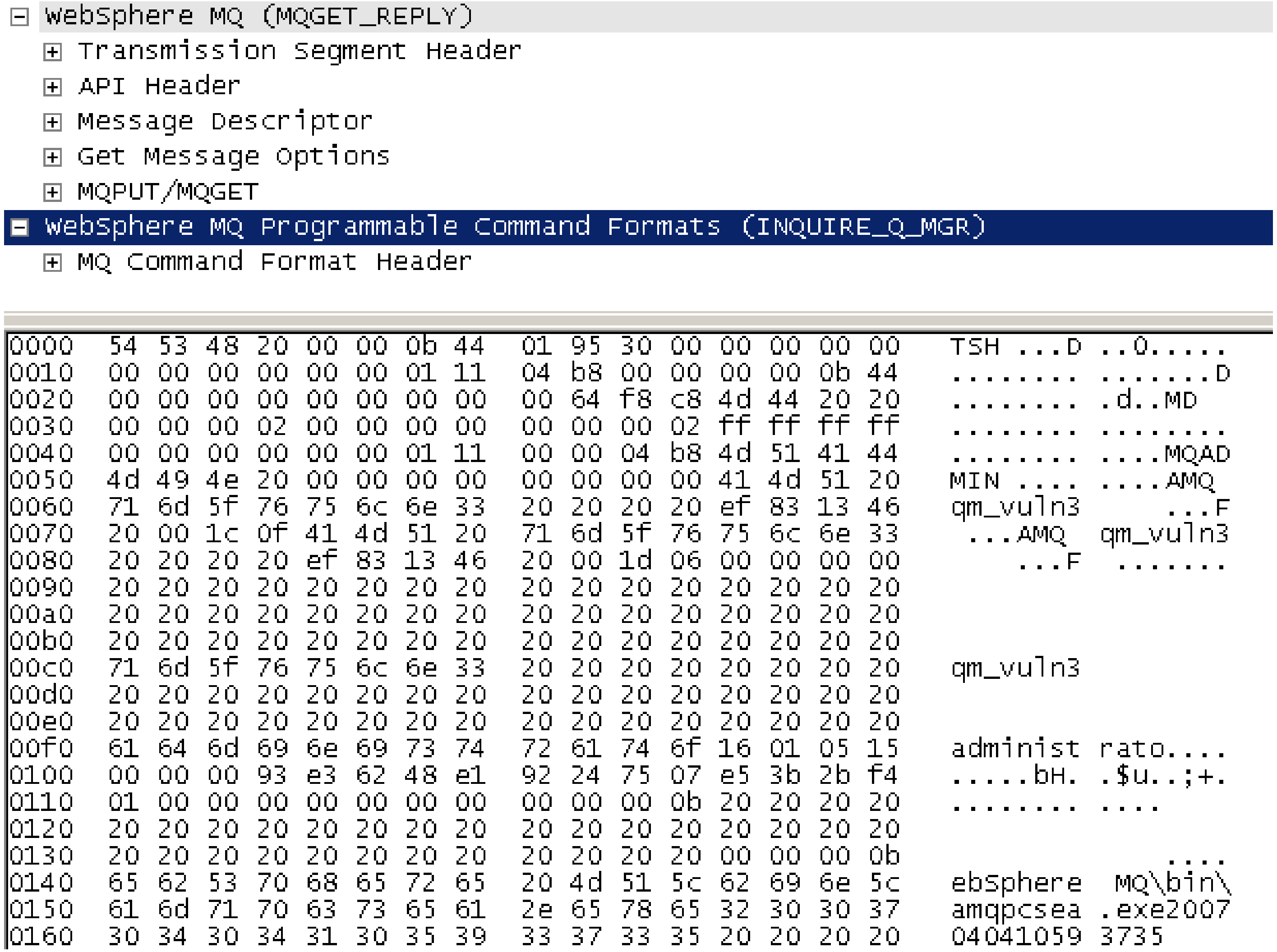
What is the OAM ?

- The Object Authority Manager (OAM) is responsible for handling authorisation decisions
- It is closely integrated with Operating System users and groups
- Most authorisation decisions occur when opening an object

The WebSphere MQ Protocol

- Information about the protocol is not public but is in Ethereal/Wireshark (prior to version 7)
- Each packet contains a series of discrete sections
- The layers in each packet depend on the type of operation
- All packets contain a Transmission Segment Header (TSH) (prior to version 7)

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
```

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

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

MQ Security Features

Security Features

There are essentially three types of security feature

- MCAUSER – A method for limiting the permissions associated with a channel

- 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

MCAUSER – The Basics

- The MCAUSER parameter on a channel basically tells MQ which user to run under
- There are lots of rules about how the interaction between the MCAUSER and the OAM actually works
- A user can be identified by the UserID they place in network data packets
- It is widely used as a method for controlling access based on the user running a process which opens a queue

MCAUSER - Limitations

- By default a blank MCAUSER will be present on SYSTEM channels
- The UserID 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

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

Security Exits – Limitations

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

SSL Support – The Basics

- MQ can support SSL and TLS connections on a per channel basis
- The Queue Manager can communicate using both clear text and encryption on the same TCP port
- Only one cipher suite is valid on a channel at any given time
- 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

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 clear text

- Remote host authentication is based on the trusted CAs in the key repository

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

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

Testing WebSphere MQ

Connecting to MQ

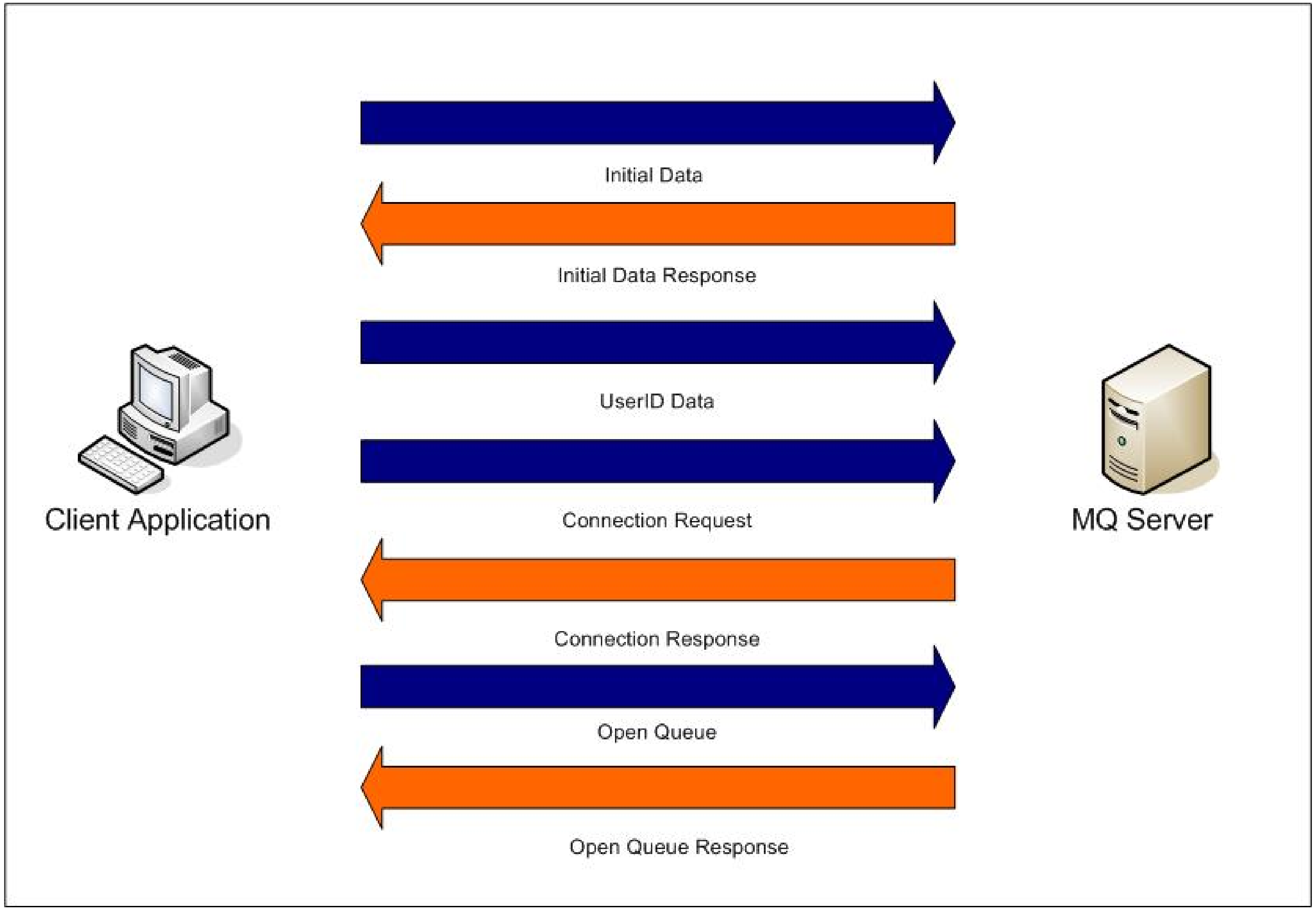
The success of connection will depend on a number of things: -

- 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

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
- We will focus on Server Connection channels

How to Connect



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 gain unauthorised access

Once Connected

Once connected to MQ your actions are dependent on the MCAUSER and OAM permissions on the channel and other objects but you could: -

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

Useful PCF Commands

If you can execute PCF often it is game over, but there are still useful things to try

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

Executing Commands – Method 1

- WebSphere Version 6.0 supports “Services” that cannot be disabled
- 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 usually Operating System commands can as well

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

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

WebSphere MQ Vulnerabilities

- The research has revealed a number of remotely exploitable vulnerabilities
- IBM have produced a patch covering 2 of them which allows access to channels that are otherwise protected
- The other issues are being resolved but I can’t say anything else about them at the moment

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

Exploit Details

- To authenticate to the Queue Manager a UserID is normally sent
- What happens if we don’t send the UserID packet and just skip to the Connection Request ?
- The result is that we gain access to the channel !

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

Exploit Details

- We perform the handshake and then issue the Connection Request

- The Queue Manager sends us a “2035 Not Authorised“ response but we ignore it

- We continue to interact with the Queue Manager and have the equivalent of administrative access

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

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

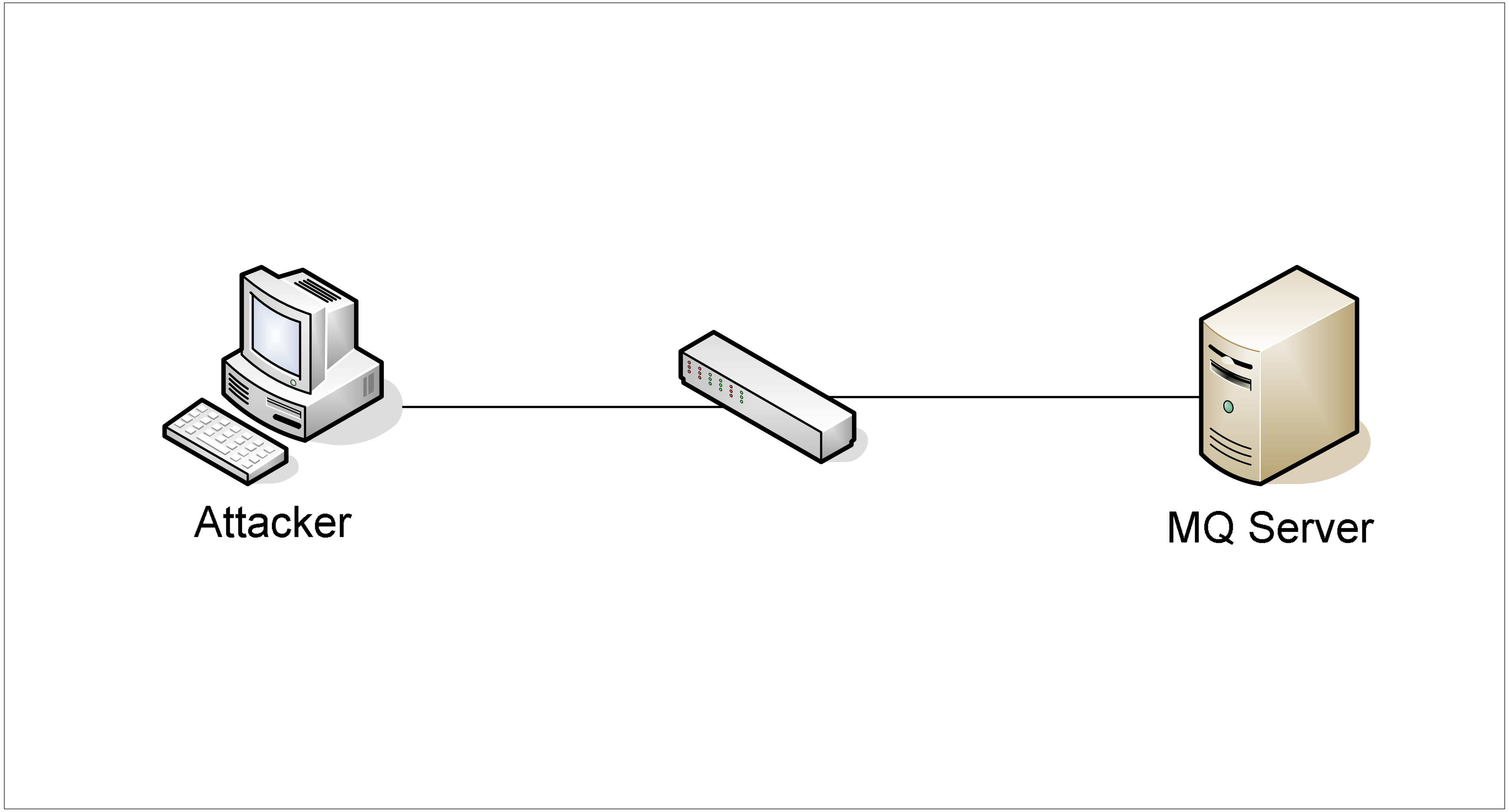
The Tools

- I have written a set of classes for defining MQ traffic and various useful payloads
- The tools are written in Python and are still in active development
- I am now working on using the dradis framework to define a testing methodology with integrated toolkit

More Information

- The first part of my white paper on IBM WebSphere MQ Security has just been published
- Part 2 will have lots of detail about other areas that I haven’t talked about today
- This is intended to be published within the next 6 months

Demo – The Setup



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
- Escalate access to a secure Queue Manager

MWR InfoSecurity

Recommendations for Securing MQ

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

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

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

High Level Recommendations – Part 2

Each environment needs securing

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

Preview of Version 7

- An HTTP based help facility with Java methods remotely exposed – Watch this space !
- New HTTP interfaces to the Queue Manager
- Changes to the protocol – New Wireshark dissectors needed ?
- Multiple connections inside a single TCP session

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 do MSMQ, Sun MQ, ActiveMQ compare

Summary

- If you don’t get the basics right you could 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

Questions ?