B.Tech. Project

on

Digital Payment Apps

Mid-Term Presentation
September 2024

Submitted By :

Tushman Khalse 2019CS10411
Shreejeet Golhait 2019CS10351

Supervised by: **Prof. Tarun Mangla**

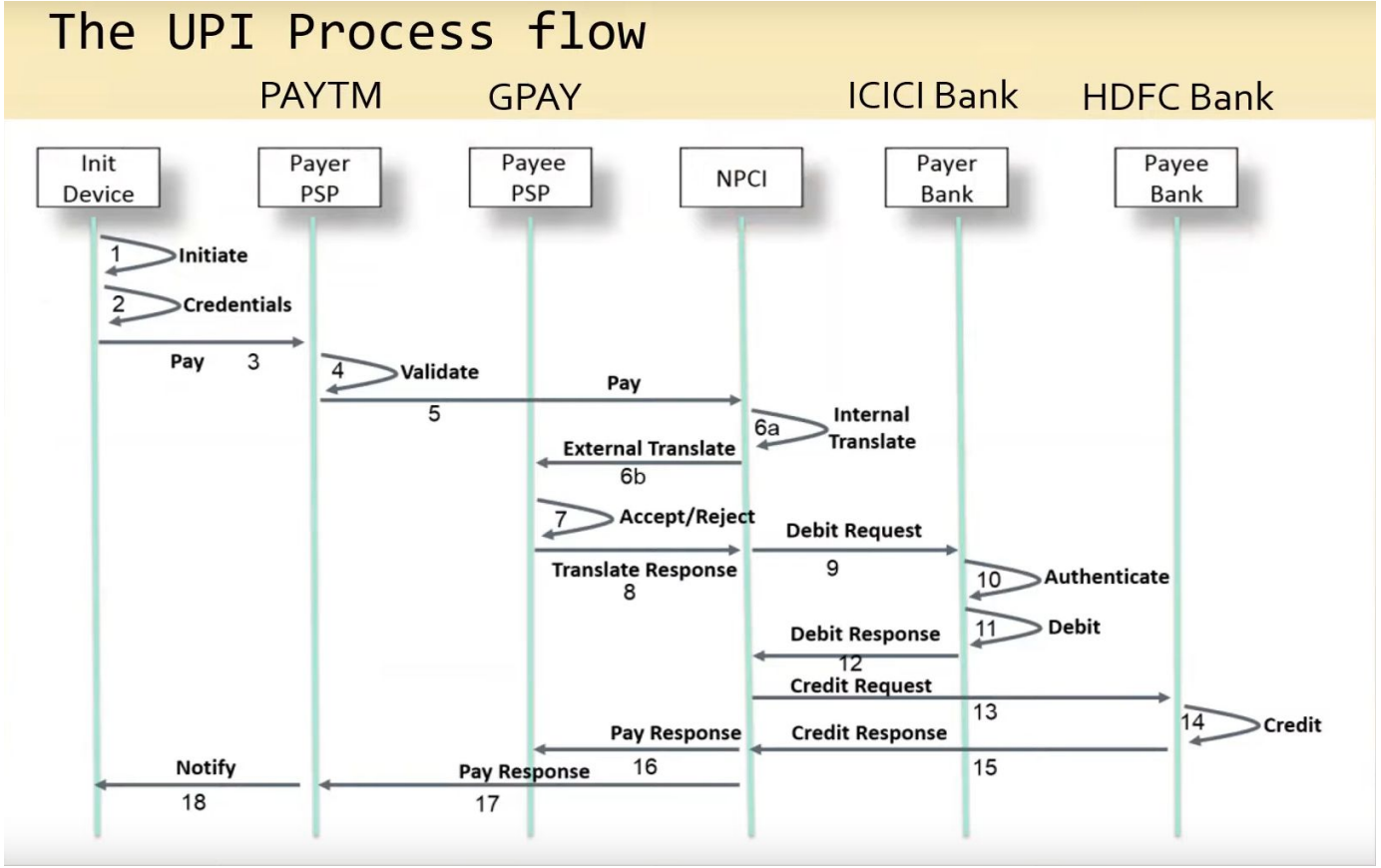
Introduction

- **UPI apps are the backbone of India's digital economy**, enabling millions of secure, instant transactions daily.
- **The rapid adoption of UPI emphasizes the need to optimize transaction performance**, especially under varying network conditions.
- **We aim to analyze network traffic and interactions during UPI transactions**, identifying which steps take the most time.
- **By evaluating UPI apps under different conditions**, we establish benchmarks to improve transaction efficiency.
- **Our goal is to recommend measures to optimize transaction times**, ensuring UPI apps perform efficiently and minimize delays.

Project Objectives

- **Investigating network traffic** generated during UPI payment transactions to uncover patterns and key insights.
- **Decrypting and analyzing data** exchanged in network calls during digital transactions to understand the flow of information.
- **Testing and comparing network behavior** across different UPI apps to identify variations in traffic patterns.
- **Measuring the impact of network conditions** like latency, bandwidth, and packet loss on transaction success rates and performance.
- **Establishing performance benchmarks** for UPI apps to ensure faster transactions and optimized efficiency under varying network conditions.

Theory


The UPI Process flow
PAYTM
GPAY
ICICI Bank
HDFC Bank
Init Device
Payer PSP
Payee PSP
NPCI
Payer Bank
Payee Bank
1 Initiate
2 Credentials
Pay 3
4 Validate
Pay 5
6a Internal Translate
External Translate 6b
7 Accept/Reject
Translate Response 8
Debit Request 9
10 Authenticate
11 Debit
Debit Response 12
Credit Request 13
14 Credit
Credit Response 15
Pay Response 16
Pay Response 17
Notify 18

Theory

Certificate Pinning:

- Certificate pinning is a security measure used by apps to ensure only trusted certificates are accepted for communication.
- It protects against **man-in-the-middle** (MITM) attacks by ensuring the app only communicates with known, valid servers.
- Apps embed a trusted certificate within the code or maintain a predefined list of acceptable certificates.

Theory

Static Certificate Unpinning:

- **APK-MITM**: This tool automates the removal of certificate pinning from APKs to allow traffic interception.
- **Smali Files**: Decompiling APKs with tools like Jadx provides access to smali code, which represents the app's logic.
- **Concept:** This method bypasses pinning by altering the app's original code, and does not require root access.

Dynamic Certificate Unpinning:

- **Frida Framework**: A dynamic instrumentation toolkit that allows runtime code manipulation in apps.
- **Script Injection**: We inject JavaScript into the app during runtime to intercept and disable SSL certificate checks.
- **Concept**: Unlike static unpinning, this method bypasses pinning at runtime without altering the app's original code, but requires root access.

Work Process

1. **Capturing Network Calls using PCAPdroid and Wireshark:**

- Used PCAPdroid to perform MITM attack and capture network traffic.
- Targeted one app in the network capture (specifically PayTM).
- However, captured data was encrypted due to Integrity Checks.
- Analysed captured PCAP file using Wireshark software.

Work Process

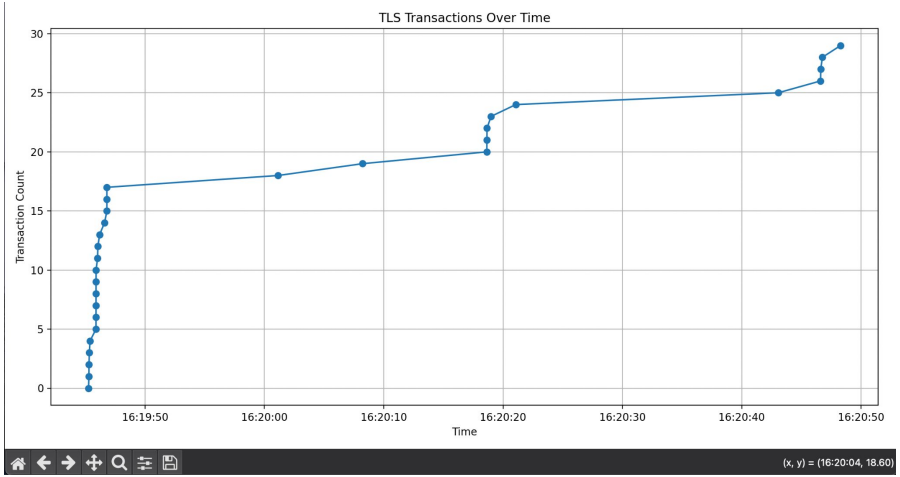
Finding common SNIs for transactions:

- Created a python script using dpkt to filter TLS calls from pcap file.
- Found out common SNI for these apps.
- The script plots TLS calls too.

```
Total packets processed: 738
IP packets found: 738
TCP packets found: 652
Possible TLS packets (port 443): 602
TLS Handshakes found: 30
ClientHello messages found: 14
SNIs extracted: 14

SNI found:
- sig.paytm.com
- graph.facebook.com
- securegw-online.paytm.in
- storefront.paytm.com
- tvybx4-launches.appsflyersdk.com
- assetscdn1.paytm.com
- ws-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com
- digitalapiproxy.paytm.com
- crashlyticsreports-pa.googleapis.com
- api-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com
- kyc.paytmbank.com

Total TLS transactions: 14
```



These are the common SNIs called during transactions:

- PayTM : digitalapiproxy.paytm.com
- GPay:paymentsincentives-pa.googleapis.com, india-paisa-pa.googleapis.com
- PhonePe : apicp2.phonepe.com

Work Process

2. **<u>Modifying APK files to perform Static Certificate Unpinning</u>:**

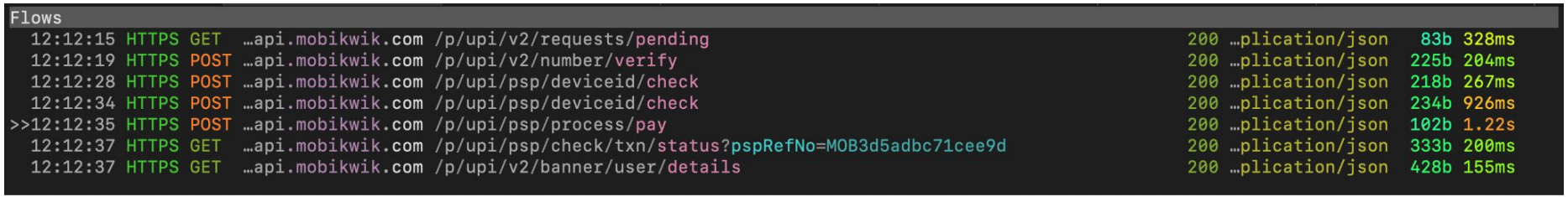
- **Rebuilding APK with apk-mitm**: Used apk-mitm to modify and rebuild the APK after bypassing SSL pinning to capture unencrypted traffic.
- **APK Inspection with Jadx**: Decompiled the APK using Jadx to analyze classes like `TLSSocketFactory` and `VisaCertificateData` for SSL pinning mechanisms.
- **Exploring Certificate Pinning**: Identified that Paytm uses `CertificatePinner` for dynamic pinning, with no static certificate storage in the APK.
- **Understanding Certificate Trust Flow**: Discovered server-side certificate validation bypasses client-side checks, with dynamic pinning instead of embedded certificates.

Work Process

3. **Using Frida tool to perform Dynamic Certificate Unpinning:**

- **Running Frida with the target app**: Attached Frida to the app during runtime to dynamically intercept SSL pinning methods.
- **Bypassing SSL Pinning**: Employed Frida scripts to bypass SSL pinning by overriding methods like `checkServerTrusted` in `TrustManager` (MobiKwik app).
- **Live Traffic Interception**: Enabled real-time inspection of network traffic by dynamically unpinning certificates without modifying the APK.
- **Validation of Unencrypted Traffic**: Confirmed interception of unencrypted HTTPS traffic using MITMProxy after Frida successfully bypassed the app's SSL verification.

Prominent Network Calls involved in a UPI transaction



- **/p/upi/v2/requests/pending**: Payment initiation and checking pending transactions.
- **/p/upi/v2/number/verify**: Verification of contact and UPI ID information.
- **/p/upi/psp/deviceid/check**: Device ID validation for security purposes.
- **/p/upi/psp/process/pay**: Processing the payment and authorizing the transaction.
- **/p/upi/psp/check/txn/status?pspRefNo=…**: Verifying transaction status after processing.
- **/p/upi/v2/banner/user/details**: Fetching user details and confirming transaction completion.

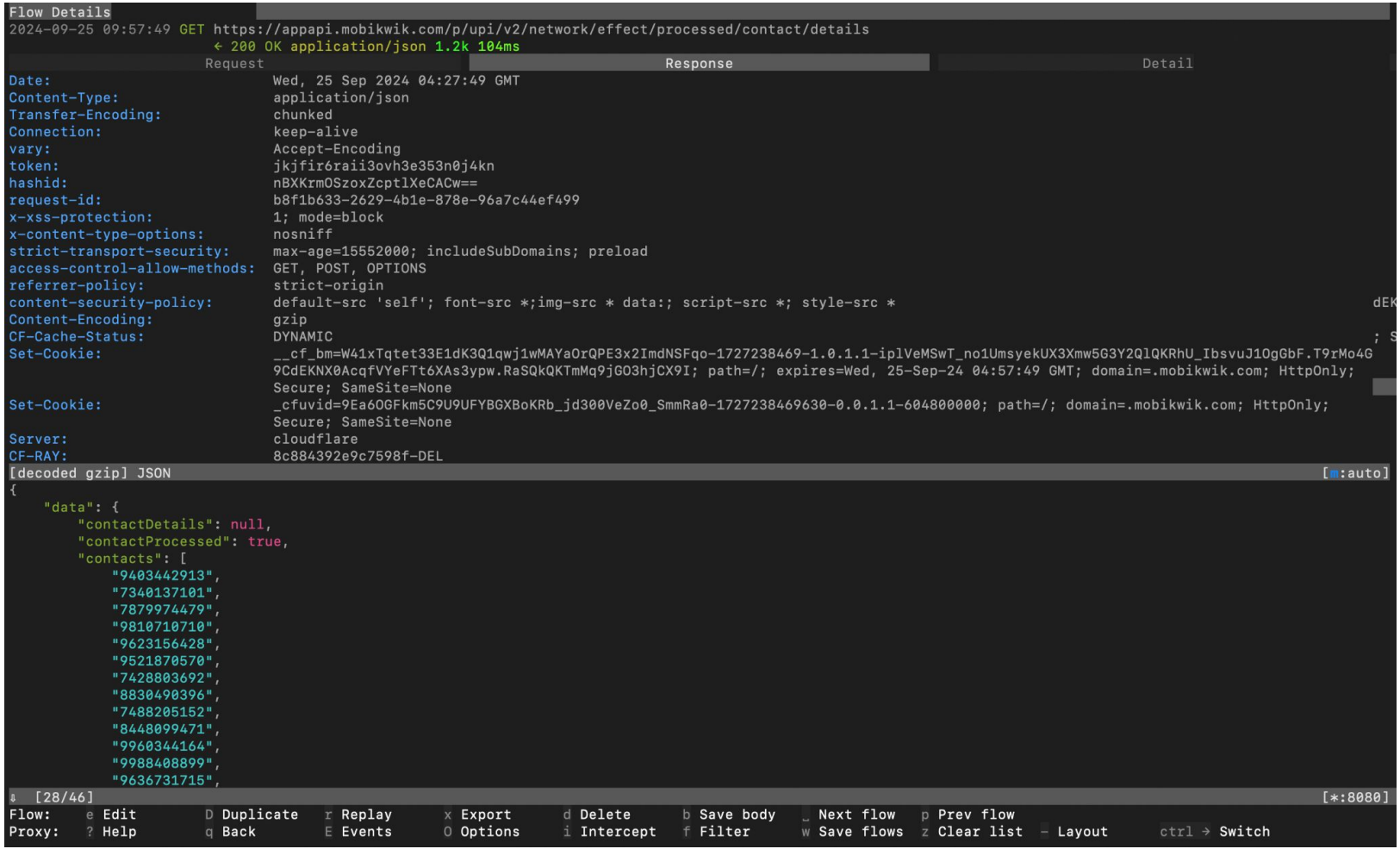
Payee's Information (MobiKwik)


```
[decoded gzip] JSON
{
    "data": {
        "accntNo": "XXXXXX3967",
        "amount": "1.00",
        "appName": "com.mobikwik",
        "credDataLength": "6",
        "credDataType": "NUM",
        "custRefNo": "426954847775",
        "deviceId": "bbbba41d2fa241bd",
        "mobileNo": "917666692875",
        "npciTransId": "HDF6158C16A89684D238BDD69CA8DDDDBCE",
        "payeeAddress": "7620959200@ikwik",
        "payerAddress": "7666692875@ikwik",
        "payerBankName": "State Bank Of India",
        "payerName": "Shreejeet Vijaykumar Golhait",
        "pspRefNo": "OMK265a36c88c64e4e",
        "refId": "",
        "refUrl": "https://upi.hdfcbank.com",
        "transDate": "2024-09-25 09:57:52",
        "transactionNote": "NA",
        "upiTransRefNo": "62154835794"
    },
```

Payer's Profile (PhonePe)


```
[decoded gzip] JSON
{
    "data": {
        "merchantPreferences": {
            "defaultUpiProvider": false,
            "merchantId": "FXM",
            "userId": "U190918180428633095528 8"
        },
        "phoneNumberModel": {
            "countryCode": "91",
            "e164FormatNumber": "+917666692875",
            "phoneNumber": "7666692875",
            "regionCode": "IN"
        },
        "profileDetails": {
            "addresses": [],
            "blacklisted": false,
            "emails": [
                {
                    "active": true,
                    "email": "tushman.khalse@gmail.com",
                    "verified": false
                }
            ],
            "language": "en",
            "name": "Tushman Khalse",
            "passwordSet": true,
            "phoneNumber": "7666692875",
            "registeredSimId": "f6d5576d74323f2ea0e4540a88afb68dd55c4d535399a30c5555882ef298d390",
            "registrationDate": 1568810074273,
            "userId": "U190918180428633095528 8",
            "userType": "PERSON"
        },
        "pspDetails": {
```

Payer's Contact List captured by MobiKwik



Location Captured by PhonePe app during UPI transaction

Flow Details

2024-09-25 10:24:07 POST https://apicp2.phonepe.com/apis/atlas/v3/location/entity/USER/U190918180428633095528 8/multiClassUpdate HTTP/2.0

← 200 application/json 520b 573ms

Request | Response | Detail

[decoded gzip] JSON

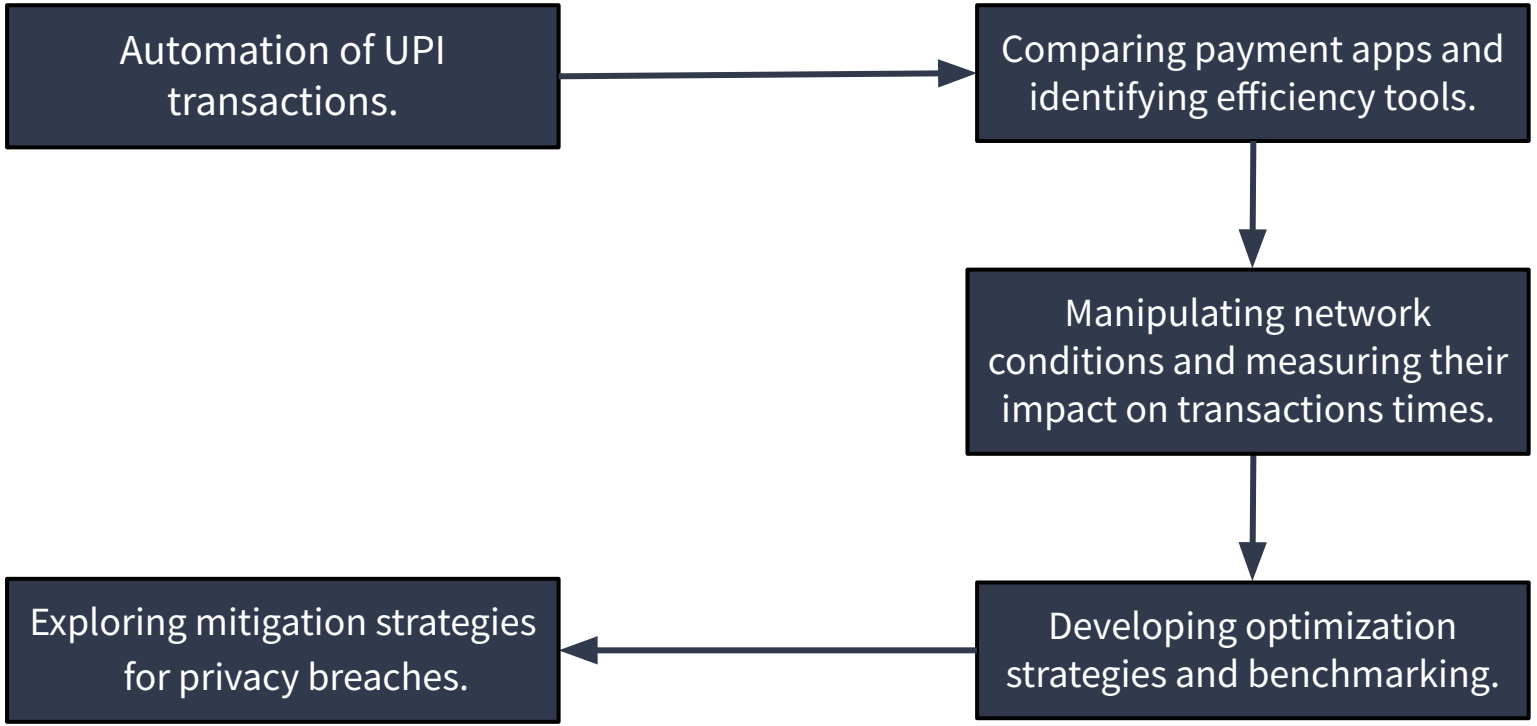

```
{
    "code": "SUCCESS",
    "data": {
        "location": {
            "CURRENT_LOCATION": {
                "created": 1727240047871,
                "entity": "USER",
                "entityId": "U190918180428633095528 8",
                "place": {
                    "city": "New Delhi",
                    "cityCode": "DL1",
                    "country": "India",
                    "countryCode": "IN",
                    "district": "South District",
                    "formattedAddress": "38 m from Nirvaha O Cafe, IIT Delhi, Hauzkhas, Indian Institute of Technology Delhi Hauz Khas, New Delhi, Mehrauli
Subdistrict, South District, Delhi, India, 110016",
                    "id": "9e4fe2be-42d2-3b26-a8f5-d7731c921767",
                    "latitude": 28.546786,
                    "locality": "Indian Institute of Technology Delhi Hauz Khas",
                    "longitude": 77.186312,
                    "nearestPOI": {
                        "distanceInMeters": 37.162715253955476,
                        "name": "Nirvaha O Cafe"
                    },
                    "pincode": "110016",
                    "placeId": "23bf50e7-1ce1-3b81-b3d7-3d1e4a311767",
                    "priority": 0,
                    "state": "Delhi",
                    "stateCode": "DL",
                    "subDistrict": "Mehrauli Subdistrict",
                    "subTitle": "South, Delhi, India",
                    "title": "New Delhi"
                }
            },
```

Important Insights

- **Static Certificate Unpinning:** Despite modifying methods for certificate checks, the rebuilt apps with the MITM certificate installed failed to run properly on the Android device.
- **Dynamic Certificate Unpinning**: While all UPI apps have strong security measures, we only successfully bypassed root detection on **Mobikwik** and **PhonePe** via **Frida**.
- **PhonePe**: PhonePe generates a large volume of **advertisement**-related network calls during payment transactions, potentially slowing down payment processing, while also collecting unnecessary user location data for ad purposes.
- **Mobikwik**: Mobikwik sends the entire list of **user contacts** to the server during every payment, which raises privacy concerns and introduces unnecessary network load.
- **Bottleneck Call**: The /p/upi/psp/process/pay call takes the longest time (>1 sec), making it a bottleneck in the payment process.

Future Works

For the second half of the project, we have planned the following goals for the project:



Thank You