OSS Security
“What you need to know”

Callum Barclay
CTO and Founder
Computer Security Products Inc.
About CSP

- Based in Toronto, Canada with Partners, Agents and Distributors worldwide
- NonStop® Alliance One Partner since 1987.
- Develop, Support and Distribute Security, Compliance and Audit Solutions for the HP NonStop® Market.
- Large number of Customers and over 1000+ licenses World Wide

Customers include:
- Largest Banks
- Major Stock Exchanges
- Defense and Healthcare organizations
- Telecommunications
- Manufacturers
Agenda

- Current applications in OSS
- What people told us about OSS security
- OSS Specific Security Settings
- Procedures and tools
- CSP – How we can help OSS users
Applications in OSS

- NonStop Web services related:
  - SOAP
  - iTP Web server
  - JSP, JBOSS, Spring, Apache C
  - SQL/MX
Applications in OSS

3rd Party:
- Base24 EPS (TSS)
- Lusis Tango
- ReD Fraud
- IBM MQ
- GGS
- AJB
- LIG
- Others....
OSS Security Survey Results:

- Survey sent to 369 Users, -> 73 competed surveys.
- 82% using or planning to use OSS
- Most popular are SQLMX and IBMMQ
- 90% though it important or critical to have a secure OSS environment
- A plethora of security strategies!!
OSS Security Survey Results (cont’d)

- Over 43% said it would be difficult or very difficult
- Yet over 80% want better granularity and visibility of OSS security settings!
- Primary concerns: Lack of knowledge or difficulty of integration with existing schemes.
- Room for Improvement:
  - Visability
  - Command Control and auto-elevation of privilege
- NonStop-X??
NonStop system security context

- Safeguard Globals
- OSS specifics:
  - Filesets
  - User and admin access
  - Default shell and file permissions
  - Audit setup
Define and control access to OSS by users.

- Set default directories
- Security-OSS-Administrator group: allows the delegation of file permission management
- Set audit parameters

Safeguard is configured with super user under the following parameters:

- AUTHENTICATE-MAXIMUM-ATTEMPTS = 4
- AUTHENTICATE-FAIL-TIMEOUT = 60 SECONDS
- AUTHENTICATE-FAIL-FREEZE = ON
- PROMPT-BEFORE-STOP = ON

- PASSWORD-REQUIRED = ON
- PASSWORD-HISTORY = 3
- PASSWORD-ENCRYPT = ON
- PASSWORD-MINIMUM-LENGTH = 4
- PASSWORD-MAXIMUM-LENGTH = 30
- PASSWORD-ALGORITHM = HMAC256
- PASSWORD-COMPATIBILITY-MODE = OFF
- PASSWORD-UPPERCASE-REQUIRED = OFF
- PASSWORD-LOWERCASE-REQUIRED = OFF
- PASSWORD-NUMERIC-REQUIRED = OFF
- PASSWORD-SPECIALCHAR-REQUIRED = OFF
- PASSWORD-SPACES-ALLOWED = ON
- PASSWORD-ALPHA-REQUIRED = OFF
- PASSWORD-MIN-MINIMUM-QUALITY-REQUIRED = 0
OSS Filesets

- OSS filesets – analogous to the Unix “mount” operation, with NonStop OSS specifics.
- Managed through SCF:
  - Audit set ON if needed.
  - Access options:
    - Lock–out SUPER.SUPER.
    - Make read–only.
Audit in OSS

- Set by fileset
- Set ON for Security–OSS–Administrator.
- Turn on the OSS Client audit in Safeguard
- Warning: injudicious audit settings may overwhelm your audit pool...
Access Rights for OSS files

- Not subject to Safeguard rules.
- Secured using Unix like permission strings:

<table>
<thead>
<tr>
<th>Owner</th>
<th>Group</th>
<th>World</th>
</tr>
</thead>
<tbody>
<tr>
<td>r w_x</td>
<td>r w_x</td>
<td>r w x</td>
</tr>
</tbody>
</table>

- Options for setuid, setgid etc.
- Managed with chmod, chown, chrgrp commands.
OSS Basic Permissions

- OSS uses the Unix format (owner/group/world)
- Don’t rely on the defaults!
- Common issues (just like Guardian):
  - Orphan Files
  - Excessive Privileges
  - Files Accessible to all users
- How are you checking yours?
Visibility and reportability

The three categories (owner/group/world) are sometimes not granular enough.

Managed from the command line and/or scripts
OSS Extended ACLs

- Recommended by HP to provide improved granularity.
- Based on the HP-UX implementation.
- Allow for:
  - specific permissions for users/groups on files/directories.
  - default ACLs on directories
- Managed with setacl, and viewed through getacl.
- Awkward to set and to read.
- Just like Safeguard ACLs, these can get messy very quickly...
Safeguard

Fileset

File Security

Application

-Globals
-Users
-Security Groups
-Audit management

-Restrict access
-Audit enable

-Basic permissions
-Extended ACLs
-Setuid/setgid

-Application access rules
-Log management
Ongoing OSS Compliance

- Data collection
- Batch
- Interactive

- Compliance
- Permissions
- Change

- Monitor
- Alarm

- Globals
- Users
- File perms & acls

- Report
- Merge
- Forward

Snapshot
Correct
Analyze
Events
CSP Tools for the task:

- **Initial Snapshot:**
  - Protect–UX – Capture and visualize file permissions
  - File Integrity Checker (FIC): Monitor Files for changes.
  - Set up monitoring and event streams with Alert–Plus and Auditview for merged Audit.

- **Ongoing:**
  - Snapshot the directory tree and check contents for changes (log files OK)
  - Review for erroneous or excessive privilege, Orphan files, etc.
Protect-UX – a closer look:

Protect-UX Fileset Macros (user-defined or templates) automates file management tasks based on attribute or name, to:

- discover current state
- apply settings or actions.

Protect-UX Master Node is used to store policies files, credentials etc.

List matching files

...and/or apply changes.
Protect-UX Policy is used to manage files for an application deployed on multiple systems with:

• Automated implementation
• Review and analysis tools

Protect-UX Master Node is used to store policies files, credentials etc.

Application X

Application X

Application X
File integrity monitoring is a crucial requirement of PCI. It includes checking of:
- MD5/MD5-Inc
- File Type
- Last Modified
- Status Changed
- Owner
- Security Type
- Safeguard
- Security Mask
- Group
- Set UId
- Set GId
- EOF (also EOF Incremental)
Let’s look a specific example: IBM MQ

- **Pre-installation:**
  - Adding the user and group mqm.mqm
  - Ensure the initial location permissions are open
  - Create a fileset (if necessary) to contain files.

- **Post-installation:**
  - Snapshot the directory tree and contents
  - Review for erroneous or excessive privilege
  - Set up monitoring and event streams
CSP Protect XP: Add the user and group
## FIC - Create Snapshot

**Show Check Results, category: ALL**

<table>
<thead>
<tr>
<th>Fileset Name</th>
<th>Check Type</th>
<th>Comment</th>
<th>Fileset Record Count</th>
<th>Number of Fails</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/mqm/<em>/</em></td>
<td>File Type ...</td>
<td>4</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>/var/mqm/*</td>
<td>File Type ...</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>/var/mqm/qmgrs/<em>/</em>:ini</td>
<td>MD5</td>
<td>4</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**Object Name**

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Result</th>
<th>Last Function</th>
<th>Check Type</th>
<th>Last Updated</th>
<th>Change</th>
<th>Filter by Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/mqm/qmgrs/@SYSTEM/mq:....</td>
<td>Pass/No Difference</td>
<td>Base</td>
<td>MD5</td>
<td>2015-02-05, 17:08:26</td>
<td>super-b</td>
<td>All</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/@SYSTEM/proc:....</td>
<td>Pass/No Difference</td>
<td>Base</td>
<td>MD5</td>
<td>2015-02-05, 17:08:36</td>
<td>super-b</td>
<td>All</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/@SYSTEM/qm:ini</td>
<td>Pass/No Difference</td>
<td>Base</td>
<td>MD5</td>
<td>2015-02-05, 17:08:45</td>
<td>super-b</td>
<td>All</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/@SYSTEM/qnp:....</td>
<td>Pass/No Difference</td>
<td>Base</td>
<td>MD5</td>
<td>2015-02-05, 17:08:53</td>
<td>super-b</td>
<td>All</td>
</tr>
</tbody>
</table>

Filter by Result: **All**

Entries: 4 | No Status Filter available | Check Type: MD5
Change detection

- Email alert of a change
- Detailed change history in FIC
- Auditview audit trail report
Verifying the permissions

<table>
<thead>
<tr>
<th>Full Path Name</th>
<th>Size</th>
<th>Permissions</th>
<th>Owner</th>
<th>Group</th>
<th>Date modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/mqm</td>
<td></td>
<td>drwxr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:07:15 PM</td>
</tr>
<tr>
<td>/var/mqm/@SYSTEM</td>
<td></td>
<td>drwxr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:16:34 PM</td>
</tr>
<tr>
<td>/var/mqm/mqsi.init</td>
<td>6 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:06:46 PM</td>
</tr>
<tr>
<td>/var/mqm/proc.ini</td>
<td>7 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:06:58 PM</td>
</tr>
<tr>
<td>/var/mqm/qmgrs</td>
<td></td>
<td>drwxr-xr-x</td>
<td>MQM</td>
<td>MQM</td>
<td>2/5/2015 5:21:27 PM</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/@SYSTEM/mqsi.init</td>
<td>11 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/6/2015 10:38:52 AM</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/@SYSTEM/proc.ini</td>
<td>0 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:08:36 PM</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/@SYSTEM/qm.ini</td>
<td>7 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/6/2015 10:06:43 AM</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/@SYSTEM/qmgr...</td>
<td>0 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:06:53 PM</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/xxx</td>
<td>0 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:08:45 PM</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/ddd</td>
<td>0 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:08:52 PM</td>
</tr>
<tr>
<td>/var/mqm/qmgrs/xxx</td>
<td>0 b</td>
<td>r-xr-xr-x</td>
<td>MQM.MQM</td>
<td>MQM</td>
<td>2/5/2015 5:08:36 PM</td>
</tr>
</tbody>
</table>
Apply ACLs as needed
OSS application security requires a combination of:

- System settings (Safeguard, fileset etc.)
- File permission validation and control
- Change detection and management
- Event and audit review
- Application specifics (e.g. for MQM the internal authorization settings etc.)

You can do it all with native tools, but...
CSP Solutions deliver:

- Manage and review Safeguard settings easily.
- Apply permission templates from a GUI console.
- Establish baseline and snapshot views of your OSS environment with regular checks.
- Review and verify settings and file attributes as needed.
- Alerts, reports and correlation of OSS events.
2015 enhancements to Protect-UX

- Improved Product Work Flows.
- OSS Command Control.
- Implement an HTML5 based web interface.
- Optional Authorization Streams.
Thank you!

Questions?