irm InformationRiskManagement

WebSphere MQ Threats – A Management Summary

An IRM Research Briefing Document by

John Yeo

WebSphere MQ Threats – A Management Summary

Businesses around the world use WebSphere MQ due to its reputation as a proven and reliable data transport mechanism.

As with all technologies a lack of security awareness combined with demanding requirements from business units often leads to an insecure implementation. At IRM we have identified a number of inherent software vulnerabilities and common configuration weaknesses that real world WebSphere MQ Enterprise environments are exposed to.

Due to the types of data typically transported by WebSphere MQ - confidential business intelligence or B2B transaction logs, the endgame scenario is not necessarily a full system compromise; unauthorised read access to the messages may have equally adverse consequences.

Our focussed security research, combined with consulting exposure to complex WebSphere MQ environments has enabled us to develop an extensive testing methodology; in turn we are able to provide WebSphere MQ specific technical assurance testing, alongside our existing WebSphere MQ architecture and design review service offering.

The purpose of this document is to provide a high level management summary of the threats against WebSphere MQ when installed in an Enterprise environment.

High Level Threat Analysis

For the following threats we employ an abstract WebSphere MQ architecture which is being used as the message bus for a generic financial application.

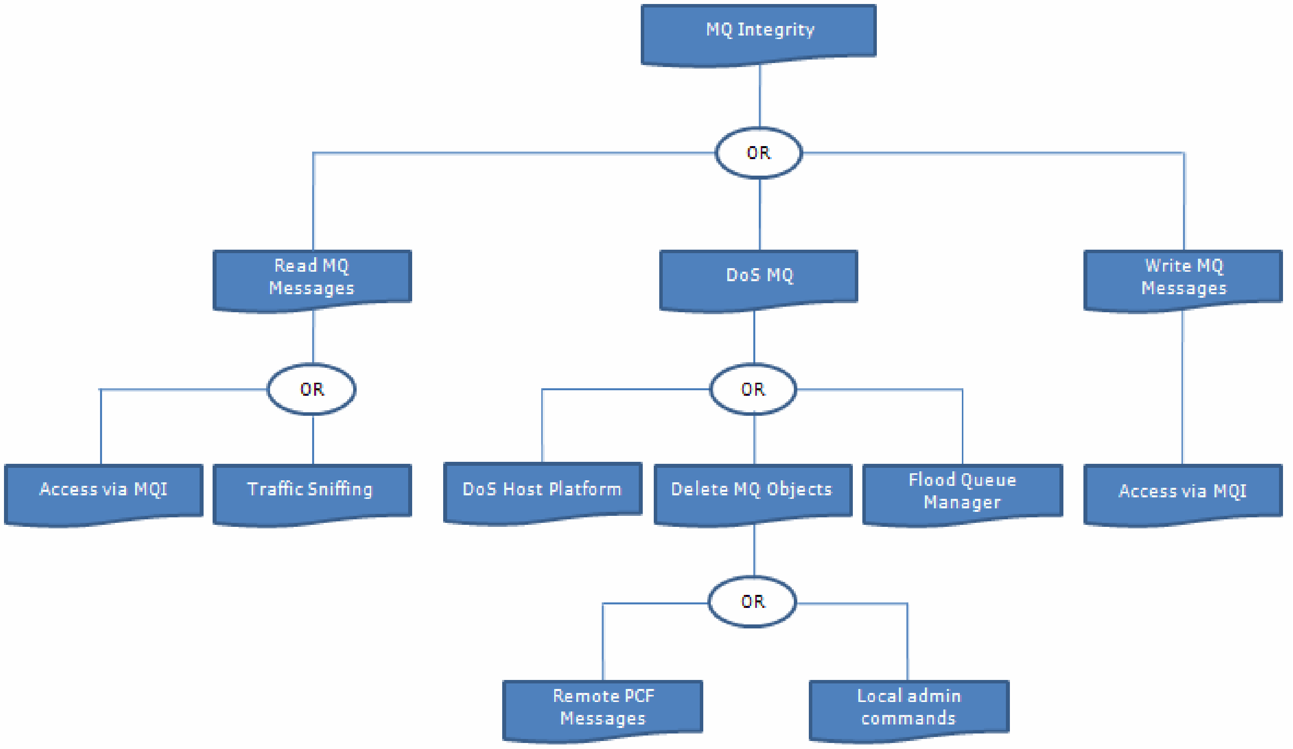

Figure 1: Abstract *attack tree* with the root node being the compromise of integrity of a hypothetical MQ environment

Traffic Sniffing

By default WebSphere MQ traffic is unencrypted and exposed to the same threat of traffic sniffing as other plaintext protocols; allowing an attacker to passively read sensitive financial account data and transaction details as well as viewing authentication information in any remote administration commands being issued.

Denial of Service

Downtime is expensive; in our scenario traders rely on the application to deliver them with up to date business intelligence. In a typical scenario a misconfigured UAT or development client-application has the potential to severely degrade the service for production users. Furthermore, the software vulnerabilities identified by IRM could be exploited by a malicious employee to invoke a DoS attack on a WebSphere MQ server. IRM continue to report security-related software flaws within WebSphere MQ to IBM, following responsible disclosure and are working closely with them to resolve the vulnerabilities identified.

Unauthorised Queue Access

Often queue managers are misconfigured, more so within distributed WebSphere MQ environments, and will allow for an unauthorised user to read and write messages to message queues. Reading messages from the application's message queue will expose customer and financial account data; but the ability to arbitrarily write to the message queue compromises the integrity of the business unit and corrupts the audit trail. Moreover without authentication it may be possible to spoof the administrative identifier allowing for the remote issuing of commands to a queue manager.

Unauthorised Decryption

The use of cryptographically weak cipher suites for compatibility or legacy reasons may be unwittingly exposing data to the risk of 'store and decrypt' type attacks and does little to future-proof the WebSphere MQ environment.

Application Design Flaws

When development teams operate without security guidance during the early phases of the software development lifecycle for MQ clients, it can potentially undermine the entire WebSphere MQ environment; which is later costly and technically challenging to secure. An enforced and clearly defined WebSphere MQ security policy can deliver a long term return on investment.

Contact research@irmplc.com to further understand how our WebSphere MQ security expertise can assist your business. Also, more information about messaging systems security is available on the IRM website at the following URL:

http://www.irmplc.com/index.php/158-Messaging-System-Security

About IRM

Information Risk Management Plc (IRM) is a vendor independent information risk consultancy, founded in 1998. IRM has become a leader in client side risk assessment, technical level auditing and in the research and development of security vulnerabilities and tools. IRM is headquartered in London with Technical Centres in Europe and Asia as well as Regional Offices in the Far East and North America. Please visit our website at www.irmplc.com for further information.