ti&m expert series

WebSphere MQ Security

Tales of Scowling Wolves among Unglamorous Sheep

Dr. Johannes Böhm-Mäder

With foreword by T.Rob

ti&m expert series

WebSphere MQ Security

Tales of Scowling Wolves among Unglamorous Sheep

Dr. Johannes Böhm-Mäder

With foreword by T.Rob

WebSphere MQ Security

Tales of Scowling Wolves among Unglamorous Sheep

Dr. Johannes Böhm-Mäder
ti&m AG

First Edition
August 2011

Books on Demand

Feedback to:
ti&m AG
Buckhauserstrasse 24
CH-8048 Zürich
T. 0041 (0)44 497 77 77
F. 0041 (0)44 497 77 78
www.ti8m.ch

1st Edition 2011
Copyright © 2011 by ti&m AG, Zürich

ISBN 9783842387867

Manufactured and published by

Books on Demand GmbH, Norderstedt, Germany

Dedicated to
my wonderful wife, lover, and best friend
Beatrice
who was ready to weather through all this with me
with great patience.

“Please stop waiting for a map.
We reward those who draw maps,
not those who follow them.”
Seth Godin

“Success is not counted
by how high you have climbed
but by how many you brought with you.”
Wil Rose

Imprint

ti&m – technology, innovation & management is the communication platform of ti&m AG that I have the privilege to preside over as CEO and founder.

The publication at hand, “WebSphere MQ Security”, widens this platform by a new channel ti&m experts. It now features four related formats that in their particular ways take up novel approaches to current themes in technology:

- ti&m special: Our annual journal on today’s most current and relevant IT topics, debated critically, provokingly, and always competently by the featured practitioners and visionaries.

- ti&m forum: Our series of semiannual presentations and discussions, designed to maintain a keen exchange with thought leaders from business and research.

- ti&m seminars: Our seminars and workshops where gathered key players on the most noteworthy topics and trends in IT exchange knowledge at the highest levels.

- ti&m experts: The in-depth skills of IT technologists, the expertise and experience of our men and women in the trenches on customer projects, is documented concisely; representing our sound and established know-how – of experts and for experts.

More than ever, ti&m – technology, innovation & management is positioned to highlight innovative technologies from multiple perspectives. Well-founded facts

are supplemented by critical discussions and ample vision. In so doing, ti&m reflects on the interaction of user strategies, offerings of software vendors, consulting approaches, applied research. The common denominator is the combined themes, their relevance to enterprises and ultimately enhanced potential for success.

Going beyond this platform of knowledge transfer and discussion, we want to broaden the technological realm by making room for creative and sometimes provocative viewpoints on our current themes: “art@work” (www.a-r-t-a-t-w-o-r-k.ch) features current art exhibitions that integrate contemporary art into the work lives and activities of our engineers and consultants.

The significant potential of the “Swiss IT factory” poses a great challenge for us as an IT provider. In the ever changing playing-field of innovation, added demand on requirements, greater stability, and enhanced security, we take the opportunity to probe and elaborate with our customers and partners in building on an IT vision for the future.

ti&m experts – WebSphere MQ Security is another tile in the mosaic of this vision. Dr. Johannes Böhm has been able to successfully present a highly complex subject in a very coherent and readable manner. Security experts and novices alike will benefit from his paper that we are confident you will enjoy reading.

Thomas Wüst and your *ti&m editorial board*

Thomas Wüst - CEO, ti&m AG

Martin Fabini - Principal, ti&m AG

Sandra Kutsche - Marketing, ti&m AG

Table of Contens

Imprint

Foreword

Preface

- Objectives and Target Audience
- Scope and Validity
- About the Author
- Acknowledgements

1. Introduction

- 1.1. Unspectacularly Creeping Threats
- 1.2. Dynamic Configuration Evolving
- 1.3. The New Power to Launch Whatever You Want
- 1.4. And Now the Ultimate Power: Multiply, Fork, Feed, Bridge …
- 1.5. The Devil in the Details

2. Security – What It’s All About

- 2.1. Separation of Duties
- 2.2. Basic Security Terms

3. Threat Scenarios for MQ

3.1. Attacker from the Internet

3.2. Network Snooping of Data Transported over MQ Channels

3.3. Attacker from a Partner Enterprise

3.4. Unauthorized MQ Client Access

3.5. Application Developer Gains MQ Administrative Authority

3.6. Malicious New Cluster Queue Manager

3.7. Unauthorized Copy of a Queue Manager Key Store

3.8. Misuse of Idle Channel Objects (System Templates)

3.9. Client Connecting with Blank User Id

3.10. Misuse of Disabled Accounts

3.11. End User Feeds Applications with Report Messages

4. MQ Connections Unveiled

4.1. TLS Roles with MQ

4.2. Message Channels

4.3. Client Channels

5. MQ Connection Security

5.1. Security Provisions for MQ Channels

5.1.1. Channel Proxy User