

Session 3: Application Security/ Common Risk Areas

Kurt Hagerman

CISSP, QSA

Director of IT Governance
and Compliance Services



Agenda

- Session 1: An Overview of the Payment Card Industry
- Session 2: Self Assessment Questionnaire and PCI Scans
- **Session 3: Application Security**
- Q & A

Application Security

- Application Vulnerabilities are on the rise
- Some estimate that more than 95% of all websites are vulnerable to attack (SQL, XSS, etc.)
- Starting June 30th, 2008, the DSS requires:
 1. A Web Application Firewall **or**
 2. Periodic Secure Code review
- PCI recently released a new standard for third party applications, called the PA-DSS

PCI DSS requirement 6.6

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by *either* of the following methods:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes
- Installing a web-application firewall in front of public-facing web applications

6.6 For *public-facing* web applications, ensure that *either* one of the following methods are in place as follows:

- Verify that public-facing web applications are reviewed (using either manual or automated vulnerability security assessment tools or methods), as follows:
 - At least annually
 - After any changes
 - By an organization that specializes in application security
 - That all vulnerabilities are corrected
 - That the application is re-evaluated after the corrections
- Verify that a web-application firewall is in place in front of public-facing web applications to detect and prevent web-based attacks.

Note: "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.

Web Application Firewall

- Imperva – Secure Sphere
- Barracuda - Web Application Gateway
- Bee Ware - iSentry
- Breach Security – Web Defend
- Citrix – Application Firewall
- F5 – Big IP Application Security Manager

Information Security Magazine review – March 2008

New Mandates

Payment Application Mandates



Visa USA plans to aggressively drive the adoption of secure payment applications in the marketplace

Phase	Compliance Mandate	Effective Date
I.	Newly boarded merchants must not use known vulnerable payment application and VNP and agents must not certify known vulnerable payment applications	1/1/08
II.	VNP and agents must certify only PABP-compliant payment applications to their platforms	7/1/08
III.	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or utilize PABP-compliant payment applications*	10/1/08
IV.	VNP and agents must decertify all known vulnerable payment applications**	10/1/09
V.	Members must ensure their merchants, VNP and agents use PABP-compliant payment applications	7/1/10***

Application Security

- PA-DSS is an acronym for:
Payment Application - Data Security Standard
- The PA-DSS was just recently released
- The PA-DSS is based on the PABP v1.4 standard,
but with some changes and updates
- PABP was a Visa-only initiative. PA-DSS is a PCI
Council initiative that is recognized by all major
card brands

Application Security

- Using PA-DSS validated applications facilitates PCI DSS compliance & supports the security of the CC transaction.
- Beware of applications that aren't PA-DSS/PABP compliant because they may:
 - Store magnetic stripe data in the merchant's network after authorization;
 - Require merchants to disable other features required by PCI Data Security Standard, like anti-virus software or firewalls, in order to get the POS application to work properly; and/or
 - Use unsecured methods to connect to the application to provide support to the merchant.

www.visa.com/cisp

Home Personal Small Business **Merchants** Mid-Size & Large Companies Government

VISA Search: **GO**

New Acceptance Operations & Procedures **Risk Management** Marketing Center Payment Technologies Merchant Resources

Fraud Control Basics Online Safety **Cardholder Information Security Program** Verified by Visa Zero Liability

CARDHOLDER INFORMATION SECURITY PROGRAM

- Overview
- Merchants
- Service Providers
- Payment Applications
- PIN Security
- If Compromised
- Assessors
- Alerts, Bulletins & Webinars
- Tools and FAQ

Upholding the Highest Cardholder Data Security Standards for Visa Stakeholders

The Visa Cardholder Information Security Program (CISP) aims to secure Visa cardholder data wherever it resides, requiring that members, merchants, and service providers maintain the highest information security standards.

CISP compliance is required of all entities that store, process, or transmit Visa cardholder data.

Visa PCI CAP Successfully Drives Merchant Compliance

In December 2006, Visa launched its U.S. [PCI Compliance Acceleration Program \(CAP\)](#) featuring incentives and sanctions to further U.S. merchant compliance with the PCI DSS. [Over three-fourths of largest U.S. merchants are now PCI compliant.](#)

Quick Links

- [PCI Data Security Standards](#)
- [CISP List of Compliant Service Providers PDF | 132k](#)
- [Validated Payment Applications PDF | 244k](#)

Key Points

- Who does the PA-DSS apply to?
- What new requirement will become effective June 30th, 2008?
- Where can you go to search for PABP compliant applications, and certified Service Providers?



Final Thoughts

Latest Alerts



Visa Data Security Alert

Packet Sniffing Vulnerability

January 31, 2008



To promote the security and integrity of the payment system, Visa is committed to helping clients and payment system participants better understand their responsibilities related to securing cardholder data and protecting the payment industry. As part of this commitment, Visa issues Data Security Alerts when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Clients may share this alert with their stakeholders to help ensure they are aware of these emerging

Packet sniffers are typically used in conjunction with malicious software or “malware.” Once network intruders gain entry into a critical system using backdoor programs or deploying rootkits, the sniffer programs are installed, making the malware more difficult to detect.

Intruders can then “sniff” packets between network users and collect sensitive information such as usernames, passwords, payment card data or social security numbers. Once a critical system or network

Visa's Top Concerns

- Storage of magnetic stripe data (Requirement 3.2). It is important to note that many compromised entities are unaware that their systems are storing this data.
- Inadequate access controls due to improperly installed merchant POS systems, allowing hackers in via paths intended for POS vendors (Requirements 7.1, 7.2, 8.2 and 8.3)
- Default system settings and passwords not changed when system was set up (Requirement 2.1)
- Unnecessary and vulnerable services not removed or fixed when system was set up (Requirement 2.2.2)
- Poorly coded web applications resulting in SQL injection and other vulnerabilities, which allow access to the database storing cardholder data directly from the web site (Requirement 6.5)
- Missing and outdated security patches (Requirement 6.1)
- Lack of logging (Requirement 10)
- Lack of monitoring (via log reviews, intrusion detection/prevention, quarterly vulnerability scans, and file integrity monitoring systems) (Requirements 10.6, 11.2, 11.4 and 11.5)
- Lack of segmentation in a network, making cardholder data easily accessible through weaknesses in other parts of the network (e.g., from wireless access points, employee e-mail, and web browsing) (Requirements 1.3 and 1.4)

What We've Seen

- Supporting weak encryption protocol or ciphers (ie. SSLv2 or SSHv1)
- Default vendor configurations not changed (IIS, Apache)
- Unnecessary ports open (FTP, Telnet, SSH, RDP)
- Non-Microsoft applications are not updated
- Default accounts and passwords
- Unknown IP addresses
- Misconfigured firewalls
- Application/ Website vulnerabilities

Common CAPEX

1. Enterprise Firewall	1.3, 1.5
2. Personal Firewalls	1.3.9
3. Integrity Management	1.3.6
4. Centralized encryption management	3.4
5. Anti-virus	5.1.1, 5.2
6. Application firewall	6.6
7. Multi-factor Authentication	8.2, 8.3
8. Logging and monitoring solutions	10.2, 10.5
9. IDS/IPS	11.4

Remember 8:35?

- What is the PCI DSS FAQ for SAQ's (aka. ASA)?
- When does the PABP become the PA-DSS, and is it still part of the CISP or is it now run by the PCI SSC?
- How do you search for CVV2 or PAN in your CDE?