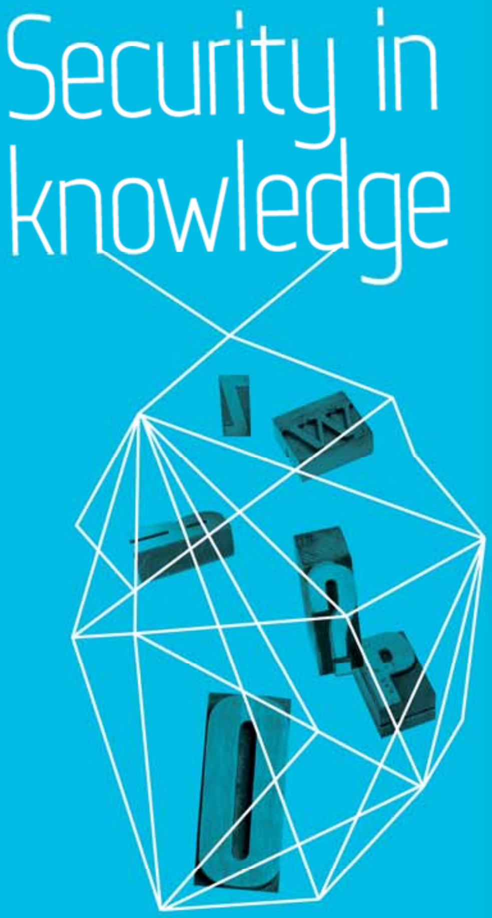
RSA CONFERENCE ASIA PACIFIC 2013



SECURE MOBILE APP DEVELOPMENT: DIFFERENCES FROM TRADITIONAL APPROACH

Suhas Desai
Aujas Information Risk Services

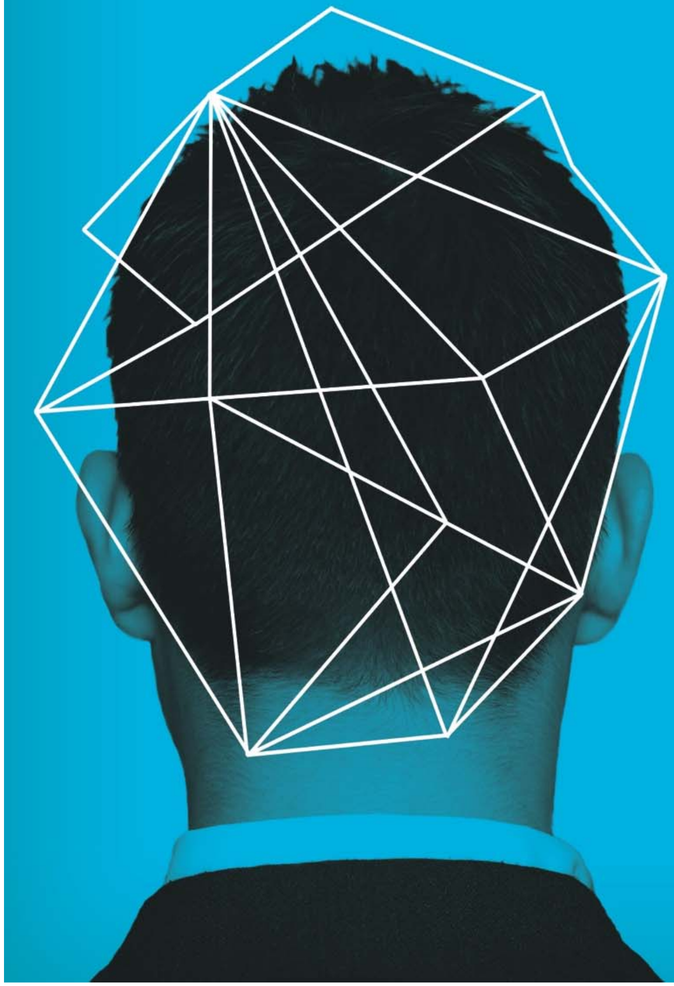
Session ID: MBS-T02

Session Classification: Intermediate

Agenda

- Trends in Mobile Technology
- Mobile App SDLC Challenges
- Security Risks in mobile applications
- Secure SDLC Approach

RSA® CONFERENCE
ASIA PACIFIC 2013



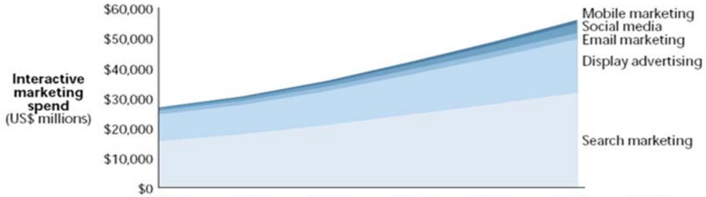
Trends in Mobile Technology

Trends in Mobile Technology

- By 2014, over 3 billion adults will be able to transact electronically
- By 2013, mobile phones will overtake PCs

(Source : Gartner)

Fig : Mobile in Marketing Industry, Forecast : 2009 -2014



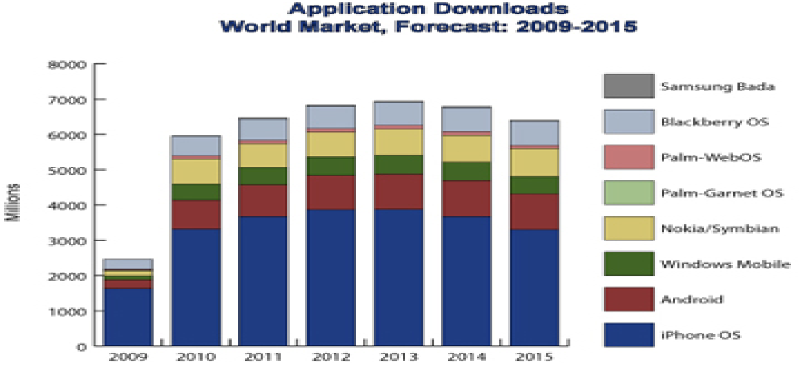
	2009	2010	2011	2012	2013	2014	CAGR
Mobile marketing	$391	$561	$748	$950	$1,131	$1,274	27%
Social media	$716	$935	$1,217	$1,649	$2,254	$3,113	34%
Email marketing	$1,248	$1,355	$1,504	$1,676	$1,867	$2,081	11%
Display advertising	$7,829	$8,395	$9,846	$11,732	$14,339	$16,900	17%
Search marketing	$15,393	$17,765	$20, 763	$24,299	$27,786	$31,588	15%
Total	**$25,577**	**$29,012**	**$34,077**	**$40,306**	**$47,378**	**$54,956**	17%
Percent of all ad spend	12%	13%	15%	17%	19%	21%	

Source: Forrester's Interactive Advertising Models, 4/09 and 10/08 (US only)

47730

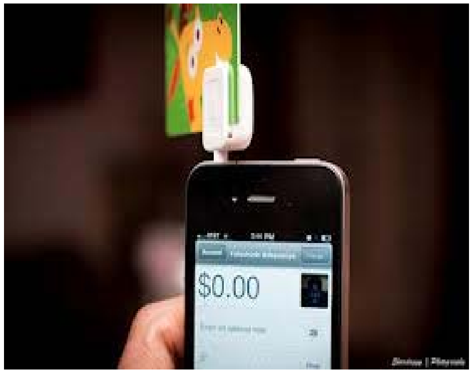
Source: Forrester Research, Inc.

Fig: Mobile App Download Market, Forecast : 2009 -2015



Source: ABI Research

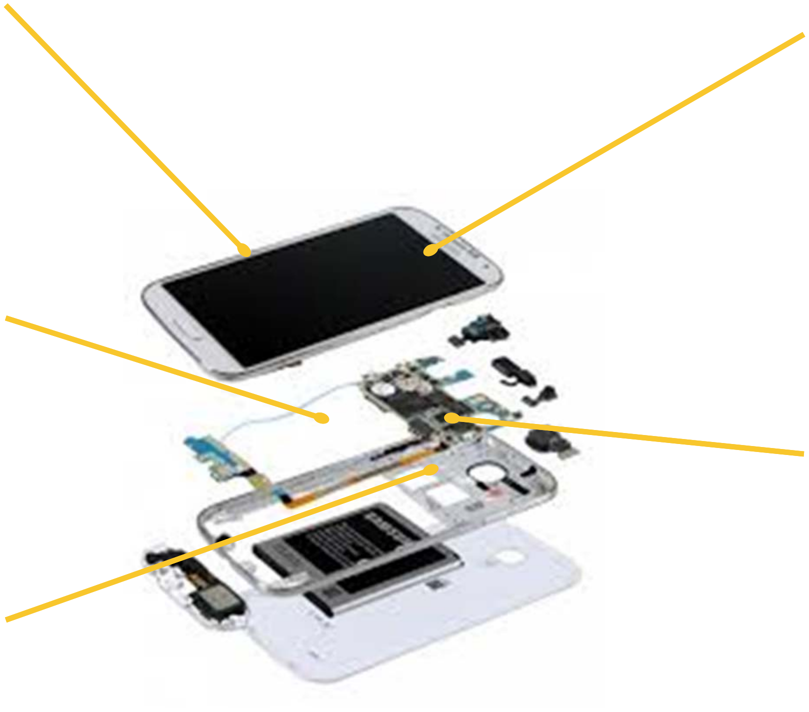
Mobile Apps are everywhere!



RSA CONFERENCE ASIA PACIFIC 2013

Mobile App SDLC Challenges over traditional application SDLC

Mobile App SDLC Challenges



Support for various displays and screen sizes

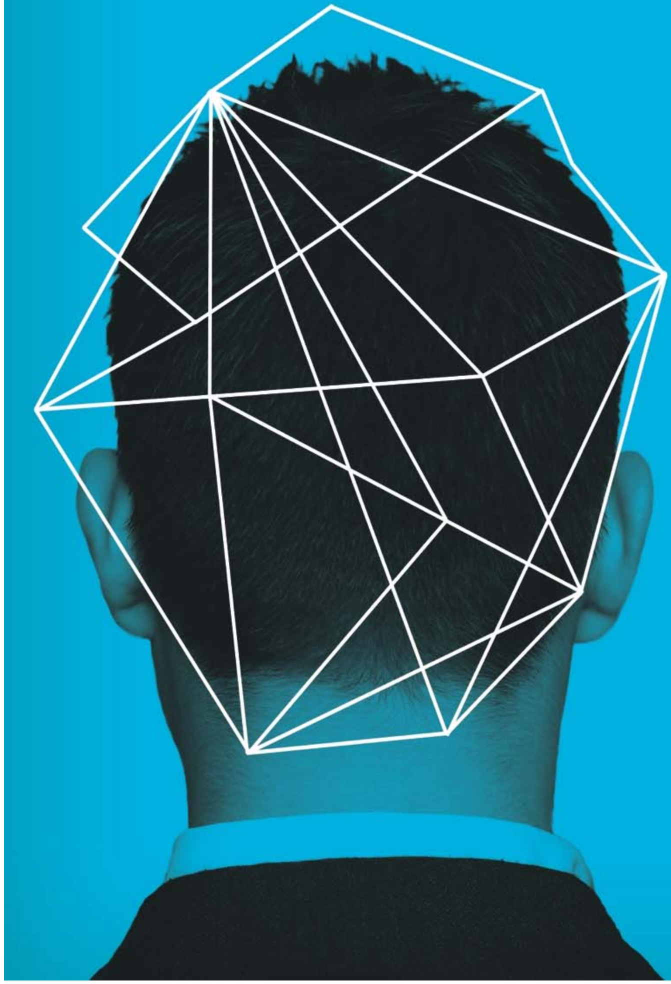
Effective usage of local device database & memory

Releasing secure (signed) application executables

Rich user interfaces with push notifications (Wherever applicable)

Effective usage of communication channels – SMS / USSD (Unstructured Supplementary Service Data) / IP and web services

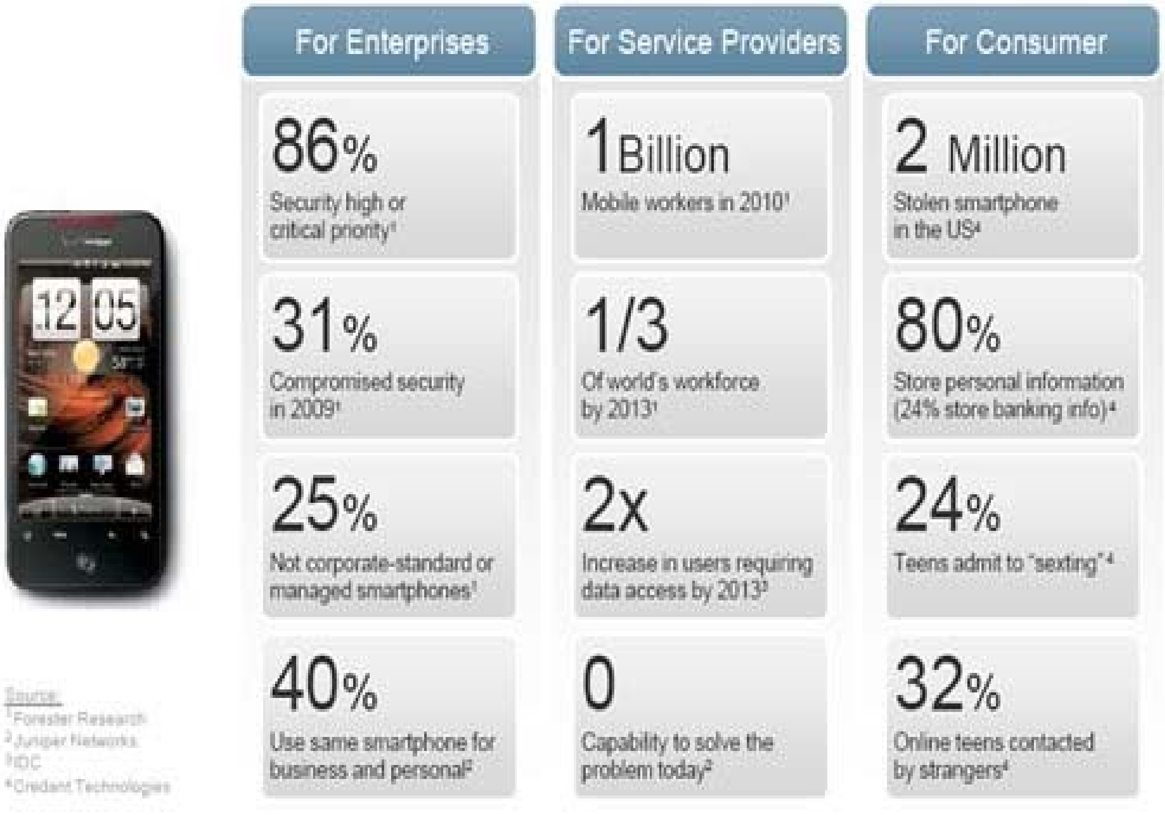
RSA CONFERENCE ASIA PACIFIC 2013



Security Risks in Mobile Applications

Stats : Mobile threats

"The Smartphone OS will become a major security target," said Android Security Leader Rich Cannings, speaking at the Usenix Security Symposium.



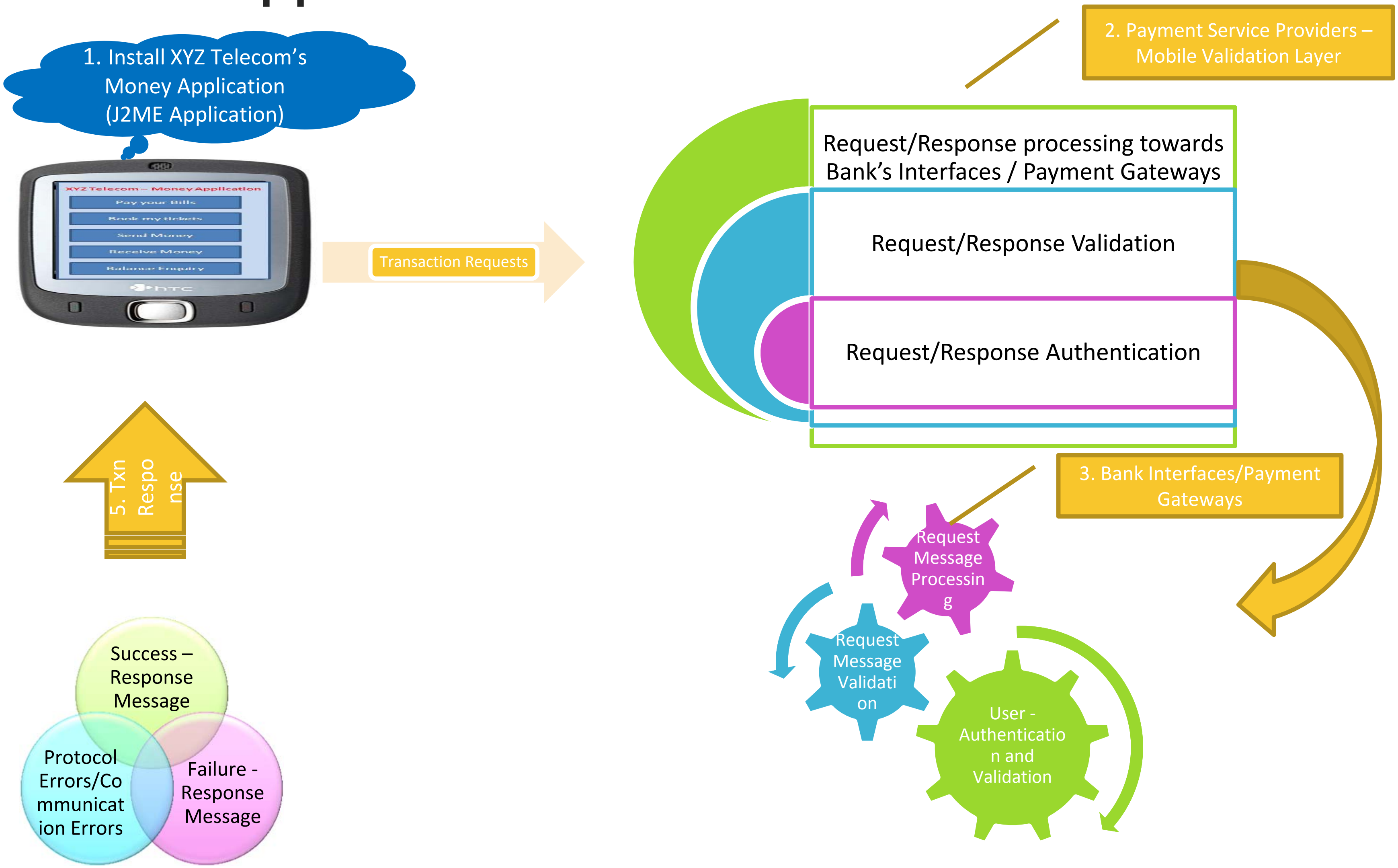
For Enterprises	For Service Providers	For Consumer
86% Security high or critical priority[1]	1 Billion Mobile workers in 2010[1]	2 Million Stolen smartphone in the US[4]
31% Compromised security in 2009[1]	1/3 Of world's workforce by 2013[1]	80% Store personal information (24% store banking info)[4]
25% Not corporate-standard or managed smartphones[1]	2x Increase in users requiring data access by 2013[3]	24% Teens admit to "sexting"[4]
40% Use same smartphone for business and personal[2]	0 Capability to solve the problem today[2]	32% Online teens contacted by strangers[4]

Source:
[1] Forester Research
[2] Juniper Networks
[3] IDC
[4] Credant Technologies

Risks in Mobile Applications

- Fraudulent Transactions through message tampering
- Weak Cryptography
- Mobile Application Server Issues
- Reverse Engineering Threats
- Communication Channel Attacks – SMS / USSD
- Web Services Attacks
- Device lost/theft case scenarios

Mobile Application Architecture



1. Install XYZ Telecom's Money Application (J2ME Application)

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 Processin g

Request Message Validati on

User - Authenticatio n and Validation

5. Txn Respo nse

Success – Response Message

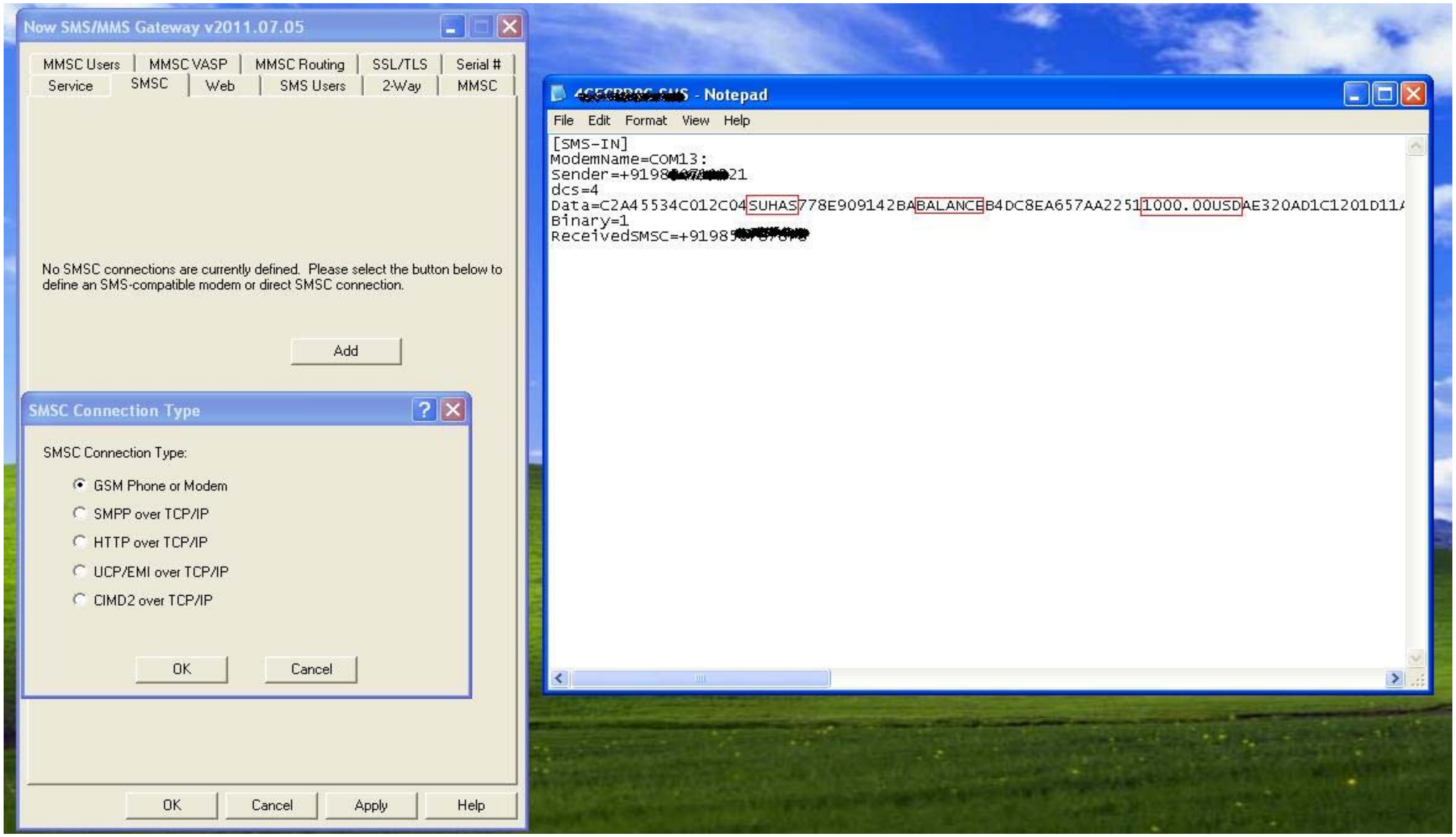
Protocol Errors/Co mmunicat ion Errors

Failure - Response Message

Attack vector

- Reverse engineering of mobile application
- Transactions Request/Response Attacks
- Message Replay Attack
- Fraudulent Transactions through Data storage
- Verify strong Cryptographic Implementation
- Improper Session Management
- Authentication Attacks
- Web Services Attacks

PoC – SMS Req/Res Attacks



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

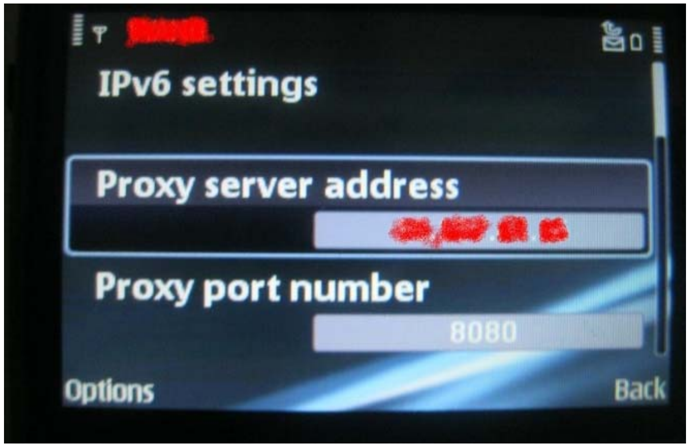
SMSC Connection Type:

- ● GSM Phone or Modem
- ○ SMPP over TCP/IP
- ○ HTTP over TCP/IP
- ○ UCP/EMI over TCP/IP
- ○ CIMD2 over TCP/IP

```
[SMS-IN]
ModemName=COM13:
Sender=+9198[redacted]21
dcs=4
Data=C2A45534C012C04SUHAS778E909142BABALANCEB4DC8EA657AA22511000.00USDAE320AD1C1201D11
Binary=1
ReceivedSMSC=+9198[redacted]
```

Figure 1. Application SMS Req / Res Attack

PoC – Message Replay Attacks



[redacted]

IPv6 settings

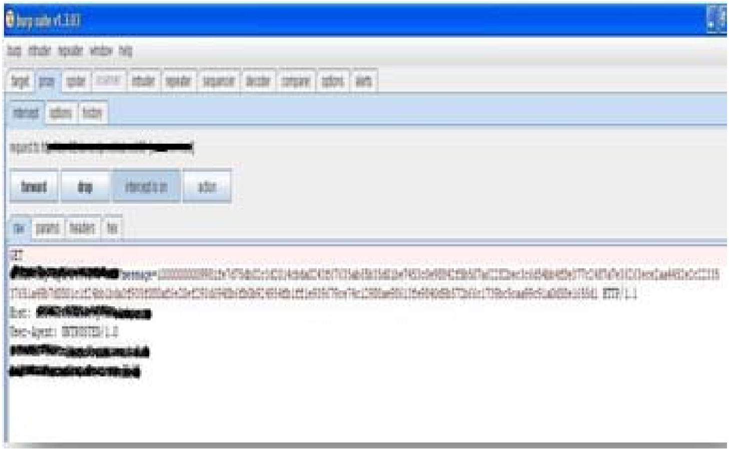
Proxy server address

[redacted]

Proxy port number

8080

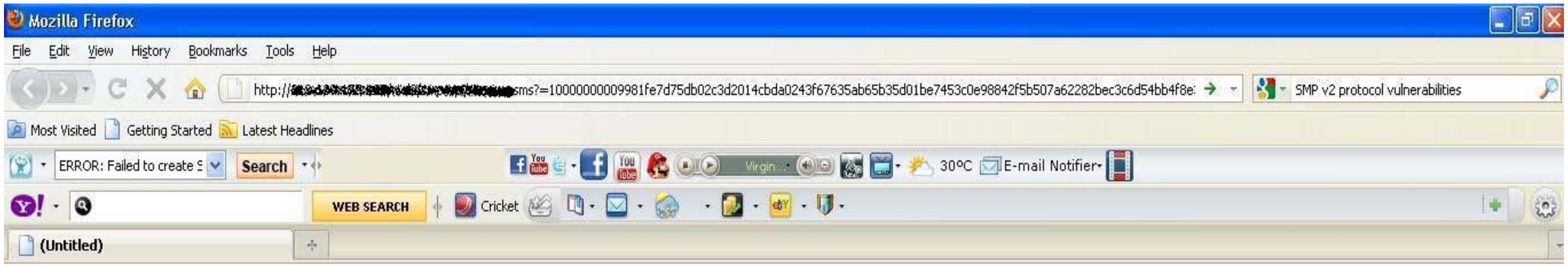
Figure 1. Proxy Settings



request to [redacted]

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

Figure 2. Intercepted Message

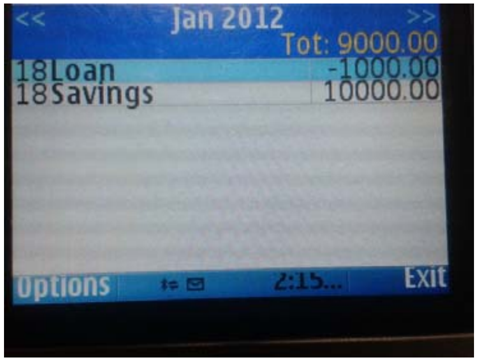


http://[redacted]sms?=10000000009981fe7d75db02c3d2014cbda0243f67635ab65b35d01be7453c0e98842f5b507a62282bec3c6d54bb4f8e:

SMP v2 protocol vulnerabilities

Figure 3. Message Replay Attack

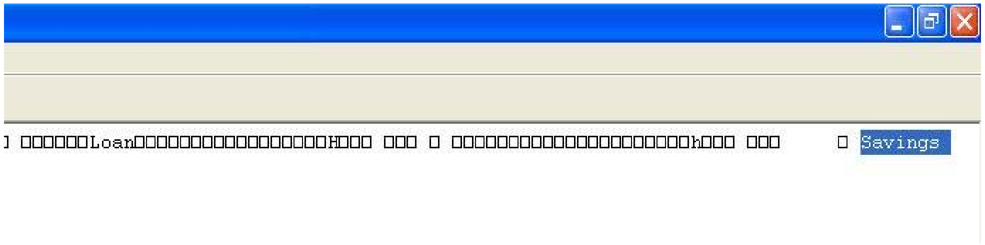
PoC – Local data modification



Tot: 9000.00

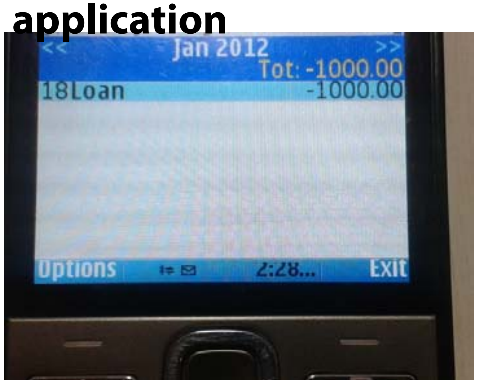
18Loan	-1000.00
18Savings	10000.00

Figure 1. Original application



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

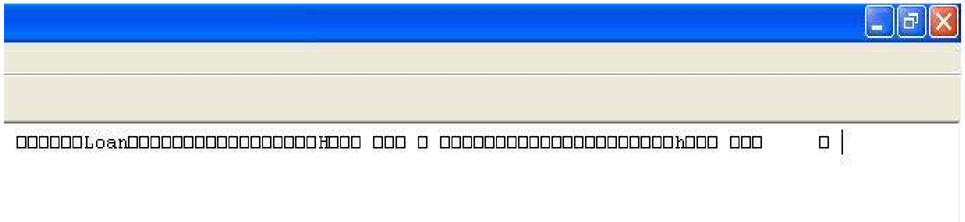
Figure 2. Local database modification



Tot: -1000.00

18Loan	-1000.00

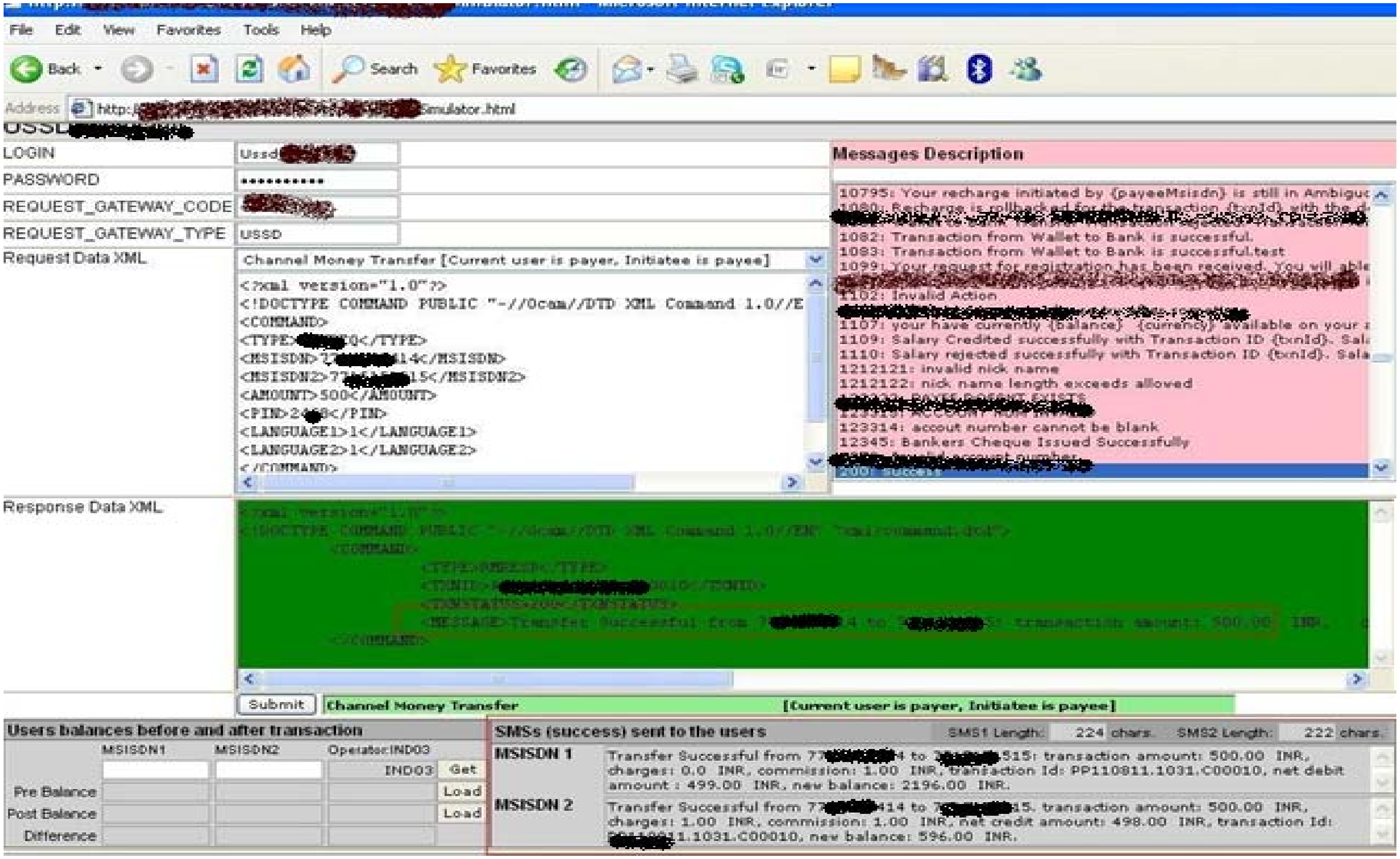
Figure 4. Modified application



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

Figure 3. Local database modified

PoC – USSD Gateway Attack



http:[redacted] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http:[redacted]Simulator.html

USSD[redacted]

LOGIN	Ussd[redacted]
PASSWORD	***********
REQUEST_GATEWAY_CODE	[redacted]
REQUEST_GATEWAY_TYPE	USSD
Request Data XML	Channel Money Transfer [Current user is payer, Initiatee is payee]

```
<?xml version="1.0"?>
<!DOCTYPE COMMAND PUBLIC "-//Ocam//DTD XML Command 1.0//E
<COMMAND>
<TYPE>[redacted]Q</TYPE>
<MSISDN>7[redacted]14</MSISDN>
<MSISDN2>77[redacted]15</MSISDN2>
<AMOUNT>500</AMOUNT>
<PIN>24[redacted]</PIN>
<LANGUAGE1>1</LANGUAGE1>
<LANGUAGE2>1</LANGUAGE2>
</COMMAND>
```

Messages Description

```
10795: Your recharge initiated by {payeeMsisdn} is still in Ambiguc
1080: Recharge is rollbacked for the transaction {txnId} with the d
[redacted]
1082: Transaction from Wallet to Bank is successful.
1083: Transaction from Wallet to Bank is successful.test
1099: Your request for registration has been received. You will able
[redacted]
1102: Invalid Action
[redacted]
1107: your have currently {balance}  {currency} available on your a
1109: Salary Credited successfully with Transaction ID {txnId}. Sala
1110: Salary rejected successfully with Transaction ID {txnId}. Sala
1212121: invalid nick name
1212122: nick name length exceeds allowed
[redacted]
123314: accout number cannot be blank
12345: Bankers Cheque Issued Successfully
[redacted]
200: success
```

Response Data XML

```
<?xml version="1.0"?>
<!DOCTYPE COMMAND PUBLIC "-//Ocam//DTD XML Command 1.0//EN" "xml/command.dtd">
        <COMMAND>
                <TYPE>[illegible]</TYPE>
                <TXNID>[redacted]0010</TXNID>
                <TXNSTATUS>200</TXNSTATUS>
                <MESSAGE>Transfer Successful from 7[redacted]4 to 7[redacted]5: transaction amount: 500.00  INR,  c
        </COMMAND>
```

Submit | Channel Money Transfer [Current user is payer, Initiatee is payee]

Users balances before and after transaction

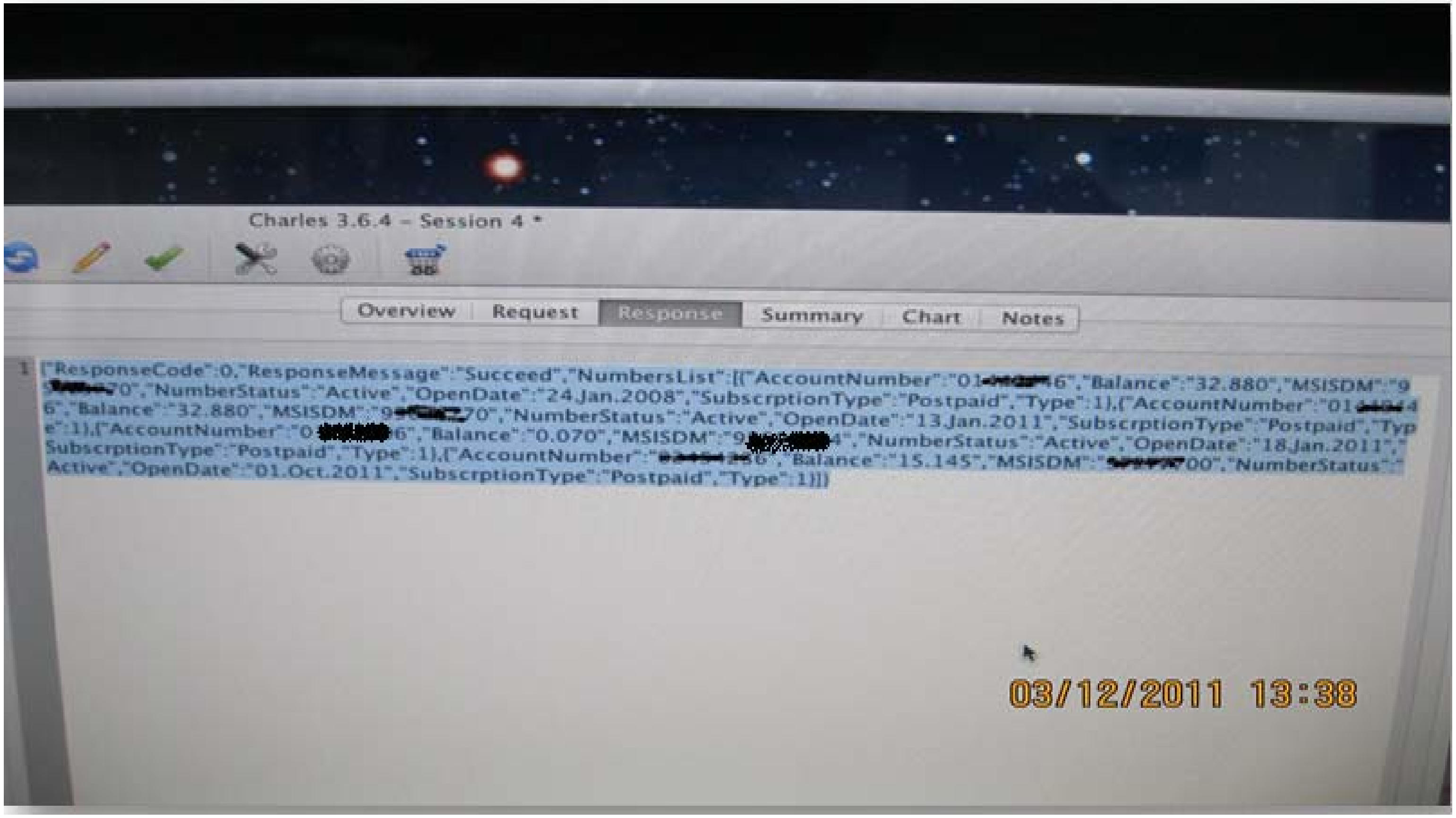
	MSISDN1	MSISDN2	Operator:IND03	
			IND03	Get
Pre Balance				Load
Post Balance				Load
Difference				

SMSs (success) sent to the users SMS1 Length: 224 chars. SMS2 Length: 222 chars.

MSISDN 1	Transfer Successful from 77[redacted]4 to 7[redacted]515: transaction amount: 500.00 INR, charges: 0.0 INR, commission: 1.00 INR, transaction Id: PP110811.1031.C00010, net debit amount : 499.00 INR, new balance: 2196.00 INR.
MSISDN 2	Transfer Successful from 77[redacted]414 to 7[redacted]15. transaction amount: 500.00 INR, charges: 1.00 INR, commission: 1.00 INR, net credit amount: 498.00 INR, transaction Id: [redacted]1.1031.C00010, new balance: 596.00 INR.

Figure 1. USSD Gateway Emulator

PoC: iOS App R/R capture

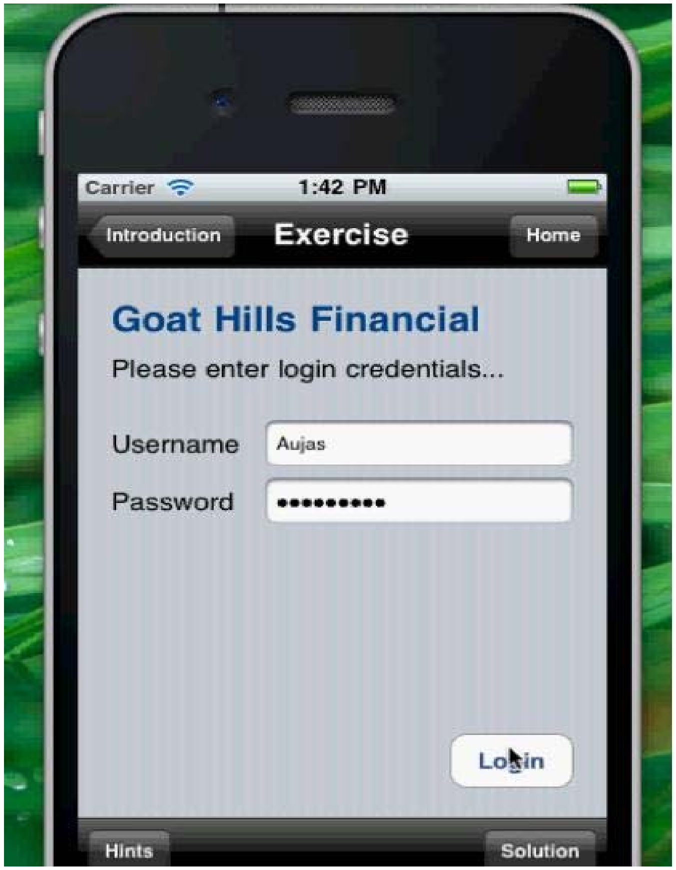


```
{"ResponseCode":0,"ResponseMessage":"Succeed","NumbersList":[{"AccountNumber":"01[redacted]6","Balance":"32.880","MSISDM":"9
[redacted]0","NumberStatus":"Active","OpenDate":"24Jan.2008","SubscrptionType":"Postpaid","Type":1},{"AccountNumber":"01[redacted]4
6","Balance":"32.880","MSISDM":"9[redacted]70","NumberStatus":"Active","OpenDate":"13Jan.2011","SubscrptionType":"Postpaid","Typ
e":1},{"AccountNumber":"0[redacted]6","Balance":"0.070","MSISDM":"9[redacted]4","NumberStatus":"Active","OpenDate":"18Jan.2011","
SubscrptionType":"Postpaid","Type":1},{"AccountNumber":"[redacted]6","Balance":"15.145","MSISDM":"[redacted]00","NumberStatus":"
Active","OpenDate":"01.Oct.2011","SubscrptionType":"Postpaid","Type":1}]}
```

03/12/2011 13:38

Figure 1. Request/Response Capture

PoC: iOS App R/R Tampering



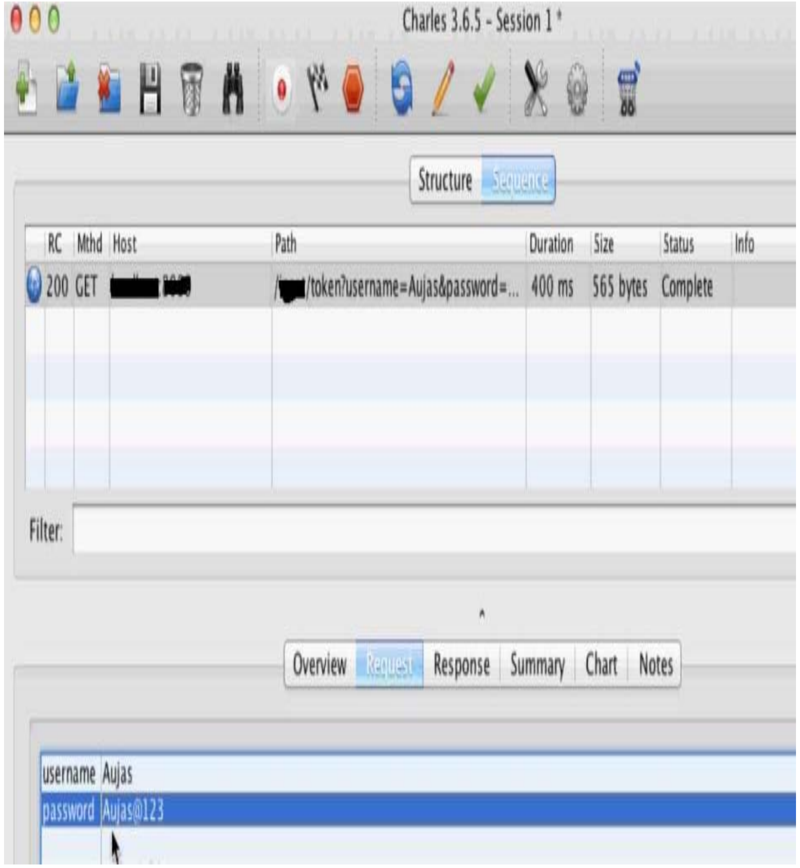
Goat Hills Financial

Please enter login credentials...

Username: Aujas

Password: ••••••••••

Figure 1. Entering Credentials



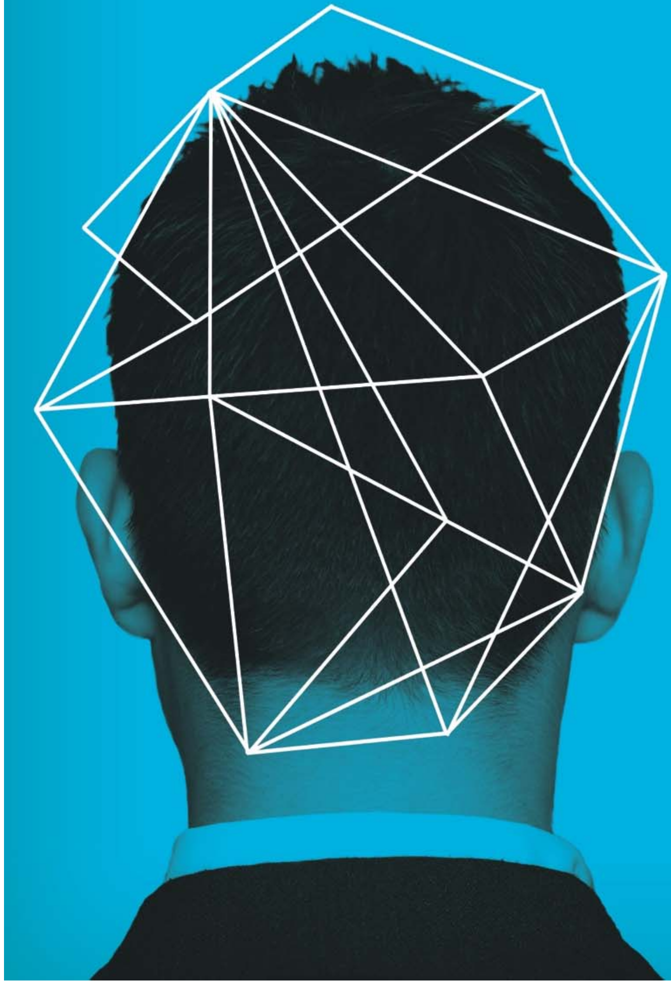
RC	Mthd	Host	Path	Duration	Size	Status	Info
200	GET	[redacted]	/[redacted]/token?username=Aujas&password=...	400 ms	565 bytes	Complete	

Filter:

username	Aujas
password	Aujas@123

Figure 2. Intercepted Message

RSA®CONFERENCE ASIA PACIFIC 2013



Secure SDLC Approach

Secure SDLC Approach

Requirements

- Software risk profile
- Security requirement definition
- Security investment analysis

Design

- Threat modeling
- Security arch design
- Security controls
- Developer training

Development

- Secure coding best practices
- Secure code libraries
- Pair programming / peer reviews

Release

- Functional, architecture, code & deployment testing
- Security controls validation
- Remediation

Sustenance

- Security metrics analysis
- Change management
- Incident & consequence management

Secure SDLC – Best Practices

- Secure data transmission
- Secure data storage
- Ensure to implement proper session management
- Validate all trusted and un-trusted inputs
- Ensure to implement strong authentication mechanism

Contd..

- Ensure to implement response and request messages encryption
- Ensure to implement proper message authentication mechanism to validate requests/responses are generated through authenticated users
- Ensure to implement and use Secure SMS/USSD/IP communication channels
- Secure Interface between payment gateways and mobile payment application

RSA CONFERENCE ASIA PACIFIC 2013

Thank You!

www.aujas.com