RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Mobile Payment Services: Security Risks, Trends and Countermeasures

SESSION ID: MBS-T07

Suhas Desai

Practice Head – Cloud & Mobile Security
Aujas Information Risk Services

#RSAC

Agenda

Mobile Payments Overview

Mobile Channels & Payment Trends

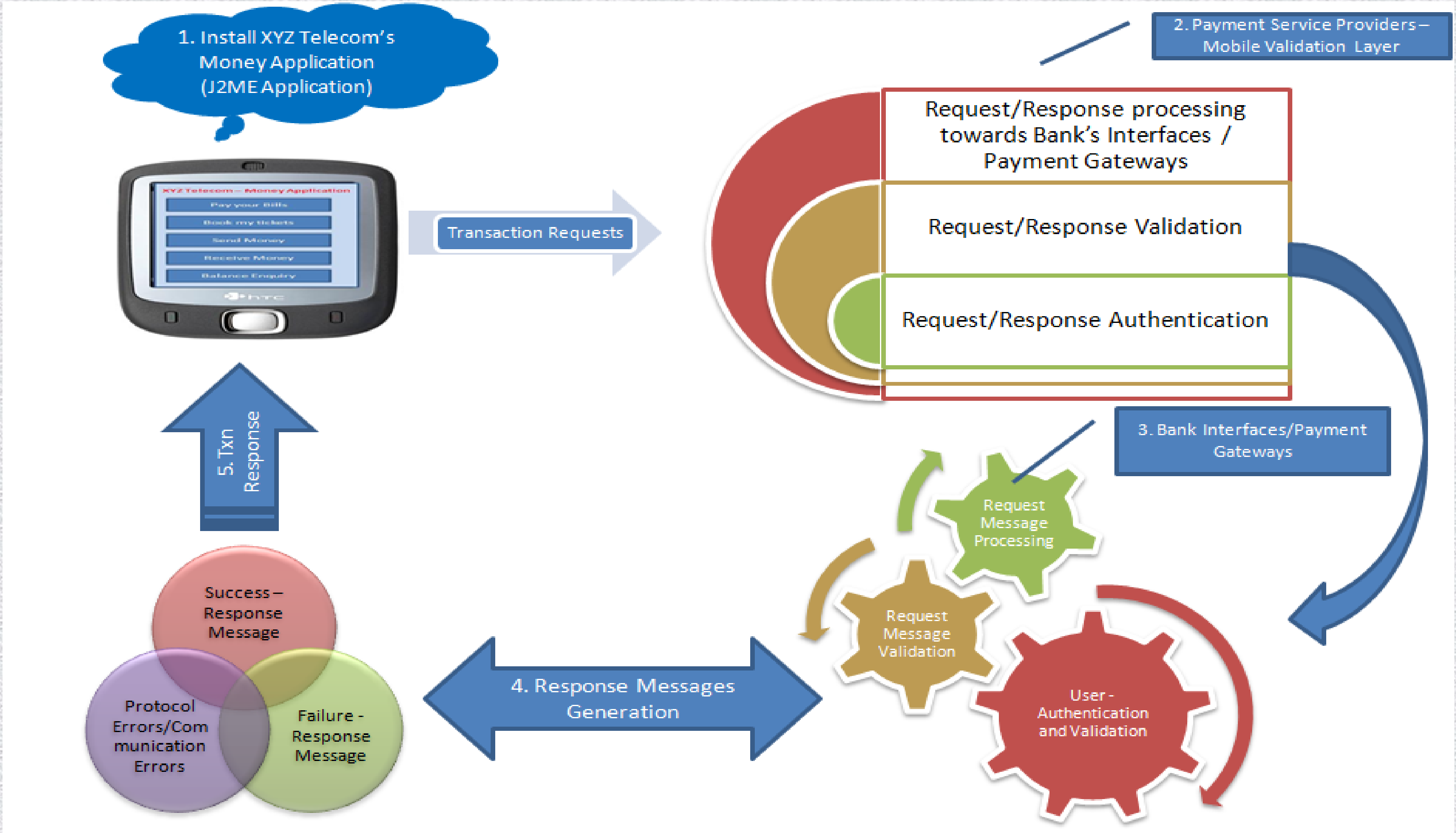
Security Risks

Securing Mobile Payments

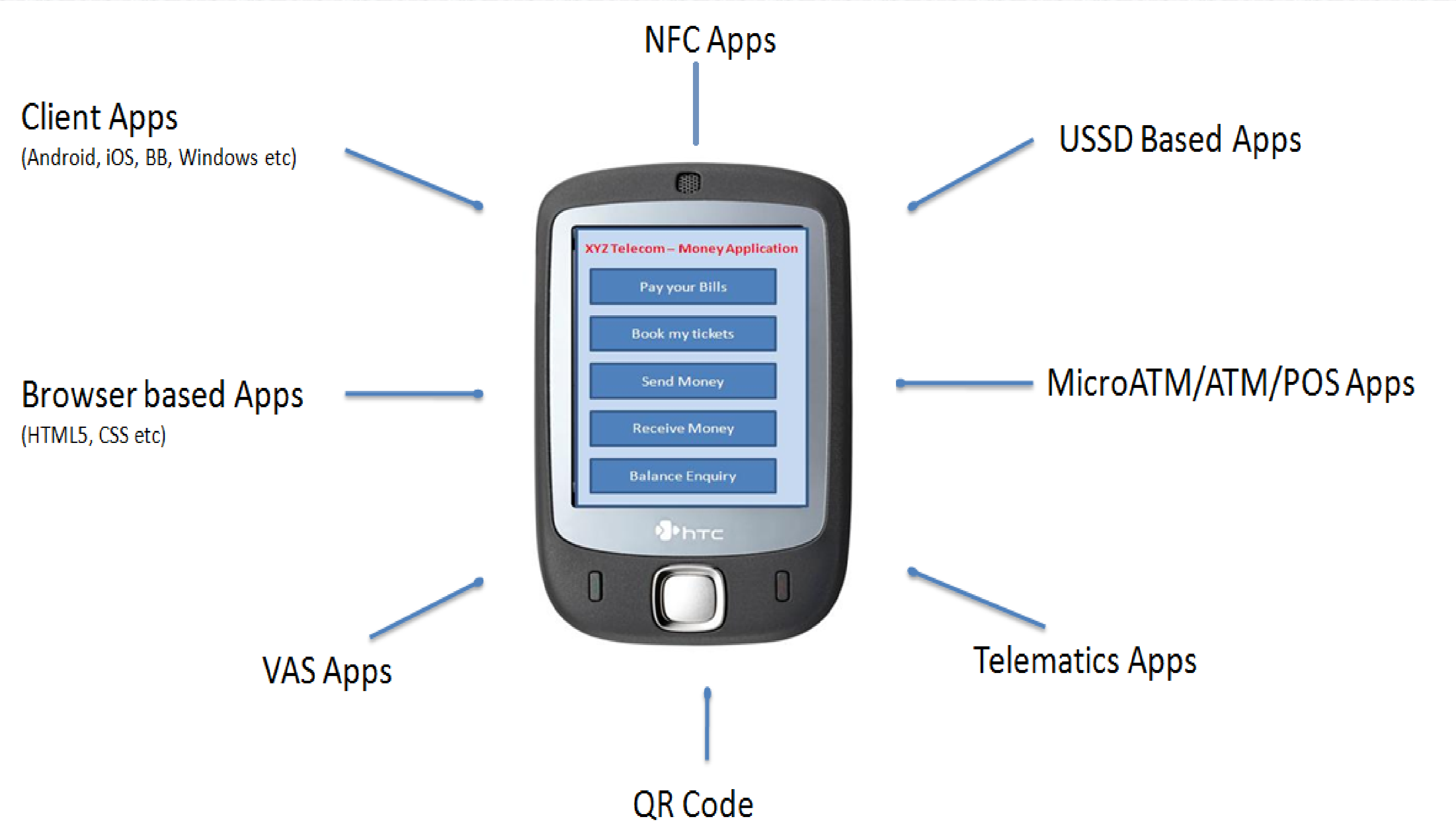
Mobile Payments

Source: Mobile payment image via Flickr by http://commons.wikimedia.org/wiki/File:Mobile_payment_03.JPG

Mobile Payments Architecture


1. Install XYZ Telecom's Money Application (J2ME Application)
XYZ Telecom – Money Application
Pay your Bills
Book my tickets
Send Money
Receive Money
Balance Enquiry
Transaction Requests
2. Payment Service Providers – Mobile Validation Layer
Request/Response processing towards Bank's Interfaces / Payment Gateways
Request/Response Validation
Request/Response Authentication
3. Bank Interfaces/Payment Gateways
Request Message Processing
Request Message Validation
User - Authentication and Validation
4. Response Messages Generation
5. Txn Response
Success – Response Message
Protocol Errors/Communication Errors
Failure - Response Message

Mobile Channels and Payment Trends



Challenges in Mobile Payments

- Microfinance vs. Higher payment transfers
- Mobile Payment Transfer Policy Standardization
- Service Providers and Bank dependencies
- Mobile Payment Apps & Mobile Devices compatibility
- **Mobile Payment Services Security**
- Government Policies for Mobile Payments

Security Risks

- Fraudulent Transactions
- Weak Cryptography
- Mobile Application Server threats
- Mobile Payment Application’s Database threats
- SIM Card Application (USSD /DSTK) Attacks
- Mobile Payment Native Application Security

Business Impact

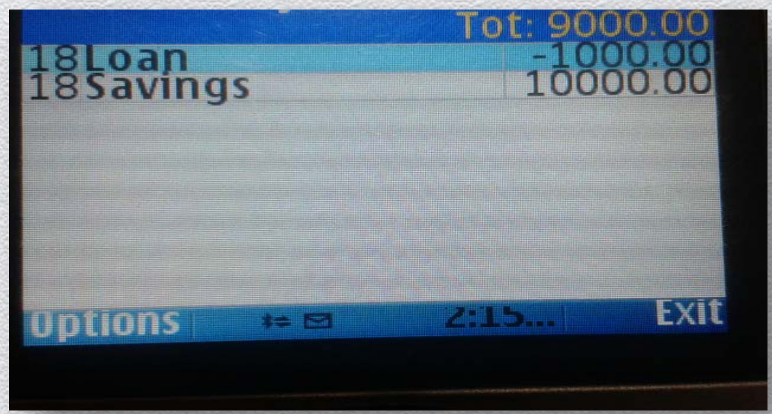
- Fraudulent Transactions (Revenue Loss)
- Confidentiality (Users Sensitive Data – Credit/Debit Card Data, PIN , User Credentials)
- Communications Services Misuse
- SIM Card & Applications Misuse

Mobile App Risks

- Code Obfuscation
- Insecure Local Device database storage
- Insecure App Permissions
- Mobile Payment App Reputation

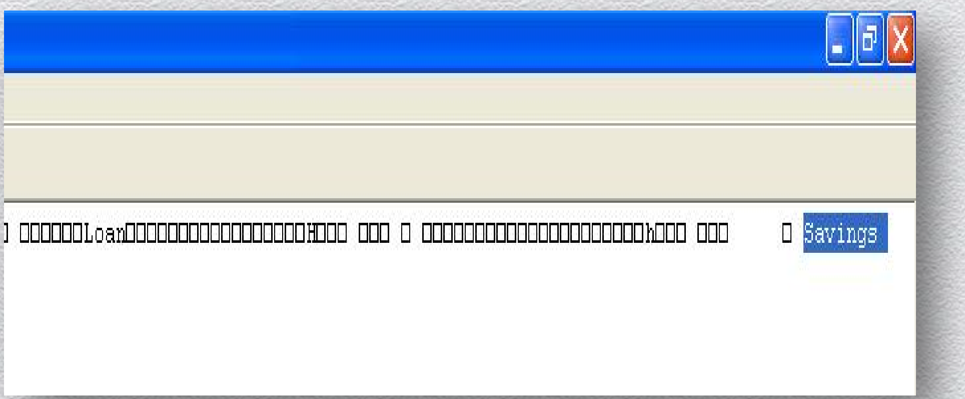
Code Obfuscation

Insecure Local Device database storage



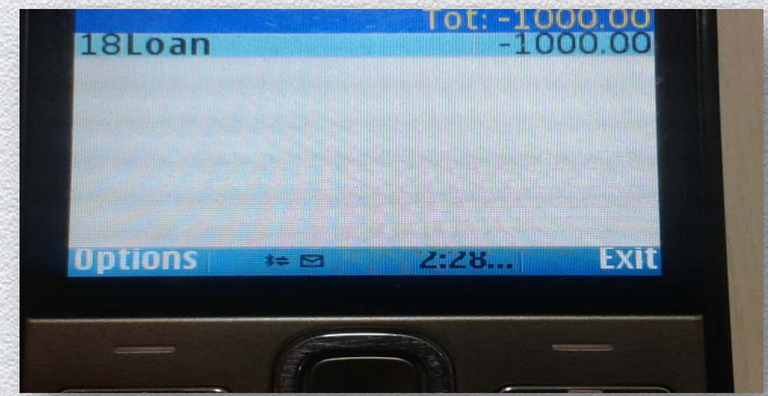
```
                    Tot: 9000.00
18Loan                  -1000.00
18Savings               10000.00

Options                 2:15...   Exit
```

Figure 1. Original application



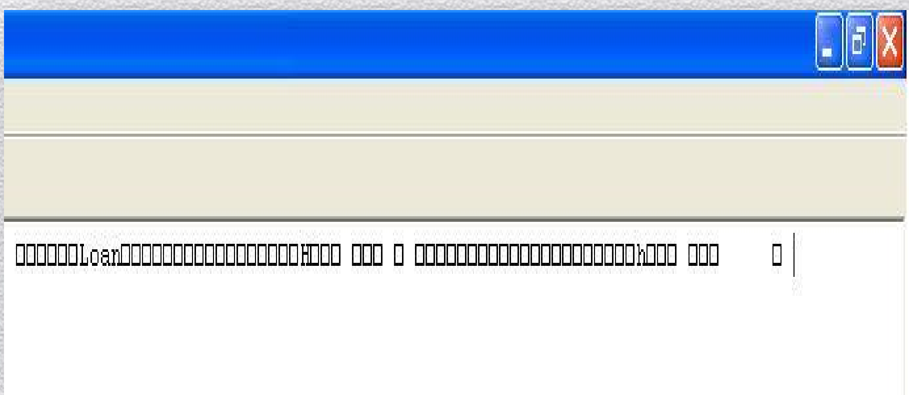
```
] □□□□□□Loan□□□□□□□□□□□□□□□□□□□□H□□□ □□□ □ □□□□□□□□□□□□□□□□□□□□□□□h□□□ □□□    □ Savings
```

Figure 2. Local database modification



```
                 Tot: -1000.00
18Loan               -1000.00

Options          2:28...   Exit
```

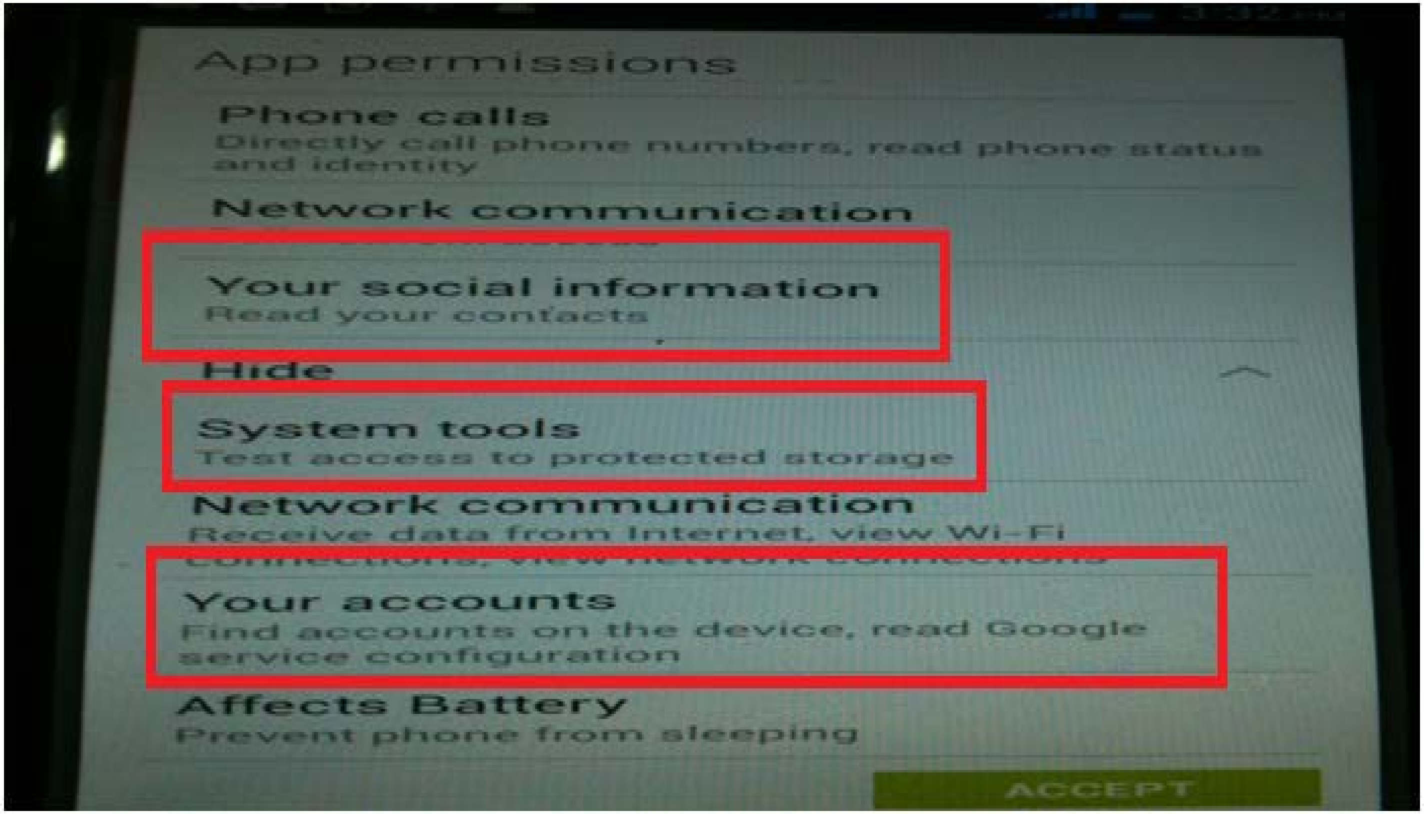
Figure 4. Modified application



```
□□□□□□Loan□□□□□□□□□□□□□□□□□□□□H□□□ □□□ □ □□□□□□□□□□□□□□□□□□□□□□□h□□□ □□□    □
```

Figure 3. Local database modified

Insecure App Permissions



App permissions

Phone calls
Directly call phone numbers, read phone status and identity

Network communication

Your social information
Read your contacts

Hide

System tools
Test access to protected storage

Network communication
Receive data from Internet, view Wi-Fi connections, view network connections

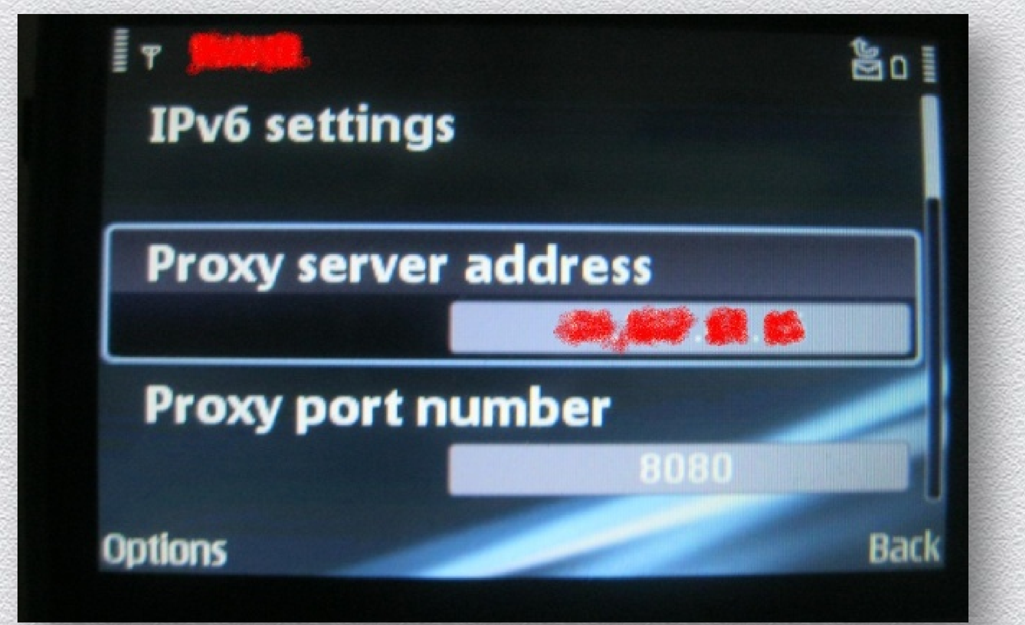
Your accounts
Find accounts on the device, read Google service configuration

Affects Battery
Prevent phone from sleeping

Figure 1. Insecure App Permissions

Mobile Application Server Issues

Message Replay Attack

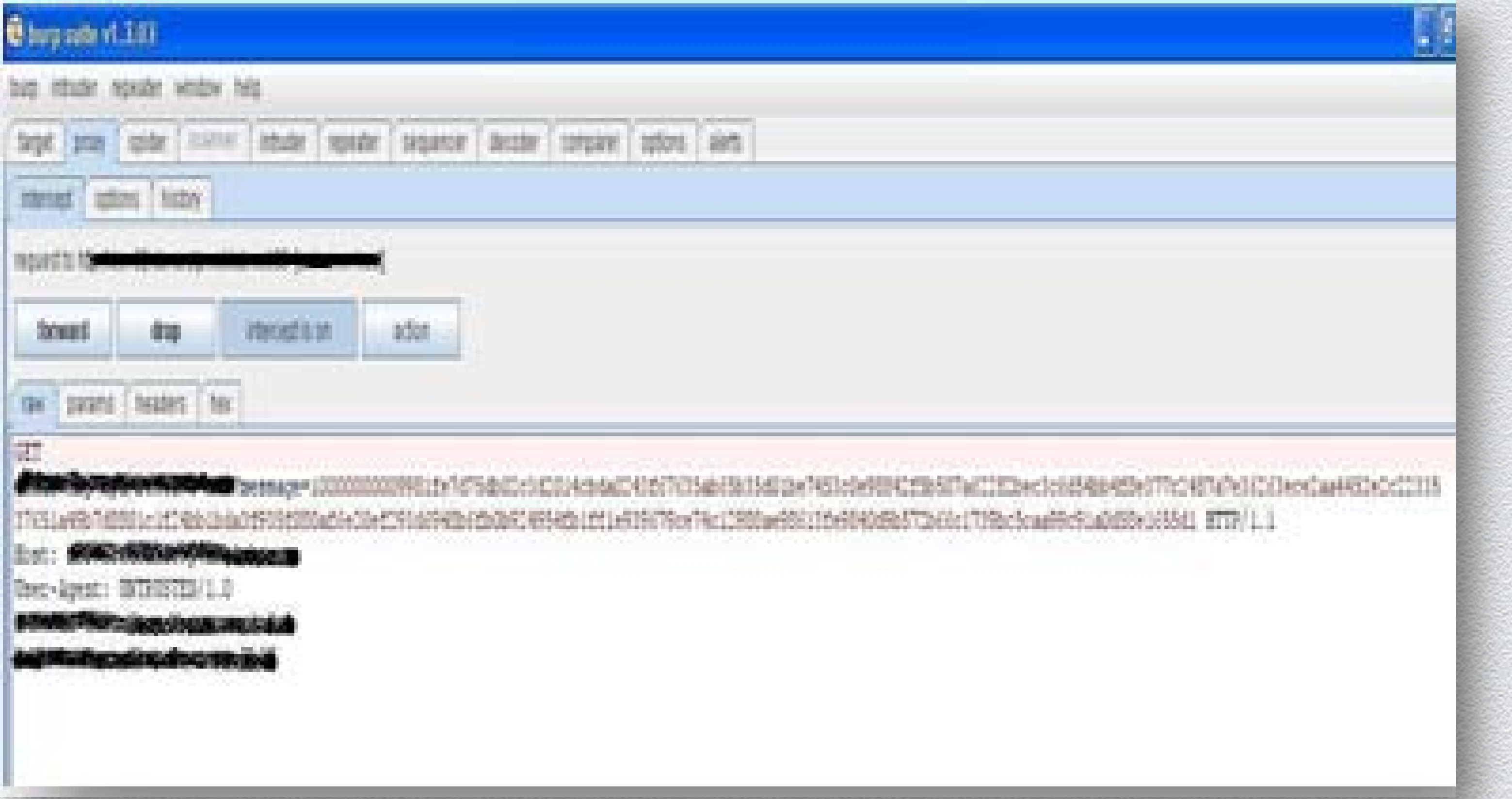

[redacted]

IPv6 settings

Proxy server address
[redacted]

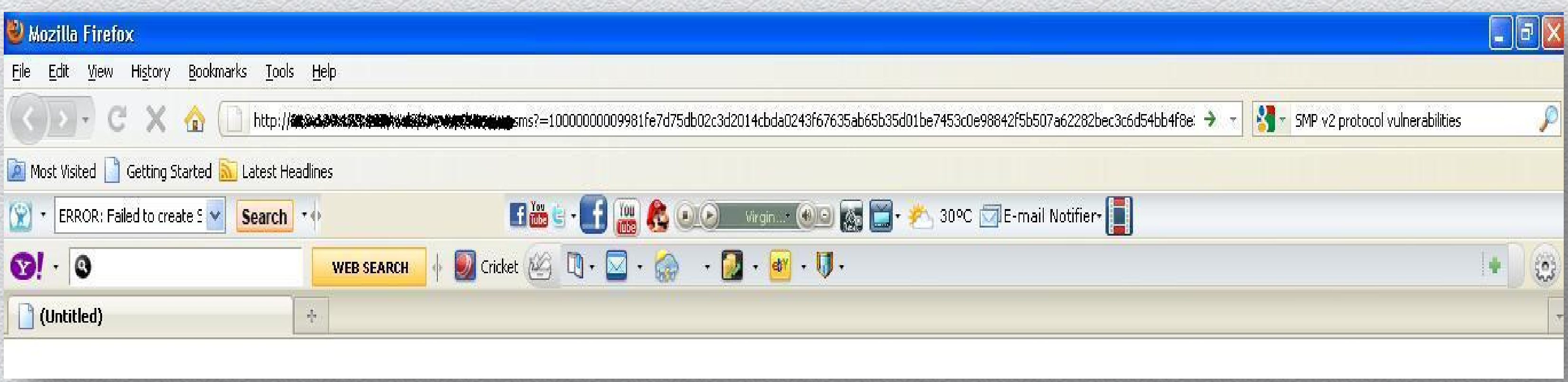
Proxy port number
8080

Figure 1. Proxy Settings


burp suite v1.3.03
burp intruder repeater window help
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
intercept options history
request to h[redacted]
forward
drop
intercept is on
action
raw params headers hex

```
GET
[redacted]message=[illegible] HTTP/1.1
Host: [redacted]
User-Agent: [illegible]/1.0
[redacted]
```

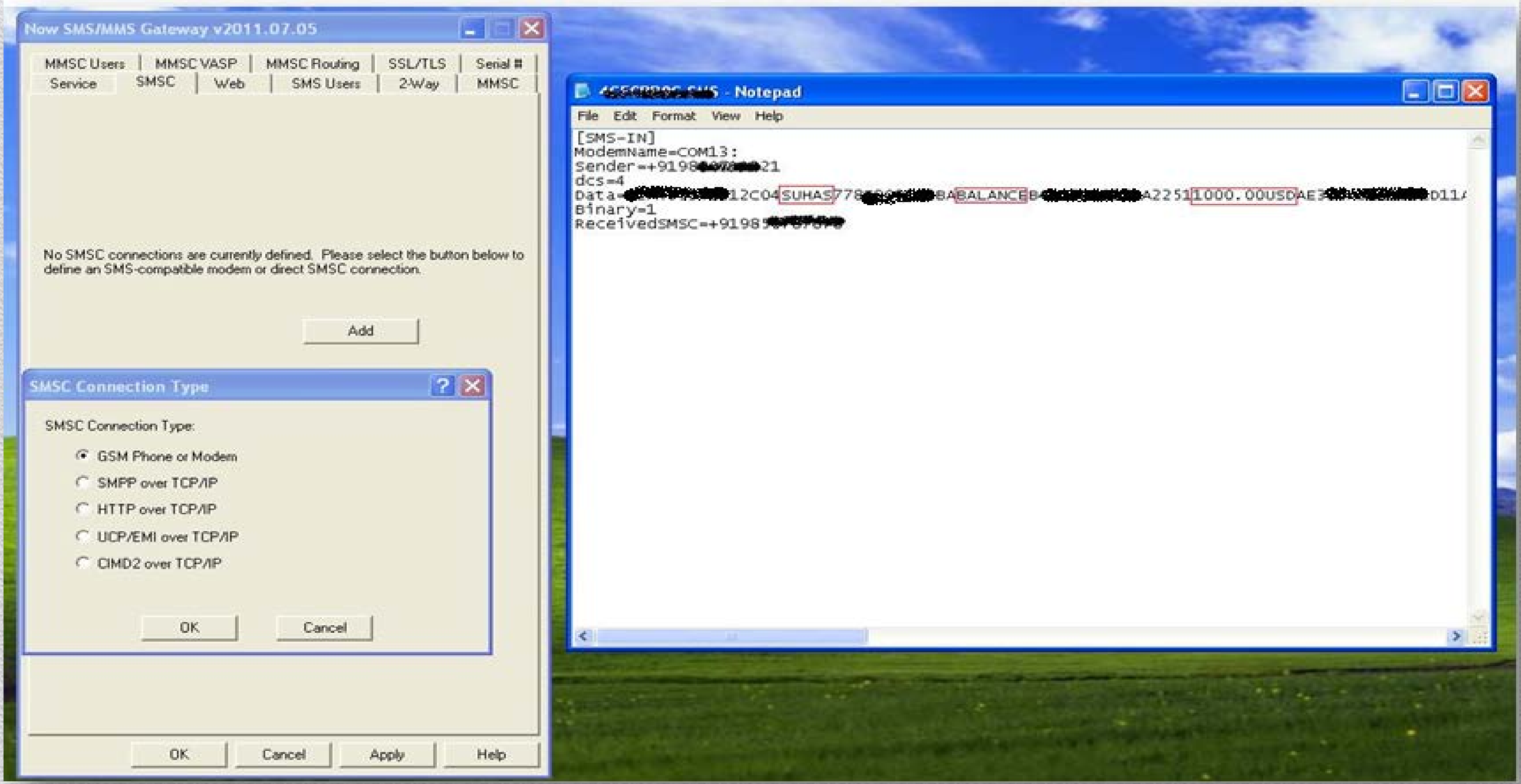
Figure 2. Intercepted Message



http://[redacted]sms?=10000000009981fe7d75db02c3d2014cbda0243f67635ab65b35d01be7453c0e98842f5b507a62282bec3c6d54bb4f8e:

Figure 3. Message Replay Attack

Communication Channel Risks



Now SMS/MMS Gateway v2011.07.05

No SMSC connections are currently defined. Please select the button below to define an SMS-compatible modem or direct SMSC connection.

SMSC Connection Type

SMSC Connection Type:

● GSM Phone or Modem

○ SMPP over TCP/IP

○ HTTP over TCP/IP

○ UCP/EMI over TCP/IP

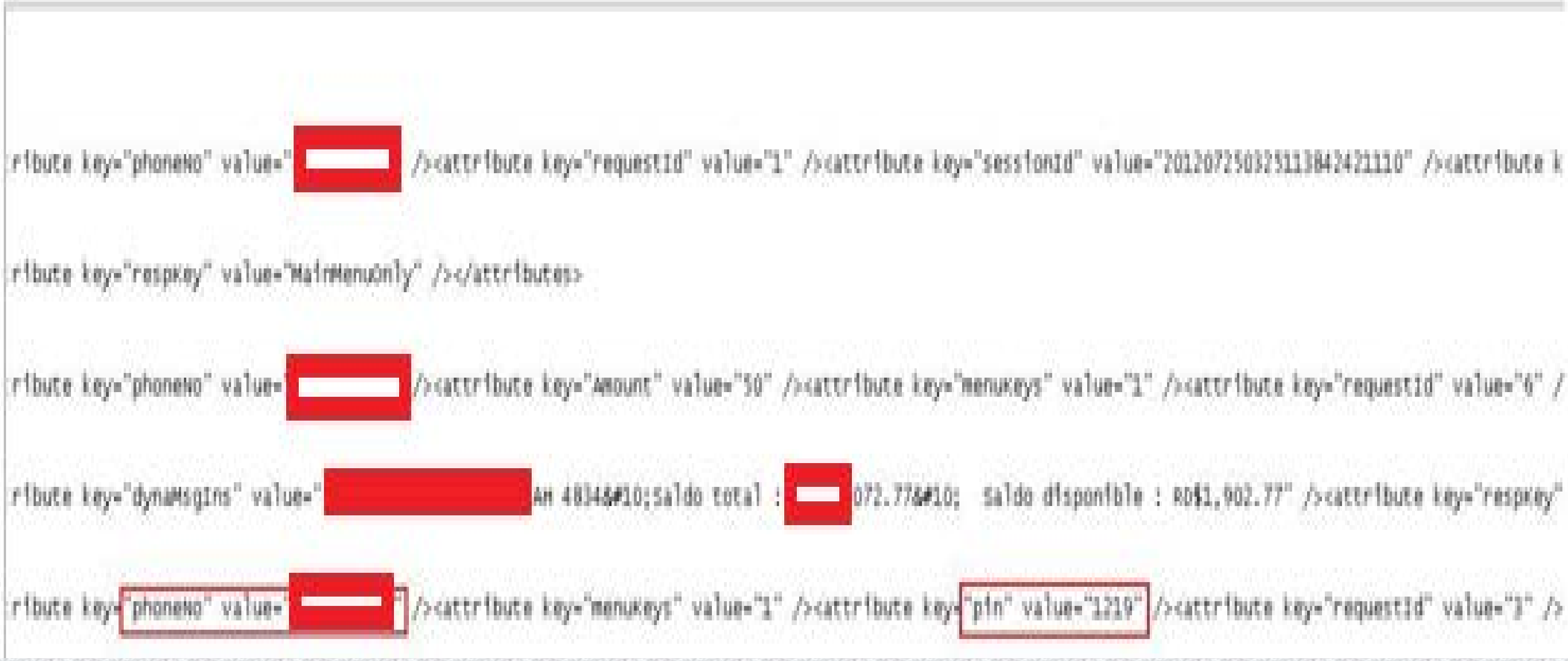
○ CIMD2 over TCP/IP

[redacted] - Notepad

```
[SMS-IN]
ModemName=COM13:
Sender=+9198[redacted]21
dcs=4
Data=[redacted]12C04SUHAS778[redacted]8ABALANCEB[redacted]A22511000.00USDAE3[redacted]D11/
Binary=1
ReceivedSMSC=+91985[redacted]
```

Figure 1. SMS R/R Capture

Note – Performed for traditional mobile app having SMS as a communication channel



```
ribute key="phoneNo" value=" [redacted] /><attribute key="requestId" value="1" /><attribute key="sessionId" value="20120725032511384242111O" /><attribute k

ribute key="respkey" value="MainMenuOnly" /></attributes>

ribute key="phoneNo" value= [redacted] /><attribute key="Amount" value="50" /><attribute key="menukeys" value="1" /><attribute key="requestId" value="6" /

ribute key="dynaMsgIns" value=" [redacted] AM 4834&#10;Saldo total : [redacted] 072.77&#10;  Saldo disponible : R0$1,902.77" /><attribute key="respkey"

ribute key="phoneNo" value= [redacted] " /><attribute key="menukeys" value="1" /><attribute key="pin" value="1219" /><attribute key="requestId" value="3" />
```

Figure 1. USSD Gateway Sample data

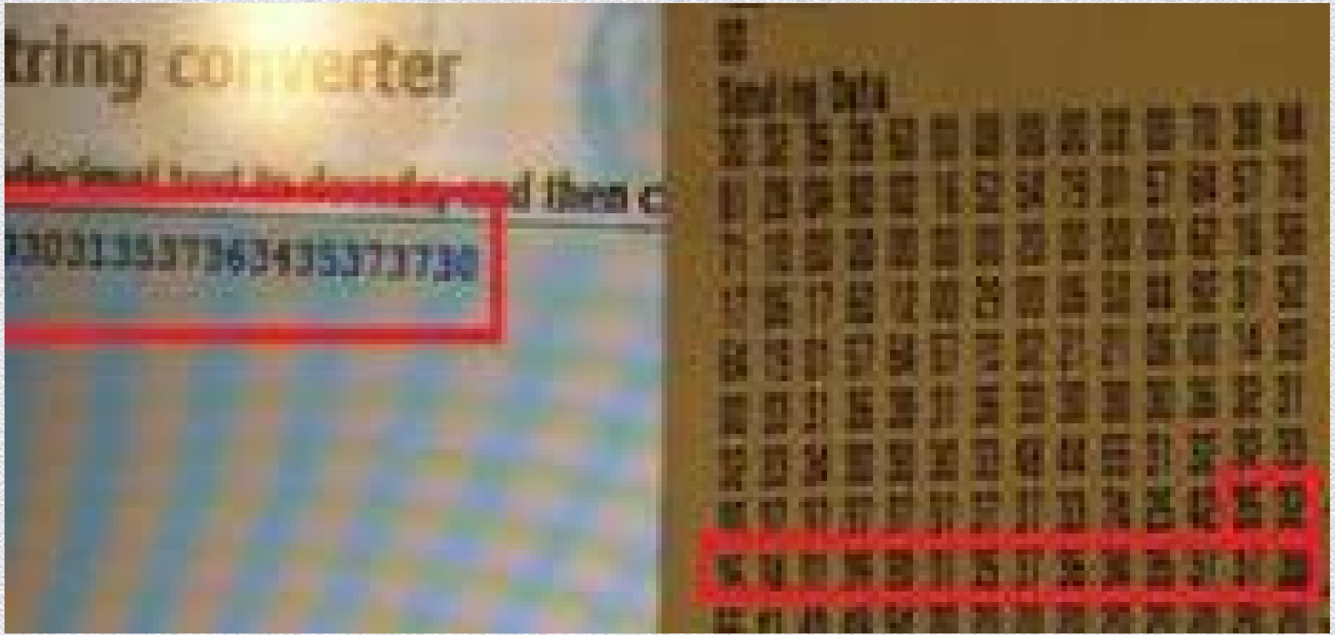
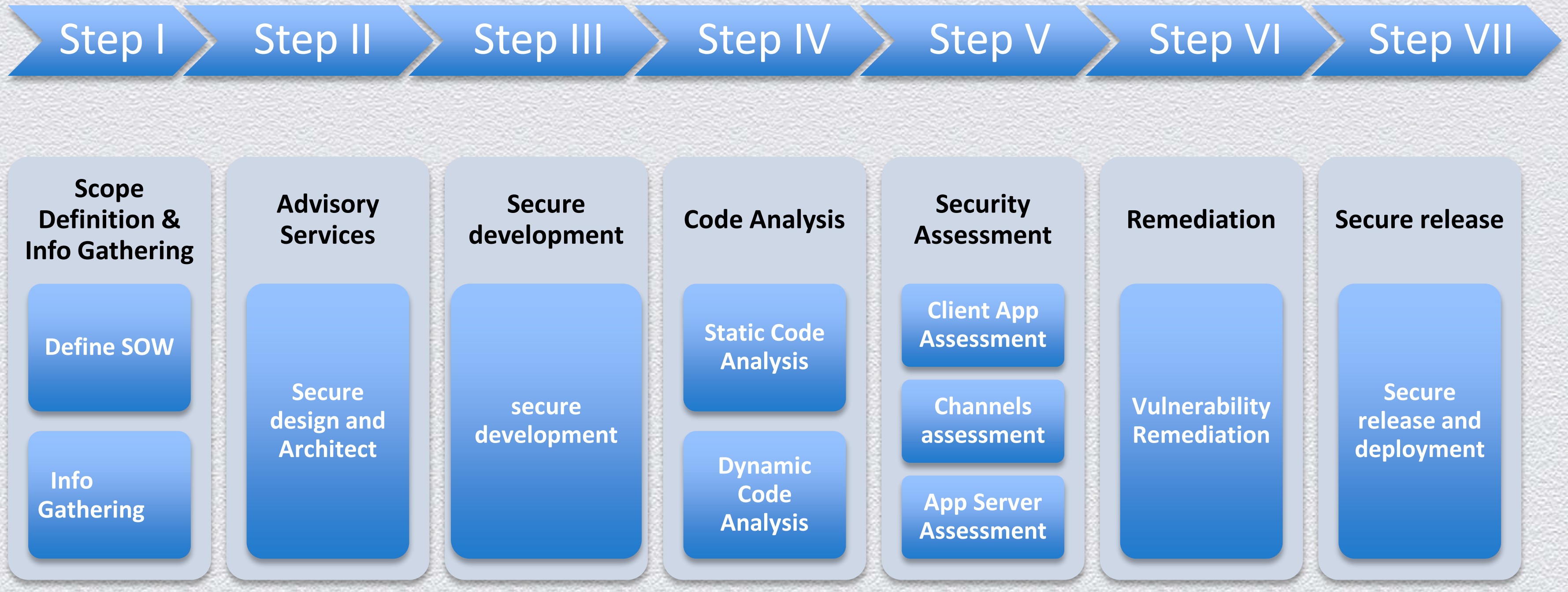


Figure 1. POS Devices Receipt in Debug Mode

Quiz : Cross Platform Support

```
int i = 7;
{
printf(“%d”, i++ * i++);
}
```

Secure SDLC Approach



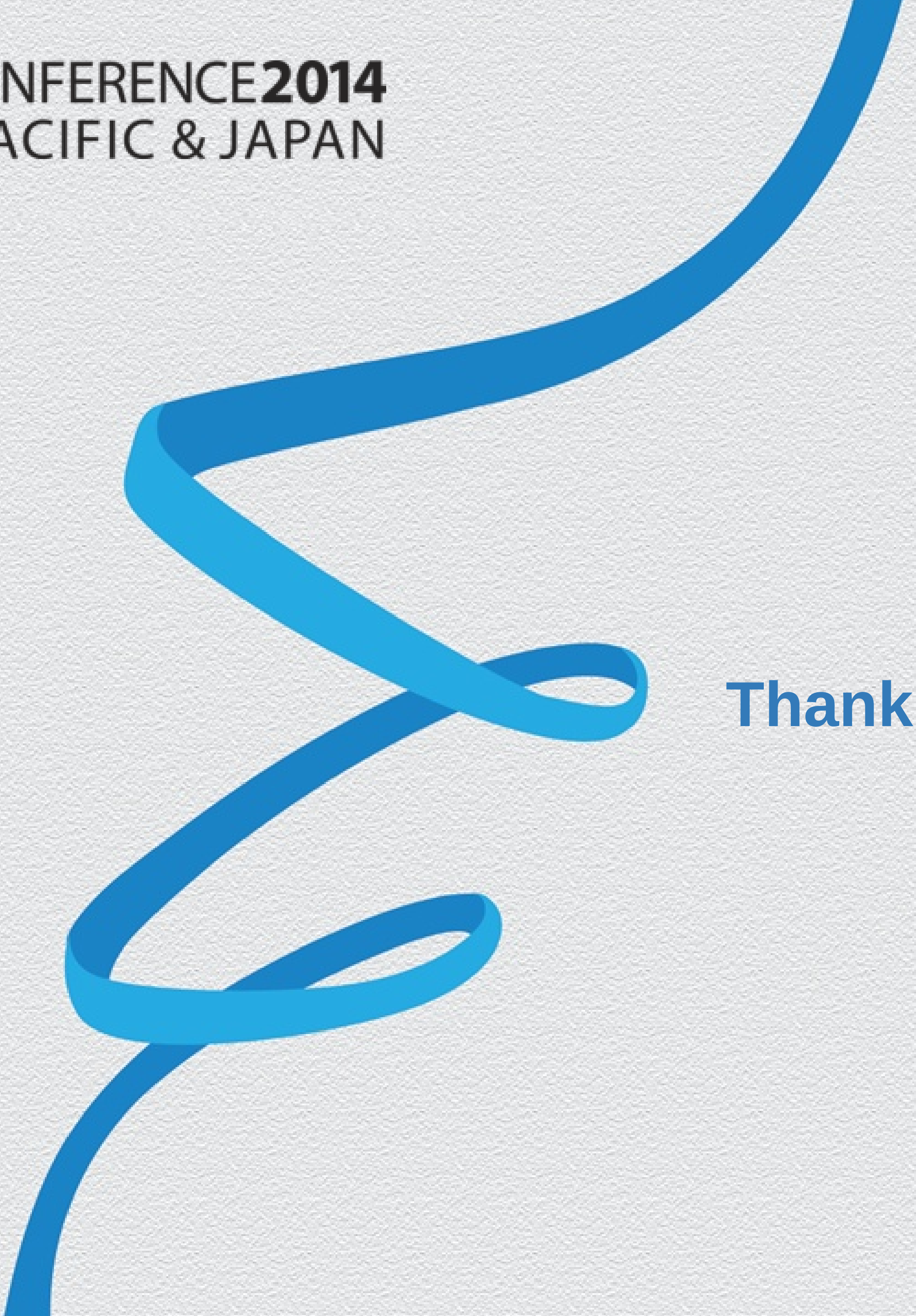
Step I	Step II	Step III	Step IV	Step V	Step VI	Step VII
Scope Definition & Info Gathering	Advisory Services	Secure development	Code Analysis	Security Assessment	Remediation	Secure release
Define SOW Info Gathering	Secure design and Architect	secure development	Static Code Analysis Dynamic Code Analysis	Client App Assessment Channels assessment App Server Assessment	Vulnerability Remediation	Secure release and deployment

Securing Mobile Payments

- ❑ Secure data transmission from handheld devices to Application Server
- ❑ Secure data storage on local handheld devices
- ❑ Ensure to implement proper session management in application
- ❑ Ensure to applications executables security
- ❑ Validate all trusted and un-trusted (Invalid user inputs e.g. -special characters) inputs in the application
- ❑ Ensure to implement strong authentication mechanism in the application
- ❑ Secure web services and Interfaces
- ❑ Ensure mobile device security in case of device lost and theft

Future of Mobile Payments

- Microfinance for Developing Countries
- Larger Funds Transfer (Substitute for Net Banking)
- Reservation/Bookings for Airlines, Railways & Bus
- Mobile Payments Services for Small Scale Business
- Visibility - Earnings & Taxation



Thank you!