MOBILE GOVERNANCE AND MOBILE PAYMENT SECURITY

Dr. V. N. Sastry
Professor, IDRBT
Head, Centre for Mobile Banking (CMB)
Chairman, Expert Committee on m-Governance, MEITY, GoI
Co-founder & Executive Secretary, Mobile Payment Forum of India (MPFI)
Institute for Development and Research in Banking Technology (IDRBT)
Road No.1, Castle Hills, Masab Tank, Hyderabad 500057, Telangana, India
E-Mail: vnsastry@idrbt.ac.in  Ph: 91-40-23294999
October 5, 2018
Outline

• Mobile Services & Delivery Models
  – Mobile Governance
  – Mobile Financial Services
• Mobile Payments
• Mobile Security
  – Classification - Device, Communication & Service Levels
  – Threats, Vulnerabilities & Control Measures
  – Standards & Security Testing
Mobile Service

• Any service that can be obtained, delivered and accessed on a Mobile Phone by a user in the form of voice, data and multimedia.

• Mobile Phone has become an identity, companion and gateway of a person as it provides worldwide access of information at any time, digital services from anywhere, location based, context based and customized services online.
Mobile Service Delivery

• Entities

• Models
  – Client-Server, Web Service, SOA, m-Cloud

• Flow Architecture
Mobile Service : Entities

• Mobile User :
  – Consumer of Service, Demands service.

• Service Provider:
  – MNO, WiFi AP, Social Media, Government, App & API Developers, Mobile Cloud, Testers, Banks & Financial Institutions etc.

• Enabler:
  – Regulator, App stores, MDM, Aggregators etc.
# Public Service

A service provided or organized by the government in order to benefit all the people in a particular society or community.

- **Electricity**
- **Education**
- **Emergency Services**
- **Environmental protection**
- **Gas and Oil**
- **Health Care**
- **Military**
- **Postal Service**
- **Public Bank**

- **Public broadcasting**
- **Public library**
- **Public security**
- **Public transportation**
- **Social services**
- **Telecommunications**
- **Urban planning**
- **Transportation infrastructure**
- **Waste management**
- **Water supply network**
Service Delivery Model

Citizen ←→ Government

International Governance

CITIZENS

Local Government

National Government
### Classification of Government Services

Services help in Social Development and Growth.

<table>
<thead>
<tr>
<th>General Public Services</th>
<th>Housing and Community Amenities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense</td>
<td>Health</td>
</tr>
<tr>
<td>Public Order and Safety</td>
<td>Recreation, Culture and Religion</td>
</tr>
<tr>
<td>Economic Services</td>
<td>Education</td>
</tr>
<tr>
<td>Environment Protection</td>
<td>Social Protection</td>
</tr>
</tbody>
</table>

Technology helps in faster, Convenient and effective service delivery,
M-Governance

- Providing all Government services accessible through Citizen’s Mobile Phone.
- It helps people to get public services fast, cheaper and round-the-clock even in rural areas.
- It empowers citizens for greater involvement and interaction with Govt. thereby strengthening democracy.
- It helps to deliver timely, accurate and real time information to citizens in an interactive manner.
- It facilitates enhanced utilization of public resources.
## Examples of m-Governance Services for residents

<table>
<thead>
<tr>
<th>Service Type</th>
<th>Students</th>
<th>Parents/Workers</th>
<th>Citizens</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enquiry</td>
<td>Fellowship, Games and Sports</td>
<td>Pensions, Government Orders</td>
<td>Employment, Government Benefits</td>
</tr>
<tr>
<td>Registration</td>
<td>Competitive Examinations, Part Time Job, Employment</td>
<td>Driving License, LPG Connection</td>
<td>Vehicle, Voter, Right To Information (RTI), GST</td>
</tr>
<tr>
<td>Status</td>
<td>Passport, Bus Pass</td>
<td>Reservation, Doctor’s Appointment</td>
<td>Train, Flight, Medical Report</td>
</tr>
<tr>
<td>Alerts</td>
<td>Strikes, Examination Schedule, Last date of submission</td>
<td>Power Cuts, Due date for payment, Vaccination</td>
<td>Traffic, Weather</td>
</tr>
<tr>
<td>Search</td>
<td>Charts, Map, Contact details, Employment Opportunities</td>
<td>Address, Location, Statistics, Tourist Place</td>
<td>Directory of m-Governance Services</td>
</tr>
<tr>
<td>Results</td>
<td>Examination</td>
<td>Diagnostic, Policy Maturity</td>
<td>Election, Selection</td>
</tr>
<tr>
<td>Opening Account</td>
<td>Bank, e-Locker, e-Sign</td>
<td>Term deposit, Employee Provident Fund, Gold Loan</td>
<td>Public Provident Fund, Demat, Pension Scheme</td>
</tr>
<tr>
<td>Certificate</td>
<td>Birth, Pass, Character</td>
<td>Income, Medical Certificate</td>
<td>Community, Domicile, AADHAR</td>
</tr>
<tr>
<td>Payment</td>
<td>Tuition Fees, Payment Receipt</td>
<td>Property Tax, Income Tax</td>
<td>Utility Bills, Service Tax, Pension</td>
</tr>
<tr>
<td>Cost</td>
<td>Application, Registration</td>
<td>Insurance Product, Diagnostic Tests</td>
<td>Loan Items, Collateral</td>
</tr>
</tbody>
</table>
## Mobile Financial Services - Entities

<table>
<thead>
<tr>
<th>Demand side (Users)</th>
<th>Supply Side (Providers)</th>
<th>Facilitation Side (Enablers)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customers and Merchants of</td>
<td>Bank</td>
<td><strong>Regulators:</strong> RBI, TRAI</td>
</tr>
<tr>
<td>• a bank</td>
<td>• Telco,</td>
<td>• Govt. Bodies: DoT, CDAC</td>
</tr>
<tr>
<td>• a Telco,</td>
<td>• Financial institution</td>
<td>• FinTech companies</td>
</tr>
<tr>
<td>• a financial institution,</td>
<td>• Mobile payment service provider</td>
<td>(Payment Gateway,</td>
</tr>
<tr>
<td>• a mobile payment service provider,</td>
<td>• Device Manufactures</td>
<td>Switching and Settlement</td>
</tr>
<tr>
<td>• a post office etc</td>
<td>• Developers</td>
<td>Organizations as NPCI,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CCIL)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• NGO s, Academic, R &amp; D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Org. etc. (MPFI, COAI,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IAMAI, IDRBT etc.)</td>
</tr>
</tbody>
</table>
## Mobile Banking (MB)

*Banking Services through a Mobile Phone*

<table>
<thead>
<tr>
<th>Information Based Services</th>
<th>Payment Transaction Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Balance enquiry</td>
<td>• Fund Transfer Instruction</td>
</tr>
<tr>
<td>• Account opening</td>
<td>• Term deposit Instruction</td>
</tr>
<tr>
<td>• Statement of account</td>
<td>• Issue of draft</td>
</tr>
<tr>
<td>• Check book request</td>
<td>• Standing instruction for</td>
</tr>
<tr>
<td>• Issue of Debit/credit card</td>
<td>periodic payments</td>
</tr>
<tr>
<td>• PIN/Password change</td>
<td>• Utility bill payments</td>
</tr>
<tr>
<td>• ATM Location</td>
<td>• Loans request</td>
</tr>
<tr>
<td>• Complaints</td>
<td>• Foreign Exchange delivery</td>
</tr>
<tr>
<td>• IFSC Code etc.</td>
<td>etc.</td>
</tr>
</tbody>
</table>
Mobile Payment (MP) 
( Models, Methods & Types )

- **MP Models**: Bank Centric, Telecom Operator Centric, Application Provider Centric, Hybrid

- **MP Methods**:
  - *Push method*: Payer (Customer-x) initiates the payment instruction for debiting his/her account to pay to the beneficiary (Customer – y)
  - *Pull method*: Payee (Beneficiary-y) initiates the payment request for crediting his/her account from customer-x

- **MP Types**:
  - *Type 1*: Complete details of both payer and payee are required for each transaction.
  - *Type 2*: Minimal details of either or both of Payer and Payee are required for payment transactions.
Classification of Mobile Payments

Based on Value
- Micro Payments
- Mini Payments
- Macro Payments

Based on Location
- Remote Payments
- Proximity Payments

Based on Charging Method
- Post-paid
- Pre-paid

Based on the validation of the tokens exchanged
- Online Payments
- Offline Payments (ex: e-coins)
Enabling Mobile Technologies

Transport
- Long-range
  - GSM
  - GPRS
  - 3G, 4G, 5G
  - LTE
- Short-range
  - Infrared
  - Bluetooth
  - RFID
  - NFC

Security enablers
- SIM
- USIM
- MicroSD Card

Platforms
- SAT
- Java ME
- Android, i-OS, Blackberry, Simbian, Windows CE etc

User Interface
- Voice
- SMS
- USSD
- MMS
# Mobile Payment through wireless channels

<table>
<thead>
<tr>
<th>Mobile Wireless Channel</th>
<th>Type of Mobile Payment</th>
</tr>
</thead>
<tbody>
<tr>
<td>USSD</td>
<td>NUUP *99#</td>
</tr>
<tr>
<td>SMS</td>
<td>SMS Banking</td>
</tr>
<tr>
<td>GPRS / UMTS/ WIFI</td>
<td>Mobile Banking Application</td>
</tr>
<tr>
<td></td>
<td>Mobile UPI Applications</td>
</tr>
<tr>
<td></td>
<td>Mobile Wallet Application</td>
</tr>
<tr>
<td>Voice</td>
<td>Voice Banking</td>
</tr>
<tr>
<td></td>
<td>IVRS Banking</td>
</tr>
<tr>
<td>NFC</td>
<td>Tap &amp; Pay</td>
</tr>
</tbody>
</table>
Mobile Payment

UIDAI Server

Payment Gateway (NPCI)

Settlement (RBI)

Bank – A (ISSUER)

Bank – B (ACQUIRER)

(Payer-X)

(IMPS, AEPS, NEFT, UPI)

(Payee-Y)
Encrypted SMS based Mobile Payments using ECC (Common Short Code with Interoperability)

Bank – A (ISSUER)

3 6

NPCI

4 5

Bank – B (ACQUIRER)

7

INFINET
Signed and Encrypted

2

IDRBT

1

Payer-X

8

Payee- Y

10/5/2018
NFC based Payment

1. Issuer Bank
2. Generate UID_c
3. CUSTOMER
4. NFC
5. NFC enabled Reader of MERCHANT/BC
6. Generate UID_m
7. Acquirer Bank
8. Switch NPCI
9. 10/5/2018
m-Application

Native
- Android
- iOS
- Blackberry
- Windows
- etc

Hybrid

Web
Mobile Cloud Services
<table>
<thead>
<tr>
<th>Websites</th>
<th>Normal</th>
<th>Responsive</th>
<th>Adaptive (Mobile Website)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓ A single website</td>
<td>✓ A single website</td>
<td>✓ Multiple websites</td>
</tr>
<tr>
<td></td>
<td>✓ Designed only for desktops</td>
<td>✓ Designed to work on all devices</td>
<td>✓ Designed specifically for each device</td>
</tr>
<tr>
<td></td>
<td>✓ Improper display on mobile phones</td>
<td>✓ Good display (UI) on mobile phones</td>
<td>✓ Best display (UI) on each device</td>
</tr>
<tr>
<td></td>
<td>✓ Need to zoom-in &amp; zoom-out</td>
<td>✓ Need not to zoom-in &amp; zoom-out</td>
<td>✓ Need not to zoom-in &amp; zoom-out</td>
</tr>
<tr>
<td></td>
<td>✓ Need horizontal scrolling</td>
<td>✓ Need not horizontal scrolling</td>
<td>✓ Need not horizontal scrolling</td>
</tr>
<tr>
<td></td>
<td>✓ More loading time</td>
<td>✓ Partially mobile and small device friendly</td>
<td>✓ Completely device friendly</td>
</tr>
<tr>
<td></td>
<td>✓ Only desktop friendly</td>
<td>✓ Frameworks like Bootstrap, Foundation3, skeleton etc.</td>
<td>✓ Frameworks like JQuery Mobile, Sencha Touch etc.</td>
</tr>
<tr>
<td></td>
<td>✓ No framework is required for design</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Composite Service
Service Composition

- Let us consider an application with a set \{ti\} of m tasks.
- Let each task \( ti \) can be executed by any of the \( xi \) number of service entities with similar performance from the set \( Sti \) where \( Sti = \{sti_1, sti_2, ..., sti_{xi}\} \). Each \( xi \)-th service entity \( sti_{xi} \) can execute the task \( ti \).
- Let \( S \) be the Set of all service entities for all the tasks \( tm \) where \( S = \{st1, st2, ..., stm\} \) and
  \[
  st1 = \{st11, st12, ..., s1x1\}, \\
  st2 = \{st21, st22, ..., st2x2\}, \\
  stim = \{sm, 1, sm, 2, ..., sm, p\}.
  \]
- The objective of service composition is to select a service entity for executing each task of an application for its completion in minimum time.
- Hence the solution to the given application is the composition of the services such that only one service among the \( x \) similar services of each task should be considered for the composition.
m-Banking & Payment

- Website through URL
- My accounts
- Bill payments
- Enquire profile
- e fixed deposit
- e tax
- e service
- e cards
  - +money transfer
  - +receiving payment

Payment transfer

Fund Transfer
- within SBI
  - own account
  - Account of others
- outside SBI
  - Inter bank beneficiary
  - Credit card beneficiary
Types of API

- Web Services API
  - REST
  - SOAP
  - HTML
  - XML

- Source Code API
  - Class based API
  - Library based API

- Object Remoting API

- Hardware API
API specification language

- JSON (JavaScript Object Notation)
- XML (Extensible Markup Language)
- XSD (XML Schema Definition)
- XBRL (eXtensible Business Reporting Language)
## Creating RESTful Web Service

### Example to create a web service for user management

<table>
<thead>
<tr>
<th>Sr.No</th>
<th>HTTP Method</th>
<th>URI</th>
<th>Operation</th>
<th>Operation Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>GET</td>
<td>/UserService/Users</td>
<td>Get list of users</td>
<td>Read Only</td>
</tr>
<tr>
<td>2.</td>
<td>GET</td>
<td>/UserService/Users/1</td>
<td>Get User with ID 1</td>
<td>Read Only</td>
</tr>
<tr>
<td>3.</td>
<td>PUT</td>
<td>/UserService/Users/2</td>
<td>Get User with ID 2</td>
<td>Idempotent</td>
</tr>
<tr>
<td>4.</td>
<td>POST</td>
<td>/UserService/Users/2</td>
<td>Get User with ID 2</td>
<td>N/A</td>
</tr>
<tr>
<td>5.</td>
<td>DELETE</td>
<td>/UserService/Users/1</td>
<td>Get User with ID 1</td>
<td>Idempotent</td>
</tr>
<tr>
<td>6.</td>
<td>OPTIONS</td>
<td>/UserService/Users</td>
<td>List the supported operations in web service</td>
<td>Read Only</td>
</tr>
</tbody>
</table>
Message Flow

PSP 1

ReqPav

RespPav

Existing NPCI Products

Account Provider 1

020

PSP 2

RespAuthDetail

ReqAuthDetail

Account Provider 2

020

021

021
Mobile Risks, Threats & Vulnerabilities

- Risks (Natural & Intentional)
  - Health hazard due to signal radiation and abnormal use.
  - Accidental injuries during its use while walking, driving etc.
  - Loss of Sensitive Data, Privacy & Device

- Threats arise due to existence of exploitable vulnerabilities in an entity or system.
- Identification of the mobile security vulnerabilities is necessary to plug and insulate them from attackers.
Mobile Security

• Basic Properties/Goals of Security
• Security Policy & Access Control Models
• Security Enforcement
  – Technology, Business, Regulatory & Legal Control

• Technology: Cryptology (Cryptography & Cryptanalysis)
  • Encryption & Decryption
  • Key Generation (Symmetric & Asymmetric)
  • Hash Functions
  • Digital Signature

• Ensure Security at each of the 7 Layers of OSI Model
## Basic Properties of Information Security:

<table>
<thead>
<tr>
<th>Security Property</th>
<th>Definition</th>
<th>Enabling concept / Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>Property that ensures that transaction information cannot be viewed by unauthorized persons</td>
<td>Encryption</td>
</tr>
<tr>
<td>Authentication</td>
<td>Property that the transaction information actually originates from the presumed transaction partner</td>
<td>Possession (e.g. of a mobile phone), knowledge (e.g. of a PIN) and property (e.g. biometric property)</td>
</tr>
<tr>
<td>Integrity</td>
<td>Property that the transaction information remains intact during transmission and cannot be altered</td>
<td>Digital signatures</td>
</tr>
<tr>
<td>Authorization</td>
<td>Property that parties involved must be able to verify if everyone involved in a transaction is allowed to make the transaction</td>
<td>Digital certificates</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Property that no one should be able to claim that the transaction on his/her behalf was made without their knowledge</td>
<td>Digital certificates &amp; Digital signatures</td>
</tr>
</tbody>
</table>
Mobile Communication Architecture

Mobile Stations

Base Station Subsystem

Network Management

Subscriber and terminal equipment databases

OMC

Exchange System

BTS

BSC

MSC

VLR

HLR

AUC

EIR
**MP bearer channels of wireless medium:**

- **IVRS** : Interactive Voice Response System
- **SMS** : Short Message Service
- **USSD** : Un-structured Supplementary Service Data
- **GPRS** : General Packet Radio service
- **WAP** : Wireless Application Protocol
- **WiFi** : Wireless Fidelity
- **RFID** : Radio Frequency Identification
- **NFC** : Near Field Communication
- **Bluetooth**
- **WiMax** : Wireless Interoperability of Mobile Access
- **LTE** : Long Term Evolution etc.
Proprietary Tools

- HP Fortify
- IBM Appscan
- TCS-HI8

Open Source Tools

- Mercury Framework (Android, Dynamic Analysis)
- Burp Suite (Capture Network Traffic)
- Wire shark (Capture Air Traffic)
- APK Analyzer
- Agnitio
- VirusTotal
Mapping Mobile Security Threats of OWASP

**Device Level**
- SD Card
- SIM
- Operating System
- SQLite DB
- Insecure Data Storage (M1)
- SQL Injection (M7)

**App Level**
- Side Channel Data Leakage (M4)
- Security Decisions via Untrusted Inputs (M8)
- Lack of Binary Protections (M10)
- Poor Authorization & Authentication (M5)
- Broken Cryptography (M6)

**Communication Level**
- Improper Session Handling (M9)
- Weak Server Side Controls (M2)
- Insufficient Transport Layer Protection (M3)
Source of Mobile Security Threats

- A) Rouge malicious applications- impersonate mobile application or compromise the code of a genuine app and inject malicious software into the app.

- B) SMS phishing/spoofing- “smishing.” – Impersonating a text message (SMS) to obtain customer information. SMS eavesdropping – intercepting and Stealing information from text messages.

- C) Mobile enabled web application vulnerabilities- mobile- enabled websites are subject to the same vulnerabilities as a standard website, including cross-site scripting (xss), SQL injections, malicious software, and URL redirects.

- D) Unauthorized Mobile Applications- mobile applications that are not authorized by the manufacturer/bank or listed out in a mobile application store pose higher risk to the institution.
E) Device Rooting/Jail breaking- removing or bypassing manufacturer controls to gain root access to the device, providing additional access to the device’s operating system and files, which increases risk.

F) Plain-text data storage- storing data on mobile device (including usernames, passwords, account numbers, purchases, location information, etc.)

G) Insecure application development- since mobile applications reside or operate over numerous levels of telcos, networks(2g,3g,4g/wi-fi), operating systems, device types, and app stores, this decentralized mobile ecosystems can lead to different vulnerabilities that require patches and updates at different levels, increasing risk to the institution and the user.
• H) Lost/stolen device- a mobile device is much easier to be lost or have been stolen than a desktop (or even a laptop)
• Unauthorised payments/transfers- theft or unauthorised access can lead to payments or transactions being performed by unauthorised individuals.
• J) Wireless eavesdropping- mobile payment systems may be intercepted between the device and the point-of-sale terminal if proper encryption is not implemented.
• K) Identity theft- unauthorised access to mobile services may lead to stealing customer or transaction information, which may, in turn, lead to identity theft.
• L) Fake accounts- using stolen identity information one can create fake accounts on stolen devices.
### Mobile Security Standards:

- Device
- Communication
- Application Development
- OS
- Database
- User Interface
- Network Equipment
- Device Interfaces
- Data Privacy etc..

- OWASP
- NIST
- ISO
- IEEE
- ITU
- EMV
- PCI
- NFC Forum
- MTC, CERT-IN, RBI, TRAI, STQC, MPFI etc..
Light Weight Cryptography

- Elliptic Curve Cryptography (ECC)
- Grain
- SIMON
- Photon
- SPECK
- DESL
## Comparison of RSA and ECC

<table>
<thead>
<tr>
<th>Symmetric cipher key size</th>
<th>ECC key size</th>
<th>RSA key size</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>112</td>
<td>512</td>
</tr>
<tr>
<td>80</td>
<td>160</td>
<td>1024</td>
</tr>
<tr>
<td>112</td>
<td>224</td>
<td>2048</td>
</tr>
<tr>
<td>128</td>
<td>256</td>
<td>3072</td>
</tr>
<tr>
<td>192</td>
<td>384</td>
<td>7680</td>
</tr>
<tr>
<td>256</td>
<td>512</td>
<td>15360</td>
</tr>
</tbody>
</table>

*Table 3: Comparison of Key Sizes Providing Similar Security for Different Algorithms (SECG 2000)*
QR Code
Captcha
Bio-metrics
OTP
M-PKI
Mobile Device Level Security

• Mobile phone is an integration or content, container, computing, communication and co-ordination.

• Mobile Device consists of hardware, software and interfaces.

• From a system’s perceptive is has following 5 sections.
  – Input Section
  – Processing Section
  – Power Section
  – Communication Section
  – Output Section
Techniques used in mobile operating systems to control threats

• Rootkit Detectors
• Process Isolation
• File Permissions
• Memory Protection
• Development through runtime environments
• Security Software
• Secure Operating System
• Trusted Execution Environment (TEE)
• Secure Element (SE)
THANK YOU