

# WebSphere MQ Enterprise Security: A Series of Defenses to Withstand the Test of Time

A 3D graphic featuring the word 'Smart' in a white, cursive script font, positioned above the letters 'SOA' which are rendered in large, blue, blocky 3D characters. The entire graphic is set against a dark blue background with a grid pattern on the floor and a light blue glow behind the letters.

**A.J. Aronoff**  
Solution Architect

Session Number: # 2726A Session Track: Birds-of-a-Feather

# Agenda

- About Prolifics
- Security Incidents in 2007
- MQ Security Strategy and Tactics
  - Automated Security Monitoring
  - External Defense
  - Zone Defense
  - Security Best Practices (MQ Risk Review group)
- MQ Security Practices - That Stand the Test of Time
- Summary
- MQ Support Pacs and Links - email [mqsecurity@prolifics.com](mailto:mqsecurity@prolifics.com)

# Prolifics As Your Technology Partner

Over 30 years of solving business problems with technology solutions

- Partner to deliver **high-value, total solutions**
- Translating **business requirements to technology solutions**
- **Industry leader** in Portal and SOA solutions
- Methodologies to **leverage current IT investments**
- Analyst-measured **96% success rate** deploying systems on-time, on-budget and to-specification
- Highly skilled, **well-rounded consultants**
- **Ability to react** to customer requirements in a timely and flexible manner
- **Cost effective** pricing options based on objectives and budget



Servicing Customers Around the World

# Prolifics and IBM Strategic Relationship

- Partnering with IBM --- bringing vision and market leadership
- Providing solutions on a solid foundation of best-of-breed products from IBM
- Prolifics is a Premier IBM Business Partner
- Access to IBM resources, labs and early technology releases
- Prolifics helps you select the solution that best fits your needs by providing guidance and advisement

## Prolifics Specializing in...

- SOA and Process Integration
- Portal and Workplace Solutions
- Tivoli Security for Web, Portal and Enterprise Applications
- Managing WebSphere and Portal Applications with ITCAM
- Information Management
- WebSphere Migrations and upgrades

# Prolifics is Award Winning

**2008 Winner of IBM Award for Overall  
Technical Excellence**

**2008 Winner of IBM Award for Outstanding  
WebSphere SOA Solution**



2007 Winner of IBM Award for Overall Technical Excellence

2007 Winner of IBM IMPACT SOA Process Solution Award

2006 Winner of IBM Lotus Award for Best Portal Solution

2005 Winner of Five-Star Partner Award



# Security Incidents in 2007

## ■ Recent Issues:

- Société Générale lost 4.9 billion euros (7 billion dollars)
  - Early detection of the problem could have saved billions
- Security Incidents and Accidents were a major issue in 2007

## ■ Today's Topic:

- Strategies and Tactics to help MQ Security stand the test of time

### SocGen's controls 'lacked depth'

An internal investigation into billions of euros of losses at Societe Generale has found that controls at the French bank "lacked depth".

The results of the investigation also show that rogue trades were first made back in 2005.

The bank set up an independent committee to investigate the 4.9bn euros (\$7bn; £3.7bn) in losses.



Mr Kerviel has said he never considered "running away"

### Ten Most Important Stories of 2007

**TJX, Bank of India Top the List of the Year's Biggest News**

December 21, 2007 - Linda McGlasson, Managing Editor

The TJX data breach. The Bank of India hack. The San Diego County wildfires. It's been a year full of memorable disasters - and some notable recoveries and regulations, too.

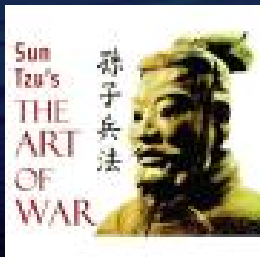
As we reflect on the biggest stories of 2007, it's clear that bad news was big. Some of our most popular stories were about Commerce Bank, Ameritrade and the ever-increasing threat of identity theft.

But common themes emerge as well. From the well-publicized hacks, we know that information security crimes abide by no geographic or national boundaries. Wherever banking institutions conduct online business, so do criminals. From the disasters, we've seen business continuity plans put to the test, and we've seen institutions derive lessons learned to build into their risk management strategies. From the myriad regulations handed down by the feds, we see new emphasis on familiar topics that may well prove to be the biggest stories of 2008:



# MQ Security Strategy and Tactics

- Common MQ Security Tactics
  - Channel Security: SSL and/or BlockIP2 (MQ Exits), MCAUSER, Removing system/default channels, etc.
  - Queue Security: OAM, MQ ESE
- MQ Security Strategies
  - Minimizing MQ downtime?
  - MQ High Availability?
  - Automated MQ health monitoring



“Strategy without tactics is the slowest route to victory.  
Tactics without strategy is the noise before defeat”

*Sun Tzu "The Art of War"*

# Automated Security Monitoring

## Tactic:

The *saveqmgr* support pac lets you take and compare snapshots of:

- Baseline system
- Current system

## An automated script compares the Current vs. Baseline System

- Gives an early warning of changes made to the system
  - The -1 argument to *saveqmgr*
  - Skips information that changes at runtime (i.e. curdepth)
  - Information about each queue or channel on 1 line
- Quick detection of accidental changes

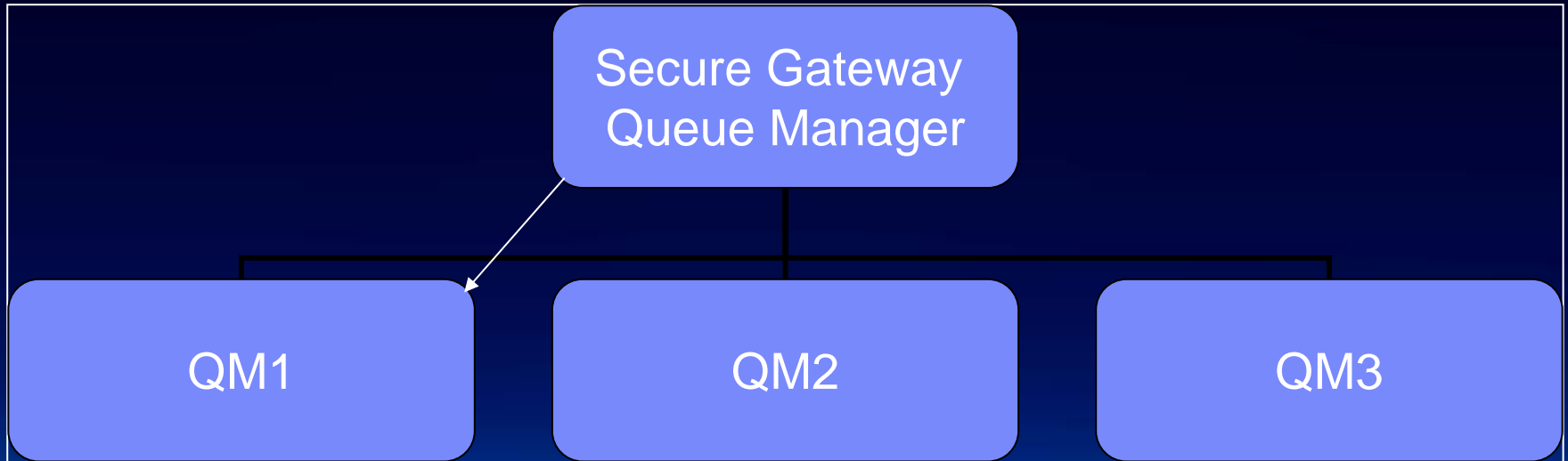
```
./saveqmgr.exe -1 -o -m A -F A.MQconfig  
-Z A.MQpermissions  
SAVEQMGR V6.0.3  
Compiled for Websphere MQ V6.0 on Aug 22 2006  
Requesting attributes of the queue manager...  
Writing Queue Manager definition to A.MQconfig.  
Generating attributes for Websphere MQ Release  
6.0.0  
Writing AuthInfo definitions to A.MQconfig.  
Writing Queue definitions to A.MQconfig.  
Writing Channel definitions to A.MQconfig.  
Writing Process definitions to A.MQconfig.  
Writing Namelist definitions to A.MQconfig.  
Writing Listener definitions to A.MQconfig.  
Writing Service definitions to A.MQconfig.  
Writing OAM definitions to A.MQpermissions.
```

# Automated Security Monitoring

- Saveqmgr validates security compliance conditions
  - System/Default Channels deactivated?
  - Channels protected by
    - SSL?
    - BlockIP2 (or other MQ exit)?
    - MCAUSER, etc.?
  - Restricted access to Transmission queues?
  - Non-mqm groups able to access user queue?
- Run validation script every time:
  - A queue manager starts / stops
  - A change is made to the queue manager
- Early detection can:
  - Reduce cost
  - Severity of problems

```
DEFINE  
CHANNEL('SYSTEM.ADMIN.SVRCONN')+  
CHLTYPE(SVRCONN) +  
TRPTYPE(TCP) +  
MAXMSGL(4194304) +  
MCAUSER('MUSR_MQADMIN') +  
RCVDATA(' ') +  
RCVEXIT(' ') +  
SCYDATA(' ') +  
SCYEXIT(' ') +  
SENDDATA(' ') +  
SENDEXIT(' ') +  
SSLCAUTH(REQUIRED) +  
SSLCIPH(' ') +  
SSLPEER(' ') +  
KAINT(AUTO) +  
MONCHL(QMGR) +  
REPLACE
```

# External Defense: A Multi-Layered Security Strategy



- What is the security equivalent of High Availability?
  - In the above diagram, the outer layer of defense can protect an inner system that has temporarily become vulnerable.
  - The attacker needs to break through the hardened outer system before reaching an inner system.

# External Defense: A Multi-Layered Security Strategy

- A metaphor for Layered Defense Metaphor:
  - The guards on the main floor (outer defense) restrict access into the building.
  - A badge reader (inner defense) is more selective & controls access to inner systems.
  - Even if a floor's badge reader breaks:
    - Unauthorized personnel can't enter the building, & can't get to the vulnerable floor.
- A hardened gateway queue manager is the first line of defense
  - All external message traffic should pass through here
  - Remote queue definitions (plus security precautions OAM, SSL etc) can restrict external message traffic to authorized queues on internal queue managers)
    - Message level firewall
  - Deny connection information to outside systems
    - (IP address of inner systems, ports, channel names, ...)



# External Defense

- How much time and resources, do you have allocated for security?
  - How is it divided up among all your queue managers?
- Gateway queue managers enable more efficient targeting of resources.
  - Gateway queue managers are configured for heightened security.
    - Adding that extra security to all queue managers would be inefficient and impractical.
    - This queue manager needs the most careful auditing and the most stringent administration controls. This level of auditing and control would be impractical if used for every queue manager.
- This technique works well with automated security monitoring.
  - Strategy: Find/Fix vulnerabilities before an attacker can exploit them.
    - Find vulnerabilities faster with automated security monitoring
    - Delay the exploitation of a security vulnerability with a gateway QM



# Zone Defense (Internal Defense / Accident Prevention)

- Zone defense (block traffic between production and non-production)
  - Accidents have occasionally caused traffic between production systems and non-production systems (development, QA, DR)
- Metaphors
  - Controlling radio transmission in a blast zone
  - Quarantine Zones in a hospital
- How have you isolated production and non-production systems?
  - Non-production systems are more vulnerable than production systems
    - Non-production systems have more changes, less monitoring and fewer security precautions
- Do you use:
  - Separate subnets and/or firewall / routers for isolation?
  - SSL certificates/naming-conventions that prevent traffic between production and non-production systems?
  - BlockIP2? MQ Extended Security Edition? Other MQ Exits?
- Do you use MQ Client in production?
  - How do you prevent development from accidentally connecting?
- How do you handle security with Staging and DR systems

# Security Best Practices: MQ Risk Review Group

- Systems keep growing and need periodic review
  - New applications are added
  - New fields have stronger security requirements
    - Social Security Numbers, Credit Card information
  - New security standards are mandated (HIPPA, etc.)
- An MQ Risk Review Group should analyze new applications and scenarios
  - Does the new application require/warrant extra security?
  - A proactive approach to identifying and remediating risks
- This group should be a central point for MQ Risk analysis
  - Collect and analyze authorization event reports & incident reports
- Must meet on both a regularly scheduled and an as needed basis
  - New scenarios that require analysis
  - New mandates, new regulations, new technology
  - Expansion (new locations)
  - Incident analysis
  - Mentoring/Knowledge transfer



# MQ Security Practices *That Stand the Test of Time*

- Time is a key element of security strategies
  - Find/Fix vulnerabilities before:
    - an attacker can exploit them
    - an accident happens
  - Find vulnerabilities faster with automated security monitoring
  - Delay the exploitation of a security vulnerability with a gateway queue manager
    - Combining gateway QMs (layered defense) and automated security monitoring increase the odds that an attack will be detected before it succeeds
  - Decrease accidents with a zone defense
    - Prevent accidental traffic from reaching production
  - Keep defenses up to date with an MQ Risk Review Group



# MQ Support Pacs and Links

- Keep MQ Fix Pacs up to date:
  - <http://www-1.ibm.com/support/docview.wss?rs=171&uid=swg27006037>
- Save Queue Manager Support Pac
  - <http://www-1.ibm.com/support/docview.wss?rs=171&q1=mA1J&uid=swg24000673>
- SSL Check support Pac (Great time saver)
  - <http://www-1.ibm.com/support/docview.wss?rs=171&uid=swg24014179>
- BlockIP2
  - <http://www.mrmq.dk/index.htm?BlockIP2.ht>
- MQ Listserver
  - [MQSERIES@LISTSERV.MEDUNIWIEN.AC.AT](mailto:MQSERIES@LISTSERV.MEDUNIWIEN.AC.AT)

Email - [mqsecurity@prolifics.com](mailto:mqsecurity@prolifics.com)

# Hear Prolifics Present at the following IBM Sessions

## Monday, April 7

12:30 – 1:30 pm

### **WebSphere MQ Enterprise Security: A Series of Defenses to Withstand the Test of Time**

Session# 2726A

Room 113

## Wednesday, April 9

4:45 – 6:00 pm

### **End-to-End Enterprise SOA Implementation**

Session# 2290A

Room 116

## Thursday, April 10

10:30 am – 11:45 am

### **Defining a WebSphere Enterprise Service Bus SOA Approach to Enterprise Application Integration**

Session# 2291A

Room 115

4:45 pm – 6:00 pm

### **Case Study: Ensuring Service Availability and Scalability by Monitoring your SOA Solution**

Session# 2691A

Room 124

# Join Prolifics at our Booth for SOA Smart Talks

Monday, April 7

10:30 am

**Optimizing Order Management in an EDI World**

12:30 pm

**Making SOA a Reality for the  
Insurance Sector**

1:30 pm

**Showcasing the Prolifics 2008  
Award-Winning SOA Solution**

**Tuesday, April 8**

**12:00 pm**

**Solution Center Theater Presentation  
Prolifics Presents:  
“Smart-aleck SOA” – a Comedy Show**

Wednesday, April 9

10:15 am

**Automating Your SOA Software  
Development Lifecycle**

1:00 pm

**Getting PCI Compliant with SOA**

# 2008 IMPACT

## Questions & Answers

© IBM Corporation 2008. All Rights Reserved.

The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided

AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

AIX, CICS, CICSplex, DB2, DB2 Universal Database, i5/OS, IBM, the IBM logo, IMS, iSeries, Lotus, MQSeries, OMEGAMON, OS/390, Parallel Sysplex, pureXML, Rational, RACF, Redbooks, Sametime, Smart SOA, System i, System i5, System z, Tivoli, WebSphere, zSeries, and z/OS.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.