SANAsms: Secure Short Messaging System for Secure GSM Mobile Communication

Nor Badrul Anuar, Ibrahim Muhammad Azlan, Abdul Wahab Ainuddin Wahid and Zakaria Zakaria
University of Malaya, Kuala Lumpur, Malaysia
badrul@um.edu.my
cadefoster117@perdana.um.edu.my
ainuddin@um.edu.my
omarzakaria@um.edu.my

Abstract: SANAsms or Short Messaging System (SMS) Encryption System is an application on mobile phone that enables to send, receive, and store encrypted text messages. Users are able to exchange sensitive messages using SMS because the message is in an encrypted and a protected form, which it is hard for the attacker or non-authorize person to read the messages. As a result, the system makes the confidential data in SMS text become safer and secure in such case of the device lost or stolen. SANAsms is capable to send confidential encrypted information in SMS via normal GSM and it only can be read by person who can decrypt it. Currently, normal SMS using GSM communication is not secured and safe enough. One of the solutions is to have a security application implemented in mobile phone device. Therefore, SANAsms system ensures that information (SMS) interchange between sender and receiver is secured and protected because the messages containing delicate information are stored securely and remain undisclosed even when the device is accessed by an adversary. The system is developed using Java 2 Micro Edition (J2ME) which is written in Java. J2ME phone and Symbian Operating System (OS) as the platform for the application to run. The encryption algorithm that implemented in the system is Advanced Encryption Standard (AES) with 128-bit block size and together with the SHA1 (Secure Hash Algorithm) hash functions. The application is designed to satisfy the user friendly interfaces and intent to be used by the end user without having the advanced knowledge in mobile security. Besides, mobile phone that able to run J2ME application is being chosen because it was designed specifically for mobile devices which support small memory footprint and low power consumption.

Keywords: Keywords: Secure Short Messaging System, SANAsms

1. Introduction

By default, SMS content is sent over the Global System for Mobile communications (GSM) network in plain text or non-encrypted form. If a non-encrypted text message contains confidential information, then it can be read easily by adversary. Some examples of confidential information are ATM password, bank account number, or personal information which is needed to be encrypted in order to avoid from being read by adversary. Furthermore, there is no security for the SMS message in case where the sender typing error in selecting number of recipient or the device lost or stolen (Hassinen & Markovski, 2003). In the usage of mobile phone devices within companies, sensitive business information and messages should be encrypted because this can be compromised, lost, or stolen.

By encryption, we mean a process of converting information to a disguised form in order to send it across a potentially unsafe channel. The reverse process is called decryption. Using strong encryption techniques, sensitive, valuable information can be protected against organized criminals, malicious hackers, or spies from a foreign military power, for example. Indeed, cryptography used to be almost exclusively a tool for the military. However, in moving into an information society, the value of cryptography in everyday life in such areas as privacy, trust, electronic payments, and access control has become evident. In this way, the field of cryptography has broadened from classical encryption techniques into areas such as authentication, data integrity, and non-repudiation of data transfer.

In order to make SMS messages communication become more secure and protected, a SANAsms - SMS Encryption System has been developed. The system is a J2ME application which is specially built for mobile phone platform. With this application, it is hard for attacker or non-authorize person to read the encrypted messages. The SMS message only can be read if the user inserts the right password. At the same time, the application has been developed to make it easy to use and user-friendly for the user.

2. SANAsms

SANAsms or SMS Encryption System is an application on mobile phone which it can sends, receives, and stores encrypted text messages. SANAsms is a Mobile Information Device toolkit (MIDlet) which is Java program for embedded devices. Users can exchanges sensitive messages using this SMS because the message is encrypted and protected. When message is encrypted, it's hard for the attacker or non-authorize person to read the messages. The system makes the confidential data in SMS text become safer and secure in such case of the device lost or stolen.

There are two categories of objectives for this project: immediate objectives and long term objective. Immediate objectives for this project are:

- To develop a program that capable to send encrypted confidential information in SMS that send via GSM mobile communication and it only can be read by person who can decrypt it.
- To also develop an application compacts enough for use in a mobile phone.

For the long term objective, the project aims to make SMS communications become more secure and safer by making to encryption system application in mobile phone platform as one of security elements by individual and businesses.

The processes of SMS encryption in this application begin when the sender types the text message. After the text message has been typed, the sender selects the recipient's phone number. The encryption system application requests a password for the SMS which is to be used to open the SMS message received by a recipient. The password is the key for both encryption and decryption process. This password is shared between sender and recipient. The text message is encrypted before it sends to the recipient via GSM mobile communication. When the recipient receives the SMS message, the recipient has to input the same password with the sender. If the recipient inserts the right password/key, the application will decrypt the text message and display the decrypted text message.

Normal SMS communication is not secured and safe enough. One of the solutions is to have a security application implemented in mobile phone device. SANAsms system is ensured information (SMS) interchange between sender and receiver secured and protected. Most importantly, the messages containing delicate information are stored securely and remain undisclosed even when the device is accessed by an adversary.

2.1 SANAsms design

SANAsms is mobile solution for secure communication using SMS. Sender needs to encrypt the message using shared key or password that previously agreed with the receiver. Receiver has to decrypt the message using the shared password. In the other word, only right person with the correct key can read the message content. The encrypted SMS only can be read by a person who has the application installed in their phone (refer to Figure 1,2, 3, 4 and 5). Beside that, symmetric encryption has faster performance rate compare to asymmetric algorithm encryption.

The SMS is simply a byte array containing a header, the ciphered text, and message's digest. The header includes two bytes of metadata and two bytes containing the size of the cipher text. The first two bytes can be used to indicate properties of the message.

On the receiving end, the application listens for incoming messages and upon their arrival it prompts for the password to be used in the decryption process. A message has a digest to verify the integrity of the message.

The next subsection will discusses on software components of SANAsms design such as Open Mobile Alliance (OMA), Advanced Encryption Standard (AES), **SHA-1** (Secure Hash Algorithm), J2ME phone, Symbian OS and J2ME Wireless Toolkit

2.1.1 Open mobile alliance (OMA)

OMA is a standard body which develops open standards for mobile phone industry. OMA, in other words, is the reorganized form for Wireless Application Protocol (WAP). This standard is allowed for Java interface such as Mobile Information Device Profile (MIDP) 2.0. It is as part of J2ME and

used by mobile device to run Java applications. A MIDlet is a Java program for embedded devices, more specifically the Java ME virtual machine. MIDlet cannot run without MIDP interface. Symmetric-key algorithm is built in the MIDlet using API.

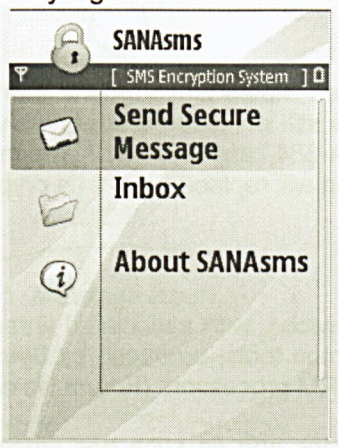

Figure 1: Main menu of SMS encryption system application

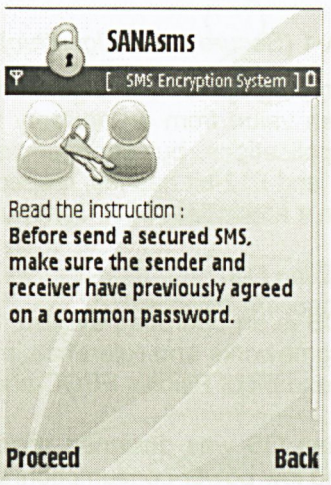

Figure 2: Instruction message proceed to the send message forms

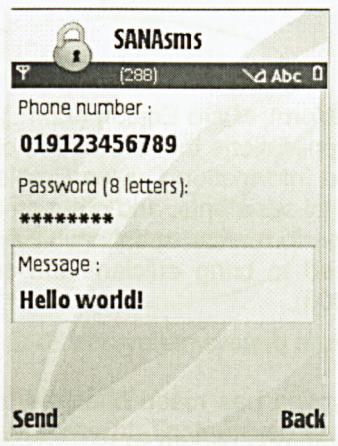

Figure 3: Send message forms

Figure 4: Receive message form

Figure 5: Display decrypted message

2.1.2 Advanced encryption standard (AES)

Bearing the growing feasibility of attacks against DES in mind, NIST launched a call for proposals for an official successor that meets 21st century security needs. This successor is called the Advanced Encryption Standard (AES) (SSH Communication Security).

All the ciphers have a 128-bit block size and they support 128, 192, and 256 bit keys. The rather large key sizes are probably required to give means for construction of efficient hash functions (SSH Communication Security).

2.1.2 SHA-1 *(Secure Hash Algorithm)*

This is a cryptographic hash algorithm published by the United States Government. It produces a 160 bit hash value from an arbitrary length string. SHA-1 is still considered adequately safe for practical applications, but stronger versions, SHA-256, SHA-384, and SHA-512, which produce 256-, 384-, and 512-bit hashes, respectively, are available and will replace SHA-1 as crypto logical research on it advances (SSH Communication Security).

2.1.3 Symbian OS

Symbian OS is an operating system, designed for mobile devices, with associated libraries, user interface frameworks and reference implementations of common tools, produced by Symbian Ltd. It is a descendant of Psion's EPOC and runs exclusively on ARM processors (Forum Nokia, 2003).

The Symbian OS was designed specifically for mobile devices and as such has small memory footprint and low power consumption. It is an open OS, enabling third party developers to write and install applications independently from the device manufacturers. An extensive C++ API is provided which allows access to services such as telephony and messaging, in addition to basic OS functionality (Forum Nokia, 2003).

2.1.4 J2ME Wireless Toolkit

The Sun Java Wireless Toolkit (formerly known as Java 2 Platform, Micro Edition (J2ME) Wireless Toolkit) is a state-of-the-art toolbox for developing wireless applications that are based on J2ME's Connected Limited Device Configuration (CLDC) and Mobile Information Device Profile (MIDP), and designed to run on cell phones, mainstream personal digital assistants, and other small mobile devices. The toolkit includes the emulation environments, performance optimization and tuning features, documentation, and examples that developers need to bring efficient and successful wireless applications to market quickly (Sun Microsystems, 2008).

3. The SANAsms interface

The architecture for mobile SMS using symmetric-key encryption has made changes to existing structure. There will be a verification process running in mobile device itself, to validate message decryption.

SANAsms provides secure encryption for wireless communication. Figure 6 illustrates the mobile SANAsms process. SANAsms uses symmetric-key cryptography, methods in which both the sender and receiver share the same key. The application uses Advanced Encryption Standard (AES) encryption algorithm with 128-bit encryption key and the message integrity and authentication is check using SHA-1 hashing algorithm.

4. Why SANAsms is chosen?

Currently, mobile SMS does not offer any specific security features. By implementing symmetric-key encryption in SMS architecture, eavesdropping by man-in-the-middle attack can be avoided. The secret end-to-end encryption will ensure the message to be read by only the right person. Personal and corporate privacy and confidentiality of message content can be retained.

Every message encrypted by the application can only opened by person who knows the password. Plus, in case of the sender entered the wrong receiver's phone number, the SMS still can't open by whoever have received the SMS without the application itself.

Besides that, concept of using symmetric-key encryption for message encryption and decryption is easy for public to understand, accept and use. The implementation cost of SANAsms is cheap and will not cause any major issues on violating intellectual property right.

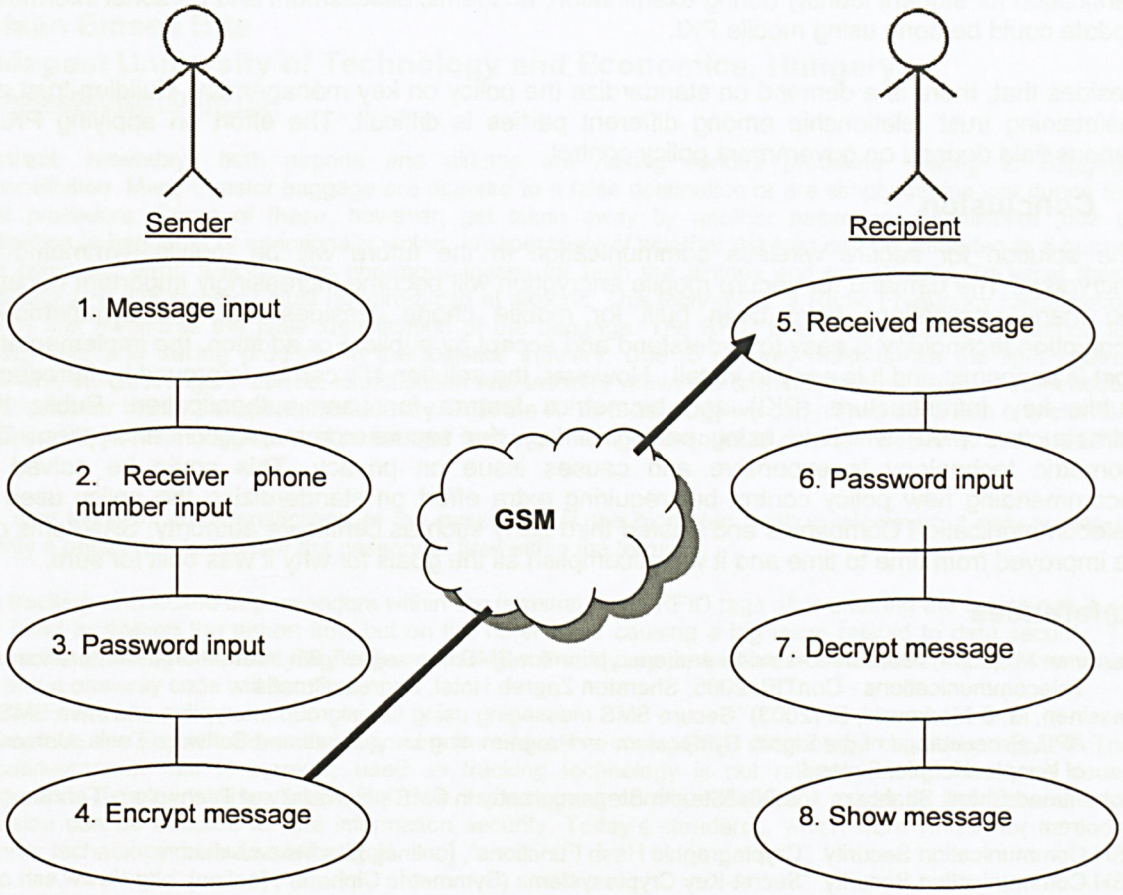

Figure 6: SMS encryption system architecture

5. Future works

The significant use of mobile communication has raised the need to communicate privately. The proposed solution can be used for further research in terms of quality improvement and performance enhancement.

Symmetric-key encryption is a proven solution for secure communication encryption. This concept is applied in this paper to offer security control on wireless communication. Further effort on transforming the SANAsms from mobile SMS into various wireless applications on handheld devices is encouraged.

SANAsms will be added with contact list database. The database will contain with receiver's phone numbers and also with shared keys. The purpose of the database, sender doesn't have to type the shared-key or password each time to send a message. Implementation another symmetric algorithm such as Blowfish into SANAsms will be the future enhancement for the application.

Introducing Public Key Infrastructure (PKI) in encryption and decryption process in the mobile enviroment will be the further study for this area. Asymmetric encryption is similar with Public Key Infrastructure (PKI) encryption. Both is using mathematic algorithm to generate public key and private key. This encryption can be used for communication security but it is difficult to manage the key distribution.

Research on applying PKI in voice communication will be interesting and meaningful. The voice communication is the main attraction in mobile and internet applications. The repudiation in PKI will help in verifying the identity of target party. The recorded conversion can be used as legal evidence because all parties involved could not deny the content and their participation on that conversion.

In future, perhaps new features or applications will be carried out for education purpose. The verification for student identity during examination, academic assessment and personal information update could be done using mobile PKI.

Besides that, there is a demand on standardize the policy on key management. Building trust and maintaining trust relationship among different parties is difficult. The effort on applying PKI in various field depend on government policy control.

6. Conclusion

The solution for secure wireless communication in the future will be mobile symmetric-key encryption. The demand for secure mobile encryption will become increasingly important because too many applications have been built for mobile phone. Besides that, the symmetric-key encryption technology is easy to understand and accept by public. For addition, the implementation cost is economic and it is easy to install. However, the solution still can be improved by introducing Public key Infrastructure (PKI) and biometrics feature for user authentication. Public Key Infrastructure (PKI) which is using pairing of key, for secure communication encryption. This biometric technology is expensive and causes issue on privacy. This could be solved by recommending new policy control but requiring extra effort on standardizing the policy used by Telecommunication Companies and trusted third party such as certificate authority. SANAsms can be improved from time to time and it will accomplish all the goals for why it was built for sure.

References

Hassinen M. (2003) "SafeSMS - End-to-end encryption for SMS messages", 8th International Conference on Telecommunications - ConTEL 2005, Sheraton Zagreb Hotel, Zagreb, Croatia.

Hassinen, M. & Markovski, S. (2003) "Secure SMS messaging using Quasigroup encryption and Java SMS API", Proceedings of the Eighth Symposium on Programming Languages and Software Tools. University of Kuopio, Kuopio, Finland.

Mohammad Shirali Shahreza . (2006) "Stealth Steganography in SMS", University of Technology Tehran, Iran.

SSH Communication Security. "Cryptographic Hash Functions", [online], http://www.ssh.com

SSH Communication Security. "Secret-Key Cryptosystems (Symmetric Ciphers)", [online], http://www.ssh.com , [accessed 25 December 2007].

Sun Microsystems "Sun Java Wireless Toolkit for CLDC", [online], http://java.sun.com/products/sjwtoolkit/

William E. (Bill) Burr (2003) "Selecting the Advanced Encryption Standard", National Institute of Standards and Technology, United States.