Payment Card Industry Data Security Standards

Version 1.1, September 2006

Carl Grayson

Agenda

- Overview of PCI DSS
- Compliance Levels and Requirements
- PCI DSS v1.1 in More Detail
- Discussion, Questions and Clarifications

- Topics in this section
  - PCI DSS Defined
  - Brief History
  - Responsibilities
  - Who's Who Terminology
  - Confusion: PCI vs. AIS, CISP, SDP…
  - PCI Assessments
  - PCI Enforcement

PCI DSS Defined

- Payment Card Industry Data Security Standards

  A collaborative effort to achieve a common set of security standards for use by entities that process, store or transport payment card data.

- Multiple Credit Card organisations participating in PCI efforts

  Members include Visa, MasterCard, American Express (Amex), Diner's Club, Discover Card, and JCB

- Other PCI efforts underway

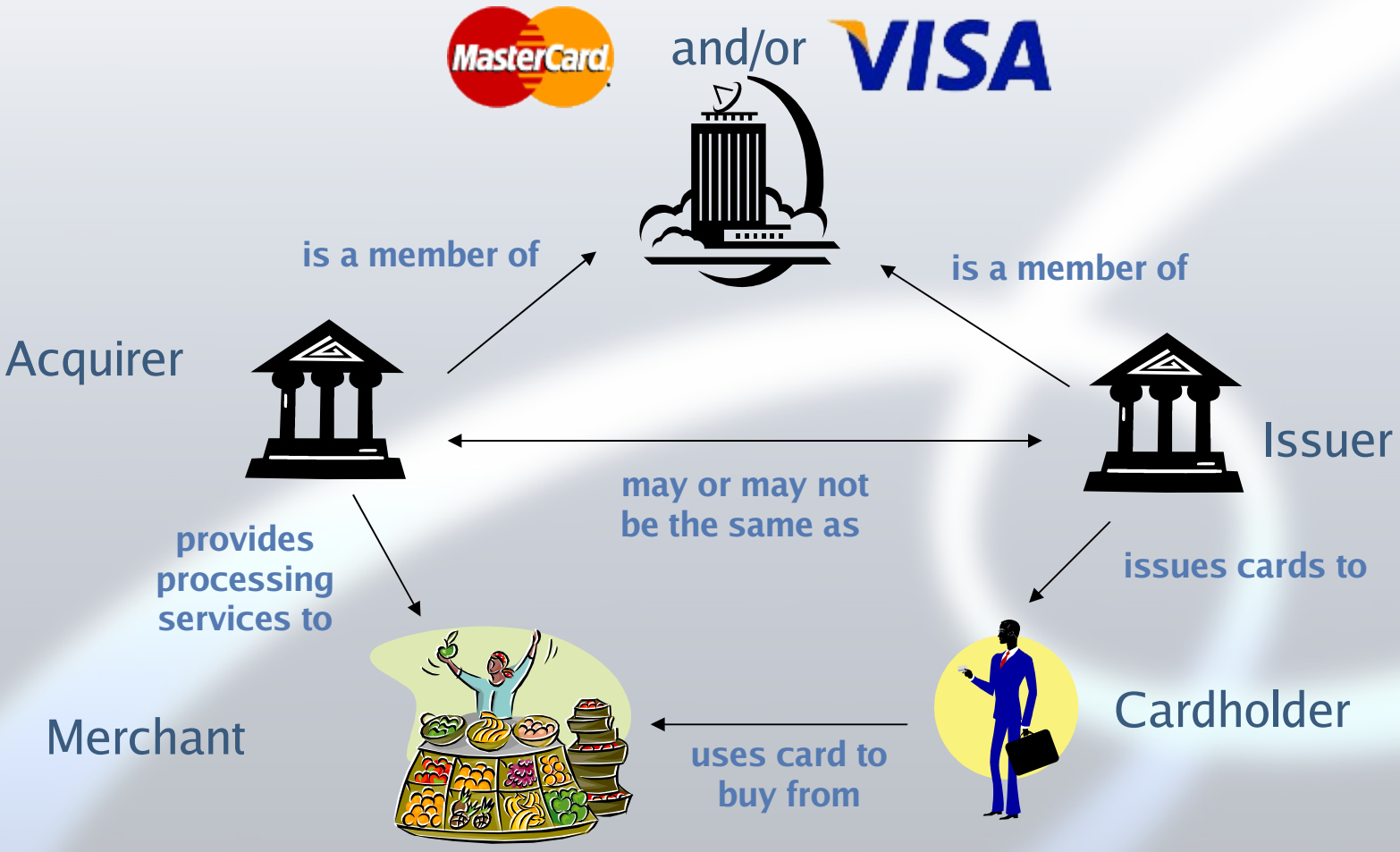
  (PABP) Payment Application Best Practices → (PASS) Payment Application Security Standards (June 30, 2008?)

- Companies developed and managed own standards independently
  - Visa: (AIS) Account Information Security
  - MasterCard: (SDP) Site Data Protection
  - American Express: (DSS) Data Security Standards
  - Discover Card: (DISC) Discover Card Information Security and Compliance
- Current PCI standards have evolved from the more mature Visa AIS standards and is heavily based on ISO17799
  - Present iteration of (version 1.1) was published September 2006 (earlier version 1.0 was December 2004)

- The Payment Card Industry Security Standards Council (PCI SSC or PCICo) is responsible for:
  - Overseeing the development of PCI standards
  - Certifying products and companies capable of fulfilling the Scanning requirements, called Approved Scanning Vendors (ASVs)
  - Training and certifying companies (called Qualified Security Assessors or QSAs) and individuals (called Qualified Security Assessor Personnel or QSAPs) capable of fulfilling the Onsite Review requirements
- The PCI organisations (Visa, MasterCard, Amex, Diners, Discover, JCB, etc are contributors to the standards)

Who's Who Terminology

- Visa and MasterCard are made up of Member organisations who can be either Acquirers or Issuers (or both)
- Acquirers are the Members of the Visa or MasterCard organisations which handle Merchants
- Issuers are the Members of the Visa or MasterCard organisations that issue the cards to Cardholders
- Merchants are those entities who "accept" card transactions
- Cardholders are, well, card holders…
- Service Providers are the entities that provide any service requiring the processing, storing or transport of card information on behalf of any of the above
- Other terms are usually specific to the card organisation



Confusion: PCI vs. AIS, CISP, SDP…

- PCI is the collaborative effort at standards
- The AIS Program is the Visa management of compliance to PCI for Acquirers, Merchants and Service Providers for most regions (compliance is managed regionally)

  (They apologise for any confusion with legacy AIS…)
- CISP is Visa USA's Card Information Security Program; basically equivalent to the AIS Program but further along (not used in Asia-Pacific)
- SDP is MasterCard's (global) program for management of compliance to PCI for Acquirers, Merchants and Service Providers

ALWAYS ENSURE YOU ARE REFERRING TO REGIONAL PRACTICES

- Scanning is only acceptable from PCI SSC certified products and providers (ASVs)
- Onsite Reviews are to be performed by PCI SSC certified assessors (QSAs)

- Merchants and Service Providers submit Reports on Compliance to their Acquirers
- Visa's Acquirers should provide an annual "Certificate of Compliance" on Merchants and Service Providers
- MasterCard's Acquirers complete a similar (quarterly?) "Acquirer Submission and Status Compliance" form

- Acquirers are responsible for ensuring that their Merchants use Service Providers that are PCI DSS compliant

- Visa and MasterCard require their Acquirers to ensure the compliance of their Merchants and Service Providers
- Visa and MasterCard are able to penalise their Acquirers for having Merchants or Service Providers that are non-compliant.
- Acquirers can pass on penalties to their Merchants and Service Providers through their contractual relationships
- Penalties can presently be financial against the Acquirer and restrict a Merchant's / Service Provider's ability to accept transactions.

Fines are ALREADY being issued overseas

- Topics in this section
  - Merchant Levels
  - Service Provider Levels
  - Merchant Requirements
  - Service Provider Requirements
  - Network Security Scanning
  - Self Assessment Questionnaire
  - QSA Onsite Review

- MasterCard and Visa declare to their Acquirers which of their Merchants are at what Level, but the breakdown is approximately (similar across Visa AP and MasterCard):

Level 1	Any Merchant processing over 6,000,000 transactions per year, compromised in the last year, or identified by another payment card brand as Level 1
Level 2	Any Merchant processing between 150,000 and 6,000,000 e-commerce transactions per year, or identified by another payment card brand as Level 2
Level 3	Any Merchant processing between 20,000 and 150,000 e-commerce transactions per year, or identified by another payment card brand as Level 3
Level 4	Any Merchant processing less than 20,000 e-commerce transactions per year, and all other Merchants processing up to 6,000,000 transactions per year

- MasterCard and Visa declare to their Acquirers which of their Service Providers are at what Level, but the breakdown is approximately (similar across Visa AP and MasterCard):

Level 1	All Service Providers that process, store or transmit over 600,000 transactions or accounts annually for Visa or that process card data at all or store card data for Level 1 or 2 Merchants for MasterCard
Level 2	Any Service Provider that is not in Level 1 and stores, processes or transmits more than 120,000 accounts or transactions annually for Visa or that store card data for Level 3 Merchants for MasterCard
Level 3	Any Service Provider that stores, processes or transmits less than 120,000 accounts or transactions annually for Visa or all other Data Storage Entities not in Levels 1 or 2 for MasterCard

	QSA Onsite Review	Self Assessment	Network Security Scan
Level 1	REQUIRED (annually)	Not Required	REQUIRED (quarterly)
Level 2	Not Required	REQUIRED (annually)	REQUIRED (quarterly)
Level 3	Not Required	REQUIRED (annually)	REQUIRED (quarterly)
Level 4	Not Required	Recommended (annually)	Recommended (annually)

	QSA Onsite Review	Self Assessment	Network Security Scan
Level 1	REQUIRED (annually)	Not Required	REQUIRED (quarterly)
Level 2	REQUIRED (annually) *for MasterCard*	REQUIRED (annually) *for Visa*	REQUIRED (quarterly)
Level 3	Not Required	REQUIRED (annually)	REQUIRED (quarterly)

- Targets all Internet facing devices, systems and applications including:
  - Routers and firewalls
  - Servers and hosts (including virtual!)
  - Applications
- Must be performed using an offering from a Approved Scanning Vendor:

  https://www.pcisecuritystandards.org/pdfs/pci_asv_list.pdf
- May not have any Severity 3 or greater issues:
  - 5 (Urgent): Trojan Horses, file read and write exploits, remote command execution
  - 4 (Critical): Potential Trojan Horses, file read exploit
  - 3 (High): Limited exploit of read, directory browsing and denial of service

Self Assessment Questionnaire

- Is a selected subset of the full Onsite Audit criteria (still version 1.0)
- Is completed by the Merchant or Service Provider themselves
- Is submitted to Acquirer(s)
- Is made up mainly of Yes/No/Not Applicable responses
- Is broken into five of the six sections from PCI DSS:
  - Build and Maintain a Secure Network
  - Protect Cardholder Data
  - Implement Strong Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy

QSA Onsite Review

- Is a detailed audit against the PCI Data Security Standard
- Potentially targets all systems and networks that store, process and/or transmit cardholder information
- Includes review of contractual relationships, but not assessment of the Third Parties themselves
- Must be performed using an offering from a Qualified Security Assessor:

  https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

- Biggest difficulties in having onsite reviews are the initial scoping and the subsequent cost of correction to compliant levels
- QSA provides a Report on Compliance when compliant for submission to the Acquirer. Interim reports may be asked for by the Acquirer

- Topics in this section
  - Authoritative Documentation
  - PCI DSS Structure
  - PCI DSS Control Evaluation
  - What Actually Changed in Version 1.1?
  - Onsite Review Practicalities

Authoritative Documentation

- Payment Card Industry Security Standards Council

  http://www.pcisecuritystandards.org

- PCI Data Security Standards can be downloaded via

  https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

- Other relevant documents, including Self Assessment Questionnaire and full Onsite Review Information

  https://www.pcisecuritystandards.org/tech/supporting_documents.htm

- Visa and MasterCard card security programmes:

  http://www.visa-asia.com/secured or

  http://sdp.mastercardintl.com

PCI DSS Structure

- Is made up of six key sections:
  - Build and Maintain a Secure Network
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy
- Each section has a set of Requirements, for example:
  - Build and Maintain a Secure Network
    - Requirement 1: Install and maintain a firewall configuration to protect data.
    - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

- Each Requirement has a rationale and a set of sub-requirements specified for review, for example:
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

    Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

    All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

    1.1 Establish firewall configuration standards that include the following:

    1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration

    1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks

    1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

- and so on… (interminably)

- There are presently twelve Requirements, with a total of about 180 specific controls to comply with (potentially implemented across every system in the card processing environment).

- QSAPs have to validate about 220 points, many of which are sampled across an appropriate number of systems, processes and individuals.

My last "PASS" report came to about 90 pages… and that was for was a small, well architected and operated environment.

- The PCI Security Audit Procedures give some guidance on what will be checked for during an Onsite Review. An example of this is shown below:
  - 6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.

    TESTING PROCEDURE
    - 6.3.7.a Obtain and review any written policies to confirm that code reviews are required, and must be performed by individuals other then the originating code author.
    - 6.3.7.b Confirm that code reviews are conducted for new code and after code changes.

What Actually Changed in Version 1.1?

- Lots more clarification
  - General clarifications, specifically to “card holder data” and “sensitive authentication data”; reduces and limits scope of compliance requirements somewhat
  - Timing clarified to have specific periods for regular tasks
- Enhancement of third party requirements (hosting, service providers, etc)
  - Mainly contractual, but some technical
- Removal of redundant (and sometimes dumb) statements
- Introduction of code reviews as formal requirements
  - Will get more interesting next year
- Enhancement of wireless rules
- Specific help with database encryption for “too hard” cases

SAQ Practicalities

- Highly recommend reading the PCI Data Security Standard first; it's what the answers will be interpreted against
- Get your scans done on time
- There isn't much flexibility for "yes (or no), but…" unless you speak with your Acquirer
- Don't lie
  - Card organisations have started spot-checking and fining those that are found to have been creative in other parts of the world

Onsite Review Practicalities

- Make sure you scope correctly
  - The appropriate placement of a stateful firewall can reduce the scope dramatically
- If not compliant, it will be necessary to submit planning information on how compliance will be achieved
  - This will be monitored and policed both by your QSA and Acquirer
- It may be possible to use compensating controls to meet a requirement
  - Must be controls over and above what is already specified, and must meet the intent of the Requirement
- Try not to make life too hard for your assessor ☺
  - Time and cost
  - They help adjudicate compensating controls

Questions?

http://www.security-assessment.com
carl.grayson@security-assessment.com