Guiding open standards for global payment card security

About PCI

Emerging Technologies

OWASP and Mobile Guidelines
About the PCI Council

Open, global forum
Founded 2006

Guiding open standards for payment card security

• Development
• Management
• Education
• Awareness
PCI Security Standards Suite
Protection of Cardholder Payment Data

Ecosystem of payment devices, applications, infrastructure and users

Guiding open standards for global payment card security
Getting Ready for PCI 3.0

2013 Focus: Updating PCI Standards and supporting documents based on Community feedback
Emerging Technologies

About PCI

Emerging Technologies

OWASP and Mobile Guidelines
Emerging Technologies

- **Mobile**
  - Guidelines
  - MWG/MTF
  - Standards?

- **Tokenization**
  - Guidelines
  - Standards
  - TkTF
Understanding Mobile Payments

Making Payments  Accepting Payments  Applications

Guiding open standards for global payment card security
Mobile Payment Acceptance

payment accepted

Thank You!

Guiding open standards for global payment card security
PCI on Mobile Payment Acceptance Security

- Identified mobile applications that can be validated to PA-DSS
- Published merchant guidance for ‘mobile’ solutions leveraging P2PE
- Developed best practices for developers
- New merchant guidelines
Areas of Focus for Mobile

“MOBILE”

- Devices
  Tamper-responsive, PTS Devices (e.g. SCR) using P2PE

- Applications
  Requirements and/or Best Practices for authorization and settlement

- Service Providers
  Service provider protection of cardholder data and validation

Guiding open standards for global payment card security
Guidance on Mobile Payment Acceptance Security

Accepting Mobile Payments with a Smartphone or Tablet

Many merchants seek innovative ways to engage customers and improve the shopping experience. The ever-expanding capabilities of mobile devices such as smartphones or tablets now include payment acceptance. Along with the increased convenience at the Point of Sale, mobile payment acceptance can also bring new risks to the security of cardholder data. Securing account data at the point of capture is one way that you can actively help in controlling these risks. In 2012, validated Point-to-Point Encryption (P2PE) solutions were listed on the PCI Council (PCI SSC) website. If you choose to accept mobile payments, these solutions may help you in your responsibilities under PCI DSS.

This at a Glance provides an example of a P2PE solution that leverages a mobile device’s display and communication functions to secure mobile payments. Central to the example is the use of an approved hardware accessory in conjunction with a validated P2PE solution. Combining a validated P2PE solution with mobile devices such as phones or tablets helps to maintain data security throughout the payment lifecycle.

PROTECT CARDHOLDER DATA

The PCI Data Security Standard (PCI DSS) requires merchants to protect cardholder data. You must protect any payment card information, whether it is printed, processed, transmitted or stored.

For merchants interested in utilizing an off-the-shelf mobile payment acceptance solution:

Partner with a Provider of a Validated Solution

Validated P2PE solutions ensure that cardholder data is encrypted before it enters a mobile device. Using a validated and properly implemented P2PE solution greatly reduces the risk that a malicious person could intercept and use cardholder data. Solution providers will often provide you with a card reader that works with your mobile device. Validated solution providers will have a list of approved card readers (also called Card of Interaction or PCI) that have been tested to work securely with their solution. The solution provider is responsible for ensuring that any P2PE used with their solution has been validated as compliant with the appropriate PCI SSC security requirements, including the Secure Reading and Exchange of Data (SRED).

Your solution provider will also tell you how to safeguard your mobile payment acceptance system. This guidance is contained in a P2PE Instructional Manual (IM). Your acquirer or payment brand may ask you to complete a P2PE Self-assessment Questionnaire as part of your annual PCI DSS validation – including confirming that you are following the solution provider’s PIM. You should coordinate with your acquirer or payment brand.

Guiding open standards for global payment card security
New Merchant Guidelines

For Merchants as End-Users

• Objectives and guidance for the security of a payment transaction
• Guidelines for securing the mobile device
• Guidelines for securing the payment acceptance solution

Guiding open standards for global payment card security
Purpose of Best Practices

Controls are broken into two categories:

- Payment Transaction
- Supporting Environment

Guiding open standards for global payment card security
Guiding open standards for global payment card security

Transactional Controls

CHD entering device: Prevent account data from being intercepted when entered into device.

CHD inside of device: Prevent account data from compromise while processed or stored within the mobile device.

CHD leaving device: Prevent account data from interception upon transmission out of the mobile device.

PCI Security Standards Council
Why It Is Important to Get It Right: **People**

- New group of merchants
- New group of application developers
- New payment channel for administrators
Why Is Mobile Different: Process

- May not use enterprise equipment
- Process changes as “terminal” travels
- Process to detect tampering and revoke card acceptance
Why Is Mobile Different: **Technology**

- **POS:**
  - Lack of traditional controls
  - Lack of experience of securing this type of device

- Other entities

- Tampering

- Challenges with Encrypting PIN Pad
OWASP Top 10 Mobile Risks*

M1 – Insecure Data Storage
M2 – Weak Server Side Controls
M3 - Insufficient Transport Layer Protection
M4 - Client Side Injection
M5 - Poor Authorization and Authentication
M6 - Improper Session Handling
M7 - Security Decisions Via Untrusted Inputs
M8 - Side Channel Data Leakage
M9 - Broken Cryptography
M10 - Sensitive Information Disclosure

*https://www.owasp.org/index.php/Mobile#tab=Top_Ten_Mobile_Risks

Guiding open standards for global payment card security
1. Insecure Data Storage

• **Objective 2:** Prevent account data from compromise while processed or stored within the mobile device
  
  • If account data is stored on the mobile device post-authorization, that data should be rendered unreadable per PCI DSS Requirement 3.4. If encrypted account data is stored, any related cryptographic keys need to be managed in accordance with PCI DSS Requirement 3.5 so keys are not accessible to unauthorized people, applications, and/or processes.
2. Weak Server Side Controls

• § 4.2 Create server-side controls and report unauthorized access.

• Ensure Develop the overall payment-acceptance solution to include capabilities for preventing and reporting unauthorized access attempts, identifying and reporting abnormal activity, and discontinuing access (i.e., the payment-acceptance solution would prevent further access by the mobile payment-acceptance app on that device until an administrator restores access). Controls include, but are not limited to:
  – Support for authorized access (e.g., access control list)
  – Ability to monitor events and to distinguish normal from abnormal events
  – Ability to report events (e.g., via a log, message, or signal) including cryptographic key changes, escalation of privileges, invalid login attempts exceeding a threshold, updates to application software or firmware, and similar actions
3. Insufficient Transport Layer Security

- **Objective 3:** Prevent account data from interception upon transmission out of the mobile device.
  - Ensure that account data is encrypted (i.e., using strong symmetric or asymmetric cryptography) per PCI DSS Requirement 4, prior to transmission out of the trusted execution environment of the mobile device.
4. Client Side Injection

**Objective 1:** Prevent account data from being intercepted when entered into a mobile device.

- Regardless of the process used, assure the account data entry channel is secured against client-side injections. Client-side injections include but are not limited to buffer overflows, data-type mismatches, embedded code or other unexpected data, and malicious or unauthorized apps and services on the mobile device.
5. Poor Authorization and Authentication

• § 4.5 Detect theft or loss.
  • ... the use of GPS or other location technology with the ability to set geographic boundaries, periodic re-authentication of the user, and periodic re-authentication of the device

• § 4.10 Protect the mobile device from unauthorized applications.
  • All authorized mobile apps, drivers and other software that form part of the payment solution should have a mechanism that permits authentication of the source and integrity of the executable file. The system should prevent the loading and subsequent execution of applications that cannot be authenticated.
6. Improper Session Handling

• § 4.15 Provide an indication of secure state.
  • A trusted execution environment (or equivalent) should include a mechanism for indicating to the mobile device user that the payment-acceptance mobile app is executing in a secure state. This would be similar to the indication that an SSL session is active in a browser.
7. Security Decisions via Untrusted Inputs

§ 4.3 Prevent escalation of privileges.

- Controls should exist to prevent the escalation of privileges on the device (e.g., root or group privileges). Bypassing permissions can allow untrusted security decisions to be made, thus increasing the number of possible attack vectors. Controls should include but are not limited to:
  - Providing the capability for the device to produce an alarm or warning if there is an attempt to “root” or “jail-break” the device;
  - Providing the capability within the payment-acceptance solution for identifying authorized objects and designing controls to limit access to only those objects.
8. Side Channel Data Leakage

• **Objective 2:** Prevent account data from compromise while processed or stored within the mobile device.
  
  • Ensure that account data is only processed inside a trusted execution environment. In order to prevent data leakage, account data should not be accessible outside a trusted execution environment. A data leakage prevention methodology should be adopted based on industry best practices and guidelines. The methodology should include, but is not limited to:
    
    – …
    
    – Prevention of unintentional or side-channel data leakage
9. **Broken Cryptography**

- Ensure that account data is encrypted (i.e., using strong symmetric or asymmetric cryptography) per PCI DSS Requirement 4, prior to transmission out of the trusted execution environment of the mobile device.
- If account data is stored on the mobile device post-authorization, that data should be rendered unreadable per PCI DSS Requirement 3.4. If encrypted account data is stored, any related cryptographic keys need to be managed in accordance with PCI DSS Requirement 3.5 so keys are not accessible to unauthorized people, applications, and/or processes.
- If the external device is wireless (e.g., Wi-Fi or Bluetooth), the wireless communication channel should be secured via strong cryptography.
10. Sensitive Information Disclosure

• **Objective 2:** Prevent account data from compromise while processed or stored within the mobile device.

  • Ensure that account data is only processed inside a trusted execution environment. In order to prevent data leakage, account data should not be accessible outside a trusted execution environment. A data leakage prevention methodology should be adopted based on industry best practices and guidelines. The methodology should include, but is not limited to:
    – Secure distribution of account data
    – Secure access to and storage of account data
    – Controls over account data while in use (e.g., preventing copy/paste, screen shots, file sharing, and printing)
    – Prevention of unintentional or side-channel data leakage
Questions?

Please visit our website at www.pcisecuritystandards.org

Guiding open standards for global payment card security
About the PCI Council

Open, global forum
Founded 2006

Guiding open standards for payment card security

- Development
- Management
- Education
- Awareness
SAVE THE DATES!

2013 COMMUNITY MEETINGS

NORTH AMERICAN COMMUNITY MEETING
24–26 September 2013
Mandalay Bay Convention Center
Las Vegas, Nevada

EUROPEAN COMMUNITY MEETING
29–31 October 2013
Nice Acropolis
Nice, France

ASIA–PACIFIC COMMUNITY MEETING
20 November 2013
Shangri-La Hotel
Kuala Lumpur, Malaysia

Guiding open standards for global payment card security