MOBILE PAYMENT SECURITY RISK AND RESPONSE

Shaoliang Chen
Senior Security Expert
Shaoliang Chen
Senior Security Expert

Email: stevenchen2081@gmail.com
Twitter: @stevenchen2081
WeChat:

- **Position**: Senior Security Expert at PricewaterhouseCoopers (PwC) Beijing office
- **Security experience**: A decade of experience in the information security area
- **Finance Industry experience**: As a Chief Security Architect role in mobile payment system construction
- **Social activities**: Presenter at security and financial conferences
- **Personal contributions**: A series of papers on mobile payment security
Agenda

• Mobile Payment Ecosystem
• Mobile Payment Risk Analysis
• How to Build Security Mobile System
Part 1

Mobile Payment Ecosystem
Mobile Payment Definition and Methods

- Mobile Payment
  - QR code Payment
  - NFC Payment
  - RFID
  - Smart Card
- Near field communication classical scenarios: Near Field Communication (NFC) technology, POS
- Remote payment classical scenarios: mobile payment by QR code, sound waves, fingerprint, etc.
Global Mobile Payment Well-Known Brands

- China
  - Alipay: NFC, QR code
  - WeChat Pay: QR code
  - UnionPay: NFC, QR code

- United States
  - Apple Pay: NFC
  - Google Pay: NFC
  - Square: QR code
  - PayPal: QR code

- Other Brands
  - South Korea: Samsung Pay
  - India: Paytm
  - Europe: Wirecard
  - ......

reference: xinhuanet.com, Chinadaily.com, various report
Mobile Payment Security Incidents

Apple Pay: Fraudsters Exploit Authentication
Mobile a Breeding Ground for Counterfeit Card Fraud
Tracy Kittner (FraudBlogger) - March 3, 2015  0 Comments

reference: bankinfosecurity.com

Samsung Pay: Tokenized Numbers, Flaws and Issues
Salvador Mendoza
July 14, 2016

reference: zdnet.com/blackhat.com
Security Issues for Payment

Base on Capgemini & BNP Paribas “world-payments-report-2017”

Survey revealed that bank executives are most concerned about cybersecurity (65.0%) and data privacy (35.0%)

More and more people focus on cyber security for payment

reference: www.worldpaymentsreport.com
Mobile Payment Architecture—QR payment

Online QR Payment

Mobile Payment User → Mobile Payment Device → Mobile Payment APP → Backend Data Communication → Content Communication

Payment Content Module

Mobile Payment Platform

Accounting System  Deal System  Security Protection  Risk Control

Network  Hardware  Software
Mobile Payment Process—QR payment

Online QR Payment

1. Open the payment app
2. Scan commodity OR code
3. OR code is identified
4. Confirm information

Mobile Payment User

Mobile Device

Merchant OR code

Merchant

Server

Database

Mobile Payment System

5. Send payment request
6. Return payment result

6.1 Return payment result
6.2 Return payment result
Online NFC Payment

Payment Content Module

Mobile Payment Platform

Accounting System  Deal System  Security Protection  Risk Control

Network  Hardware  Software

Mobile Payment User

Mobile Payment Device

NFC Module

POS

Merchant

NFC Communication

Backend Data Communication

Content Communication
Mobile Payment Process- NFC payment

1. Open the payment app
2. Send NFC payment request
3. Read NFC account

Device with NFC Module

Merchant POS

4. Send order information and deduct money request
5.1 Return payment result
5.2 Return payment result

Mobile Payment User

Mobile Payment System

Server
Database
Part 2

Risk and Analysis
Mobile Payment Risk Demo—QR Payment

1. Open the payment app
2. Hacker forge fake OR code and decoy victim to scan
3. Scan OR code
4. Malware infection/back door
5. Hackers control victim account

Hacker website

Malicious OR code

Hacker

Payment Gateway

Server
Database

Victim
Mobile Payment Risk Demo—Phishing

1. Hacker build fake base station
2. Send phishing SMS
3. Open URL in SMS
4. Malware infection/backdoor
5. Hackers control user account

Hacker website
Fake base station
Payment Gateway
Server
Database
Victim

Email: stevenchen2081@gmail.com
Risk Analysis — Device

- Phishing
- Cross Frame
- Clickjacking
- Man-in-the-Middle
- Buffer Overflow

- Sensitive Data Storage
- No Encryption/Weak Encryption
- Improper SSL Certificate Validation
- Source Code Vulnerability
- Incorrect Default Permissions
- Escalated Privileges
- Malware

- No Passcode
- Weak Passcode
- Operating System Vulnerability
- Software Vulnerability
- No Encryption
- Weak Encryption

- Side Channel Attack
- Baseband Attack
- SMS Phishing
- Device Lost
Risk Analysis — Network

**Protocol**
- Man-in-the-Middle (MITM)
- Session Hijacking
- DNS (Domain Name System) Poisoning
- Fake SSL Certificate

**Access**
- Wi-Fi (No Encryption/Weak Encryption)
- Rogue Access Point
- Packet Sniffing
Risk Analysis — Backend System

- **Platform Vulnerabilities**
- **Brute-Force Attack**
- **OWASP Listed Web Vulnerabilities**

1. **Web Application**
   - SQL Injection
   - Privilege Escalation
   - Data Dumping
   - OS Command Execution

2. **Database**
   - APT Attack
   - Server Misconfiguration
Part 3

How to build security mobile payment system
Mobile Payment Security Architecture

**People & Device**
- Device environment security check
- Malware software check

**APP**
- APP source code security
- File encryption locally
- SDLC

**Communication**
- Encryption protocol
- Security check of access

**Server**
- Server OS update
- Server application update
- Anti-DDoS
- API

**User Account**
- Identity authentication
- Strong authentication
- User privacy management

**Risk Control**
- User transaction identification
- Risk management
- Anti-Fraud

---

**Security Assessment**

**Account Authority Management**

**Security Operation**

**Privacy Protection**

**Security Intelligence**

**Compliance**

**Authentication System**

**Anti-Fraud**

**Data Security**

**SDLC**
# Best Practice
– Authentication Technology Comparison

<table>
<thead>
<tr>
<th>Technology</th>
<th>Features</th>
<th>Key Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security key</td>
<td>• Strong encryption&lt;br&gt;• Hardware key/USBkey&lt;br&gt;• Key file (*.key...)&lt;br&gt;</td>
<td>• Build the key management system and ensure security&lt;br&gt;• Hardware key/USBkey is proved more secure by now</td>
</tr>
<tr>
<td>Biometric (fingerprint, facial recognition)</td>
<td>• Higher identification rate&lt;br&gt;• User unique&lt;br&gt;</td>
<td>• Risk of permanent leakage&lt;br&gt;• Natural person property&lt;br&gt;• Privacy protection and legal compliance</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>• Hardware tokens&lt;br&gt;• Software tokens&lt;br&gt;• Smartphone tokens&lt;br&gt;• Email, SMS&lt;br&gt;</td>
<td>• Mandatory to use when register&lt;br&gt;• Anti-fraud combination</td>
</tr>
<tr>
<td>Multi-factor Authentication</td>
<td>• Multi-dimension&lt;br&gt;• Knowledge, possession&lt;br&gt;• Various technologies (Security key, SMS, and etc.)</td>
<td>• Backend analysis&lt;br&gt;• Risk model judgement</td>
</tr>
<tr>
<td>National IDs and ePassports</td>
<td>• Name&lt;br&gt;• ID number</td>
<td>• Verified by public security department&lt;br&gt;• Response whether match between name and ID number&lt;br&gt;• Privacy</td>
</tr>
</tbody>
</table>
Best Practice – Key Points for Security Testing

Sample test scenarios:
- Check **block mechanism** whether effectively deployment of payment process when **using proxy IP address**.
- Check **lock mechanism** whether effectively deployment of login process with **wrong user credential**.
- Check **block mechanism** whether effectively deployment of payment process when **replacing SSL certificates**.

Device
- Root
- OS version
- Access point/wireless/4G
- Proxy
- SSL certificates
- Malware

APP
- Communication
- Sensitive information
- Login identity authentication
- Logic check

Payment Backend
- SQL Injection/OWASP
- Database permission
- Interfaces
- Transaction quota
- Data Encryption
- Blacklist (IP address or high risk account)
- PCI-DSS

Bank1
Bank2
Best Practice – Anti-Fraud 1

**Account**
- Account status, active account or not
- Black account list
- Account risk rate

**Device information**
- Device serial number
- Device network MAC address
- Device IMEI number
- Device MEID number

**Big data analysis**
- Frequency statistics
- Biggest statistic

**Behaviour habit**
- Trade time
- Trade device
- Trade amount number
- Trade bank credit card

**Suspicious transaction**
- Abnormal operation, such as quickly transfer to multiple accounts.
- Change account payment password in late night

**Account Relationship**
- Multiple accounts with the same identified individuals
- Geographical position
**Scenario:** Transaction IP address change in short time for one person with one account.
First transaction IP address in China. Second transaction IP address in USA.

**Cause:** Account information has been stolen or used proxy.

**Solution:**
1. Block transaction directly
2. Manual verification
3. Deep analysis/Model
Mobile Payment Challenge—Method Selection

- Which is more security?
  - NFC & QR code (Two principles)
    - Base on your business requirement
    - Every technology has vulnerabilities

### NFC VS QR code?

<table>
<thead>
<tr>
<th>Method</th>
<th>Security Authentication mode</th>
<th>Security Control</th>
<th>Reference Standard</th>
<th>Main Risk Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFC</td>
<td>• Security SE</td>
<td>• Small amount transaction(no password and signature)</td>
<td>• GSMA Organization</td>
<td>• Lost device</td>
</tr>
<tr>
<td></td>
<td>• Security chip</td>
<td>• Backend quota one day one account</td>
<td>• ECMA Organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>QR code</td>
<td>• Encrypted URL</td>
<td>Transaction amount control one day with one account&lt;500 CNY</td>
<td>China UnionPay has independent QR code standard and ecosystem, “EMVCo QR Code Specification for Payment Systems: Consumer Presented Mode 1.0”</td>
<td>• Malware Phishing</td>
</tr>
<tr>
<td></td>
<td>• Security software</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

URL:https://www.emvco.com/emv-technologies/qrcodes
Mobile Payment Challenge – Smart Device

• Various payment methods
  • i.e. wearable device payment

• More complicated ecosystem
• More interfaces
• More dimensional attacks
• More risk points

Reference: csoonline.com

Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON

The results from this year’s IoT hacking contest are in and it’s not a pretty picture.
Conclusions

- Identification authentication is the key factor for mobile payment security.
- New authentication technology does not mean that it is more secure.
- Pay more attention to privacy protection.
- Accumulating bad samples is the key to building a risk control model.
- Machine learning will become good solution to against mobile payment attack in the future.
- Rules and risk control models must be worked together now.
THANK YOU

Email: stevenchen2081@gmail.com
Twitter: @stevenchen2081
WeChat: