Payment Card Industry Compliance

OWASP – January 23, 2006

Pat Massey
Ralf Durkee
Maureen Baran

www.americanexpress.com

www.dinersclubus.com

www.discoverbiz.com

www.jcbusa.com

www.mastercardmerchant.com

www.visa.com

Background

- Due to the increasing fraud levels and theft of credit card information, the major card agencies (Visa, MasterCard, etc.) enacted merchant requirements for securing cardholder information in *June 2001*
- Compliance requirements apply to retailers, payment processors,

  and financial institutions
- Compliance deadline for merchant programs- June 30, 2005
- Assessment Scope includes any system, or network component that

  stores, processes, or transmits credit card data, ***plus***…

  - All Network Components- Routers, Firewalls, DNS, Mail
  - Servers- web, application, database
  - Web Accessible Applications, Shopping Carts, etc.

What is Cardholder Data?

- Cardholder data is any personally identifiable data associated with a cardholder
  - **Payment card account number**
  - Expiration date
  - Cardholder name and address
  - Social Security number
  - CVV or CVC (Card Verification Values)
  - Card track data (magnetic stripe)

- Scope includes:
  - All card types (credit, debit, stored value, etc.)
  - Anywhere and anyone with access to cardholder information

Organization Risks of Non-Compliance

- Potential of identity theft due to compromised data
- Ability to accept payment cards may be revoked
- Financial Penalties imposed by payment card agencies
- Financial Implications
  - Loss of revenue
  - Potential lawsuits
- Unwanted Media Attention- (i.e. ChoicePoint, BJ's, Lexis/Nexis, DSW Shoe Warehouse, CardSystems Solutions)
- Impact to Business Reputation

PCI Compliance Requirements- Merchants

Merchant programs are required to certify compliance for any systems that *store, process, or transmit* credit card information; requirements are based on transaction

Merchant Level	Description	Compliance Requirement	Due Date
1	Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year. Any merchant that has suffered a hack or an attack that resulted in an account data compromise. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system. Any merchant identified by any other payment card brand as Level 1.	Annual On-Site Security Audit and Quarterly Network Scan	9/30/2004
2	Any merchant processing 150,000 to 6,000,000 Visa e-commerce transactions per year. Any merchant identified by another payment brand as Level 2	Annual Self-Assessment Questionnaire and Quarterly Network Scan	6/30/2005
3	Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per year. Any merchant identified by another payment brand as Level 3	Annual Self-Assessment Questionnaire and Quarterly Network Scan	6/30/2005
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 6,000,000 Visa transactions per year.	Recommended Annual Self-Assessment Questionnaire & Quarterly Network Scan	TBD

Members are subject to fines, up to $500,000 per incident, for any merchant or service provider that is compromised and not PCI-compliant at the time of the incident.

PCI Compliance Requirements- Service Providers

Service providers are organizations that *store, process, or transmit* cardholder data on behalf of card company's members, merchants, or other service providers.

Service Provider Level	Description	Validation Action	Validated by	Due date
1	All VisaNet processors (member and Nonmember) and all payment gateways.*	Annual On-Site PCI Data Security Assessment Quarterly Network Scan	Qualified Data Security Company Qualified Independent Scan Vendor	9/30/2004
2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/transactions annually.	Annual On-Site PCI Data Security Assessment Quarterly Network Scan	Qualified Data Security Company Qualified Independent Scan Vendor	9/30/2004
3	Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 Visa accounts/transactions annually.	Service provider Quarterly Network Scan	Service provider Qualified Independent Scan Vendor	9/30/2004

*Payment gateways are a category of agent or service provider that stores, processes, and/or transmits cardholder data as part of a payment transaction. Specifically, they enable payment transactions (e.g., authorization or settlement) between merchants and processors (VisaNet endpoints). Merchants may send their payment transactions directly to an endpoint, or indirectly to a payment gateway.
Source: *: Visa Cardholder Information Security Program*
http://www.usa.visa.com/business/accepting_visa/ops_risk_management/cisp_service_providers.html

PCI "Digital Dozen"

PCI Data Security Standard	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

PCI Data Security Standards cross all security sectors & consist of 12 technology requirements for *securing networks & applications*, *protecting cardholder data*, *maintaining a vulnerability management program*, & *regularly validating compliance via a third party assessment*

PCI Lessons Learned

- Must have **high-level management support** (funding & resources)
- **Identifying all systems, applications,etc. that store, process, or transmit payment card information** may be more problematic than expected- Do it first!!
- The definition of **"PCI" network segment** may sweep other applications, systems, etc. that don't process/store/transmit payment card information into the PCI scope.
- **This is not just an information security initiative.** It will impact multiple groups w/in an organization- Application Developers, Network Engineering, Operations, Training, Incident Response, Security, HR, Business Process Owners… and possibly others
- **Some PCI compliance requirements are vague** and acquirers & third party consultants are still trying to figure them out
  - SOX Compliance does not equal PCI compliance
  - Work with a consultant who is PCI certified
  - Develop a network of peers in other companies

PCI Lessons Learned

- Requirements can change. Watch the Visa and MasterCard web sites for changes!
  - Level 1 assessment requirements
  - Scanning requirements

- **Visa Cardholder Information Security Program**
  - http://usa.visa.com/business/accepting_visa/ops_risk_management/c

- **MasterCard Site Data Protection Program**
  - https://sdp.mastercardintl.com/

What is Web Application Security?

It's **NOT** Traditional Network Security Layers!

Traditional Layers	Traditional Security Controls
Network Protocols	Firewalls, Routers, Operating System IP Stack Configuration and Filtering, VPNs, and Vulnerability Scanners
Operating System	Operating System Patches and OS Configuration, Authentication, Authorization, Encryption, and Vulnerability Scanners
3rd Party Applications	Minimize Services, Application Configuration, Vendor Patches, Application Level Authentication and Authorization, and Vulnerability Scanners

What is Web Application Security?

Traditional Layers	Traditional Security Controls
Network Protocols	Firewalls, Routers, Operating System IP Stack Configuration and Filtering, VPNs, and Vulnerability Scanners
Operating System	Operating System Patches and OS Configuration, Authentication, Authorization, Encryption, and Vulnerability Scanners
3rd Party Applications	Minimize Services, Application configuration, Vendor Patches, Application level Authentication Authorization, and
Custom Web Applications	**Architecture, Design and Code Reviews, Application Scanners, Testing Applications with Malicious Input**

Web Applications Vulnerabilities

- Sanctum reports 97% of 300 Web Applications Audited were Vulnerable
- Vulnerabilities in 3rd Party Web Applications are consistently ranked highest
- Average Vulnerabilities per week *(Dec 2005 SANS Inst.)*
  - Windows OS = 1
  - Linux = 1
  - Network Device = 3
  - 3rd Party Windows Apps = 6
  - Cross Platform = 20
  - **Web Applications = 55**

PCI 1.0 Install and Maintain a Firewall Configuration to Protect Data

- Goes way beyond just having a firewall
- 20 detailed requirements include:
  - Specific FW and Router configuration standards
  - Multi-tiered DMZ architecture
  - Documentation and justification for firewall and router configuration.
  - Formal configuration management process
  - DB must be firewalled from DMZ
  - Wireless must be firewalled as well

PCI 1.0 Lessons Learned

- Requirement for the DB to firewalled is a commonly requires expensive application architecture changes.
- When PCI DBs and applications share systems with non-PCI applications, all will be forced to be PCI compliant unless application and DB's are moved to separate systems
- Application with less than 3 layers or with multiple layer per system may need architectural changes
- Application using insecure network protocols such as ftp or WebDAV require changes.
- Firewall and router configuration changes are the easiest of the requirements for 1.0.

PCI 2.0 Do Not Use Vendor-Supplied Defaults . . .

- Systems must be security hardened to organizational standards and industry best practice.
- One primary function per server (Separate Web, DNS, Application, DB etc.)
- Disable all unnecessary and any insecure services
- Secure all administrative access

PCI 2.0 Lessons Learned

- Application Architecture changes continue to have the biggest impact
  - Separating services to individual servers
  - Migrating applications and processes from insecure services and protocols
  - Virtualization (Virtual servers) can save on hardware cost if configured securely.
  - Changes in administrative access typically meet resistance

PCI 3.0 Protect Stored Data

- Do not store payment card validation or verification codes or pins.
- Mask account numbers when displayed
- Encrypt sensitive cardholder data
- Protect all encryption keys, 10 detailed requirements including:
  - Formal documented secure key management process
  - Implement specific security controls and process to protect the keys
  - Such as: Split knowledge or dual control of keys required.

PCI 3.0 Lessons Learned

- Key protection and management must meet 10 detailed requirements
- Field level DB Encryption typically implemented.
- Any Non-DB storage of payment card numbers also needs to be encrypted
- Temporary storage as part of a transmission process may need special review and controls.

PCI 4.0 Encrypt Transmission of Sensitive Information Over Public Net

- Industry standard algorithms required
- 128 bit or stronger
- Sensitive information includes passwords which would give access to cardholder information.
- Wireless must be WPA, WEP not secure enough, without VPN.
- What's a Public Network?
- Recommendation: Check your providers service agreement; does it guarantee private communication?

PCI 4.0 Lessons Learned

- Application developers love to invent their own encryption algorithms. Don't let them!
- Use Industry standard protocols SSLv3, TLS, SSH, IPSec etc.
- SSL Servers, VPN's and browsers should be configured to not accept SSLv2 or < 128 bit ciphers.
- Don't assume you don't have wireless unless you have checked.
- Be conservative and encrypt transmission of sensitive information on internal networks as well.

PCI 5.0 Use and Update Anti-virus Software

- Deploy anti-virus software on all servers and all desktops.
- Typically understood to include Unix / Linux servers as well as Windows.
- Main Frames are not required to have AV.
- AV must be running, must be regularly updated and must generate audit logs.
- AV on Mail, Web, and file transfer servers is especially important.

PCI 5.0 Lessons Learned

- Many Unix and Linux systems have not run AV in the past.
- Continuing trend to have AV on key Unix systems, due to other regulation as well as PCI.
- AV on MS Windows is mostly a given for most organizations, except for occasional legacy server, appliance or DB servers.
- Consider if AV is appropriate for the various network appliances and some printers.

PCI 6.0 Develop and Maintain Secure Systems and Applications

- Apply all security updates within 1 month or release
- Include Information Security Best Practice throughout the entire development life cycle.
- Separation of duties for development/test and production
- Code Reviews of all custom code prior to production
- Formal System and Software Configuration Management required

PCI 6.0 Develop and Maintain Secure Systems and Applications (2)

- Develop web software and applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. The 2004 OWASP top 10:
  - Unvalidated input
  - Broken access control
  - Broken authentication / session management
  - Cross-site scripting (XSS) attacks
  - Buffer overflows
  - Injection flaws (e.g., SQL injection)
  - Improper error handling
  - Insecure storage
  - Denial of service

PCI 6.0 Lessons Learned

- Most development projects do not include security review throughout the lifecycle.
- Web projects often have same system and/or the same team members for development and production.
- Code reviews not yet commonly practiced.
- Formal System and Software configuration management often has to be added.
- Need to educate development teams on security requirement and development issues.

PCI 6.0 Lessons Learned (2)

- OWASP security issues typically involve rearchitecture, redesign and redevelopment and retesting; Best to catch security issues up front
- Changing the Software development process to include security is difficult in most organizational cultures
- Finding the manpower for design and code reviews is difficult.
- Not enough developers have security training, and not enough security professionals have development

PCI 7.0: Restrict Access to Data by Business Need-to-Know

- Limit access to cardholder information to those whose job requires such access
- Mechanism to grant access to multiple user systems with multiple users based on need to know
  - Set to “deny all” unless specifically allowed

PCI 8.0: Assign a Unique ID to Each Person with Computer Access

- All users authenticate using, at a minimum, a unique username and password
- Remote access software is configured with
  - A unique username
  - Encryption
  - Other security features enabled
- Passwords must be encrypted
- Enable accounts used by vendors for remote maintenance only when needed
- Authenticate all access to any database containing cardholder information

PCI 8.0: Assign a Unique ID to Each Person with Computer Access (2)

- Account management
  - Revoke user accounts when employee leaves company
  - Review accounts
  - Inactive accounts disabled at least every 90 days
  - No shared, group or generic accounts/passwords
  - Verify user identify prior to password resets

PCI 8.0: Assign a Unique ID to Each Person with Computer Access (3)

- Password policy
  - First-time passwords must be pre-expired
  - Passwords expire every 90 days
  - Minimum length of 7 characters, comprised of letters and numbers
  - Password History: Cannot reuse previous 4 passwords
  - Lockout after 6 unsuccessful authentication attempts
  - Lockout duration 30 minutes or until administrator enable the user ID
- User must re-authenticate after session has been idle for 15 minutes

PCI 7.0 & 8.0: Lessons Learned

- Most overlap with Sarbanes-Oxley requirements
- Many PCI web applications allow customers to authenticate without https, and most store customer passwords unencrypted. The second requires significant application changes.

PCI 7.0 & 8.0: Lessons Learned (2)

- Most PCI web applications are are woefully short on most of the password management requirements for non-consumers, and implementation of these is a major redesign for most web applications.

PCI 9.0: Restrict Physical Access to Cardholder Data

- Use appropriate facility entry controls to limit and monitor physical access
- Restrict access to:
  - Wireless access points
  - Wireless gateways
  - Wireless handheld devices
- Equipment and media containing cardholder data must be physically secured against unauthorized access
- Physically secure all paper and electronic media that contain cardholder data
- Destroy media containing cardholder information when it is no longer needed for business or legal reasons
- Receipts should not display the entire account number

PCI 9.0: Lessons Learned

- Check wireless equipment/software provided to assure PCI compliance
- Check swiping equipment provided to assure PCI compliance

PCI 10.0: Track and Monitor all Access to Network Resources and Cardholder Data

- Establish a process for linking all access to an individual user
- Record the following for each event, for all system components
  - User Identification
  - Type of event
  - Data and time
  - Success or failure indication
  - Origination of event
  - Identity of name of affected data, component or resource
- Synchronize all critical system clocks and times

PCI 10.0:Track and Monitor all Access to Network Resources and Cardholder Data (2)

- Regularly review logs for unauthorized traffic
- Back-up, secure and retain audit logs for at least 3 months online and 1 year offline for all critical systems

PCI 10.0: Lessons Learned

- Audit logs requirements may require application changes
- Audit log review requirements may meet resistance
- Most PCI web applications don't generate the required logs, let alone get them monitored
- For most situations, manually monitoring without some automated assistance from a commercial or custom log processing / IDS system is not feasible given the volume
- Back-up requirements may drive the requirement for additional storage capacity

PCI 11.0: Regularly Test Security Systems and Processes

- Use a wireless analyzer periodically to identify all wireless devices in use
- Perform a vulnerability scan or penetration test on all Internet-facing applications and systems before promote-to-production at least quarterly and after any significant change
- Use network intrusion detection, host-based intrusion detection and/or intrusion prevention systems and keep them up-to-date

PCI 11.0: Lessons Learned

- The requirement for scanning prior-to-promote to production may extend beyond applications/systems that store, process or transmit payment card information
- The largest cost associated with IDS/IPS is the personnel to required to maintain and run it

PCI 12.0: Maintain a Policy that Addresses Information Security

- Establish, publish and maintain a security policy (review at least annually)
- Disseminate security policies/information to all system users (including third parties)
- Define information security roles/responsibilities
- Have an up-to-date security awareness and training program for all system users
- Employees must sign an agreement stating they have read and understand security policies and procedures

PCI 12.0: Maintain a Policy that Addresses Information Security (2)

- Perform a background investigation on all employees with access to account numbers
- Third parties with access to sensitive cardholder data must be contractually obligated to comply with card association security standards
- Document and disseminate security incident response plan to appropriate responsible parties
- Report security incidents to person responsible for security investigation
- Have an incident response team ready to be deployed in case of cardholder compromise

PCI 12.0: Lessons Learned

- The requirement for the following may be limited in countries outside the US:
  - Employee sign off on reading/understanding security policy
  - Background checks
- Start early on contract changes

➔ Legal advice is key!

Payment Card Industry Compliance

Any Questions?

Pat Massey
Ralf Durkee
Maureen Baran

www.americanexpress.com

www.dinersclubus.com

www.discoverbiz.com

www.jcbusa.com

www.mastercardmerchant.com

www.visa.com