What’s New in PCI DSS 2.0
Agenda

- PCI Overview
- PCI 2.0 Changes
- PCI Advanced Technology Update
- PCI Solutions
PCI Overview
Quick Security Facts

79% PCI in scope organizations that suffered a data breach not yet PCI compliant

85% attacks were not considered highly difficult

48% breaches caused by internal users (90% deliberate)

The vast majority of data breaches would have been prevented if security changes already planned were implemented
The PCI Data Security Standard

- Originally published January 2005, current version is 2.0
- PCI DSS 2.0 standard becomes mandatory January 1st, 2012
- Impacts ALL who
  - Process
  - Transmit
  - Store: cardholder data
- PCI is a private sector security standard. It is a contract between merchants and banks
Why Should You Care About PCI

• First and foremost, it is a tool you can use to secure your business

• It promotes security awareness throughout the organization

• Fines can be hefty for non-compliance:
  AMEX non-filing fees: $50,000 non-compliance fee. Additional $150,000 if not compliant in 30 days. Additional $200,000 if 60 days past due. Termination of contract if more than 60 days plus previous fees.

• Fines and costs are even heavier for card-number breaches
Cost of a Data Breach

• Raising awareness for PCI
  Industry data helps
  Specific cost data that is personalized always prevails
  Use PCI as a mechanism to expose these costs to the business

• Data breach costs
  Average cost per breached record: US$204 (was US$138 in 2005)
  Average cost to a breached organization: US$6.75 million
  Legal costs up 56% from 2008 due to increase in successful class-action lawsuits and threat thereof

MasterCard Merchant Compliance Update

• Starting 30 June 2011

• Level 2 Merchants need to either:
  
  Complete annual self-assessment by certified Internal Security Assessor (ISA)

  or…

  Complete an annual onsite assessment by a QSA

PCI Training

• The PCI SSC Internal Security Assessor (ISA) Program:
  • PCI DSS training and qualification program
  • 3 day on-site training course with exam
  • Must be a full time employee of an ISA Sponsor Company and qualified as an ISA
  • Passing results in 12 month ISA certification

• 2-day PCI awareness training—available to anyone

• QSA certification limited to QSA companies/employees
## 12 PCI DSS Requirements

| Build and Maintain a Secure Network | 1. Install and maintain a firewall configuration to protect data  
2. Do not use vendor-supplied defaults for system passwords and other security requirements |
|-----------------------------------|--------------------------------------------------------------------------------------------------|
| Protect Cardholder Data           | 3. Protect stored data  
4. Encrypt transmission of cardholder data and sensitive information across public networks |
| Maintain a Vulnerability Management Program | 5. Use and regularly update anti-virus software  
6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 7. Restrict access to data by business need-to-know  
8. Assign a unique ID to each person with computer access  
9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data  
11. Regularly test security systems and processes |
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security |
PCI 2.0 Changes
PCI 2.0 Change Breakdown by Category

- 119 changes to provide clarification
- 15 changes for additional guidance
- 2 changes that are evolving requirements

We will only touch on some of the main ones that we think have some significance
Methodology for Determining PCI Scope

New requirement to annually confirm the accuracy and appropriateness of PCI DSS scope in your environment

- Fully document your discovery methodology
- Document the location of your PCI data
- Make documentation available to assessor
Virtualization Added to Scope

‘System components’ also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.

- Requirement 2.2.1 updated: Where virtualization technologies are in use, implement only one primary function per virtual system component.
Wireless Rogue Detection Updates

• 11.1: Wireless access point detection updated with new methods:
  • Wireless network scans
  • Physical/logical inspections
  • NAC
  • Wireless IDS and IPS

• 11.1b: Verify wireless test methods for accurate detection of:
  • WLAN cards
  • Portable wireless devices (USB, etc.)
  • Attached wireless devices and access points

PCI Note: “Whichever methods are used, they must be sufficient to detect and identify any unauthorized wireless devices.”
Virtualization Updates

Guidance

• All virtual components in scope
• All virtual communications and data flows must be identified and documented
• Virtualized environment must maintain proper segmentation
• Must meet intent of all 12 PCI requirements

Authentication

• Virtual management protocols in system documentation
• Define roles/permissions
• Enforce separation of duties and least privilege
• Distinguish privileges between the guest VMs and the hypervisor

Source: PCI council “Navigating DSS v2.0.pdf”
Wireless Considerations

Risk

Sophistication

Physical inspection  WIPS  Clean Air
SAQ C-VT Added

- Applies only to merchants who manually enter a single transaction via a keyboard into an Internet-based virtual terminal solution provided by a 3rd party

- Computer is isolated in a single location, and is not connected to other systems within your environment (this can be achieved via a firewall or network segmentation)

- Greatly simplified and targeted audit requirements
Additional 2.0 Developments

• Vulnerability Risk Ranking: req 6.2 (July 2012)
  Establish a process to identify and assign a risk ranking to newly
discovered security vulnerabilities

• Secure Coding: req 6.5
  Secure development for all applications, not just web
  More best practice examples sited
New Information Supplements and Advanced Technology Guidance
How the Council Approaches Emerging Technology and Change

• Special Interest Groups (SIGs)
• Solicits outside studies like the PWC Study
• Technical Working Group (TWG)
• Individual brands release guidance or requirements
• Feedback/input from participating organizations
  • Every single comment during the 1.2 comment period was reviewed!
• Anyone can submit a question to the FAQ @ https://www.pcisecuritystandards.org/
Point-to-Point Encryption Guidance

- Roadmap focused on encryption at the point-of-interaction (POI) terminal, not site to site (S2S)

- Roadmap conclusions
  - Validation methods still immature
  - Can simplify PCI; must meet testing validation
  - Will not eliminate PCI; may reduce scope
  - Independent validation of P2PE required

- Validation requirements guide to be released in 2011
Virtualization Guidance Coming

- New guidance and mapping document currently in review

- Guidance likely will include:
  - Common virtualization definition
  - Component definitions and scoping considerations
  - Risks
  - Use cases
  - Recommendations

- Hotly debated subject is use of mixed mode
Tokenization

- Tokenization defined
- Shifts the risk to the financial institution
- POS: Still at risk
- Use cases for tokenization
- Not a silver bullet
Chip & Pin

- EMV defined
- EMV: face-to-face compared to online transactions
- Magstripe still accepted
- PAN not confidential
- EMV and PCI together

Therefore, in securing the current face-to-face acceptance environment one should not consider it to be a case of either EMV or PCI DSS, but rather EMV and PCI DSS. Both are essential elements in the fight against fraud and data exposure. Together they provide the greatest level of security for cardholder data throughout the entire transaction process.

PCI DSS Applicability in an EMV Environment: A Guidance Document Version 1, release date October 5, 2010
PCI Design Best Practices—How Cisco Can Help with PCI
PCI DSS 2.0 Scope Definition

• PCI security requirements apply to all ‘system components.’

• System components are defined as:

> Any network component, server, or application that is included in or connected to the cardholder data environment.
> Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desks, and hypervisors.

• The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data.

• Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment.

Source: PCI DSS 2.0
Scoping with Segmentation

Entire Network is in Scope

Can scope be reduced with segmentation?
Scoping with Segmentation

Entire Network is in Scope

Branch

Warehouse

Data Center

Wide Area Accelerated Network

Core

Server Access

Server Access

Inventory Servers

POS Servers

Storage

Determine Scope

Can scope be reduced with segmentation?

NOT IN PLACE

Entire network is in scope for PCI DSS review
Scoping with Segmentation

Entire Network is in Scope

Determine Scope

Can scope be reduced with segmentation?

- NOT IN PLACE
- IN PLACE

Did assessor validate segmentation effectiveness?

- No
- Yes

Assessor documents segmentation in place and effective

Entire network is in scope for PCI DSS review

Scope limited for PCI DSS review

Only Devices Passing Card Holder Data Are in Scope

Branch

Warehouse

Data Center

Wide Area Accelerated Network

WAN Access

CORE

Server Access

POS Servers

Storage

Branch

Warehouse

Data Center

Wide Area Accelerated Network

WAN Access

CORE

Server Access

POS Servers

Storage

© 2010 Cisco and/or its affiliates. All rights reserved.
Scoping with Segmentation

Entire Network is in Scope

Determine Scope

Can scope be reduced with segmentation?

- NOT IN PLACE
- IN PLACE

Did assessor validate segmentation effectiveness?

- No
- Yes

Assessor documents segmentation in place and effective

Entire network is in scope for PCI DSS review

Scope limited for PCI DSS review

Audit Performed

Only Devices Passing Card Holder Data Are in Scope
Approaching PCI

• Reduce your scope
• Secure the perimeter of the cardholder data scope
• Maintain and simplify
PCI Simplified:
A Comprehensive Solution

PCI DSS 2.0 Solution Framework

Endpoints
- **Point of Sale**: Servers, and Applications
- **Voice**: Phones and Contact Center Applications
- **Email**: Data Loss Prevention
- **Physical**: Surveillance and Badge Access

Administration
- **Authentication**
- **Management**
- **Encryption**
- **Monitoring**

Infrastructure
- **Network**: Routers, Switches, and Wireless
- **Security**: Firewalls and Intrusion Detection

Services
- **Assess**
- **Design**
- **Implement**
- **Audit**

Endpoints | Administration | Infrastructure | Services
Cisco PCI Solution

Campus or HQ
- POS Servers
- POS Register
- PC
- Mobile POS

Store
- Catalyst Switch
- Integrated Services Router
- LWAPP
- POS Servers
- POS Register
- PC
- Mobile POS and Inventory

Data Center
AGGREGATION
- WAN Aggregation
- Core
- Service Aggregation

INTERNET EDGE
- Adaptive Security Appliance
- Web App FW
- DMZ
- Web Servers

SERVER ACCESS
- Access
- Authentication
- Network Management
- Security Management
- Monitoring
- POS Servers
- Business Servers
- Database
- Network Services
- MDS 9000 SAN Switches

STORAGE
- Disk Arrays
- Tape Storage

External Locations
- Remote Workers
- Partners

INTERNET
- VPN
Requirement 1: Install and Maintain a Firewall Configuration to Protect Data

Campus or HQ
- POS Servers
- POS Register
- Payment Devices
- Mobile POS/Inventory
- Security Management: Key Manager Client

Data Center
- WAN Aggregation Core
- Service Aggregation
- INTERNET EDGE
  - Adaptive Security Appliance
  - Web App FW
  - DMZ
    - Web Servers

Server Access
- Authentication
- Network Management: CiscoWorks LMS
- Security Management: Cisco Security Manager
- Monitoring: SIEM

Storage
- POS Servers
- Business Servers
- Database
- Network Services
- MDS 9000 SAN Switches
- Disk Arrays
- Tape Storage
- File Security Adapter +

Store
- Integrated Services Router
  - LWAPP
- POS Register
- Payment Devices
- Mobile POS and Inventory
- Security Management: Key Manager Client
- File Security Adapter +
- Payment Devices
- Mobile POS and Inventory

INTERNET
- Service Provider
- External Locations
- Remote Workers
- Partners
Cisco PCI Design and Implementation Guides

- Recommended architectures for networks, payment data at rest, and data in transit
- Testing in a simulated retail enterprise, which includes POS terminals, application servers, wireless devices, Internet connection, and security systems
- Configuration, monitoring, and authentication management systems
- Design was validated by a third-party QSA
Cisco PCI Compliance Professional Services

<table>
<thead>
<tr>
<th>Penetration and Vulnerability Testing (Req. 11)</th>
<th>• Cisco® Security Posture Assessment (SPA) Service performs penetration testing on the customer’s network to determine gaps in the network, holes, and vulnerabilities that can be used to attack the system. This is a PCI requirement that must be performed regularly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Risk Analysis</td>
<td>• Cisco IT GRC Assessment Service addresses PCI (and other relevant regulations) to determine scope and risk to the business</td>
</tr>
<tr>
<td>Technical Control Mapping</td>
<td>• Analysis of the security controls in place and whether they meet the PCI requirements as designed and implemented</td>
</tr>
<tr>
<td>Security Management Program Analysis</td>
<td>• Review of customer security management program and assessment against PCI standards and ISO (27001 and 38500) to identify areas for improvement</td>
</tr>
</tbody>
</table>
In Summary

- PCI Overview: Update on new PCI lifecycle and overview of changes

- PCI Obstacles: Advanced technologies still being investigated, driving need for end-to-end solution

- PCI Solution: PCI simplified with Cisco
Important URLs

- Cisco PCI Resources
  - www.cisco.com/go/pci
  - www.cisco.com/go/retail
  - www.cisco.com/go/healthcare

- PCI Design and Implementation Guide—Retail

- PCI Security Standards Council
  - http://www.pcisecuritystandards.org

- Bank Heist Case Study
  - http://news.bbc.co.uk/2/hi/uk_news/7909595.stm
Q and A