About 403 Labs

- 403 Labs, a division of Sikich LLP, is a full-service information security and compliance consultancy
  - Qualified Security Assessor (QSA)
  - Payment Application Qualified Security Assessor (PA-QSA)
  - Approved Scanning Vendor (ASV)
  - PCI Forensic Investigator (PFI)
  - QSA for Point-to-Point Encryption (QSA (P2PE))
  - PA-QSA for Point-to-Point Encryption (PA-QSA (P2PE))
About the Presenter

• A graduate of Bellevue University with a:
  • Master of Science Degree in Security Management
  • Bachelor of Science Degree in Computer Science
• Became a QSA in May 2007
• Manager at 403 Labs
About the Presenter

• Experience includes:
  • PCI DSS assessments
  • FISMA security control assessments
  • Risk assessments
  • Host configuration reviews, vulnerability and penetration testing, etc.
Agenda

- Definitions
- Foundation
- Data Flow Diagram
- Segmentation and Penetration Tests
- Risk-Driven Policies and Procedures
- ArtiFACTS
Agenda

• Definitions
• Foundation
  • Data Flow Diagram
  • Segmentation and Penetration Tests
  • Risk-Driven Policies and Procedures
  • ArtiFACTS
Definitions

• The *Payment Card Industry (PCI)* is a self-regulated industry driven by the five major card brands

• The *PCI Data Security Standard (PCI DSS)* is a group of security requirements that apply to all system components included in or connected to the cardholder data environment (CDE)
Definitions

• The **cardholder data environment (CDE)** is comprised of people, processes and technologies that store, process or transmit cardholder data or sensitive authentication data

• **Account Data** or **Card Data** is cardholder data and/or sensitive authentication data

• **Cardholder data (CHD)** is made up of the primary account number (PAN), cardholder name, expiration date and service code
Definitions

• **SAD (Sensitive Authentication Data)** is comprised of full track data (magnetic-stripe data or equivalent on a chip), card verification codes or values and PINs/PIN blocks

• An **information system** is an integrated set of system components (software and hardware) organized expressly for the collection, processing, maintenance, use, sharing, dissemination or disposition of information
Definitions

- **Segmentation** is the isolation of systems that store, process or transmit CHD from those that do not.

- A **data flow diagram (DFD)** is a graphical representation of the "flow" of data through an information system, modeling its process aspects.
Definitions

- A **penetration test** is a security test focused on testing the effectiveness of the security controls designed to prevent unauthorized access to networks, systems or data.

- **Artifacts** are physical evidence as opposed to attestations or statements (e.g., configuration files, logs, reports, screenshots of system configuration consoles).
Definitions

• A **PCI risk assessment** is the process of identifying card data assets, threats to card data and vulnerabilities in processes and technology that comprise the PCI in-scope environment; the assessment should produce a formal report with recommendations on mitigating identified risks.
Agenda

- Definitions
- **Foundation**
  - Data Flow Diagram
  - Segmentation and Penetration Tests
  - Risk-Driven Policies and Procedures
  - ArtiFACTS
Foundation

• Organizations must validate PCI DSS compliance; the assessment is a method to accomplish this card brand mandate

• Organizations should be actively engaged in the assessment process
  • Vet the evidence of compliance that your organization is providing to your QSA and make certain it is complete and fully addresses the target PCI DSS requirement
Foundation

- Organizations must present:
  - Written policies and procedures
  - Written plans, standards and diagrams
  - Artifacts or evidence demonstrating compliance

- In our experiences, we find that a lack of written policies, procedures and artifacts is the number-one reason organizations initially fail their assessment
  - Some organizations may have catastrophic failure, but almost all fail on this point
Agenda

• Definitions
• Foundation

• **Data Flow Diagram**
• Segmentation and Penetration Tests
• Risk-Driven Policies and Procedures
• ArtiFACTS
Data Flow Diagram

- PCI DSS Requirement 1.1.3 - Establish and implement firewall and router configuration standards that include current diagram(s) that shows all cardholder data flows across systems and networks.
- The data flow diagram is expected to identify the location of all CHD that is stored, processed or transmitted within the environment, not just the network.
Data Flow Diagram

• Current diagram that shows all cardholder data flows across systems and networks

• PCI DSS also requires a current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks (Requirement 1.1.2)
Data Flow Diagram

- A diagram that illustrates and documents the:
  - Applications and processes that handle CHD
  - Where the data will come from and go to
    - Sources of received CHD
    - Destinations of transmitted CHD
    - Processes that generate CHD
  - CHD storage locations (i.e., data stores, warehouses and flat files)
  - The process that destroys or purges CHD
Data Flow Diagram

- Data flow diagrams are important because they:
  - Help an organization understand and keep track of the scope of the environment
  - Identify the location of all CHD that is stored, processed or transmitted within the network
  - Show how CHD flows between individual systems, applications, processes and data stores
  - Help visualize data processing and where the data will come from and go to
Network diagram
Network diagram – not a data flow diagram

VMware VI3 Network Communication Diagram
ESX 3.5 and VC 2.5
(Version 1.0)

Based on information at
ESX Server 3 Configuration Guide (page 179)
Update Manager Administration Guide (page 19)
Virtual Machine Backup Guide (page 30)
Http://communities.vmware.com/docs/DOC-2500

(Special thanks to Nigel Metheringham & Jason Bochs)

All communication over TCP, except where stated

24/11/2008
Data flow diagram – basic diagram

Simplified Data Flow Diagram

- Kiosk POS
- Public-facing Web Applications
- Internal Web Applications
- Customer Processing System
- Retail Point-Of-Sale (POS)
- Call Center
- Loyalty Systems
- Lockbox (U.S. Mail)

- MS SQL Database
- MS SQL
- Temp CHD Storage

- CyberCash Application
- CyberSource Payment Manager (CPM)
- CyberSource Payment Gateway
- PayPal Payflow Pro Payment Gateway

- First Data Payment Processor (FDMS)
- Acme Bank (Lockbox service provider)
Data flow diagram – more context
Agenda

• Definitions
• Foundation
• Data Flow Diagram
• Segmentation and Penetration Tests
• Risk-Driven Policies and Procedures
• ArtiFACTS
Segmentation and Penetration Tests

• Segmentation = Isolation
  • Isolates systems that store, process or transmit CHD from those that do not
  • Dependent upon several factors (network configuration, deployed technologies, etc.)
Segmentation and Penetration Tests

• Segmentation = Isolation
  • Without adequate segmentation, the entire network is in scope
  • Segmentation may:
    • Reduce the scope and cost of the PCI DSS assessment
    • Reduce the cost and difficulty of implementing and maintaining PCI DSS controls
  • Network and CHD flow diagrams aid in determining that segmentation is effective at isolating the CDE
Segmentation and Penetration Tests

• Keys to successful scope reduction with segmentation
  • Consider all out-of-scope networks as the Internet
  • Remember that all systems that may impact the security of card data are in scope
  • Thoroughly document the cardholder data flow
Segmentation and Penetration Tests

- Keys to successful scope reduction with segmentation
  - Use risk assessments to determine acceptable network traffic
  - Implement additional security controls to mitigate risks
  - Be strict about network traffic permitted to the CDE
Segmentation – The Beginning
Segmentation – The Progressive Period Detailed

- Corporate Forest/Active Directory (AD) TRUSTs CDE
- Corp Users
- Enterprise – Applications
  - Corporate AD Trust CDE AD
- Security Systems
  - Corporate 2FA Server
  - Anti-Virus Server
- Enterprise – Databases
- Corp DMZ
  - VPN Concentrator 2-Factor Authentication
- Software Development & Testing
  - No direct CDE access

- IT Management LAN
  - 2-Factor Authentication To CDE 2FA server
- CDE – DMZ
  - CDE Forest/AD NO TRUST
  - CDE 2FA Server
- CDE – Applications
- CDE – Databases

Corporations Office
Corporate IT Facility
Remote Data Center

403 Labs
Segmentation and Penetration Tests

• Requirement 11.3 - Implement a methodology for penetration testing that includes the following:
  • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
  • Includes coverage for the entire CDE perimeter and critical systems
  • Includes testing from both inside and outside the network
  • Includes testing to validate any segmentation and scope-reduction control
Segmentation and Penetration Tests

• PCI penetration testing validates that segmentation and other security controls are effective

• A high-level approach is as follows:
Segmentation and Penetration Tests

1) External testing
   • The tester sits in a remote location across the Internet and attempts to gain unauthorized access to any DMZ that may provide a direct or indirect pathway to any in-scope system.
2) Internal testing:
Testing assumes the DMZ has been breached
• The tester sits in the DMZ and attempts to gain unauthorized access to systems in the DMZ or the corporate network and then tries to get into the CDE.
3) Internal testing:
Assumes a breach or a malicious internal unprivileged user
• The tester sits in the corporate user network and attempts to gain unauthorized access to local systems and then tries to get into the CDE
4) Internal testing: Performed if users or admin PCs are in the CDE; assumes a breach or malicious internal unprivileged user

- The tester sits in the CDE and attempts to gain unauthorized access to systems that process or store CHD
Agenda

• Definitions
• Foundation

Data Flow Diagram
Segmentation and Penetration Tests
Risk-Driven Policies and Procedures
ArtiFACTS
Risk-Driven Policies and Procedures

- Risk assessment focused on CHD
  - Conclusion should not be preconceived
- Policies express high-level direction to mitigate risk
- Standards to provide details on how to implement policy
Risk-Driven Policies and Procedures

• Operational procedures to integrate security into business and IT operations
• Policy and procedures for every PCI DSS requirement
Risk-Driven Policies and Procedures

• Challenge 1: No appetite for strict security policies
  • Establish a security policy for the enterprise
  • Establish a critical data security policy for the PCI environment that:
    • Establishes a separate set of rules
    • Is applicable only to the PCI in-scope environment (i.e., technology, processes and people)
Risk-Driven Policies and Procedures

• Align data security policy with the PCI DSS
  • 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
Risk-Driven Policies and Procedures

• Challenge 2: IT people aren’t writers and have no time
  • Engage a specialist to write policies and procedures
    • Canned policies and procedures off the Internet will require extensive modification
    • Utilize an expert to develop policies, plans, standards and procedures that are in line with your organization’s risks, operations and processes
Risk-Driven Policies and Procedures

- Procedure example: 1.1.2 - Procedures for keeping the network and data flow diagrams current
  - Standard requires it, how is it done?
    - As part of the change control procedure, require a diagram illustrating the change to be submitted with the change request
    - The procedure should describe this process
Risk-Driven Policies and Procedures

• Procedure example: 4.1 - Procedures for using strong cryptography/security protocols to protect CHD during transmission over open, public networks
  • Specific procedures to secure SSL/TLS certificates and keys
Risk-Driven Policies and Procedures

• Procedures for Requirement 4.1 should explain how to:
  • Configure applications to only use valid signed certificates and strong ciphers
  • Prevent modification of related configurations
  • Secure and store SSL/TLS certificates and keys
  • Set permissions on certificates and keys
  • Encrypt private keys?
Agenda

- Definitions
- Foundation
- Data Flow Diagram
- Segmentation and Penetration Tests
- Risk-Driven Policies and Procedures
- ArtiFACTS
Artifacts

- Policies and procedures present evidence of intent
- Artifacts present evidence of action
  - Configuration files
  - Reports and records
  - Results of host configuration reviews or assessments
    - Includes audit commands and results (see CIS benchmarks)
Questions and Answers
Thank You!

Jeff Tucker, QSA
jtucker@sikich.com
www.403labs.com
877.403.LABS