HTTPS APPROACH TO RESIST MITM ATTACK IN SECURE SMS

MUHAMMAD MURAD KHAN

A thesis submitted in fulfillment of the
requirements for the award of the degree of
Master of Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

30 August, 2013

DEDICATION

Specially dedicated to all mighty ALLAH who gave me skill of learning and strength to memorize, my sponsor GC University Faisalabad, Pakistan and my parents, can never thank them enough.

ACKNOWLEDGEMENT

I wish to express my gratitude to my supervisor **Dr Majid Bakhtiari** for his support and encouragement during this project proposal. I really appreciate his time and contributions in guiding me how to do research and craft thesis from findings. I also want to appreciate and acknowledged my other lecturers for their support during the study.

.

.

ABSTRACT

Short Messaging Service has become vital part of every individuals life. Like human, businesses have also gained benefit from SMS by providing business alerts, transaction services, resource management etc over it using Automated SMS. With exchange of confidential and mission critical information over SMS, security of SMS has become a big concern. Many researchers provided solutions to secure content of message using encryption but key exchange of encryption algorithm cannot be secured. Man In The Middle can observe key exchange messages and can setup MITM attack between communication. Security vulnerability inside this operation is that, secret key and encrypted messages are shared over same channel i.e. SMS. This project propose a PKI web system that distributes encryption keys for encryption of SMS over HTTPS, making MITM attack near to impossible on Secure SMS.

ABSTRAK

Khidmat Pesanan Ringkas telah menjadi sebahagian penting dalam kehidupan setiap individu. Seperti manusia, perniagaan juga telah mendapat manfaat daripada SMS dengan memberikan amaran perniagaan, perkhidmatan transaksi, pengurusan sumber dan ke atas lain-lain dengan menggunakan SMS Automatik. Dengan pertukaran sulit dan maklumat yang kritikal lebih SMS, keselamatan SMS telah menjadi satu kebimbangan besar. Ramai penyelidik menyediakan penyelesaian untuk mendapatkan kandungan mesej menggunakan penyulitan tetapi pertukaran utama algoritma penyulitan tidak boleh dijamin. Man in the Middle boleh melihat mesej pertukaran utama dan boleh setup serangan MITM antara komunikasi. Kelemahan keselamatan di dalam operasi ini adalah bahawa, mesej utama dan disulitkan rahsia dikongsi bersama melalui saluran yang sama iaitu SMS. Projek ini mencadangkan sistem web PKI yang mengedarkan kunci penyulitan untuk penyulitan SMS terhadap HTTPS, membuat serangan MITM berhampiran mustahil kepada penyelamatan SMS.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

3G	-	Third generation mobile network
4G	-	Fourth generation mobile network
AES	-	Advance Encryption Standard
API	-	Application Programming Interface
ATM	-	Automatic Teller Machine
AVD	-	Android Virtual Device
BSS	-	Base Station System
CA	-	Certification Authority
Cert	-	security Certificate
CIA	-	Confidentiality, Integrity, Authenticity
DES	-	Data Encryption Standard
ECC	-	Elliptic Curve Cryptography
EDGE	-	Enhanced Data for Global Evolution
GPS	-	Global Positioning System
GSM	-	Global System for Mobile Communications
HTML	-	Hyper Text Markup Language
HTTP	-	Hyper Text Transmission Protocol
HTTPS	-	Secure Hyper Text Transmission Protocol
IP	-	Internet Protocol
KDS	-	Key Distribution System
MITM	-	Man In The Middle
MS	-	Mobile Station
NIST	-	National Institute of Standards and Technology
OS	-	Operating System
OTA	-	On The Air
PHP	-	Personal Home Page - web scripting language
PKDS	-	PHP Key Distribution System
PKI	-	Public Key Infrastructure
RSA	-	Ron Rivest, Adi Shamir and Leonard Adleman
SDK	-	Software Development Kit
SMS	-	Short Messaging Service
SMSC	-	Short Messaging Service Center
SQL	-	Standard Query Language
SS7	-	Signaling System No. 7

SSL	-	Secure Socket Layer
WAMP	-	Windows Apache, MySQL and PHP server

CHAPTER 1

INTRODUCTION

1.1 Introduction

In today’s world, most people have double lives a physical one and a virtual one (being online). While physically we live with the things around us, virtually we are accompanied by communities of our interest and this has brought a new feeling into human being; a feeling of being connected and disconnected. The virtual world has created new platforms to interact on and communicate such as Facebook, which is widely used to share and discuss social issues within a closed community, Twitter is used to broadcast real-time updates, email has almost changed the definition of conventional mail etc. and still it continues to burgeon, providing every reason to get online. These social interaction platforms are entitled as social media. Social media does not only provide social connectivity, but also empowers each individual with freedom of speech like no other. “The other side of the story”, protests, misuse and corruption etc. facts are shared openly on social media until they become so viral that they are backed up by a huge mob and then they burst into physical world.

Smart phones are the biggest source of getting connected to the virtual world. Every social media website has provided its applications for all ranges of smart phones. Other than connectivity to the virtual world, smart phones have enabled users to manage their office work, watch movies, capture and edit images on the go and make custom applications as a result increasing the productivity of the user. Smart phones also gear up with different sensors like GPS that can give geographical location of the user, accelerometer for x,y,z movement of mobile phone, 3D Camera etc. Because of these features, it is the most wanted gadget of today.

With so many versatile features supported by variety of mobiles, Short Messaging Service (SMS) is most commonly used function supported by all kind of mobiles. For many years SMS was used for human-to-human messaging until programmable GSM devices landed international market and started an era of automated Messages. Today Facebook, Gmail etc. send SMS for verification of the user, Banks alert their customers about ATM usage over SMS and there exist many other custom applications that alert customers over SMS. Though it’s easy and effective to communicate over SMS, it has no security. Truth is, every SMS sent can be read, Modified or even generated by third party on your behalf. So big question now is, how can we fill this security gap and how?

This project will therefore aim to study and identify different algorithms available to secure SMS, design communication methods, key management between server and end user over secure channel and finally secure sms exchange between end user mobile applications.

1.2 Problem Background

Wonders of science although seem simple but possess great knowledge behind their implementation. Same is the story for SMS, which has two modes of operation, Text mode and PUD mode. In Text mode message is encoded in standard “GSM” or “8859-1” 7-bit encoding scheme and message payload is sent separate of operator/SMSC information whereas PDU format is more flexible. PDU format includes SMSC information, timestamp etc. as Header and message as SMS Payload as illustrated in Figure 1.1 PUD SMS Structure. In both cases Message is transmitted as plaintext.

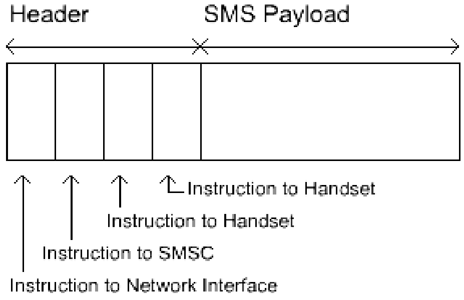

Figure 1.1 PUD SMS Structure

To counter this problem many researchers have put their effort in making SMS Payload secure using encryption, digital signature etc. but till now all of them have used same channel for key and message exchange allowing MITM to act as a mirror between communicating parties and executing attack. Multipurpose implementations over SMS payload were observed e.g. SMS Communication as transport layer for desktop application (Songyang Wu & Chengxiang Tan,2009), SMS use as banking services in Bangladesh (Md. Subrun Jamil & Fouzia Ashraf Mousumi,2008), Custom messaging systems that can send messages to network administrators for controlling and managing network (Stavros Vougioukas & Manos Rouincliotis,2001), enhancement of public transportation in Punjab Pakistan (Umar Farooq et al.,2010), electric power load management and monitoring system for peak loads in Malaysia using GSM communication (Azhar Fakharuddin et al.,2010) etc.

Despite the fact that these application share confidential, mission critical information, they are communicated in Plain text and if any security profile is implemented, its implementation cannot defend attack. For better understanding observes Figure 1.2: SMS Exchange without encryption, Figure 1.3: SMS Exchange with encryption and Figure 1.4: Man in the Middle Attack.

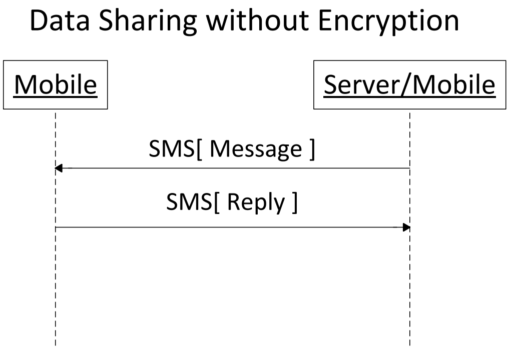

Figure 1.2 SMS Exchange without encryption

Figure 1.2 SMS Exchange without encryption illustrate sharing of information without any encryption. SMS from both sides are sent in plain text.

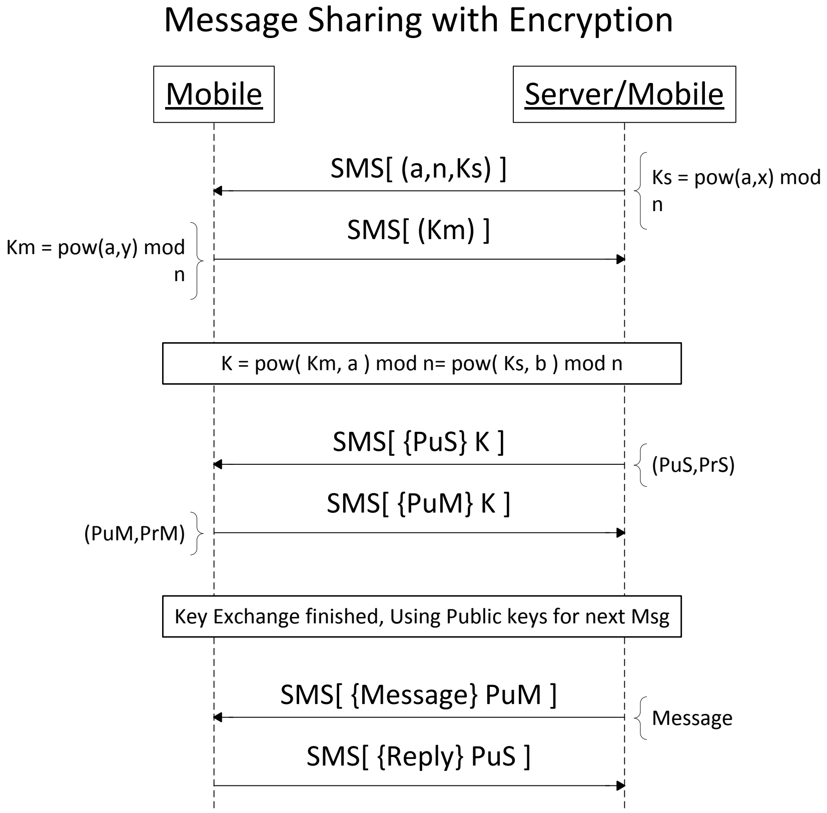

Figure 1.3 SMS Exchange with encryption

Figure 1.3: SMS Exchange with encryption, shows how two communicating

parties first use diffie-helman algorithm for key exchange, with share of public key afterwards. Similar to diffie-helman key exchange, other key exchange techniques require sharing of initial random numbers to land on a secret number on both sides which act as a key. Vulnerability in this system is identified in Figure 1.4: Man in the Middle attack.

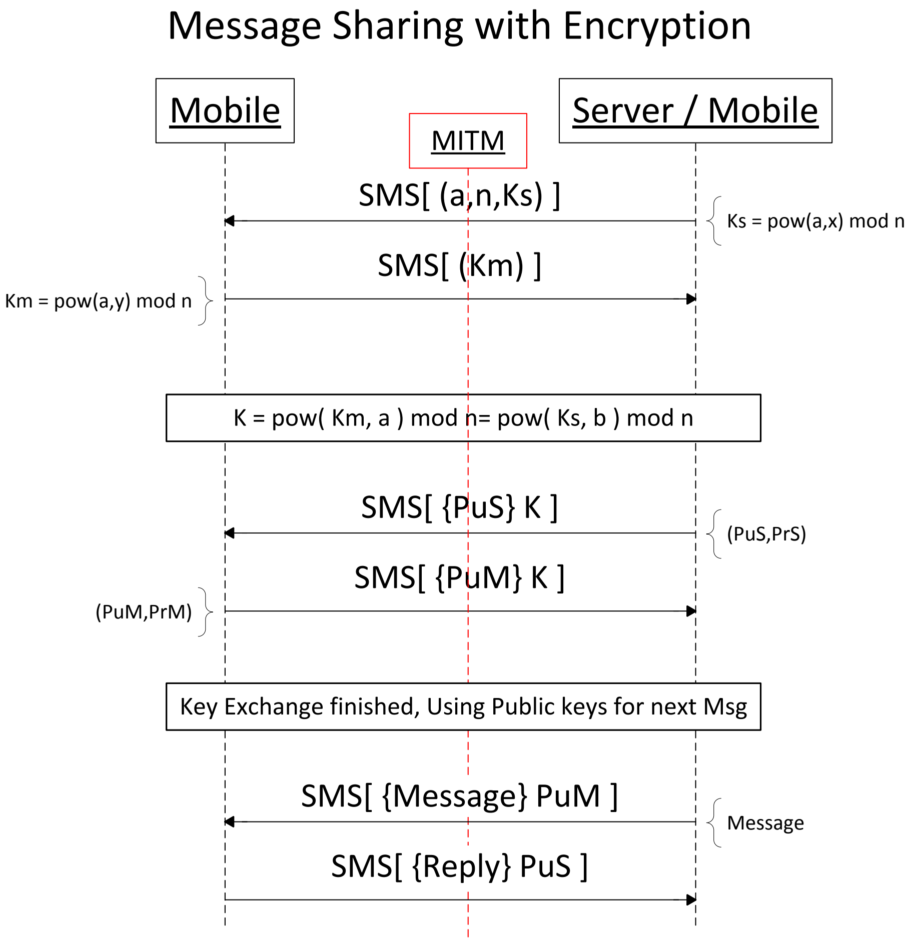

Figure 1.4 Man in the Middle attack

Figure 1.4 Man in the Middle attack, identifies weakness in this process. Server key is intercepted by MITM and MITM key is sent to client, client believes that this key is from server and replies its Key, again MITM intercepts this key and send MITM key to server. This makes both server and mobile believe that they have secured communication without knowing that MITM can clearly observe encrypted

messages and even alter them. Key exchange messages do not prove identity of sender there for MITM takes advantage and intercepts communication.

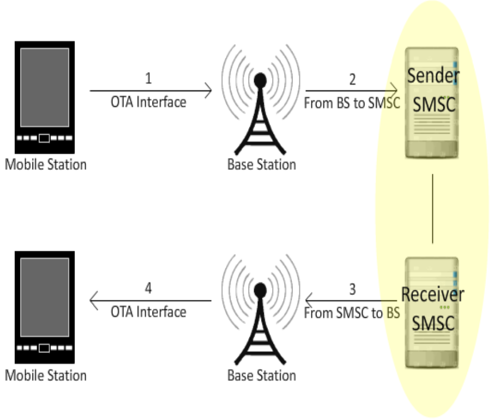

Figure1.5 SMS exchange over network

Figure1.5 SMS exchange over network, demonstrates how two mobile phone exchange SMS over network, first mobile device sends SMS it to the closest base station using standard transmission and reception channel called On-The-Air Interface, second from base station SMS is forwarded to Short Messaging Service Center over SS7,third after querying destination location, Short Messaging Service Center forwards message over SS7 to the closest base station near destination and at last through On-The-Air Interface, SMS reach its destination and a delivery report is initiated back to the sender. From source till destination, message is moved as plain text. Plain text communication over SMS will have no Confidentiality, Integrity and Authenticity (CIA).

Whereas encrypted SMS communication can provide satisfactory standard of CIA but still have possibility of man in the middle attack. Therefore this research is aiming to identify solution available to solve man in the middle problem over GSM network.

1.3 Problem Statement

With consideration that so much effort has been put into security of SMS, still Key exchange in Secure SMS communication is susceptible to man in the middle attack which can be identified as main problem in SMS security domain therefore this project will focus on study of different solutions available to defend against MITM attack, designing new approach to avoid MITM attack and implementation of framework based on designed approach.

1.4 Research Questions

Problem statement can be broken down into following study oriented questions

i. What are possible solutions available to address Man in the middle Attack over same communication channel (GSM Network)?
ii. How can secondary communication (EDGE/GPRS/4G) channel assist in key exchange to avoid Man in the Middle Attack?
iii. How can Smartphone Application use same channel or multiple channels to exchange secret keys and SMS messages?

1.5 Project Objective

The objectives of this project are to

i. To study different solutions available for addressing man in the middle attack and HTTPS communication between internet and mobile applications, for exchange of secret keys.
ii. To design a framework to exchange public keys between KDS and mobile

application.

iii. To implement Android Secure SMS application and KDS. Android application will generate encryption keys, publish it to KDS and Send, Read secure sms whereas KDS will act as a public key repository.

1.6 Project Scope

Scope of project will involve following:

i. Mobile Operating Systems that support SMS construction using applications are Android and Symbian. This project will use Android platform to conduct experiments and generate results

ii. As project environment is offline local environment, HTTPS certificate will be self-signed and there will be no certification authority.

iii. KDS will be implemented using WAMP Server which is a collection of Apache, MySQL and PHP.

iv. RSA will be used as an encryption algorithm as it is built-in security component of Android operating system.

1.7 Project goal

To design an application framework that can guarantee defense against MITM attack for secure SMS by developing framework using smart phone application and secure web application.

1.8 Significance of the Project

This project will address key management in secure SMS which is till now left vulnerable to MITM attack. Proposed framework will not use SMS to exchange encryption keys but will use HTTPS channel for this purpose which cannot be compromised by MITM if properly configured.

1.9 Contribution

This project will do following contributions in related field of study

i. This project propose a new framework to make SMS secure by managing keys over HTTPS public key infrastructure. These keys will be distributed to mobile devices for SMS encryption and decryption.
ii. As Android and PHP web development framework are open source platforms, this research and application code will be made public over "Google code" to help community.
iii. It will contribute to Android platform for creation of Secure SMS applications that can guarantee defense against MITM attack.
iv. Concepts and techniques discussed to make SMS secure can also be applied to communication over Internet, Bluetooth, WIFI etc. on Android platform giving extra benefit to Android community.
v. Automated messaging can adopt designed framework to make business communication secure with quality of service of SMS.

1.10 Organization of Report

Research report is organized into six chapters. Chapter 1 gives overview to the current situation around us related to security of SMS, identifies problem background and statement and suggests a tentative solution to the defined problems by identifying research goals and objectives. At the end it states possible contribution to the field.

Chapter 2 consists of literature review. It identifies key components of the system that are GSM nodes, confidentiality integrity authenticity over SMS, public key infrastructure with HTTPS and communication protocol. For identified components literature review is presented along with current contribution in similar fields.

Chapter 3 identifies the research methodologies available and used inside the project. It identifies the operational outline, approach and techniques used throughout the project.

Chapter 4 discusses design and implementation of the project. Design will identify components used for implementation and how they will communicate whereas implementation will identify platform and tools used to implement outlined design.

Chapter 5 will present results of the Android application and KDS. Application will be tested in a localhost environment. For this purpose application will be emulated on ANDROID emulator and HTTPS services will be provided by WAMP Server at the end results of experiments will be discussed.

Chapter 6 concludes project findings and lay foundation for future work. Different extensions of the project are discussed inside this chapter.

1.11 Summary

This chapter has identified problem statement and problem questions based on provided problem background. Project scope, goals and objective of project are identified and at the end contribution to community are outlined. Organizational structure of project is presented which will act as milestones toward completion of project.

REFERENCES

Buitron-Damaso, I., Morales-Luna, G., 2011. HTTPS connections over Android, in: 2011 8th International Conference on Electrical Engineering Computing Science and Automatic Control (CCE). Presented at the 2011 8th International Conference on Electrical Engineering Computing Science and Automatic Control (CCE), pp. 1–4.

Chavan, R.R., Sabnees, M., 2012. Secured mobile messaging, in: 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET). Presented at the 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1036–1043.

De Santis, A., Castiglione, A., Cattaneo, G., Cembalo, M., Petagna, F., Petrillo, U.F., 2010. An Extensible Framework for Efficient Secure SMS, in: 2010 International Conference on Complex, Intelligent and Software Intensive Systems (CISIS). Presented at the 2010 International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), pp. 843–850.

Farooq, Umar, Tanveer ul Haq, Muhammad Amar, Muhammad Usman Asad, and Asim Iqbal. “GPS-GSM Integration for Enhancing Public Transportation Management Services.” In *Proceedings of the 2010 Second International Conference on Computer Engineering and Applications - Volume 02*, 142–147. ICCEA ’10. Washington, DC, USA: IEEE Computer Society, 2010. doi:10.1109/ICCEA.2010.183.

Hossain, A., Jahan, S., Hussain, M.M., Amin, M.R., Newaz, S.H.S., 2008. A proposal for enhancing the security system of short message service in GSM, in: 2nd International Conference on Anti-counterfeiting, Security and Identification, 2008. ASID 2008.

International Engineering Consortium, 2002,page 268

Jamil, S., and F.A. Mousumi. "Short Messaging Service (SMS) Based M-banking System in Context of Bangladesh." In *11th International Conference on Computer and Information Technology, 2008. ICCIT 2008*, 599–604, 2008. doi:10.1109/ICCITECHN.2008.4802986.

Joseph Migga Kizza, Guide to Computer Network Security, 2013

Medani, A.; Gani, A.; Zakaria, O.; Zaidan, A.A.; Zaidan, B.B. (2011) *Review of mobile short message service security issues and techniques towards the solution.* Scientific Research and Essays, 6 (6). pp. 1147-1165. ISSN 1992-2248

Peersman, C., S. Cvetkovic, Paul Griffiths, and Hugh Spear. "The Global System for Mobile Communications Short Message Service." *IEEE Personal Communications* 7, no. 3 (2000): 15–23. doi:10.1109/98.847919.

Presented at the 2nd International Conference on Anti-counterfeiting, Security and Identification, 2008. ASID 2008, pp. 235–240.

Pochmara, J., Pałasiewicz, J., Szablata, P., 2010. Expandable GSM and GPS systems simulator, in: Mixed Design of Integrated Circuits and Systems (MIXDES), 2010 Proceedings of the 17th International Conference. Presented at the Mixed Design of Integrated Circuits and Systems (MIXDES), 2010 Proceedings of the 17th International Conference, pp. 552–556.

Puangpronpitag, S., Sriwiboon, N., 2012. Simple and Lightweight HTTPS Enforcement to Protect against SSL Striping Attack, in: 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN). Presented at the 2012 Fourth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), pp. 229–234.

Redzuan Bin Ahmad, M., M. Rauf, A. Fakharuddin, and A.N. Abdalla. "Design of Embedded Automated Monitoring System; an Intelligent Application to Reduce Peak Load Demand." In *2010 International Conference on Power*

System Technology (POWERCON), 1–5, 2010. doi:10.1109/POWERCON.2010.5666594.

Shirley Jordan, from smoke signals to email: moments in history, 2000

Tuchman, W., 1998. Internet besieged, in: Denning, D.E., Denning, P.J. (Eds.), ACM Press/Addison-Wesley Publishing Co., New York, NY, USA, pp. 275–280.

Verma, R.K., Tomar, D.S., Rathore, S.K., 2011. Extraction and Verification of Mobile Message Integrity, in: 2011 International Conference on Communication Systems and Network Technologies (CSNT). Presented at the 2011 International Conference on Communication Systems and Network Technologies (CSNT), pp. 49–53.

Vougioukas, S., and M. Roumeliotis. "A System for Basic-level Network Fault Management Based on the GSM Short Message Service (SMS)." In *EUROCON'2001, Trends in Communications, International Conference On.*, 1:218–222 vol.1, 2001. doi:10.1109/EURCON.2001.937799.

Wang, X., Yang, Y., 2009. Method and Implementation of Sending and Receiving Mobile Phone Messages, in: International Forum on Computer Science-Technology and Applications, 2009. IFCSTA '09. Presented at the International Forum on Computer Science-Technology and Applications, 2009. IFCSTA '09, pp. 173–175.William Stallings, Network Security Essentials fourth Edition , 2001

Wu, Songyang, and Chengxiang Tan. "High Security Communication Protocol for SMS." In *International Conference on Multimedia Information Networking and Security, 2009. MINES '09*, 2:53–56, 2009. doi:10.1109/MINES.2009.83.

Wu, S., Tan, C., 2009. High Security Communication Protocol for SMS, in: International Conference on Multimedia Information Networking and Security, 2009. MINES '09. Presented at the International Conference on Multimedia Information Networking and Security, 2009. MINES '09, pp. 53–56.

Zahaby, M., Gaonjur, P., Farajian, S., 2009. Location tracking in GPS using Kalman Filter through SMS, in: IEEE EUROCON 2009, EUROCON ’09. Presented at the IEEE EUROCON 2009, EUROCON ’09, pp. 1707–1711.