Security in the Payment Card Industry

Hap Huynh,  
Information Security Specialist, Visa USA  
hhuynh@visa.com

OWASP AppSec Seattle  
Oct 2006

Copyright © 2006 - The OWASP Foundation  
Permission is granted to copy, distribute and/or modify this document under the terms of the Creative Commons Attribution-ShareAlike 2.5 License. To view this license, visit http://creativecommons.org/licenses/by-sa/2.5/

The OWASP Foundation  
http://www.owasp.org/
Agenda

- Security Breaches and Vulnerability Experiences
- Overview of PCI DSS Initiative and CISP
- Payment Application Best Practices
- Questions and Comments
Security Breaches and Vulnerability Experiences
Payment Card Industry Experience

- Increased regulatory pressure to address security risk
- Risk of consumer loss of confidence in brand and payment system
- Data compromises result in fraud losses
- Globally organized criminals involved in hacks
Security Breaches

- Poorly configured remote access systems
- Integrated Point of Sale (IPOS) systems connected to the Internet
- No encryption of cardholder data
- No intrusion monitoring or Logging
- Increasing technology, increases risk!

System Vulnerabilities
Hacker Focus

- **Hackers are attacking:**
  - E-commerce merchants
  - Brick-and-mortar merchants
  - Third-party entities in the payment system

- **Hackers are using:**
  - Full track data and/or encrypted PIN block retention
  - Default accounts
  - Insecure remote access by software vendors and their resellers
  - Compatibility issues with anti-virus and encryption
  - SQL injection
### Marketplace

<table>
<thead>
<tr>
<th>Forum</th>
<th>Last Post</th>
<th>Threads</th>
<th>Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendors Plaza (REVIEWED) (1 Viewing)</td>
<td>PLASTIC (blank and embossed)... by xzib78</td>
<td>33</td>
<td>139</td>
</tr>
<tr>
<td>Open Market/Auctions/Trades/Wanted (1 Viewing)</td>
<td>Need a Nov ID Asap by funky</td>
<td>99</td>
<td>226</td>
</tr>
<tr>
<td>Reviewed vendors can post ads for products and services, customers may leave feedback in the appropriate thread. Read the sticky for how to get reviewed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>This area is for unreviewed auctions and trades. Do business in this section AT YOUR OWN RISK. For verified-legit vendors use the Vendors Plaza instead. No cvv2 or dumps in this section, use vendors or PM.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Operations

<table>
<thead>
<tr>
<th>Forum</th>
<th>Last Post</th>
<th>Threads</th>
<th>Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Carding</td>
<td>Successful Shipping Sites by real-biz</td>
<td>30</td>
<td>198</td>
</tr>
<tr>
<td>cvv2, drops, where to shop, selling merchandise, all aspects of carding online</td>
<td>2006-07-10 10:24 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instore Carding</td>
<td>How to Build a RFID Skimmer by CashNet</td>
<td>27</td>
<td>127</td>
</tr>
<tr>
<td>dumps, equipment, where to shop, where to avoid, selling merchandise</td>
<td>Yesterday 10:02 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online Banking</td>
<td>online bank cashers(tr) by ncxxi</td>
<td>19</td>
<td>57</td>
</tr>
<tr>
<td>bank logins, wire transfers, checking</td>
<td>2006-06-11 06:27 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing</td>
<td>Spammers Needed by log2neo</td>
<td>12</td>
<td>49</td>
</tr>
<tr>
<td>roots, emails, mailers/harvesters, scam templates, cashing out</td>
<td>2006-07-01 03:25 AM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacking/Security</td>
<td>How do you chat safe and... by fenster</td>
<td>22</td>
<td>83</td>
</tr>
<tr>
<td>hacking, exploits, vpn, proxies, encryption, security</td>
<td>2006-07-05 07:36 AM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Impact of Data Compromises

- Notification/disclosure
- Brand/reputation
- Loss of business/consumer confidence
- Financial liabilities
  - Compromised entity
    - Cost of forensics
    - Cost of remediation
  - Visa member
- Litigation
- Government intervention/legislation
Overview of PCI DSS Initiative and CISP
PCI DSS / CISP – Overview

- Visa USA Inc. Operating Regulations Section
  - A member must comply, and ensure that its merchants and agents comply, with the requirements of the Cardholder Information Security Program (“CISP”)
  - Effective June 2001

- PCI Data Security Standard (“DSS”) is modeled on CISP
  - Cooperative effort with Visa, MasterCard, American Express, Discover and JCB to align payment network security requirements

- CISP is Visa USA program to administer and enforce data security compliance
CISP Timeline

Visa’s concept for data security program is born

1999

Visa develops Cardholder Information Security Program (CISP), working with acquirers and merchants

2000

Visa CISP is implemented and compliance is validated for e-merchants

2001

PCI Data Security Standard developed; Visa CISP validation deadline

2002

Visa CISP validation expanded to all merchant and service provider channels

2003

2004

2005
CISP & PCI DSS Benefits

- Adhering to PCI DSS and PABP will help entities in their efforts to meet other compliance obligations, such as SOX, HIPPA, GLBA, and state privacy legislation.

- "PCI is the only standard or regulation at a low enough level to make a difference. Every other standard in security is at the 10,000-foot level." – Information Security Magazine, May 2006

- Funding for security projects can be hard to come by, but the PCI DSS can help entities justify and secure much needed resources.

- "A company with at least 10,000 accounts ... Can spend as little as $6 per customer account for just data encryption, or as much as $16 per customer account for data encryption, host based intrusion prevention and strong security audits combined. Compare that with an expenditure of at least $90 per customer account when data is compromised or exposed during a breach." – Tech Web News, June 2006
States with ‘Notice of Security Breach’ Legislation*

*As of June 2006. Subject to change. Please refer to state legislation for specifics.
New PCI DSS Version 1.1

- Issued new PCI DSS Version 1.1 on September 2006
- New requirements:
  - 2.4 Hosting provider requirement
  - 5.1.1 Requirement that malicious software, such as spyware and adware, are included in anti-virus capabilities
  - 6.6 Requirement for application code review or application firewall
    - This is a best practice until June 30, 2008 after which it will be a requirement.
  - 12.10 Requirement for a policy to manage connected entities
  - Appendix A PCI DSS Applicability for Hosting Providers that establishes requirements for providers that host merchant and service provider clients
  - Appendix B Compensating Controls defines these controls in general and discusses compensating controls when stored cardholder data cannot be rendered unreadable
Payment Application Best Practices (PABP)
Payment Application Best Practices

- Visa’s PABP released in 2005
  - Ensure vendors provide products that support PCI DSS compliance
  - Minimize compromises caused by insecure payment applications
  - Focus is elimination of the storage of full track data

- Payment application vendors have voluntarily validated products
  - 89 products across 57 vendors independently validated by a Qualified Security Assessor (“QSA”)
  - List of validated payment applications published on Visa.com

- Developing strategy to aggressively promote PABP compliance

- PABP to become the Payment Application Security Standard (“PASS”)
Timeline of Payment Application Security

- 2002: First track data compromise involving POS application
- 2003: Payment Application Best Practices developed
- 2004: Payment Application Best Practices launched
- 2005: Working with other brands for global acceptance
- 2006: PABP development into PCI requirement
Payment Application Best Practices

- PABP is applicable to any third-party payment application utilized by a merchant or service provider that is involved in authorization and settlement of credit or debit card transaction:
  - Any application that runs on a client-server environment (such as IP, wireless, etc.)

- PABP can be applied to in-house applications, but such applications should be covered by PCI DSS.

- PABP is not applicable to dumb terminals, database or web server software
Payment Application Vulnerabilities

- More than 20 applications have played a role in compromises.

- Top 5 vulnerabilities related to payment applications include:
  - Full track data and/or encrypted PIN block retention
  - Default accounts
  - Insecure remote access by software vendors and their resellers
  - Compatibility issues with anti-virus and encryption
  - SQL injection
Payment Application Best Practices

1) Do not retain full magnetic stripe or CVV2 data.
2) Protect stored data.
3) Provide secure password features.
4) Log application activity.
5) Develop secure applications.
6) Protect wireless transmissions.
7) Test applications to address vulnerabilities.
8) Facilitate secure network implementation
9) Cardholder data must never be stored on a server connected to the Internet.
10) Facilitate secure remote software updates.
11) Facilitate secure remote access to application.
12) Encrypt sensitive traffic over public networks.
13) Encrypt all non-console administrative access.
Payment Application Validation

- Payment application vendors seeking validation of their products will:
  
  ▸ Ensure availability of payment applications meeting PABP.
  
  ▸ Identify product versions that will meet PABP and be validated accordingly.
  
  ▸ Engage an assessor from the QSA list with the Qualified Payment Application Security Company (“QPASC”) designation.
  
  ▸ Ensure each of their products are validated by QPASC in a lab using the PABP testing procedures.
  
  ▸ Ensure QPASC provides Report on Validation confirming PABP compliance to Visa.
  
  ▸ Communicate product availability to customers, system integrators, and resellers.
Payment Application Validation

- Validation is specific to a product version.
- All modules and components that make up the application must be considered.
- QPASC must test actual transactions (authorization and settlement).
Reference Tools

**Payment Card Industry (PCI)**
- Data Security Standard
- Security Audit Procedures
- Self-Assessment Questionnaire
- Security Scanning Procedures
- Qualified Onsite Assessor List
- Qualified Scan Vendor List

www.pcisecuritystandards.org

**Visa CISP**
- What To Do If Compromised Guide
- Qualified CISP Incident Response Assessor List
- List of CISP-Compliant Service Providers
- Payment Application Best Practices
- List of Validated Payment Applications
- Glossary of Terms
- Frequently Asked Questions

www.visa.com/cisp
Questions or Comments?