Payment Card Industry Data Security Standard PCI-DSS

#SA7D, Platform Database, Tuning & Security

John Mason

Slides & Code - labs.fusionlink.com

Blog - www.codfusion.com

CF.Objective()

What is PCI-DSS?

- Created by the major credit card companies as a industry standard
- To protect credit card information
- Established on Dec 2004
- The last revision (1.1) was Sept 2006
- Is consider to be one of the more comprehensive data security standards
- http://www.pcisecuritystandards.org

PCI-DSS

- Speaker Bio
  - Using ColdFusion since 1997
  - Board Member of the Atlanta CF User Group
  - Founder/President of the Atlanta Flex User Group
  - President of FusionLink Inc., a ColdFusion and Flex hosting company based in Atlanta
  - Certified Advance CF
  - MBA from Georgia Southern University, 2001

PCI Security Standards Council

- Manages and updates the PCI standards
- Educates the public about those standards
- Tests and approves QSA (Qualified Security Assessors) and ASV (Approved Scanning Vendors) entities
- Does not directly enforce the standard, that's left to the individual brands

How does it apply to you?

- Any company that process, stores or transmits card card numbers is require to be PCI DSS complaint
- So not just for E-commerce, also required for..
  - Retail (brick-and-mortar)
  - Mail/Telephone ordering
- Also a very useful security standard for general use

Noncompliance can result in..

- Fines (can range between $90-$500 per card exposed)
- Civil suits
- Reimbursement of expenses incurred due to data breach
- Revoke of merchant account

There are also possible state and federal laws to consider..

- Basel II
- Gramm-Leach-Biley Act (GLBA)
- Health Insurance Portability Act (HIPAA)
- Sarbanes-Oxley Act (Sox)
- California State Bulletin 1386
- California Bill AB 779
- Minnesota, Plastic Card Security Act
- Texas BILL HB03222E
- There are always new bills being proposed to address consumers data, privacy, identity theft, etc.

Industry Structure

- Credit Card Companies - Visa, Mastercard
- Acquiring Banks - Chase,HSBC,RBS
- Independent Sales Organizations (ISO)
- Merchant Service Providers (MSP)
- Merchants

Merchant Levels

- Level 1
  - Over 6 million transactions per year
- Level 2
  - 1 million to 6 million transactions per year
- Level 3
  - 20,000 to 1 million transactions per year
- Level 4
  - Less than 20,000 transactions per year

Current implementation of PCI DSS

- Acquirers will be fined between $5,000 and $25,000 a month for each of its Level 1 and 2 merchants who have not validated by Sept 30, 2007 and Dec 31, 2007 respectively.
- Before this fines were assessed only in cases where actual data breaches occurred
- Currently, Level 4 merchants have to do yearly self assessments

What's in PCI DSS?

- There are 6 logical areas with 12 requirements. The areas are..
  - Build and Maintain a Secure Network
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy

What are the requirements?

- Bare in mind each requirement has sub-requirements that are explicitly listed on the standard

Build and Maintain a Secure Network

- Req 1 - Install and maintain a firewall
  - Document list of services and ports necessary (1.1.5)
  - Have a formal process for approving and testing all external network connections (1.1.1)
  - Quarterly review of firewall and router rule sets (1.1.8)
  - Firewall should deny all traffic not explicitly allowed (1.3.7)
  - Placing database servers in an internal network segregated from the DMZ (1.3.4)
  - Placing personal firewall software on any mobile device that has access to the organization's network (1.3.9)

Build and Maintain a Secure Network

- Req 2 - Do not use vendor-supplied defaults for system passwords and other security parameters
  - Eliminate unneccessary accounts (2.1)
  - Implement only one primary function per server (web, database, dns, etc) (2.2.1)
  - Disable all unnecessary and insecure protocols (2.2.2)
  - Remove all unneccessary scripts, drivers, features (2.2.4)
  - Encrypt all non-console administrative access - SSH,VPN,SSL/TLS (2.3)

Protect Cardholder Data

- Req 3 - Protect stored cardholder data
  - Keep card storage to a minimum (3.1)
  - Do not store the card magnetic track (3.2.1)
  - Do not store the card verification code - CVC2/CVV2/CID (3.2.2)
  - Do not store the card's PIN
  - Mask PAN when displayed, for example just the last 4 digits (3.3)
  - Encrypt PAN when it's stored (3.4)

Protect Cardholder Data

- Req 4 - Encrypt transmission of cardholder data across open, public networks
  - SSL/TLS (4.1.1)
  - Never send unencrypted PANs via Email (4.2)

Maintain a Vulnerability Management Program

- Req 5 - Use and regularly update anti-virus software
  - Ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software (5.1.1)
  - Ensure AV generates logs (5.2)

Maintain a Vulnerability Management Program

- Req 6 - Develop and maintain secure systems and applications
  - Ensure all software have the latest patches (within a month of release) (6.1)
  - Maintain separate development,test and production environments (6.3.2)
  - Live PANs are not used for testing or development (6.3.4)
  - Review code for vulnerabilities before going live (6.3.7)

Req 6.5 in light of ColdFusion

- Cover for these common coding vulnerabilities (6.5)
  - Unvalidated input
  - Broken access control (malicious use of user Ids)
  - Broken authentication and session management (use of session cookies)
  - Cross-site scripting (XSS) attacks

Req 6.5 in light of ColdFusion

- Cover for these common coding vulnerabilities (6.5)
  - Buffer overflows
  - Injection flaws (SQL to URL injections)
  - Improper error handling
  - Insecure storage
  - Denial of service attacks

Maintain a Vulnerability Management Program

- Req 6 - Develop and maintain secure systems and applications
- Must have either by June 30, 2008
  - Have all code reviewed for these common vulnerabilities by an outside organization that specializes in application security (6.6)
  - Have an web application firewall (WAF) (6.6)

Implement Strong Access Control Measures

- Req 7 - Restrict access to cardholder data by business need-to-know
  - Deny access unless explicitly allowed by authorized personnel (7.2)

Implement Strong Access Control Measures

- Req 8 - Assign a unique ID to each person with computer access
  - All users have a unique username (8.1)
  - Encrpyt all passwords during transmission and storage (8.4)
  - Passwords must have a minimum of 7 characters (8.5.10)
  - Passwords must be alphanumeric (8.5.11)
  - Lock account after not more than 6 failed attempts (8.5.13)
  - If a session is idle for more than 15 minutes, require re-login (8.5.15)

Implement Strong Access Control Measures

- Req 9 - Restrict physical access to cardholder data
  - Use proper facility that controls and monitors access (9.1)
  - Have a procedure to distinguish between employees and visitors (9.2)
  - Use visitor log (9.4)
  - Store backup media in a secure location (9.5)

Regularly Monitor and Test Networks

- Req 10 - Track and monitor all access to network resources and cardholder data
  - Implement audit trails (10.2)
  - Synchronize all critical system clocks and times (10.4)
  - Backup audit trail files (10.5.3)
  - Review logs for all system components at least daily (10.6)
  - Retain audit trail history for at least one year (10.7)

Regularly Monitor and Test Networks

- Req 11 - Regularly test security systems and processes
  - Test security controls, limitations and restrictions annually (11.1)
  - Run internal/external scans at least quarterly (11.2)
  - Perform penetration testing at least once a year (11.3)
  - Use network intrusion detection systems (11.4)

Maintain an Information Security Policy

- Req 12 - Maintain a policy that addresses informational security
  - Establish and publish your security policy (12.1.1)
  - Develop daily operational security procedures (12.2)
  - Implement a formal security awareness program to make all employees aware of the importance of cardholder data security (12.6)
  - Educate employees upon hire and at least annually (12.6.1)
  - If cardholder data is shared with service providers, then contractually the service provider must follow PCI DSS (12.8.1)

Conclusion

- Knowing and understand the PCI-DSS standard is essential for E-commerce development
- Noncompliance is dangerous for you and your business
- Most business owners/merchants will not understand PCI, you need to fill that gap.
- PCI-DSS also a solid security standard for people/businesses not dealing with E-commerce

Recommended Reading

- PCI Security Council
  - https://www.pcisecuritystandards.org/index.htn
- Visa CISP Standard
  - http://usa.visa.com/merchants/risk_management/cisp.html
- PCI DSS Compliance Demystified
  - http://pcianswers.com/

Thanks for coming!

- Presentation slides, notes and code examples can be found at..
  - labs.fusionlink.com
- Feel free to email me questions or comments to mason@fusionlink.com
- Blog - www.codfusion.com

CF.Objective()