Text Message Security

List of team members:
Sameera Jammula
Shashwath B Raghavan
Vignesh Ravishankar

Introduction and Motivation:
Short message service (SMS) is a text message service that enables users to send short messages to other users on the global system for mobile communication (GSM) network. SMS uses a store-and-forward mechanism. At the beginning of 2007, the worldwide number of mobile users reached the 2.83 billion mark. In fact, out of them 2.28 billion users (i.e. 80.5%) were using the GSM. In today's environment, most banks are using the SMS's for exchanging the information with their customers. SMS is very popular that's why the research direction are moving towards the security solutions through SMS like in M-banking, M-Commerce, value added services etc. The advantages of using SMS's are its ease of use, common messaging tool among consumers, works across all wireless operators, affordable for mobile users, no specific software required for installation, allows banks and financial institutions to provide real-time information to consumers and employees, stored messages can be accessed without a network connection.

A primary shortcoming of GSM is that, it does not offer a secure environment for confidential data during transmission and there is no standard procedure to certify the SMS sender. There is a requirement for an end to end SMS encryption with errorless message transmission in order to provide a secure with error free data transmission for communication.

List of Security Services we are planning to explore and enhance:
A secure SMS system requires solving the following three problems:

- Authentication: Confirm true identities between sender and receiver, and prevent impersonation attack from illegal intruders.
- Confidentiality: Ensure that decrypted messages are accessible only to those authorized senders and receivers.
- Integrity: Ensure that receivers can check out whether the message has been modified, and prevent tampered messages.

Detailed description of problems/hypotheses we are planning to investigate:

- Comparison of various hashing techniques and encryption algorithms implemented on transit data.
- Application specific security on different platforms.
- Comprehensive study on different types of attacks on SMS.
- Comprehensive study on different types of compression techniques implemented on data/payload.

A tentative list of questions we will be seeking an answer to:

- Step by step process used in transfer of text message between peers?
- Protocols used in text message communication?
- Key exchange between the end users?
- Security threats and attacks text messages are vulnerable to?

- Types of encryption algorithms & hashing techniques currently in use?
- Extent of text messaging application security on different platforms?
- Comparison of performances of various encryption and hashing algorithms?
- Required enhancements on the same for better security?

Procedure for verifying the results of our investigation

- Detailed study on the available literature and analysis of various cryptographic techniques.
- Comparison of results obtained from different cryptographic algorithms.
- Inputs from subject matter experts to verify the results.

Tentative Time schedule:

★ **Oct 15 -17**

- Analysis on the scheme used in text message transmission and types of protocols used.
- Analysis on the existing security threats and attacks on text messages.
- Analysis of the cryptographic techniques to mitigate the security threats and attacks.

★ **Nov. 5-7**

- Extent of text message application security on different platforms.
- Comparison of the encryption algorithm, hashing techniques and compression standards.
- Incorporating the proposed suggestions/improvements from the 1st meet.

★ **Nov. 19-21**

- Proposed enhancements on the current techniques based on the analysis.
- Detailed study on enhancements on the current techniques.
- First draft of the research paper.
- Incorporating the proposed suggestions/improvements from the 2nd meet.

Tentative Table of contents:

- Introduction
- What is an SMS?
- SMS preliminaries and architecture
- Security threats and vulnerabilities
- Cryptographic encryption and hashing techniques
- Application security on different platforms
- Performance comparison and enhancement techniques
- Evaluation and analysis
- Conclusions and future scope
- References

List of Literature:

[1] High Security Communication Protocol for SMS:
http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=5368937.
[2] Joint Channel Coding and Cryptography for SMS:
http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=6072593.
[3] Application-Layer Security Mechanism for M2M communication over SMS:

http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=6419578
[4] On Forensics: A Silent SMS Attack
http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=6320454
[5] SMS Encryption using AES Algorithm on Android:
http://research.ijcaonline.org/volume50/number19/pxc3881038.pdf
[6] SMS Encryption for Mobile Communication
http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=4725375
[7] Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks
http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=4555693
[8] Text Compression and Encryption through Smart Devices for Mobile Communication
http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=6603755
[9] GSM Infrastructure Used for Data Transmission
http://ieeexplore.ieee.org.mutex.gmu.edu/stamp/stamp.jsp?tp=&arnumber=5952239
[10] ON THE IMPACT OF GSM ENCRYPTION AND MAN-IN-THE-MIDDLE ATTACKS ON THE SECURITY OF INTEROPERATING GSM/UMTS NETWORKS
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.59.983&rep=rep1&type=pdf
[11] RFC 4462 SSH GSS-API Methods
http://www.ietf.org/rfc/rfc4462.txt