Hewlett Packard Enterprise

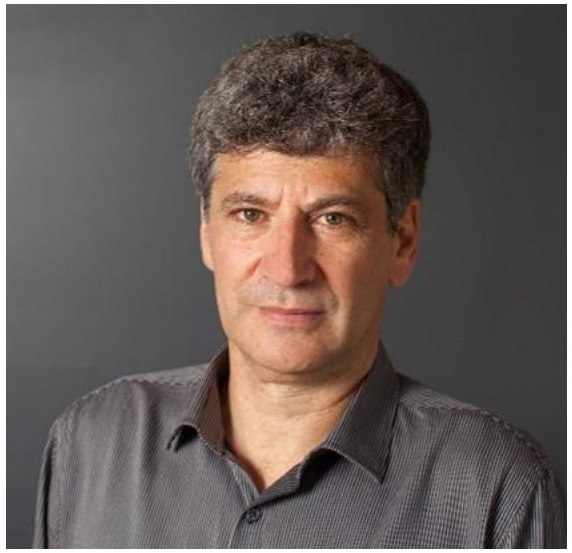
PCI DSS 3.2 and How You Can Achieve That on your NonStop Environment

Greg Swedosh, Security Specialist, Knightcraft Technology

Agenda

- Introduction
- PCI DSS 3.2 changes affecting NonStop
- Compliance vs Security
- What's really needed for compliance and security on HPE NonStop

Introduction



Greg Swedosh

Knightcraft Technology
Information Security Specialists

- Owner and senior security consultant of Knightcraft Technology.
- Working on HPE NonStop systems since 1985 (Tandem Australia).
- Providing professional services to HPE NonStop customers for 20 years.
  - Australia, New Zealand, UK, USA, Singapore, Japan, India, Indonesia, Malaysia
  - Banks and financial institutions, large retailers, telcos, governments
- HPE NonStop Security and PCI DSS Compliance Specialist.
- Hands on implementation expertise in Safeguard, XYGATE, comForte.
- Performed PCI DSS assessments on behalf of a QSA.
- Regular presenter on security at HPE NonStop Advanced Technical Bootcamp.
- Author of "*PCI DSS Compliance for HPE NonStop Servers*" white paper.
- Knightcraft security and compliance services are available through HPE SDI.

PCI DSS 3.2

What's changed that affects HPE NonStop?

PCI DSS 3.2 – Major changes affecting HPE NonStop

SSL/TLS

- SSL and early versions of TLS are vulnerable to the POODLE exploit.
- PCI DSS mandates a move to TLS 1.1 or higher for encryption of data in transit.
- Implementation deadline is **June 2018**.

Multi-Factor Authentication

- All non-console privileged access to the system must be authenticated using Multi-Factor Authentication.
  - Something you know (e.g. passphrase)
  - Something you have (e.g. token)
  - Something you are (e.g. fingerprint)
- Best practice recommendation until 31 January 2018.
- Required from **1 February 2018**.

Defining CDE

- Tighter rules around definition of Cardholder Data Environment (CDE).
- Required as of PCI DSS 3.1.
- Assessed as part of the ROC.

*** As of October 2016, all PCI DSS assessments will use version 3.2**

SSL/TLS on the HPE NonStop

“Entities using SSL and early TLS must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don’t already exist.”

PCI DSS v3.2 Appendix A2

SSL/TLS on the HPE NonStop

- PCI DSS Requirement A2 details additional PCI DSS requirements for entities using SSL/Early TLS.
- There are a number of places where SSL/TLS may typically be used. Some examples are as follows (note that this is not a definitive list):
  - Terminal emulator sessions (TACL, OSH) via NonStop SSL or vendor products.
  - Secure FTP sessions via NonStop SSL or vendor products.
  - iTP secure Webserver.
  - Connections to virtual tape devices such as VTS or VTC.
  - Communication lines between corporate entities (interchange links, file transfer links to mainframe).
  - Between the HPE NonStop and ATMs or POS devices.
- Wendy Bartlett is currently working on a white paper on TLS configuration across the HPE product line. Stay tuned for details of its release.

Multi-Factor Authentication and PCI DSS 3.2

“63% of confirmed data breaches involved leveraging weak, default or stolen passwords.”

Verizon 2016 Data Breach Investigations Report
http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

“Incorporate multi-factor authentication for all non-console access into the CDE (Cardholder Data Environment) for personnel with administrative access.”

PCI DSS 3.2 Requirement 8.3.1

Multi-Factor Authentication (MFA)

What is “Administrative Access”?

– Administrative access includes any userid or alias that has the capability of modifying the system in any way that may compromise the system’s security or cardholder data.

– On an HPE NonStop system, administrative access should apply to at least the following userids and aliases of those userids:

  – Super.super (Obviously!!)
  – All super group userids
  – Security administrator userid(s)
  – Application/Data owner userids
  – Application builder userids
  – Data replication owner ID
  – Netbatch administrators
  – Userids with the ability to modify system/subsystem/application startup or config files or objects
  – Any userids or aliases that have the ability to gain the privileges of any of the above userids using utilities such as XYGATE Access Control (XAC), SECOM, CSP Passport etc.

– All users of the above userids and aliases must authenticate using MFA for non-console access.

Multi-Factor Authentication (MFA)

Methods of authenticating to the HPE NonStop server

- MFA need not necessarily be implemented on the HPE NonStop platform. All of the following example methods of authentication are considered acceptable:
  - MFA at the time of logging on to the NonStop.
  - At the network level e.g. authentication as part of setting up a VPN prior to accessing the NonStop.
  - Authentication to a jump box from where the NonStop is accessed e.g. via a Citrix server.
  - Single Sign-On (SSO) using a mechanism such as Kerberos, as long as the initial sign-on has been authenticated using MFA.
  - SSH private/public keys with a passphrase. Note that while this method is likely to be accepted by a QSA as MFA, at least currently, it is potentially flawed due to the ability to store the passphrase within a terminal emulator.

Multi-Factor Authentication (MFA)

XYGATE User Authentication (XUA) and MFA

- XYGATE User Authentication (XUA) ships as part of the operating system in NonStop X commercial systems, otherwise available in the OS security bundle.
- Provides the ability to authenticate userids/aliases against a RSA Authentication Server.
  - Can be configured so that when a configured user is presented with the password prompt, they enter their known passcode and the number displayed on their SecurID token to authenticate.
  - Privileged userids using regular NonStop authentication should be configured to enforce two-step logon i.e. users must logon with their individual userid through MFA before being able to logon to super.super or other privileged userids (with the exception of sessions at the console). This approach provides accountability of all shared privileged userid sessions.
  - Configurable as to which userids/aliases are forced to use this mechanism and which userids/aliases use the regular NonStop logon mechanism.
    - For example: Individual userids/aliases configured to use RSA authentication. Users only able to logon to super.super and other privileged userids via regular logon after having already authenticated to their individual userid using MFA.
  - Works seamlessly in conjunction with NonStop SSH authentication mechanism.

Multi-Factor Authentication (MFA)

Privileged access via the console

– PCI DSS states that administrative access may be obtained to the system without MFA if logging in directly from the system console.

– This applies to console session where the user is physically sitting at the console in an access controlled and monitored environment.

– It **DOES NOT** apply to sessions where a user has remotely connected in to the console using Remote Desktop or other similar mechanism.

Defining the Cardholder Data Environment

“At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data”.

PCI DSS v3.2 Template for Report on Compliance, section 3.1

Defining the Cardholder Data Environment

- The template for Report On Compliance (ROC) section 3.1 is used by QSAs when performing a PCI DSS assessment. In reference to defining the cardholder data environment (CDE), it says that organizations must:
  - Describe the methods or processes used to identify and document all existences of cardholder data.
  - Describe the methods or processes used to verify that no cardholder data exists outside of the defined CDE.
- QSAs must:
  - Describe why the methods used for scope verification are considered by the assessor to be effective and accurate.

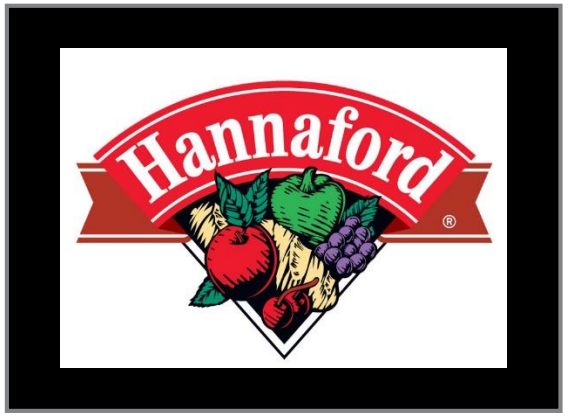
- This will likely result in a greater push by QSAs for organizations to use automated tools, to prove that cardholder data exists only where they have specified and that no cardholder data exists outside of the area defined.

The other major change in PCI DSS…

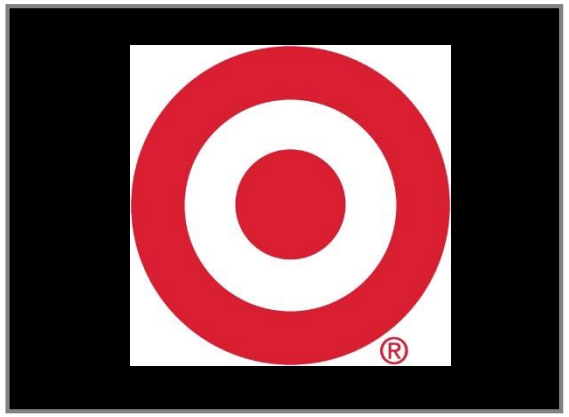
Perceptions of compliance vs security

These companies thought that they were PCI DSS compliant…

2007 - 45.6million customer payment card details stolen[1]



2008 – 4.2million debit and credit card numbers stolen[2]



2013 - More than 40million stolen payment card numbers as well as 70million PII records[3]

2014 - More than 50million cardholders' card and personal details stolen[4]

References:

1. http://www.computerworld.com/article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html
2. http://www.computerworld.com/article/2536801/cybercrime-hacking/hannaford-to-spend--millions--on-it-security-upgrades-after-breach.html
3. http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data
4. http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z

PCI DSS Compliance vs Security

Customers need to achieve and maintain both

We are PCI DSS compliant. Are our systems secure?

Many organizations seem to believe that if they are passed by a QSA as compliant with PCI DSS, then that means that their systems are secure.

This is not the case, as the high profile data breaches tell us!!!

We are PCI DSS compliant. Are our systems secure?

- PCI DSS is a **minimum** standard for security and auditing settings, procedures and documentation.
- QSAs (PCI Qualified Security Assessors) are typically not experts in HPE NonStop security. Many in fact know very little about the NonStop environment.
- PCI DSS assessments are typically based on a checklist, documentation and on responses from the customer. They are not an in-depth system security review.
- Staff may be tempted to withhold unasked-for information from QSAs so that the company is marked as compliant.

Given the above, how can compliance necessarily imply security?

We are PCI DSS compliant. Are our systems secure?

- The problem is not the PCI DSS itself. It is a robust and comprehensive platform on which organizations should base their security.
- At the time of data breaches, none of the organizations who were breached were actually compliant.
- The primary problem is in the periodic, snapshot-based assessment of organizations rather than the standard itself.
  - In the case of the HPE NonStop environment, this is often coupled with the QSA's lack of expertise on the platform.

Some examples of PCI DSS compliance

Requirement 3.4 – Protect all cardholder data

Cardholder data stored on encrypted volume using NSVLE

- Requirement 3.4 says that cardholder data (PAN) must be protected by suitable encryption or tokenization. Some customers are using NonStop Volume Level Encryption (NSVLE) to satisfy this requirement. However…
  - Once a user authenticates and logs on to a system where volumes are protected by NSVLE (NonStop Volume Level Encryption), the volumes are no longer encrypted to him or her.
    - Whether that user can read or modify the data relies completely on Safeguard protection records or Guardian security settings.
  - Requirement 3.4.1 states that there needs to be a method of authentication used, other than that used by the operating system. That is, when a user/program requires access to the encrypted volume, they should be authenticated by a mechanism other than the Guardian USERID file before gaining access. This is not the case with NSVLE.
  - Previous ACI documentation has indicated that customers can use NSVLE with BASE24 to comply with PCI DSS requirement 3.4.
  - Customers exist that are using NSVLE to protect their cardholder data and have been marked by a QSA as PCI DSS compliant, but the data isn't really encrypted at all to those who can logon to the system and have Safeguard access to it and is therefore vulnerable.

Requirement 3.4 – Protect all cardholder data

Compensating control using Safeguard security and password procedures

– When an organization can't meet a requirement, they can apply for a compensating control.

– Appendix B states that compensating controls must meet the intent and rigor of the original requirement, provide a similar level of protection and be above and beyond other PCI DSS requirements.

– A number of organizations to this point have used compensating controls to satisfy requirement 3.4.

– One large financial organization has successfully applied for a compensating control by stating that the cardholder data is protected by Safeguard so that only the application userid can access it and the application userid password is strictly controlled. They are apparently PCI DSS compliant.

However…

- The application userid is regularly used for support purposes.
- When the password is checked out, there is no control of when it is checked back in.
- There is no monitoring of the user sessions.
- This is non-compliant in a number of ways, but has been passed as compliant by a QSA.
- It is very very far from secure!!!

Real NonStop Requirements

For both PCI DSS compliance **and** security

To be truly PCI DSS compliant

A list of what HPE NonStop customers really need at a minimum

– Safeguard optimally configured to prevent unauthorized access and to provide auditing of file access.

– Security aspects of all subsystems configured to prevent users gaining unauthorized privileged access.

– XYGATE Merged Audit (XMA) installed and configured to deliver security events to a SIEM device.

– NonStop SSL/SSH implemented to provide encrypted TACL/OSH/FTPS sessions.

– XYGATE User Authentication (XUA) or alternate mechanism to provide individual accountability to all user logons (e.g. force users to logon to personal userid before logon to super.super).

– XYGATE Access Control (XAC) or similar ISV product to provide keystroke logging of user sessions.

– File Integrity Monitoring (FIM) software to detect any changes to critical files (application objects, system configuration files, startup/shutdown files etc.).

– Encryption or tokenization of cardholder data. This can now be achieved without changes to the application or database using tokenization (such as HPE SecureData) and intercept library based products such as cF Data Security or XYGATE Data Protection (XDP).

– Automated tool to verify that there is no unprotected cardholder data in unauthorized locations. Currently only PANfinder (4tech Software) provides this.

Further Information

A list of useful resources to assist with PCI DSS compliance and security

– *PCI DSS Compliance For HPE NonStop Servers* white paper (http://www.knightcraft.com/pci-dss-3.2)

– HPE NonStop TBC presentation *You may be PCI DSS compliant but are you really secure?* (http://www.knightcraft.com/2014-hp-nonstop-advanced-technical-boot-camp)

– HPE NonStop TBC presentation *Common HPE NonStop security hacks and how to avoid them* (http://www.knightcraft.com/common-hp-nonstop-security-hacks-and-how-to-avoid-them)

– HPE NonStop Security Hardening Guide (NonStop Technical Library)

– Upcoming TekTalk: Services from Knightcraft to help you secure your NonStop environment and comply with PCI DSS requirements – 26th October.

– Email greg.swedosh@Knightcraft.com

Hewlett Packard
Enterprise

Thank you

Contact information