WMQ B2B

T.Rob Wyatt
t.rob@ioptconsulting.com

Change is the only constant

This presentation reflects…

- **My current opinions regarding WMQ security**
- **The product itself continues to evolve (even in PTFs)**
- **Attacks only get better with time**
- **This version of the presentation is based on WebSphere MQ v7.1 & v7.5**
- **This content will be revised over time so please be sure to check for the latest version at https://t-rob.net/links**
- **Your thoughts and ideas are welcome**

WebSphere MQ Security Presentation Series

- This presentation is part of a series authored by T.Rob Wyatt. The introductory decks are available through https://t-rob.net.
- For the most current version of this deck, please see https://t-rob.net/links or contact the author presentations@t-rob.net.
- Ask me about on-site and remote training tailored for your organization.

Why B2B?

- **Seems to be a component in every engagement I do anymore. Lots of demand for B2B scenarios in the Redbook, in Product docs, etc.**
  - But the Best Practices have not been well defined over the years.
  - The new Redbook adds much to the discussion but the content is very deep.
  - People asking for expansion of the Redbook chapter with simpler examples.
- **This session is therefore based on the B2B Chapter in the Redbook.**

At IMPACT we had 25 slots for WebSphere Messaging content. Here we have 70! But that means we will need to get a feel for the level of presentation that best suits this audience – please provide feedback as to content!

Also, the sessions I'm presenting have fewer slides because we always tend to run out of time for Q&A.

If you wanted more written content & less Q&A, please let me know!

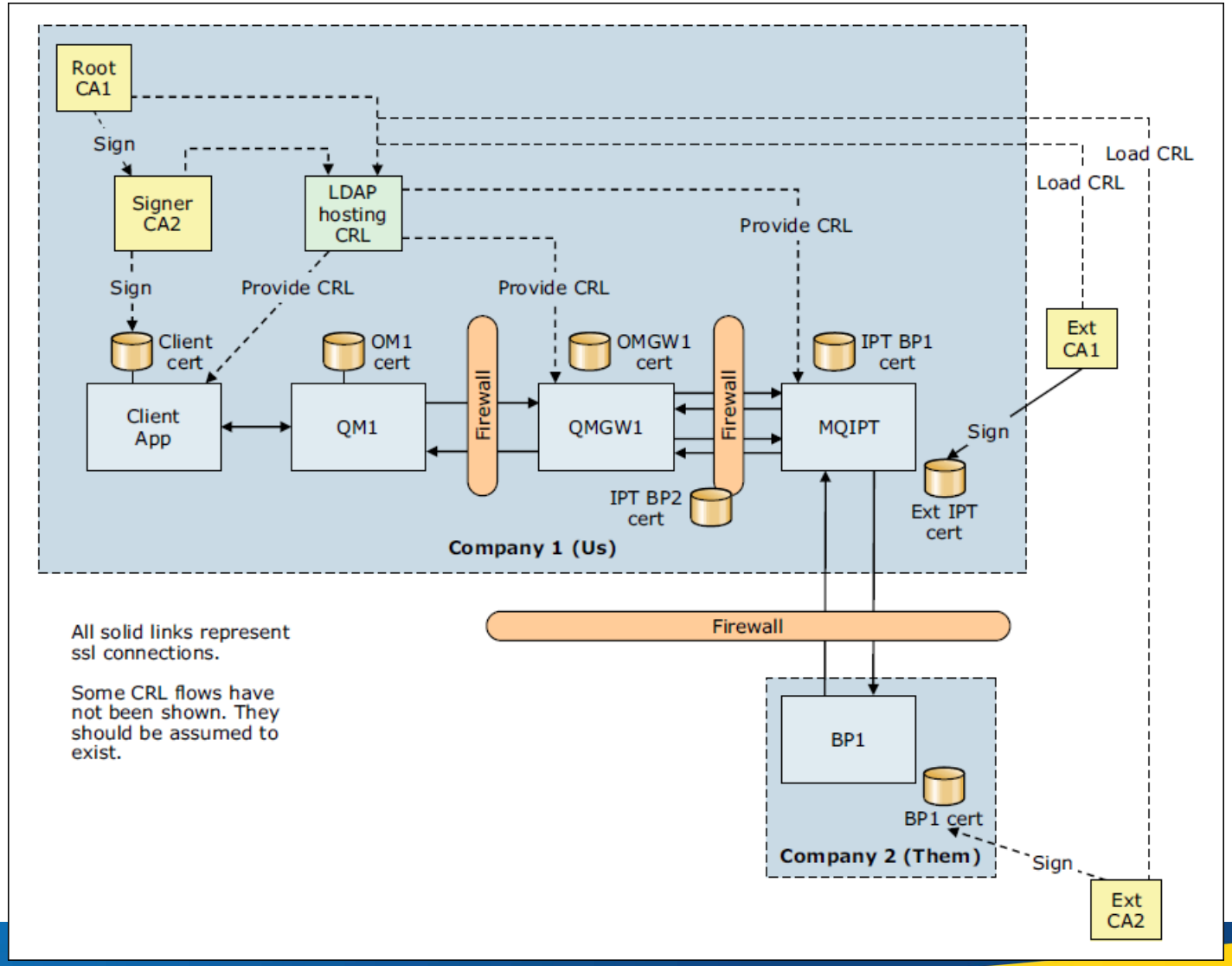
Agenda

- **Session objectives**
- Protecting business assets
- Improved isolation across security roles
- Intrusion prevention
- Intrusion detection
- Forensic analysis
- Additional Resources

Session Objectives

- Adjunct to Chapter 10 of *Secure Messaging Scenarios with WebSphere MQ*, an IBM Redbooks publication.
- Seeks to explain *why* the B2B scenario uses the controls that it does. For technical detail of the setup and extensive diagrams and scripts, please refer directly to the Redbook!
- Download the book in PDF or ePub at IBM: http://ibm.co/UU4Nkt
- Order hardcopy through Amazon: http://amzn.to/VACrvY
- I'll happily load the PDF onto your USB key after the session. ☺

The scenario



Agenda

- Session objectives
- **Protecting business assets**
- Improved isolation across security roles
- Intrusion prevention
- Intrusion detection
- Forensic analysis
- Additional Resources

Protecting business assets: Objectives

If most breaches are internal, why worry so much about B2B?

The prevalence of internal breaches might have something to do with the effectiveness of the perimeter defenses.

We are generally good about terminating connections in the DMZ, limiting to one function per server, isolating Test & Prod, etc.

Or at least we are with technologies that evolved in hostile environments such as HTTP servers, databases, SMTP servers, etc.

WebSphere MQ? Not so much. What is considered standard best practice with other technologies is often ignored with WebSphere MQ. One of the most basic objectives for a B2B security architecture is to protect the business assets by terminating external connections somewhere else. Like the DMZ or, at the very least, a gateway server/QMgr.

Protecting business assets: Mitigations

- Dedicated DMZ server.
- MQIPT or queue manager(s).
- Terminate connections in the DMZ.
- Limit inbound access from the DMZ to specific queue managers.
- Strong authentication for all connections.
- All inbound connections from the DMZ are treated as untrusted.
- All inbound routes and destinations through the DMZ are explicitly enumerated through named QAlias or QRemote objects.
- Limit the external view of the internal namespace.

Agenda

- Session objectives
- Protecting business assets
- **Improved isolation across security roles**
- Intrusion prevention
- Intrusion detection
- Forensic analysis
- Additional Resources

Improved isolation across security roles : Objectives

- Isolate regular and admin users (to the extent that regular users are allowed to access the B2B node, which should be rare).
- Isolate external users from internal users.
- Isolate external users from each other.

Improved isolation across security roles : Mitigations

- Strict limitations on access to the box. Only admins is best.
- Dedicated access path for admins. Listener, channel, etc.
- Dedicated access path for each external business partner.
- Ideally, no client access by external parties.
- Force the MCAUSER of all non-admin SVRCONN channels.
  Force the MQMD.UserID for inbound messages on MCA channels.

Agenda

- Session objectives
- Protecting business assets
- Improved isolation across security roles
- **Intrusion prevention**
- Intrusion detection
- Forensic analysis
- Additional Resources

Intrusion Prevention: Objectives

- **To keep the “bad guys” out! (Duh.)**
- **But to do so more effectively perhaps than with internal interfaces.**
  - Enforcing stricter policy at the QMgr offsets the lack of controls at the remote site.
  - Fiduciary obligations.
  - Compliance
- **To keep business partners from using your platform to attack one another.**
  - Because if direct losses are bad, liability for someone else’s losses is much worse!
- **To restrict visibility into the internal network.**

Intrusion Prevention: Mitigation

- **Strong authentication.**
- **Disable all unnecessary services.**
- **Non-login accounts for security roles.**
- **Disable DLQ for outward-facing channels.**
- **Restrict channels by IP address and listener.**
  - Multi-homed machine with internal-facing, external-facing and admin NIC.
  - Each business partner's channels bound to a specific IP and NIC.
  - Inward-facing channels bound to internal NIC.
- **Separate listeners for each interface.**
- **Message exit to disable report options and force MQMD.UserID.**

Agenda

- Session objectives
- Protecting business assets
- Improved isolation across security roles
- Intrusion prevention
- **Intrusion detection**
- Forensic analysis
- Additional Resources

Intrusion detection: Objectives

- **Greater duty to detect intrusions and anomalous activity.**
  - “Reasonable and customary.”
  - Compliance.
- **Certain actions that are OK internally are restricted in the DMZ.**
  - For example, DLQ message due to expired dynamic queue.
  - Or an FDC due to socket probing.
- **Because all gateway changes should occur inside a planned window.**

Intrusion detection: Mitigation

- **Greater range of alarm conditions**
  - Channels in retry.
  - QFull conditions.
  - TLS exceptions.
  - Etc. See the book.
- **Extremely low MAXDEPTH values**
  - Because we don’t want a lot of data stuck in the DMZ if there’s a problem.
  - Faster alert when channels fail.
- **Tight access control makes any anomalous activity more obvious.**

Agenda

- Session objectives
- Protecting business assets
- Improved isolation across security roles
- Intrusion prevention
- Intrusion detection
- **Forensic analysis**
- Additional Resources

Forensic analysis: Objectives

- Provides accountability.
- For compliance and auditing.
- To quickly and reliably trace the source of a security-relevant event.
- To assess damages related to an event.
- To identify affected customers after an event.
- To assist law enforcement.

Forensic analysis: Mitigation

- **Save your error logs!**
- **Ship logs and FDC files off the box as soon as possible.**
- **Enable events *and monitor for them.***
- **Per-channel DLQ or no DLQ.**
- **Set up a default XMitQ that goes to a honeypot QMgr.**
  - Allow all channel MCAUSERs to access the default XMitQ.
  - Alarm *anything* that shows up on the honeypot QMgr.

Agenda

- Session objectives
- Protecting business assets
- Improved isolation across security roles
- Intrusion prevention
- Intrusion detection
- Forensic analysis
- **Additional Resources**

Additional resources

- **The WMQ Security Scenarios Redbook**
  - http://ibm.co/UU4Nkt
- **The WMQ Infocenter**
  - http://bit.ly/WMQ75Infocenter
  - http://bit.ly/WMQ71Infocenter
- **MQ Internet Pass-Thru**
  - http://ibm.co/SupptPacMS81
- **GSKCapiCmd V8 User's Guide**
  - ftp://ftp.software.ibm.com/software/webserver/appserv/library/v80/GSK_CapiCmd_UserGuide.pdf
  - Sorry, URL shorteners don't seem to work on FTP links. ☹
  - But go to my site (see next bullet) for an easy link.
- **T-Rob.net at https://t-rob.net**
  - The WebSphere MQ page has links to 3rd party resources & guides.
  - The Links page has links to my conference presentations and articles.

Questions & Answers