Revisiting Network and Security Architecture in the Virtual Era

Jay Bazzinotti
Product Manager
Park Place International

Jim Fitzgerald
EVP
Park Place International
What are your organization’s top three information security priorities for the coming year?

- Improving regulatory compliance efforts: 55%
- Improving security awareness/education: 45%
- Preventing and detecting breaches: 34%
- Implementing log management and event monitoring: 32%
- Updating business continuity/disaster recovery plan: 29%
- Encrypting mobile devices: 27%
- Implementing identity and access management: 24%
- Encrypting electronic health records: 21%
- Developing a breach detection and notification plan: 20%

Source: HIMSS/CHIME 2014
In case you aren't sure about this session...

We are setting up this task to inform you of a certain hardware configuration which may make it possible for a patient to be presented with data within the portal that belongs to a patient other than themselves. This task will continue to be updated to provide you with the status on this issue and details on the deployment of changes to address. This issue has been determined to impact all 5.x and 6.x customers utilizing Patient Portal and Mobile Rounding. If your facility also uses MEDITECH’s Mobile Rounding application, a separate Mobile task is being set up with details as to how this issue can manifest itself while in Mobile Rounding.

In a more technical explanation, the TCPService listener thread will forward a request to the M-RT process and then wait for a response, listening on TCP with a 60s timeout. If the timeout occurs due to the application taking > 60s to respond we send a timeout error page to the user. However, the M-RT process is still forming the response and will eventually send that response over TCP. Due to the multiplexing, this delayed response can mistakenly be interpreted as the response to another user’s request.

This would only happen if a site has a multiplexing device in front of the web server where requests from different users are funneled into a single Web server connection and therefore handled by the same listener thread.

Still evaluate adding change in the event your organization uses multiplexing in the future. Your server team should be able to determine if this is the case. MEDITECH does not have the access to these settings.

If this configuration exists at your facility until the changes to address above are delivered, the short term and immediate solution to this issue can be resolved by turning off multiplexing.

If turning off multiplexing is not an option due to the effects it may have on other non-MEDITECH applications then MEDITECH can evaluate making a code change in IVEF that will resolve this issue.

Where this is encountered during typical Patient Portal usage, due to the potential impact on the hospital, should this issue occur, we felt it necessary to inform you of the issue and strongly recommend delivery of the changes to address.

This issue can occur under the following circumstances:

Prerequisite: Site must be configured to use multiplexing.

1) Patient A and B log into patient portal at the same time.
2) Patient A’s session timed out.
3) Patient B is presented with the screen that Patient A was viewing.

The issue affects all data found within the Patient Portal.

Detectability: This issue will not be detectable to the hospital or to the individual whose information is exposed. The patient receiving the incorrect data in error will be able to clearly see that the information belongs to another patient; however, at this point the breach has already occurred.

We have ensured all necessary resources within MEDITECH to identify and resolve
Agenda

• Thinking About Security
• A Time-Tested Security Framework
• Security Infrastructure: This Year’s Template
• New (Virtual) Infrastructure/New (Virtual) Elements
• Setting Priorities
• Taking Action
• Q & A
Thinking About Security

• Security is a process, not a product
• “80 percent of all success is just showing up”
• Behavior is more critical to success than technology
  – Our customers and employees will work against us
  – *Quis custodiet ipsos custodes?*
• 100% secure is an impossible goal
  – You’re going to get beat
  – *Illegitimi non carborundum*
A Time-Tested Security Framework

• Authentication – *Are you who you say you are?*
• Authorization – *Should you be here?*
• Data Integrity – *no more, no less than intended*
• Non-Repudiation – *Who me?*
• Physical Control – *Dude, where’s my computer?*
**A Typical Network**

- **Insider Attack!**
  - Innocent intent
  - Revenge/alienation
  - Monetary/sabotage

- **Virtualized Env.**
- **AV/HIPS**
- **RADIUS/AD**
- **VPN/FW/IPS**

- **WAN**

- **Forgotten Modem**

- **Policy**
  - Explicit Rules
  - Awareness/Education
  - Social Engineering
  - Punishment/Reward

- **Physical Security**
  - Inventory
  - Hardening
  - Uncontrolled Access Devices

- **Physical Security**

- **Patch Mgmt**
- **Auditing Behavior**
- **Inventory Whitelisting Config Mgmt**

- **Attack!**
  - Activists
  - Org. Crime
  - Foreign Govt
  - 12 year old boys
  - Hacker for Fun/Profit
  - The NSA exploiting “Heartbleed”

- **VPN/FW/IPS**
- **AV/HIPS**
- **RADIUS/AD**

- **Watering Hole Attack**
- **Phishing**
- **Porn Sites**

- **WAN**

- **WoW Personal Email**
Outsiders vs Insiders

Number of Attacks

Outsiders ▶ Insiders

$ Loss From Attacks

Outsiders ▶ Insiders

Source: US Secret Service 2010
Achieving 100% Security

“God Himself could not sink this ship!”
- J. Bruce Ismay, Chairman, White Star Line on the security of passengers on the “RMS Titanic, 1912”
Setting Priorities for External Threats

• 80% of all success is just showing up
  – Change passwords from defaults/guessables
  – Patch regularly, manage configs
  – Keep AV licenses up to date
  – Harden servers
  – Reward vigilance
  – Institute policy
  – Train regularly
Setting Priorities for Insider Threats

- Update revocation lists and passwords
- Authorization/compartamentalization
- Responding to botched security attempts
- Change passwords frequently
- Social engineering
- Audit trails
Maintain Basic Virtualized Security

• Start with a KNOWN GOOD Gold image
  – Most security problems in V-environments come from replicated viruses and flaws
• Maintain strong management access controls
• Maintain up-to-date configs and patches
• Vigilance for unauthorized replications
• Inventory/Audit Control
• Integrated AV/HIPS
Jim Fitzgerald
Operational Security Triangle

- Policy
- Security Triangle
- Technology
- Processes and Culture
Defense-In-Depth

**Core Components**
- Policies/Procedures
- User Security
- Application Security
- Platform Security
- Network Security
- Physical Security
<table>
<thead>
<tr>
<th>Physical</th>
<th>Perimeter</th>
<th>Platform</th>
<th>Application</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Badged Access</td>
<td>Multiple ISP’s</td>
<td>Daily + Backups</td>
<td>MSO</td>
<td>MSO</td>
</tr>
<tr>
<td>CCTV Monitors</td>
<td>Multiple DNS providers</td>
<td>Replicas to SDC or Cloud</td>
<td>AD &amp; LDAP</td>
<td>Radius/AD</td>
</tr>
<tr>
<td>Guards</td>
<td>Exclusion Lists &amp; ACL’s</td>
<td>AV/AM</td>
<td>SAML for Web</td>
<td>Two-Factor Authentication</td>
</tr>
<tr>
<td>Access Logs</td>
<td>VPN’s</td>
<td>Virtual Edge Firewalls</td>
<td>SSO Integration</td>
<td>Thin or Zero Clients</td>
</tr>
<tr>
<td>Work Orders Required</td>
<td>Access and Event Logging</td>
<td>Vulnerability Management</td>
<td>(Reverse) Proxies</td>
<td>No Persistent Data on Client</td>
</tr>
<tr>
<td>Secure Areas</td>
<td>IDS/IPS</td>
<td>Patch Management</td>
<td>Virtual Application Firewalls</td>
<td>Physical Port Locking on Clients</td>
</tr>
<tr>
<td>Certified Workforce</td>
<td>Firewall(s)</td>
<td>Logs/SEIM</td>
<td>Virtual Clusters</td>
<td>User Profiles</td>
</tr>
</tbody>
</table>
Virtual Security Spans Data Center to Cloud

- Infrastructure focus
- Application focus
- Business focus

Low Governance → Enterprise Hybrid Cloud → High Governance

Virtualization

Hardware Appliances

Virtualized Security

Security as a Service

IT Production → Business Production → IT as a Service

Courtesy of VMware
Compliance in Private & Hybrid Cloud

- Increases complexity: additional layers require additional controls
- Increases the impact of any compromise
- Impacts roles and responsibilities
- Creates a new attack surface that must be hardened

Courtesy of VMware
Securing the Private/Hybrid Cloud

Platform Security
- Secure hypervisor architecture
- Platform hardening features
- Secure Development Lifecycle

Secure Operations
- Prescriptive guidance for deployment and configuration
- Enterprise controls for security and compliance

Virtualization of Security
- Virtualization-aware security
- Unique Advantage of virtualization
- Leveraging automation with compliance and security

Compliance Guidance
- VMware Compliance Framework
- Security & Compliance Industry Guidance
- VMware Partner Ecosystem
- Independent Auditor Validated Reference Architectures

Courtesy of VMware
HIPAA Compliance via Virtual Security

**Data Security**
- Discover sensitive data
  - Scans environment looking for sensitive data
  - Flags affected VM's

**Dependency Mapping**
- Map application environment
  - Show where the affected systems are connected
  - Identify relationships

**Offload Resources**
- Insert partner security services on demand
  - Offloads antivirus to one place on the Hypervisor

**Continuous Compliance**
- Ensure compliance
  - Ensure the hypervisor & VM's are configured to proper templates

**Data Segmentation**
- Creates logical trust zones
  - Automatically
  - Based on App (banking) segmented
  - Inter-vSphere “firewall”

Courtesy of VMware
Is Virtual Security Enough?

• Covers:
  – Encapsulated Virtualized Infrastructure (Networks, Storage, Compute, OS, Applications)
  – Borders between Virtual and Physical world:
    • VSphere to Physical Devices
    • Virtual Desktop to Physical Networks
    • VNets to Physical Networks
• Does Not Cover:
  – Physical Systems: (Networks, Storage, Compute)
  – Non-federated Virtual Environments
  – The Public Internet
Don’t Trust AND Verify
Jim and Jay
Summary: You’re Going to Get Beat

• A computer is attacked within 15 minutes, >than 2000 times per day (U of MD, 2012)
• Innocent or nefarious insiders will let you down
• Poor code design ("Heartbleed") will undermine your best efforts
• Unscrupulous Government Entities (theirs AND ours) will seek an advantage
• If we are to get beaten we should at least make the attacker EARN IT.
Open Discussion
Other MUSE Sessions by PPI

1094 - Virtual Desktop Infrastructure – Lessons Learned for a Successful Deployment
Presenters: Matt Donahue, Leo Maguire, Samuel Mata, Park Place International, and Annette Ballard, Murray-Calloway County Hospital, Murray, Kentucky
Wednesday May 28 at 11:00 am

1100 - MEDITECH Technical Systems Update 2014
Presenters: Jim Fitzgerald, Joseph Kelly, Mark Middleton, Rob Bruno, Leo Maguire, and Samuel Mata, Park Place International
Thursday May 29 at 8:30 am

1099 - Revisiting Network and Security Architecture in the Virtual Era
Presenters: Jim Fitzgerald and Jay Bazzinotti, Park Place International
Thursday May 29 at 2:30 pm

1095 - Build a Reliable Infrastructure for Patient Care
Presenters: Matt Donahue, Park Place International and Michael Martz, Meadville Medical Center, Meadville, Pennsylvania
Friday May 30 at 9:30 am
Additional Resources

• PPI Blog “Sustaining Healthcare IT”
  – http://parkplaceintl.com/blog/

• MEDITECH Connect
  – http://meditechconnect.com/group/park-place-international

• Contact us
  jay.bazzinotti@parkplaceintl.com
  james.fitzgerald@parkplaceintl.com