An Integrated Approach for SMS-Based Secure Mobile Banking in India

*Neetesh Saxena,
Narendra S. Chaudhari
IIT Indore, India
Introduction

- Various M-banking channels SMS, USSD, GPRS, WAP and phone based applications
- Nowadays, SMS is very popular and frequently used worldwide
- Traditional SMS service does not provide any security to transmitted message
- SMS-based m-banking can be extended as a secure channel
Problem Statement

- The objective → secure mobile banking using SMS
  - for the people who are living in the rural part of India
  - don’t have java support cellular phones and Internet facility (limited)

- Presently, SMS is in clear text without any ciphering mode while transmitting

- SMS and its banking environment must be secure from various attacks

- Some banks provide change password option through SMS which is a threat

- Secure m-banking → authentication, confidentiality, integrity, non-repudiation.

- In India
  - Only banks can provide the facility of m-banking while
  - Other countries like Kenya and Philippines non-bank organizations can also do
Solving Approach

- The SIM → issued by → Govt. authorized body of Telecomm. Department of India

- Store a secret key for each bank onto the SIM at the time of manufacturing and in the database of respective banking server

- To manage SIM storage, limit a user → 3 to 5 m-banking services of different banks

- As per Reserve Bank of India (RBI) guidelines only banks can provide such facility
  - The current guidelines must be reviewed.

- An integration of service providers and different banks must be encouraged

- Proposed a separate SIM for the secure channel of communication
Continued...

Strong Authentication Protocol

Encryption
DES, Triple DES, AES, Twofish, RC6, Blowfish, CAST6, RC2, MAES

Authentication functions
MD5, SHA1

Digital Signature RSA, DSA, ECDSA

Mutual Authentication

Confidentiality

Integrity

Non-Repudiation

Prevents Redirection, Impersonation Attack
Prevents MITM and Replay Attack
Prevents SMS tampering & message disclosure
Prevents Repudiation Attack

DoS, SMS Spoof Attack

Session Keys + by key stored onto SIM + Bank Database

SMS Content + User Identity + Timestamp

SIM + handset → Registered → Bank Database
Results

- The platform used is J2ME Wireless Toolkit for user interface, MySQL database and Tomcat as server. The results have been generated with JDK1.7 and J2ME wireless messaging API.

**Fig. 1. Symmetric Encryption**

**Fig. 2. Symmetric Decryption**
Results

*Future Work*

1. Confidence interval for the MAES algorithm for ciphering;
2. Storage space for each key and algorithm: used physical, virtual and swap memory size;
3. Energy & Time Efficiency: CPU time, Encryption/Decryption time, Key generation time;
4. Implement a variant of ECDSA algorithm which is more secure than ECDSA (previous published work in ICMSAO-2013).
Thank You !! 😊