PCI Assessments 3.0
What Will the Future Bring?

Matt Halbleib, SecurityMetrics
About Us

• Matt Halbleib
  – CISSP, QSA, PA-QSA
  – Manager PCI-DSS assessments
  – With SecurityMetrics for 6+ years

• SecurityMetrics
  – Security assessments, consulting, forensics, penetration testing
  – Vulnerability assessment scanning (ASV)
  – Compliance programs
Agenda

• A brief history on the PCI DSS
• PCI DSS 3.0 changes
• Top 10 assessment issues
• Compromise case studies
• Questions
PCI DSS & QSA History

• 2000 – 2003: Card brands have separate security standards
  – Security professionals involved in on-site assessments, no required training

• 2004 – 2005: Card brands agree on a security standard
  – Payment Card Industry Data Security Standard (PCI-DSS) version 1.0 is released in 2004
  – Security professionals conduct on-site assessments, first QSA training class in 2005

• 2006: PCI Security Standards Council (PCI SSC) is formed
  – QSAs required to attend annual training certification

• 2007: PCI DSS version 1.1 released
• 2008: PCI DSS version 1.2 released
  – First assessment report scoring matrix available to QSAs
  – Council begins QSA quality assurance program
• 2010: PCI DSS version 2.0 released
• 2011: New PCI DSS reporting instructions released
• 2013: PCI DSS version 3.0 released
• Since 2005 the assessment expectation bar has been raised significantly. It will continue to raise as the industry matures.
  – 2014 assessment report is 2–3 times bigger than a 2008 assessment report
PCI DSS Lifecycle

- PCI DSS has a 3-year lifecycle
- One year adoption grace period after new version released (January 1, 2015 3.0 compliance)
When Bigger Changes Occur

- PCI Council follows a well defined pattern when larger changes to the PCI DSS occur
- New requirement is added and deemed “best practice” until a sunset date
- After the sunset date the requirement must be adopted
- Ex:
  - PCI DSS v3.0: requirement 11.3 (Updated Pen Testing requirements) a best practice till June 30, 2015
PCI DSS 3.0 Changes

- Evolving requirements
  - Clarification
  - Additional guidance
- Document from PCI SSC detailing all changes
  (Available at: "www.pcisecuritystandards.org")
“It’s about making PCI compliance part of your business, not a once-a-year, study-for-the-test kind of thing.” {Bob Russo GM, PCI SSC}
## PCI DSS Assessment

### Testing & Reporting Procedures 2.0

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
<th>ROC Reporting Details (For in-Place Requirements)</th>
<th>Reporting Methodology</th>
</tr>
</thead>
</table>
| 1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. | 1.3.5 Verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized | • Identify the document that explicitly defines authorized outbound traffic from the cardholder data environment to the Internet.  
• Describe how firewall/router configurations were observed to allow only explicitly authorized traffic.  
• Describe how observed outbound traffic from the cardholder data environment to the Internet confirms that only explicitly authorized traffic is allowed. | ✓ ✓ ✓ |
| 1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.) | 1.3.6 Verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.) | • Describe how observed firewall configurations implement stateful inspection.  
• Describe how observed network traffic confirms that stateful inspection is implemented (that is, only "established" connections are allowed into the network). | ✓ ✓ |
| 1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. | 1.3.7 Verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks. | • For all system components that store cardholder data:  
  i. Identify the diagrams and/or other document(s) which define how system components are located on an internal network zone, segregated from the DMZ and other untrusted networks.  
  ii. Describe how observed network and system configurations confirm the system components are located on an internal network zone, segregated from the DMZ and other untrusted networks.  
  iii. Describe how observed network traffic confirms that the system components are located on an internal network zone, segregated from the DMZ and other untrusted networks. | ✓ ✓ ✓ |
PCI DSS Assessment
Testing & Reporting Procedures 3.0

<table>
<thead>
<tr>
<th>PCI DSS Requirements and Testing Procedures</th>
<th>Reporting Instructions</th>
<th>ROC Reporting Details: Assessor's Response</th>
<th>Summary of Assessment Findings (check one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.5.a Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.</td>
<td>Identify the firewall and router configuration standards document(s) reviewed to verify they include a description of groups, roles and responsibilities for management of network components.</td>
<td>&lt;Report Findings Here&gt;</td>
<td>In Place In Place with CCW N/A Not Tested Not in Place</td>
</tr>
<tr>
<td>1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.</td>
<td>Identify the personnel responsible for management of network components interviewed for this testing procedure.</td>
<td>&lt;Report Findings Here&gt;</td>
<td></td>
</tr>
<tr>
<td>1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.</td>
<td>For the interview, summarize the relevant details discussed to verify that roles and responsibilities are assigned as documented for management of firewall and router components.</td>
<td>&lt;Report Findings Here&gt;</td>
<td></td>
</tr>
<tr>
<td>1.1.5.a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.</td>
<td>Identify the firewall configuration standards document(s) reviewed to verify the document(s) contains a list of all services, protocols and ports necessary for business, including a business justification for each.</td>
<td>&lt;Report Findings Here&gt;</td>
<td></td>
</tr>
<tr>
<td>1.1.5.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.</td>
<td>Identify the router configuration standards document(s) reviewed to verify the document contains a list of all services, protocols and ports necessary for business, including a business justification for each.</td>
<td>&lt;Report Findings Here&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.

If "yes," complete the instructions below for EACH insecure service, protocol, and port allowed: (add rows as needed).

- Identify whether any insecure services, protocols or ports are allowed. (yes/no)
- Identify the documented justification.  
  <Report Findings Here>
Change in Scope

• In-scope system components:
  – Systems providing security services
  – Facilitate segmentation
  – Impact security of the CDE

• Web redirection servers
Man-in-the-Middle Attack

- Merchant Website
- Merchant Shopping Cart
- 3rd Party Payment

Website Redirection Server

Attacker Data Capture
Requirement 1

• Clarified what network diagram must include (1.1.2)
  – All connections between cardholder data environment, including any wireless networks
• Current diagram showing all cardholder data flows (1.1.3)

• This is all part of the scoping exercise required on page 10 of the PCI DSS 3.0
Requirement 2

- Maintain inventory of system components in scope for PCI DSS (2.4)
  - Maintain list of hardware & software components with function descriptions
  - Interview personnel to verify list is current
Requirement 4

• Use strong cryptography & security protocols to safeguard transit data (4.1)
• Interception of unencrypted data over public network easy & common
• Updated to include satellite communications
Requirement 5

• Evaluate evolving malware threats for systems not commonly affected by malware (5.1.2)

• Ensure anti-virus solutions actively run & cannot be altered/disabled without managerial approval (5.3)
Requirement 6

• Secure development of internal & external software applications (6.3)
• Requirement for coding practices to protect against broken authentication & session management (6.5.10)*
  – Examine development policies & procedures
  – Interview responsible personnel
Requirement 7

• Define access needs for each job role (7.1.1)
  – System components & data resources
  – Level of privilege required for accessing resources
Requirement 8

• Education and training on password policy implementation (8.4)
• Service providers with remote access must use unique login credentials for each customer (8.5.1)*
• Physical/logical controls required to uniquely ID users of alternate authentication mechanisms (8.6)
  – e.g. PIN, biometric data, password
Requirement 9

• Control physical access to sensitive areas for onsite personnel (9.3)
• Protect direct contact payment devices from tampering and substitution (9.9)*
  – Maintain up-to-date list of devices (9.9.1)
  – Periodically inspect device (9.9.2)
  – Provide staff awareness training (9.9.3)
Requirement 10

• Log use of and changes to identification and authentication mechanisms (10.2.5)
• Record all pauses, stops, and initializations of audit logs (10.2.6)
• Review logs of all other system components based on policies & risk management strategy (10.6.2)
Requirement 11

• Maintain an inventory of authorized wireless access points (11.1.1)
• Implement methodology for penetration testing (11.3)*
• Implement process to respond to change-detection system alerts (11.5.1)
Requirement 12

• Document which requirements are managed by service provider & entity (12.8.5)

• Service provider written acknowledgement of data responsibility (12.9)*
Key Takeaways

- Increased documentation on processes
- Focus on monitoring (physical inspection, logs)
- Implementing layers of security
- Security of individual systems
- Focus on detecting rather than just reacting
Top 10 Assessment Issues
Top 10 Assessment Issues

• Poor or no segmentation of card data network from other networks
  – Strengthen firewall ACL’s, limit outbound ports, NetBios problems, backup location, minimize PCI scope
• Understanding flow of card data through the network
  – What systems handle card data, what is persisted (track, etc.), where it is persisted (DB, web log, etc.), how persisted (unencrypted, text files, etc.)
• Encryption Issues
  – Lack of encryption, strength of encryption, encryption key management
• Web Application Security / Web Development
  ‣ Processes to develop & test secure web apps, OWASP, web app firewall
• Patch Management
  ‣ Keeping current on critical OS and application security patches
Top 10, Continued

– Documentation and Process not in place
  • Security policies and procedures, change control, firewall/router standards, incident response plan, contracts, etc.
– Two-Factor remote access not in place
– Audit logging solution not in place: generation, management, monitoring, and centralization
– Vulnerability assessment solutions
  • External and internal VA, pen testing, IDS/IPS
– Hardware/software costs and procurement lead time issues
Where'd My Data Go
Anatomy of a Compromise
(Hospitality Industry – Two sites)

- Network Vulnerabilities Found
  - Insecure remote access
  - Common default passwords
  - Logging not enabled, no logs were being watched
  - Flat network design - limited to no segmentation
  - No IDS/IPS in place

- Attack Vectors Included
  - Compromised remote access
  - Installed suite of Malware: processor memory dump program, parser looking for credit card data in dump files, shared folder search app that looked for passwords, credit card numbers, social security numbers, etc.
Anatomy of a Compromise
(Hospitality Industry – Two sites)

- The result to the business...bottom line costs
  - Cost of the Forensic Investigation $32,000
  - Number of cards stolen 150,000
  - Fines $80,000
  - Reimburse for fraudulent uses $440,000

- All this from just two sites involved in the compromise
Anatomy of a Compromise: Small Food and Beverage Merchant

Network Vulnerabilities Found
- Insecure configuration done by outsourced IT company
- Insecure Remote Access
- Insecure Wireless Access Point
- Common default passwords
- No firewall in use to protect from Internet
- Flat network design - limited to no segmentation

Attack Vectors Included
- Compromised remote access
- Key Logger Installed
- Covert SMTP server
Anatomy of a Compromise: Small Food and Beverage Merchant

The result to the business...bottom line costs

- **Cost of the Forensic Investigation**: $16,000
- **Number of cards stolen**: 1,200
- **Fines**: $10,000
- **Reimburse for fraudulent uses**: $110,000

The outsourced IT service provider that configured this small merchant also set up 50+ other merchants...*With the exact same configuration and passwords!*
Questions?

Matt Halbleib
QSA, PA-QSA, CISSP
dustin@securitymetrics.com