PCI DSS Presentation
University of Cincinnati
- Quick PCI Level Set
- Higher Ed Challenges
- Getting Compliant
- Application w/ customers
- Q & A
PCI DSS – Payment Card Industry Data Security Standard

PCI DSS: “One Standard to Rule Them All”
What is the PCI DSS trying to protect?

What’s in your wallet?

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Magnetic Stripe
- Card Verification Value (CVV)
<table>
<thead>
<tr>
<th>Covered Data Elements</th>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder</td>
<td>PAN</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Cardholder name</td>
<td>Yes *</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Service code</td>
<td>Yes *</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Expiration date</td>
<td>Yes *</td>
<td>Yes</td>
</tr>
<tr>
<td>Sensitive authentication</td>
<td>Magnetic stripe</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
<tr>
<td></td>
<td>CVC2/CVV2/CID</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
<tr>
<td></td>
<td>PIN/PIN block</td>
<td>No</td>
<td>No storage permitted</td>
</tr>
</tbody>
</table>
## Merchant Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Visa and MasterCard</th>
<th>Amex</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&gt; 6 million Visa/MC txns/yr</td>
<td>&gt; 2.5 million Amex txns/yr</td>
</tr>
<tr>
<td>2</td>
<td>1 to 6 million Visa/MC txns/yr</td>
<td>50,000 to 2.5 million txns/yr</td>
</tr>
<tr>
<td>3</td>
<td>20,000 to 1 million Visa/MC ecommerce txns/yr</td>
<td>All other Amex Merchants</td>
</tr>
<tr>
<td>4</td>
<td>All other Visa/MC merchants</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## Merchant Levels and Compliance Validation

<table>
<thead>
<tr>
<th>Level</th>
<th>Visa and MasterCard</th>
<th>Amex</th>
</tr>
</thead>
</table>
| 1     | • Annual on-site assessment (QSA)  
  • Quarterly network scan by (ASV) | • Annual on-site assessment (QSA)  
  • Quarterly network scan (ASV) |
| 2     | • Annual on-site assessment (QSA)  
  • Quarterly network scan (ASV) | • Quarterly network scan (ASV) |
| 3     | • Annual Self-Assessment Questionnaire (SAQ)  
  • Quarterly network scan (ASV) | • Quarterly network scan (ASV) (recommended) |
| 4     | • At discretion of acquirer  
  • Annual SAQ  
  • Quarterly network scan (ASV) (recommended) | • N/A |
<table>
<thead>
<tr>
<th>Payment Method</th>
<th>Validation Requirements</th>
<th>1 Card-Not-Present, All Cardholder Data Functions Outsourced</th>
<th>2 Imprint Only, No Cardholder Data Storage</th>
<th>3 Standalone Dial Out Terminal, No Cardholder Data Storage</th>
<th>4 POS Connected to Internet</th>
<th>5 All Other Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Methods &amp; Validation Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 Move as far to the left as possible!</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>233</td>
</tr>
<tr>
<td>SAQ A 13 Questions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAQ B 24 Questions</td>
<td>No Scanning!</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAQ C 32 Questions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAQ D 233 Questions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No Scanning!
6 Objectives and 12 Requirements

1. Build and maintain a secure network
   - 1. Install and maintain a firewall configuration to protect data
   - 2. Change vendor-supplied defaults for system passwords and other security parameters
2. Protect cardholder data
   - 3. Protect stored data
   - 4. Encrypt transmission of cardholder magnetic-stripe data and sensitive information across public networks
3. Maintain a vulnerability management program
   - 5. Use and regularly update antivirus software
   - 6. Develop and maintain secure systems and applications
4. Implement strong access control measures
   - 7. Restrict access to data to a need-to-know basis
   - 8. Assign a unique ID to each person with computer access
5. Regularly monitor and test networks
   - 9. Restrict physical access to cardholder data
   - 10. Track and monitor all access to network resources and cardholder data
6. Maintain an information security policy
   - 11. Regularly test security systems and processes
   - 12. Maintain a policy that addresses information security

*Augmented by 230+ sub requirements*
Managing Compliance

- **Scanning request:**
  - Complete scan request form
  - White list scanner IP addresses in your IDS/IPS

- **Vulnerability scans will:**
  - Fingerprint the host (port scan, banner check, etc)
  - Perform checks on open ports
  - Well-known vulnerabilities
  - Mis-configurations
  - Backdoors/Trojan horse applications
Managing Compliance

### Component Compliance

<table>
<thead>
<tr>
<th>IP</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.122.121.122</td>
<td>NOT COMPLIANT</td>
</tr>
<tr>
<td>123.123.123.122</td>
<td>NOT COMPLIANT</td>
</tr>
<tr>
<td>123.123.123.124</td>
<td>NOT COMPLIANT</td>
</tr>
<tr>
<td>123.123.123.125</td>
<td>COMPLIANT</td>
</tr>
<tr>
<td>123.123.123.126</td>
<td>NOT COMPLIANT</td>
</tr>
</tbody>
</table>

Note: In accordance with the PCI SSC’s non-disruptive requirements for scanning solutions:

**Denial-of-service (DoS) attacks were not executed against any components.** If a component was found to have a potential susceptibility to DoS attacks, the vulnerability was appropriately ranked based on severity and listed with the component's findings for your further review. Since DoS attacks typically affect only the availability of components and not their confidentiality or integrity, potential susceptibility to DoS attacks have not been factored into a component's compliance.

**Buffer overflow exploits were not executed against any components.** If a component was found to have a potential susceptibility to buffer overflow exploits, the vulnerability was appropriately ranked based on severity and listed with the component's findings for your further review. Since buffer overflow exploits can affect the confidentiality, integrity and/or availability of components, potential susceptibility to buffer overflow exploits have been factored into a component's compliance.

### MS06-067: Microsoft Windows Server Service Crafted RPC Request Handling Unspecified Remote Code Execution (SSR644) (unauthorized check)

<table>
<thead>
<tr>
<th>Industry Reference Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE: CVE-2008-4250</td>
</tr>
</tbody>
</table>

**CVSS Base Score**

10.0 (CVSS2@AV:VN/AC:AU/CI:UC/IS:UC)

**Details**

The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

**Remediation Tasks**


**More info**

http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx
Validation

Self-Assessment Questionnaire D

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
<th>Yes</th>
<th>No</th>
<th>Special</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1</td>
<td>A guided process for approving and testing all external network connections and changes to the firewall and router configurations?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.2</td>
<td>Current network diagrams with all connections to cardholder data, including any wireless networks?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.3</td>
<td>Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zones?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.4</td>
<td>Description of groups, roles, and responsibilities for logical management of network components?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.5</td>
<td>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></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.6</td>
<td>Requirement to review firewall and router rules at least every six months?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Does the firewall configuration restrict connections between untrusted networks and any system in the cardholder data environment as follows: Note: An &quot;untrusted network&quot; is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's actual control or management?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.1</td>
<td>Restrict inbound and outbound traffic by which is necessary for the cardholder data environment?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.2</td>
<td>Synchronize router configuration files?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.3</td>
<td>Include installation of perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Attestation of Compliance, SAQ A
PCI Scope

No Segmentation: The “Worst Case Scenario

Where most campuses start out
Therefore, the entire network is in scope
You don’t want this!

Unzoned: EVERYTHING in scope!
Reduce Your PCI Scope!

Let’s Try That Again

Strategic Scope
Only payment systems are in scope
Better all around
Some Data Breach Stats

Who Is Behind Data Breaches?
74% from external sources
20% caused by insiders
32% implicated business partners
39% involved multiple parties

How Do Breaches Occur?
67% aided by significant errors
64% resulted from hacking
38% utilized malware
22% involved privilege misuse
9% occurred via physical attacks

What Commonalities Exist?
69% discovered by a third party
81% of victims were not PCI compliant
83% considered avoidable through simple or intermediate controls
99.9% records compromised from servers or applications

Source: Verizon 2009 Data Breach Investigations Report
Corporate Owner of T.J. Maxx, Marshall’s Says Information for 45.7 Million Cardholders Stolen

Thursday, March 29, 2007
Associated Press

In a regulatory filing that gives the first detailed account of the breach initially disclosed in January, the owner of T.J. Maxx, Marshall’s and other stores in North America and the United Kingdom also said another 405,000 customers who returned merchandise without receipts had their personal data stolen, including driver’s license numbers.

Hackers target TK Maxx customers

Hackers have stolen information from at least 45.7 million payment cards used by customers of US retailer T.J. Maxx, which owns T.J. Maxx, and UK outlet TK Maxx.

In a statement to US watchdogs the firm said it did not know the full extent of the theft and its affect on customers.

More in the US, UK, Canada, Ireland and Australia also affected.
PCI Non-Compliance

In the event of a breach the acquirer can make the merchant responsible for:

- Any fines from card associations
  - Up to $500,000 if you haven’t validated with a SAQ
- Cost to notify victims
- Cost to replace cards
- Cost for any fraudulent transactions
- Forensics
- Level 1 certification from a QSA
Many colleges and universities adopt the use of a 3rd party processor or payment system for tuition and other payments.

- Great idea
- Limits scope for the PCI DSS

Purchasing of PA-DSS compliant systems

- Can help in compliance effort
- Not a panacea
Questions……..

Contact Treasurer’s Office

Susan Albonetti 64793

susan.albonetti@uc.edu