PCI Security Standards Council

Mobile Payment Reverse Engineering & Security Invasion

Presented by: Dr. Obadare Peter Adewale

About Me

- Obadare Peter Adewale is the Co-Founder and the Chief Visionary officer of Digital Encode Limited.
- Peter is arguably the most “Credentialed” PAN-African Digital Trust Leader, Cybersecurity Strategist, GRC Thought Leader & Global Technopreneur with 56 professional certifications.
- Peter is a Forbes Technology Council Member & Forbes Best of Africa - Outstanding Digital Trust Leader, 2023 awardee.

PCI Security Standards Council

Objectives

1. Understand different mobile payment architectures

2. Demystifying mobile payment vulnerabilities

3. How PCI DSS can help to improve mobile payment security

PCI Security Standards Council

Starting Thought:

Some futurologists and industry experts predict that in years to come, mobile phones will become remote controls for our whole lives, while others forecast that in the future mobile phones will literally run our lives for us. **(Catherine Hiley, August 10, 2023)**

Cybersecurity Enablers:

Any digital asset can be digitally invaded if there is an issue with any of the following factors: “ADIO”

Architecture

Design

Implementation

Operation

Mobile Payment Infrastructures

The mobile infrastructure rides on the following to deliver services to mobile phones:

1. GSM
2. GPRS
3. EDGE
4. 4G/5G

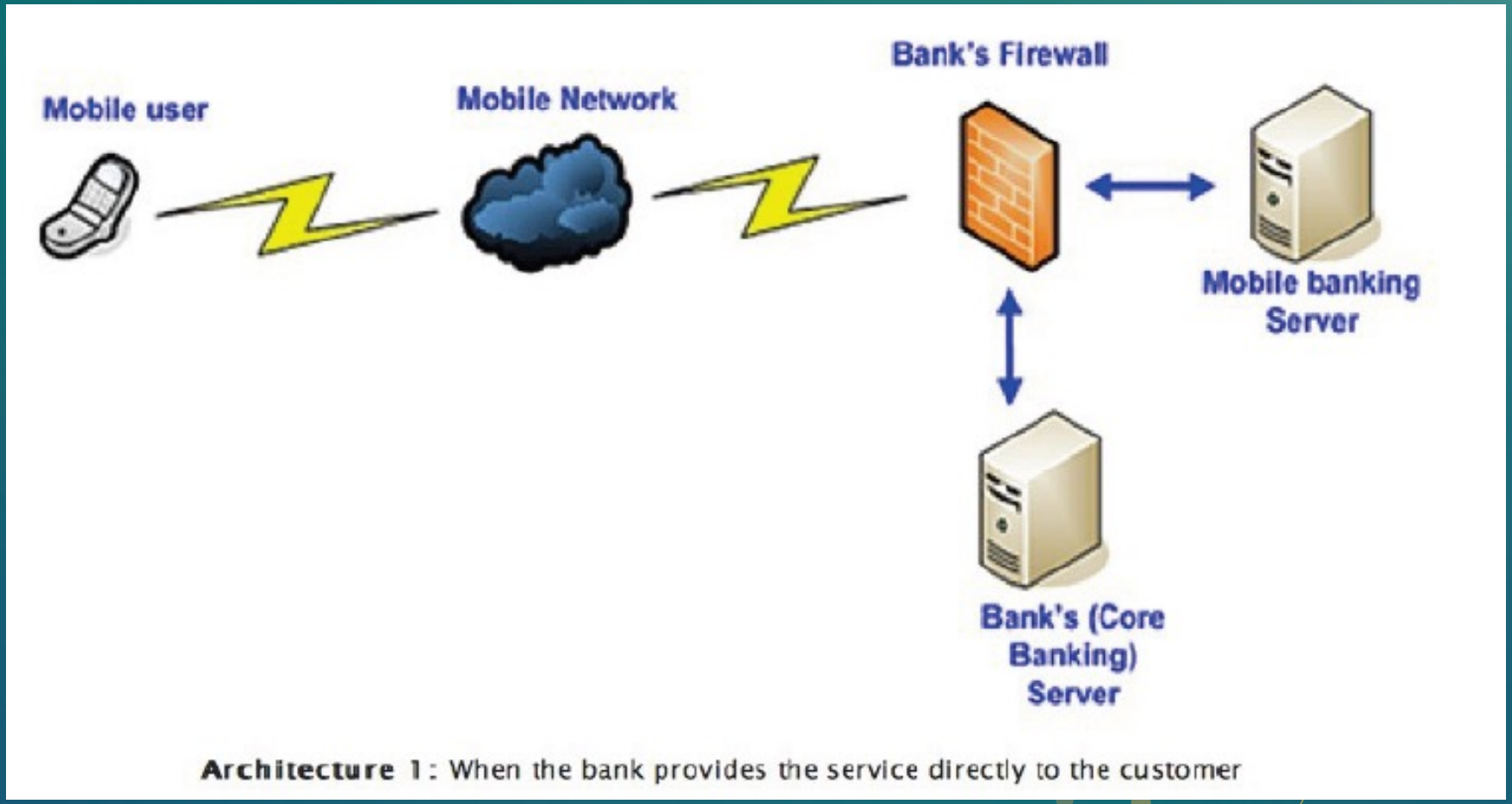
Mobile Payment Services:

1. A/C Bill Payment
2. Fund Transfer
3. Shopping Purchasing items
4. Fixed deposit enquiry
5. Viewing statement
6. Viewing Cheque status
7. Stopping Cheque Payment
8. Cheque Book Request

Mobile Payment Provisioning

The services can be provided to customers directly by the bank or through a 3rd party vendor.

Mobile Payment Architecture (Direct) - 1



Architecture 1: When the bank provides the service directly to the customer

PCI Security Standards Council

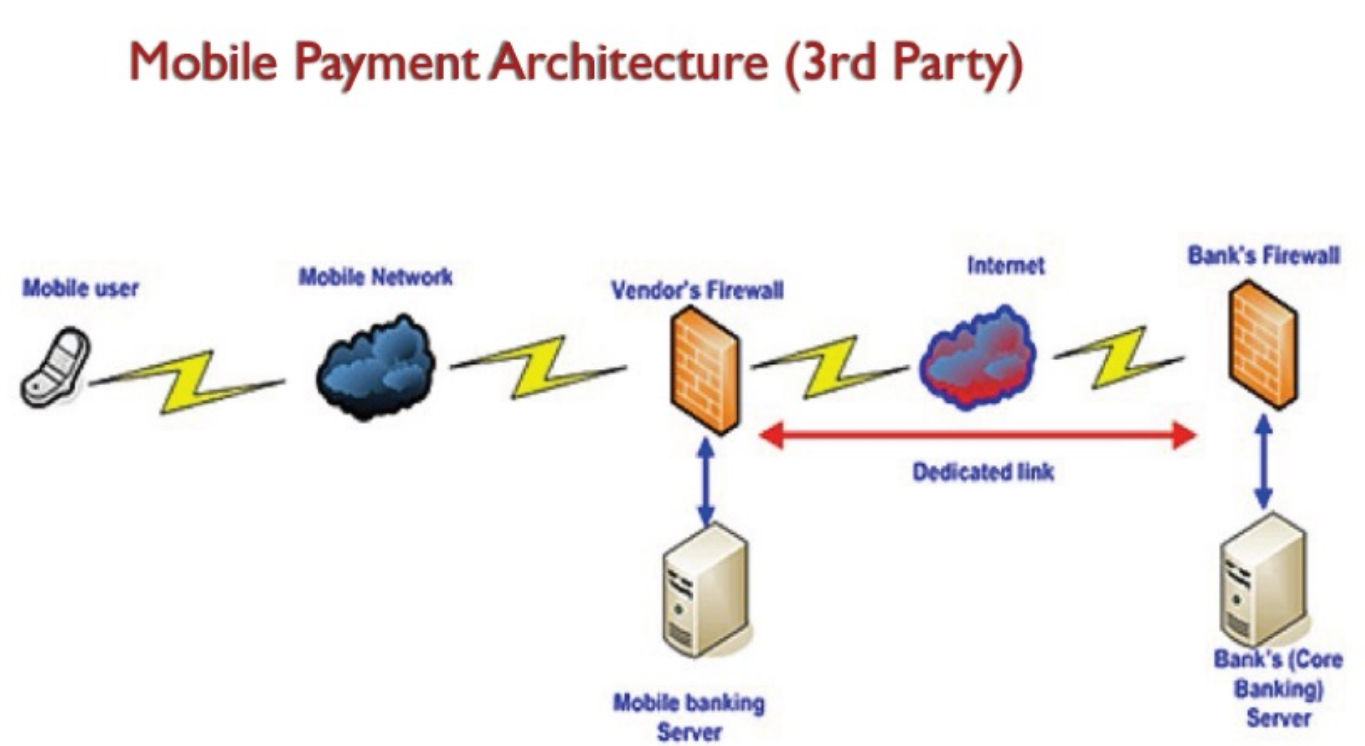
Mobile Payment Architecture (Direct) - 1

Mobile Payments Architecture I

- *The setup will have a web server, application server and the database at the bank's premises. We shall call this the mobile banking server for ease of understanding.*
- *The application will ensure what services are to be provided to the customer. The database can be the same as the Core Banking database, having another table for mobile banking users.*
- *The customer uses his/her mobile phones to transact through the mobile network. The Mobile banking server in turn talks to the Core banking systems of the bank for user authentication, processing transactions, authorization, etc*

PCI Security Standards Council

Mobile Payment Architecture (3rd Party) - 2



PCI Security Standards Council

Mobile Payment Architecture (3rd Party) - 2

Mobile Payments Architecture

- *This is another popular architecture as Banks can quickly roll out their mobile banking solutions by connecting to a 3rd party.*
- *This is also the architecture with more security issues as interconnection with a 3rd party is involved. In this architecture, the mobile banking servers are located at the 3rd party vendor's data centre.*
- *These servers will talk to the Core Banking servers of the bank through a secured channel (dedicated or shared link) for authentication, authorization and transaction processing.*

PCI Security Standards Council

User Provisioning

Prerequisites to Using the Facility

- *The customer has to first register with the Bank for using Mobile banking facility by linking the user's mobile number with the account number.*

Mobile App Platforms

1. Flutter - It is developed by Google, it is also cross-platform compatibility (it will work on both iOS and Android). Also, Dart is the programming language behind flutter

2. React Native - This is a java script mobile framework and most developer use this

3. Xamarin is a cross platform opensource integrated directly into .Net Framework with tools and libraries specifically for building apps for Android, IOS, TV OS, MacOS and Window (C#)

Top 5 Mobile App Critical Business Logic Vulnerabilities:

Insecure Input Validation (Negative value Injection)

Account Swapping

Insecure direct Object Reference - Transaction History, Account Summary etc.

Information Disclosure – PAN , Authorization Tokens, PIIs, etc

Authentication and Authorization Flaws - OTP Bypass

Practical Demonstration

Tools For Mobile App Digital Security Invasion:

1. Nox – Mobile application emulator
2. Burpsuite – Man-In-The Attack / Business Logic Tool
3. Jadx – Reverse Engineering – (Decompiler)
4. Android Debug Bridge – Debugging Andriod based devices
5. Frida – Allow interaction with Andriod APK in other to injects code so as to bypass security technique like SSL Pinning, Root detection
6. Mobsf – Mobile Static code analysis

Security Standards Council®

How PCI DSS Can Achieve Defense In Depth

Most of the PCI DSS requirements that affect the Mobile App security process fall under:

Requirement 3

Requirement 4

Requirement 6

PCI Security Standards Council

How PCI DSS Can Achieve Defense In Depth

Requirement 3: Protect Stored Account Data

- **3.1** Processes and mechanisms for protecting stored account data are defined and understood.
- **3.2** Storage of account data is kept to a minimum.
- **3.3** Sensitive authentication data (SAD) is not stored after authorization.
- **3.4** Access to displays of full PAN and ability to copy cardholder data are restricted.
- **3.5** Primary account number (PAN) is secured wherever it is stored.
- **3.6** Cryptographic keys used to protect stored account data are secured.
- **3.7** Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.

PCI Security Standards Council

How PCI DSS Can Achieve Defense In Depth

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

- **4.1** Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.
- **4.2** PAN is protected with strong cryptography during transmission

PCI Security Standards Council

How PCI DSS Can Achieve Defense In Depth

Requirement 6: Develop and Maintain Secure Systems and Software

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

6.2 Bespoke and custom software are developed securely.

6.3 Security vulnerabilities are identified and addressed.

6.4 Public-facing web applications are protected against attacks.

6.5 Changes to all system components are managed securely.

PCI Security Standards Council

Thank You

Europe Community Meeting 2023

PCI Security Standards Council