Beyond intrusion prevention

T.Rob Wyatt, IoPT Consulting
t.rob@ioptconsulting.com

Beyond intrusion prevention - Intermediate

Mention MQ security and most people think of SSL channels, user authentication and setmqaut commands. But the business drivers for security are confidentiality, integrity, and availability - abbreviated often as CIA. In that context things like intrusion detection, post-breach recovery, and forensic analysis are just as important as perimeter defenses. Attackers get through the perimeter every day. Would you know if that happened? What would you do? This session reexamines the MQ security controls you are already familiar with but in a new light. And it just might introduce you to a few new ones.

Agenda

- **A word about…**
- **Containing the blast radius**
- **The intranet is no place for a litter box**
- **A greater context for security**
  - Intrusion prevention
  - Intrusion detection
  - Mitigation
  - Incident response
  - Business continuity
  - Forensic capability

A word about security

- These slides reflect information available at the time of publication.
- With security, things change. Often quickly. Periodically check that you have the most current version of any reference materials.
- The latest version of this presentation will be posted at https://t-rob.net/links
- To be notified of updates via RSS or by email, subscribe at the web site

A word about IoPT

T.Rob left IBM to form IoPT Consulting in 2013.

The firm offers…

- **The same MQ consulting services as before**
  - Security (of course!)
  - Architecture
  - High Availability
  - Upgrades
  - HA/DR
  - Troubleshooting
  - Staff Augmentation
  - Much more
- **Conventional + retainer engagements**

MQ Security Guy

704-443-TROB (8762) https://ioptconsulting.com

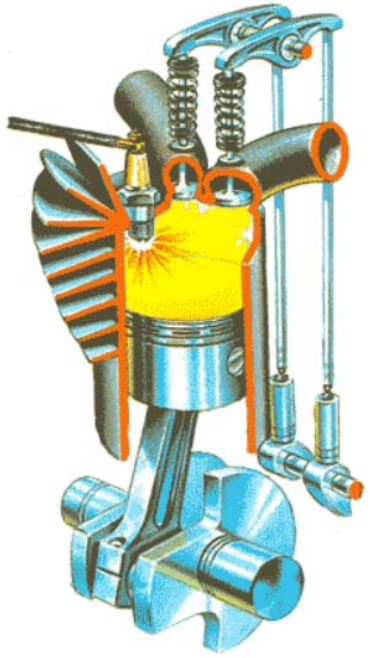
Containing the blast radius

A brief but memorable example of the detrimental effects of focusing on primarily intrusion prevention can be illustrated by examining a single aspect of the effects of a breach, specifically that of the potential scope of the compromise contrasted across two different approaches as we consider the highly technical term of the art

“blast radius.”

Containing the blast radius

If properly controlled, blasts can be made to work in our favor.



Containing the blast radius

An uncontrolled

blast will almost

Certainly

NOT

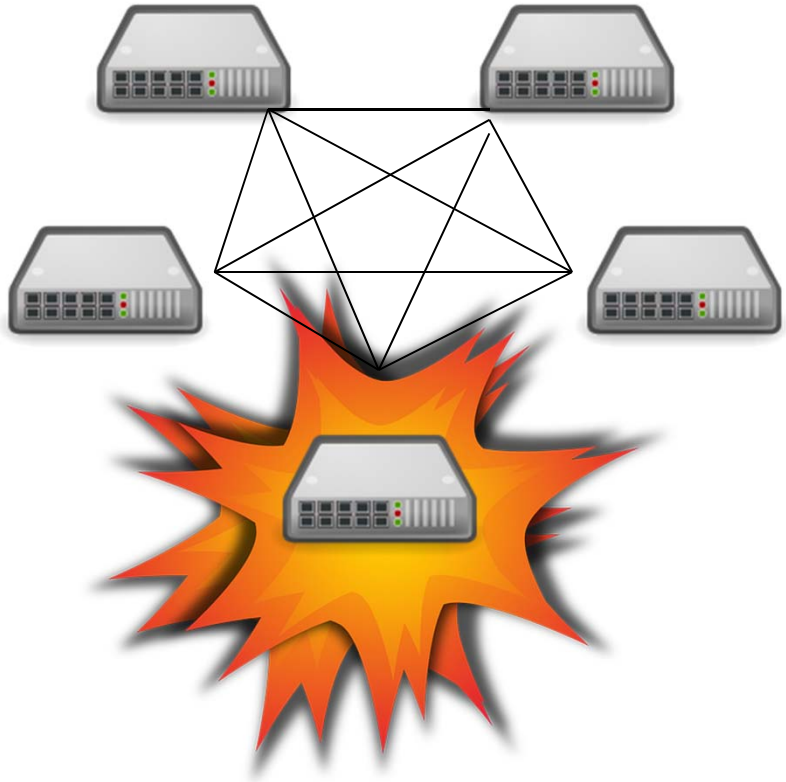
be in our favor.

Portrait of the author as a young man

Containing the blast radius

Or in network terms…

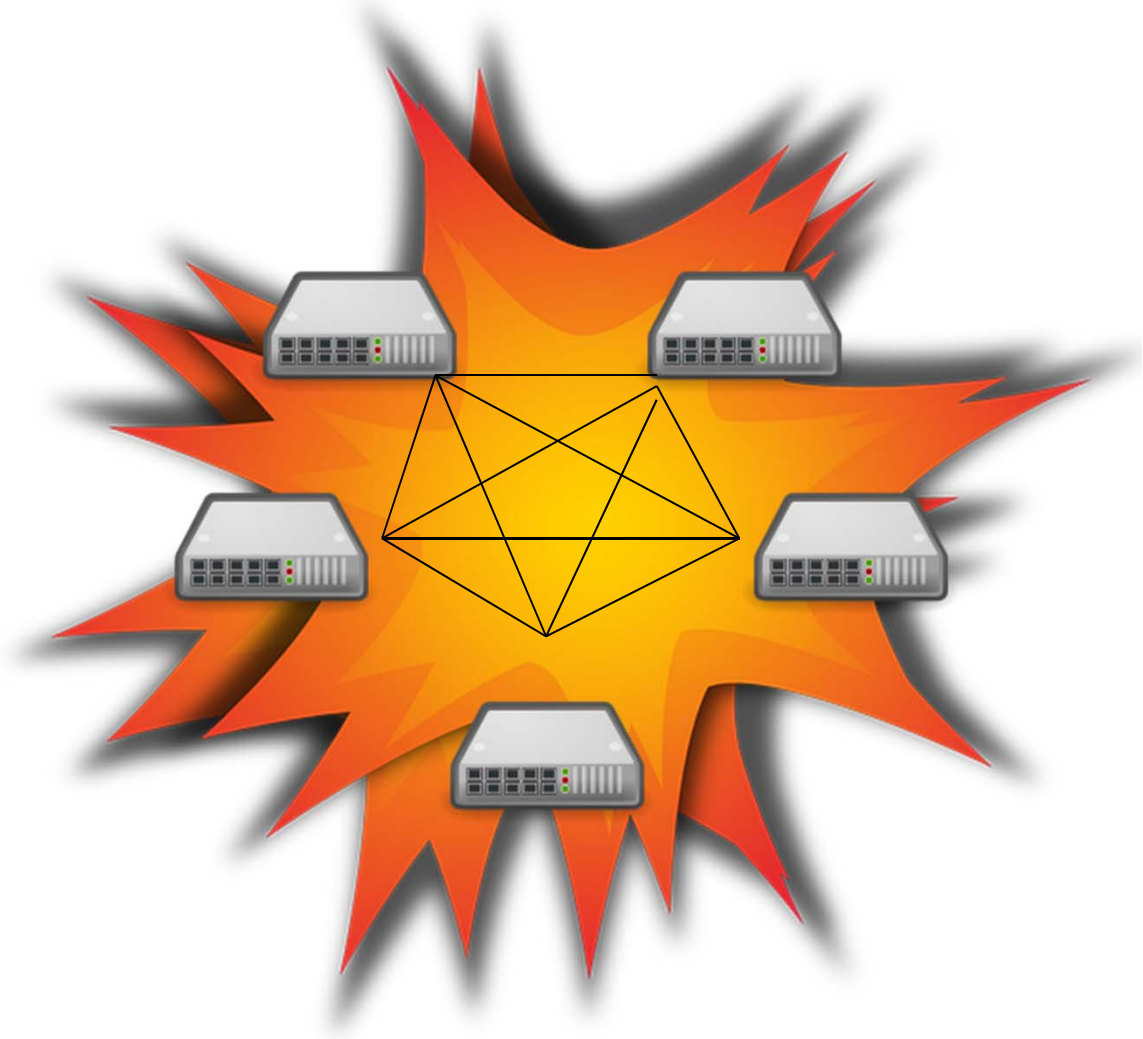
This is Bad.



Containing the blast radius

But this

Is worse.



However, this is the most likely outcome in many shops.

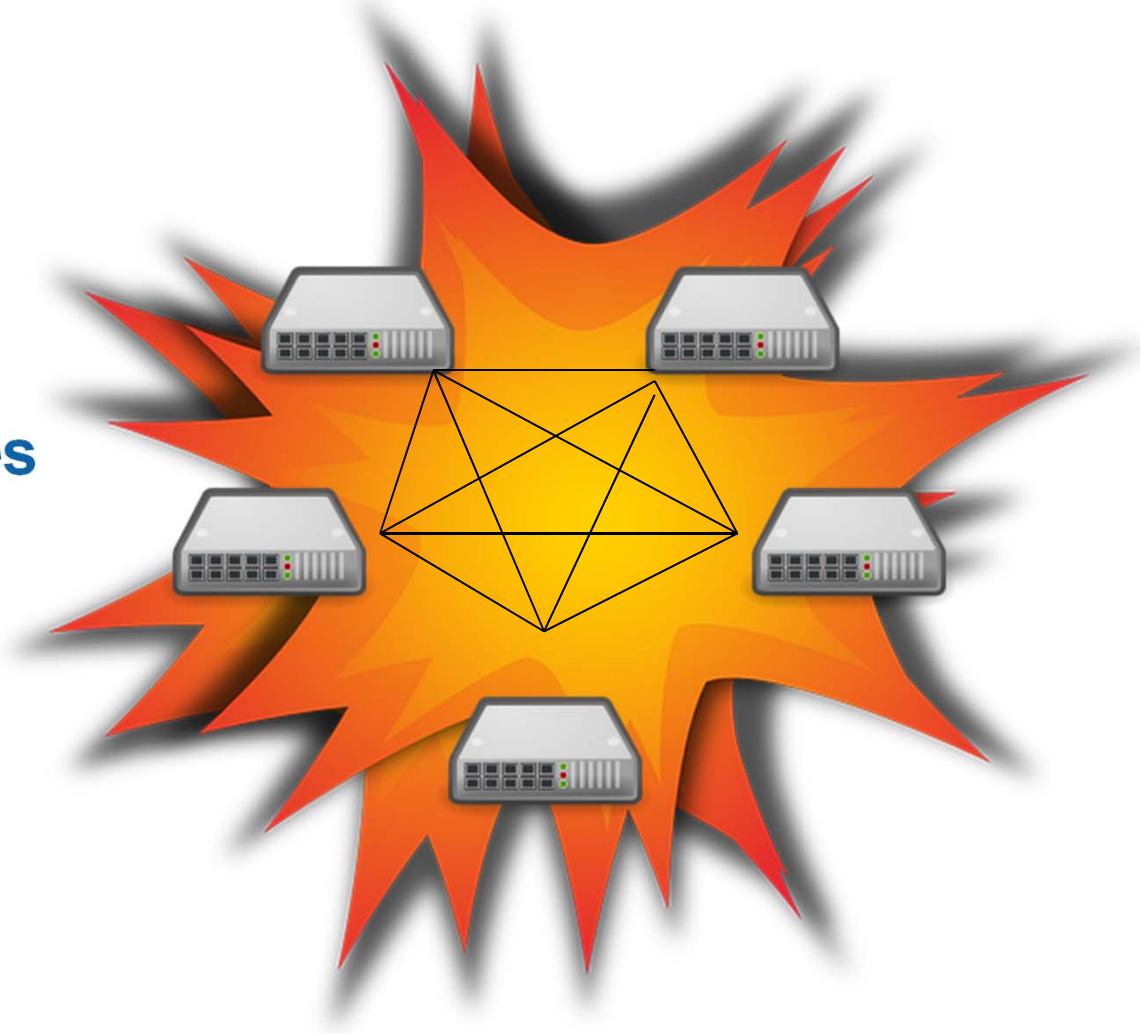
Is yours one?

Containing the blast radius

Intrusion prevention assumes that the perimeter can be protected.

All the other approaches we will cover today assume that it can't.

What is the impact of either of these assumptions being wrong?



A greater context for security

Blast radius containment (mitigation) is just one example of thinking beyond basic intrusion prevention.

Let's look at some others.

A greater context for security

Focusing primarily on intrusion prevention results in security with a hard outer shell and a soft gooey center.

Solving the “soft gooey center problem” is best approached from the business requirements, beginning with the CIA Triad:

- Confidentiality
- Integrity
- Availability

A greater context for security

In an operational context, security is a range of capabilities

- **CIA: Intrusion prevention -** Your configuration baseline, privilege escalation prevention, authentication, access revocation, secure configuration provisioning
- **CIA: Intrusion detection –** Alerts/reports on baseline variance, SSL/channel activity, 2035 events, change detection, unusual activity
- **CIA: Mitigation -** Blast radius containment at the network, QMgr, and object levels; agility to isolate, reconfigure and route around affected nodes
- **CIA: Incident response -** Reduced time-to-alert and time-to-contain, powerful administrator tools, training, planning, practice
- **CIA: Business continuity -** Retroactive configuration cloning, HA/DR, capacity planning, robust application and network design
- **CIA: Forensic capabilities -** Audit log analysis, QMgr log analysis, historical reporting

Intrusion prevention

Most MQ security deployed is of this variety. It is probably the strongest link in your security chain so we will skip it for this discussion.

Intrusion detection

When (not “if”) there’s an incident, how would you know?

- **MQ event messages, alerts and other instrumentation, of course.**
- **Baseline variance report and alert – deviation from expected configs.**
  - Especially when the deviation shows that some mitigations have been disabled.
- **DEFXMITQ – Never used for legitimate traffic, sends unrouteable messages to a dedicated QMgr where they trip alarms.**
  - Added benefit of preventing data leakage back to attacker based on channel retry.
- **Log rollover rate – Unusual activity in the transaction or error logs.**
  - MQ tells you about tx log activity, but not about error log activity. RFE time?
- **Subscribe to system notifications.**

Intrusion detection

- **REVDNS – As horribly broken as this is, the nature of the defect makes it useful for intrusion detection.**
  - Requires logging of the DNS requests made by the QMgr using tools external to MQ.
- **Honeypot – Set up unused channels and track start attempts.**
  - P2P channels to honeypot QMgrs that should never be legitimately used.
  - XMitQs with names like TXNHUB or ADMINQMGR are useful.
  - Objects with well-known names are the best honeypots.
- **Log channel start/stop events and activity reports.**
  - Unusual channel activity might be an errant app or it might signal an intrusion.

Mitigation

Design to contain the blast radius in the event of a breach.

- **Encrypted channels**
  - Provides authentication and integrity in addition to privacy of data in transit.
  - Limits intruder's knowledge of the QMgr until *after* the TLS handshake.
- **MCAUSER(*NOBODY) on every inbound channel. Map to a low-privileged account during authentication.**
  - In particular, no QMgr should be able to administer another.
  - For non-repositories, only the repository is granted access to put messages to the cluster command queue. Requires a service account to represent the repositories.
- **Dedicated full repositories.**
  - Segregate management and application traffic.
  - Can isolate compromised nodes from the cluster without shutting down the cluster.

Mitigation - continued

- **Dedicated per-application listeners, channels, queues, etc.**
  - The more sharing of resources, the greater the impact of a breach and the harder it is to isolate the compromised components.
  - Consider dedicated listeners, channels for Administrators.
- **Reasonable limits on MAXMSGL, MAXUOW, MAXHANDS, etc.**
  - Typical reaction first time hitting MAXDEPTH is to increase it across the board to a number that the underlying file system cannot possibly support. Soft limits are there to protect you. They are not “training wheels” but there for advanced users to tune.
  - Reduce MAXDEPTH on the DLQ since its default make a convenient DOS vector.
- **What, no dead letter queue?**
  - Removing the DLQ for external-facing channels makes the channels stop if there’s an error. Assuming they are instrumented to alert, that’s a Good Thing.
- **Advanced Message Security**
  - Establishes a per-message perimeter for integrity, authorization policy.
  - Prevents data leakage in logs, dumps, memory, FDC files, traces, etc.

Mitigation - continued

- **Tighten permissions in the underlying file system**
  - Executables, config files, keystores, start/stop scripts
- **Revoke access and authorizations**
  - Ideally, revocation of human users is automatic unless reviewed and approved.
  - Reconcile and report authorization rules against non-existent IDs, groups.
- **Penetration testing**
  - Pen testing validates the design and builds skill.
  - Your most effective mitigations will be against the elements that are pen tested.
- **Disallow unrestricted outbound access from the MQ server node**
  - MQ is designed to move bulk data as quickly, efficiently and silently as possible. Should the QMgr really have unrestricted outbound access to hackers-r-us.com?
- **Apply policy using B2B exit from Secure Scenarios Redbook**
  - Disable report options.
  - Set MQMD.UserID from MCAUSER value.

Incident Response

The barbarians have breached the gates! Now what?

- **The ability to respond effectively and in real time to an incident corresponds directly to the quality of administrative tools available.**
  - Command-line only? WMQ Explorer? Go get coffee. Might be here a while.
- **Design for incident response.**
  - Ability to isolate and/or relocate applications and resources dynamically.
  - Account for Recovery Point & Recovery Time Objectives in the design.
  - Clustering, DR featured of MQ are particularly helpful.
- **Best to have a plan prepared in advance.**
  - Each participant must know their roles and responsibilities in advance.
  - Practice the plan, evaluate and refine.

Business Continuity

The show must go on, but only if you design for it.

- **Data breach should be among the scenarios for which Disaster Recovery contingencies are designed and planned.**
- **Data breaches differ from other disasters in that they spread.**
  - The intrusion must be isolated and contained.
  - Need to be able to verify that the DR assets have not been breached as well.
  - Automated validation of the DR environment was always a good idea, in a breach scenario it is mandatory.
  - Another reason to start DR with an empty QMgr and not replicate data.
- **Understand and plan the granularity of isolation and failover.**
  - Entire datacenter? MQ network or subset? Per-QMgr? Per app? Per MQ object?
- **How does MQ participate in the DR and breach incident plans of apps?**

Forensic capability

Welcome, new CCSI! (Computer Crime Scene Investigator)

- **Archive rather than delete FDC files**
- **Capture error logs as they roll off**
  - Bumping the max size of the files reduces their rollover rate.
  - You'll need to supply the tools for this.
- **Capture and log/archive configuration events**
  - Even if they are not reviewed routinely, they are helpful for post-breach analysis.
- **Track changes to file permissions, configuration files, keys, etc.**
  - Changes to these should be rare and within approved change windows.
- **Build-time and run-time configurations have different requirements.**
  - Don't assume that run-time changes are routine! Is that new clustered queue instance legitimate? Because it's getting 1/5 of the traffic.

Effective security works as a system

Which of the following can you safely omit from your security program?

- **Intrusion detection –** What types of breach would you detect and how quickly?
- **Mitigation –** How quickly and easily could an attack spread? What controls are in place to isolate different applications, users and nodes?
- **Incident response** – Could a suspected breach be confirmed quickly? Would staff know who to contact and what to do?
- **Business continuity** – For each node and component in the network is there a plan for how to isolate it and quickly replace its function if it is compromised?
- **Forensic capabilities** – What assets are in place to track security relevant events to their source if you had one today?

Questions & Answers