PCI Security Standards Council®

2025 ASIA-PACIFIC COMMUNITY MEETING

2025 ASIA-PACIFIC COMMUNITY MEETING

Mobile Payment Security:

Addressing Key Risks and Seamless Auth in Alignment with PCI SSF

PCI Security Standards Council®

Abhay Anand

Head of Audit & Assurance

CRED

Dhananjay Singh Parmar

Head of Technology Risk & Compliance

CRED

CRED

PCI Security Standards Council

Agenda

- Convenience vs Complexity
- Beyond Traditional Threats:Understanding Mobile-Specific Risks
- Technical Exploits: Targeting Mobile Payment App Integrity
- Threat Actors in Action:Exploiting Trust and Technology
- The Evolving Threat: AI and Biometric Vulnerabilities
- Key SSF Principles Applied to Mobile Payment
- A Foundational Approach:The Blueprint for Secure Payment Software
- Practical Implementations
- Maintaining User Experience (UX)
- Key Takeaways

Convenience vs. Complexity

The Mobile Revolution:

The convenience of mobile payments brings unparalleled ease and speed, driving explosive global growth.

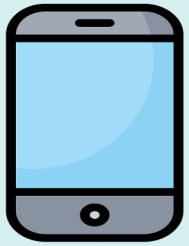
Complexity and Challenge:

This convenience introduces new, unique security complexities beyond traditional payment systems.

“How do we maintain user experience while building robust security that addresses the new mobile threat landscape?”

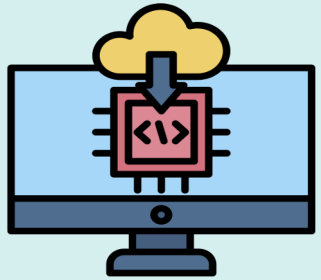
PCI Security Standards Council

Beyond Traditional Threats: Understanding Mobile-Specific Risks



Device-Centric Risks

- Lost/Stolen Devices
- Malware/Rooting/Jailbreaking
- Weak Device Security



Software & Hardware Risks

- Public Wi-Fi Vulnerabilities
- App-Specific Vulnerabilities
- Phishing & Social Engineering

User Behavioral Risks

- App Side loading
- Ignoring Security Warnings/Update.
- Weak Password Reuse

PCI Security Standards Council

Threat Actors in Action: Exploiting Trust and Technology

Telegram-based RAT (Remote Access Tool)

- Malicious APKs
- Exploits mobile permissions to read sensative details
- Silently exfiltrates stolen data via Telegram’s secure API

Fake Customer Support App Scam

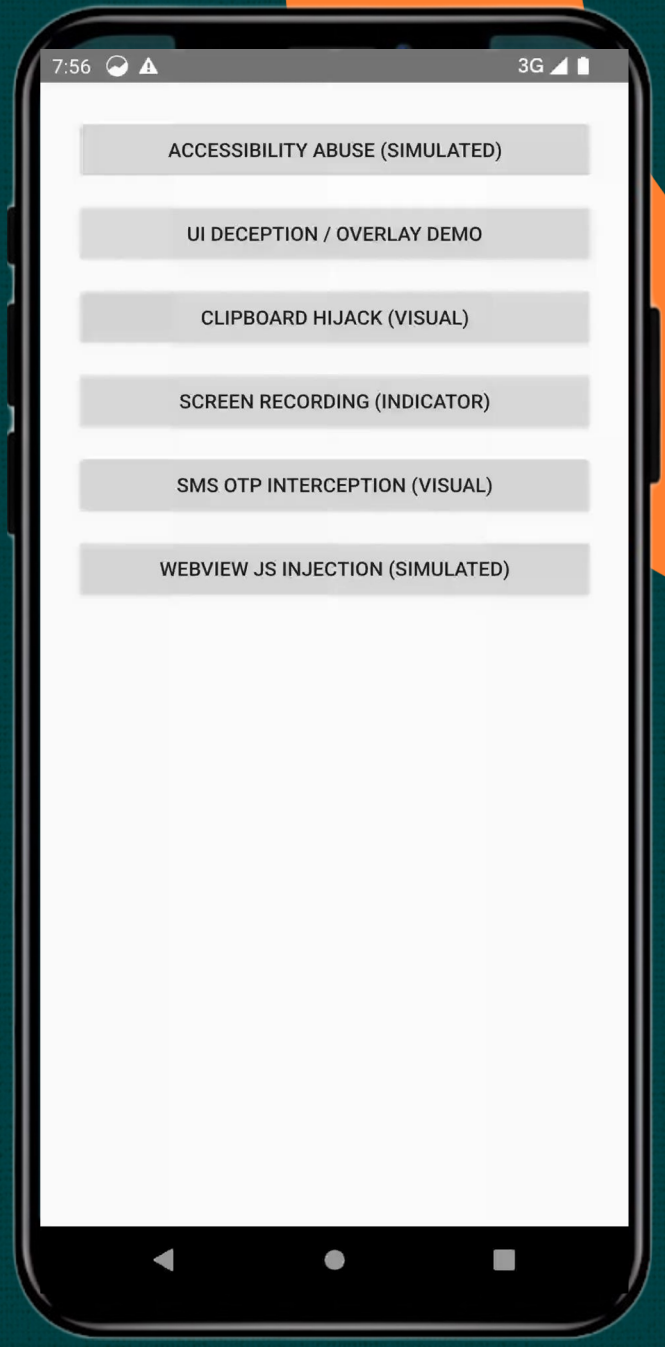
- Trick user into downloading a malicious remote access app
- Leverages Accessibility Service and Screen Recording permissions

QR Scams and Social Engineering

- Fraudulent QR codes are used to redirect payments
- Scammers send fake "Collect" requests to trick users into approving a debit by entering their PIN

Technical Exploits:
Targeting Mobile Payment App Integrity

- Abuse of Accessibility Services
- UI Deception Attacks (Overlay, Tapjacking)
- Insecure Data Storage & Clipboard Hijacking
- Improper Intent Handling / Intent Hijacking
- Third-party SDK Vulnerabilities



PCI Security Standards Council

The Evolving Threat: AI and Biometric Vulnerabilities

Biometric Authentication Weaknesses:

- Insecure Fallback
- Lack of Liveness Detection
- Blind Trust in Device-Level Results

Emerging AI-Powered Threats:

- Deepfake & Voice Phishing
- AI-Driven Malware & Smart RATs
- Behavioral Biometrics Spoofing

PCI Security Standards Council®

How to solve?

Key Principles

- Minimizing Attack Surface
- Protecting Sensitive Data
- Secure Authentication & Access Control
- Tamper Protection
- Secure Updates
- Logging & Monitoring

A Foundational Approach:
The Blueprint for Secure Payment Software

The PCI Software Security Framework (SSF) - A modern security framework designed to help software vendors to develop, distribute, and maintain secure payment applications

PCI SSF focuses on secure software development and deployment processes specifically for payment software, covering the entire software development lifecycle

PCI SSF Importance :

- Provides a comprehensive framework for secure payment software development.
- Enhances protection against security threats and data breaches.
- Streamlines compliance and certification processes.
- Supports trust and security in digital payment transactions.

PCI Security Standards Council®

Practical Implementations

PCI Security Standards Council

Practical Implementation 1: Advanced Device Binding

Tying Identity to Device: Leveraging Hardware Security

Objective : Creating a unique, cryptographic link between a payment application and a specific mobile device.

Leveraging Hardware Security:

- Trusted Execution Environment (TEE) / Secure Enclave (iOS): Isolated, secure environments for cryptographic operations and key storage.
- Android Key Attestation: Verifying hardware-backed keys and device integrity.
- SIM-based Authentication : Utilizing SIM card security for device identification.

PCI SSF - Authentication & Authorization Controls

- Creating a robust, cryptographic link between the user, their SIM, and device.

Practical Implementation 2: Multi-Layered Authentication

Beyond Passwords: A Multi-Factor Approach for Mobile Payments

Concept: Combining multiple authentication factors to strongly verify user identity.

- Leveraging PKI for Seamless Authentication:
  - PKI (Public Key Infrastructure)
    - Use digital certs and crypto keys for transaction signing
    - Mobile Integration: PKI certificates stored in secure hardware linked to biometrics
    - Benefit: Provides strong assurance for critical transactions
  - Mitigating Biometric Weaknesses
    - Enforce TEE-backed biometric to prevent replay attacks
    - Implement strong liveness detection

PCI SSF - Secure Authentication & Access Control, Sensitive Data Protection & Runtime Protection

PCI Security Standards Council

Practical Implementation 3: Tokenization Strategies

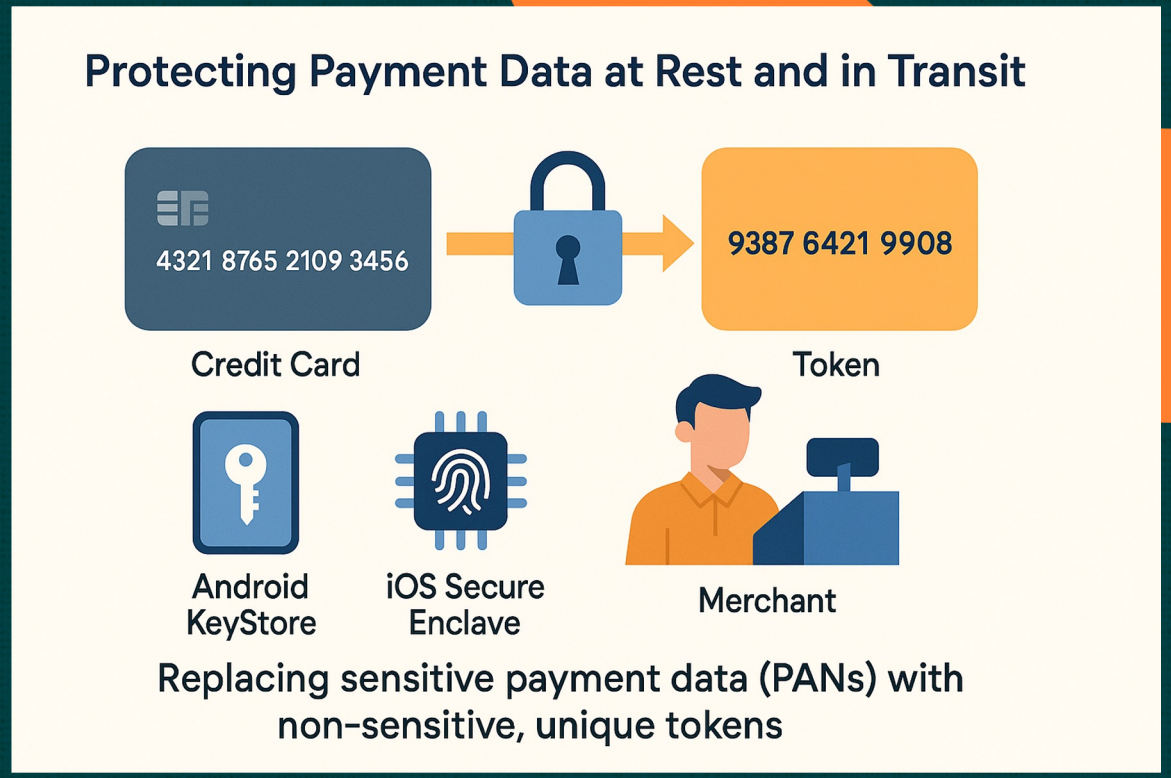
Protecting On Device Payment Data at Rest and in Transit by replacing payment data with unique tokens.

Android KeyStore

- Securely stores cryptographic keys for tokenization
- Hardware-backed keys for strong extraction resistance
- Require user device authentication for key access

iOS Secure Enclave

- Dedicated hardware module for cryptographic key storage
- Keys are isolated, ensuring sensitive data protection
- Significantly reduces PCI DSS scope



- PCI SSF - Directly addresses "Protect Stored Cardholder Data" and "Encrypt Transmission" requirements

PCI Security Standards Council

Maintaining User Experience (UX)

Security Without Sacrifice: The UX Imperative

- **Biometrics**
- **Seamless Background Processes**
- **Contextual Authentication**
- **Clear & Concise Communication**
- **Frictionless Enrolment**

Key Takeaways:
Three Pillars for the Future of Mobile Payment Security

1. New Threats, New Defences:
Dynamic threats that require specialized security strategies

2. Seamless Authentication is a Strategic Imperative:
Leverage advanced controls like PKI, biometrics, SIM binding and elevate trust and security in mobile payments

3. Security by Design is Key:
Align with PCI SSF principles in software design and leverage native platform features

PCI Security Standards Council®

THANK YOU

PCI Security Standards Council®