Encryption of Short Message Service in Global System for Mobile Communications

Gao Yu[1,a], Wei Yin[1], Ze Xu[1], Donglin Wang[2,b]

[1]EE Department, Nanjing Univ. of Posts and Telecommunications.

ECE Department, New York Institute of Tech. at Nanjing,Nanjing, China

[a]yugao829@gmail.com

[2]Department of Electrical and Computer Engineering

New York Institute of Technology at Nanjing Campus,Nanjing, China

[b]dwang09@nyit.edu

Keywords: Encryption, GSM, SMS, MD5, Message capture

Abstract. Nowadays more and more companies are using cellphone message to verify users'identities. However,because there is no data encryption in global system for mobile communications (GSM)short message service (SMS), the being sent message is easily to be listened during transmission and your identity could be replaced by somebody else.[1]In this paper, we use an open source project osmocomBB and the corresponding peripheral devices, i.e. Moto C118 and CP2120, to capture the experimental GSM SMS messages. We analyze the GSM packets with a data-packet analyzing tool, which is calledwireshark. Then, in order to accomplish the transmission safety, the SMS message is encryptedby using the message digest algorithm (MD5). The proposed application of this algorithm in GSM SMS is demonstrated by our experiments.

Introduction

As we all know well, the global system for mobile communications (GSM) is the 2nd generation mobile communication standard and widely applied in modern communications. With the development of mobile phones and communication, GSM shortmessage services (SMS) became a paramount part of people's daily life. GSM SMS can help to widely deliver the messages between family and friends. Nowadays, with the online payment popular among China, GSM plays a significant role in transmitting verification codes for companies to identify customers. However, GSM SMS in China has not been encrypted by communication operators and is transmitted with 'naked' packets [2]. Some data stealers can listen to and capture these messages and phone numbers of both senders and receivers by usingsome data-capturing devices. This kind of actionswill lead toserious privacy issues and transmission safeties. Fromthe internet, the tutorials of listening GSM short message are numerous and everywhere. The situation of GSM short message is quite serious. Therefore, these kinds of issues are well worth being focused on to be solved.

This paperproposes to apply the message digest algorithm (MD5) to GSM SMS to encrypt GSM short messagesandguarantee safety. This system has been shown to work properly after debugging and testing. The GSM messages to be transmitted can be encrypted by using MD5 and can only be deciphered by receivers.

This paper is organized as follows. Section II introduces the hardware which is used to capture short messages. Section III briefly describes the GSM SMS. Section IV depicts the MD5 algorithm. And the application of the MD5 algorithm into GSM SMS and the corresponding experimental results are provided in Section V, followed by Conclusion in Section VI.

Hardware

We use the open source project osmocomBB to capture the GSM short messages, where the being shown hardware, Moto C118, is used for data capturing. As shown in Fig.1, the following hardware consists of several modules: Crystal, Rlta TRF6151C, lota TWL 3025 ABB, SIM Card Holder, Headset/Serial Connector, Buzzer, Antenna Connector, External Antenna Connector, RF Power Amplifier, Calypso Amplifier, RAM, NOR Flash, Battery Connector, Vibrator Connector. In Fig.2, it's a CP2102 chip used to convert signal from USB to transistortransistor logic (TTL)

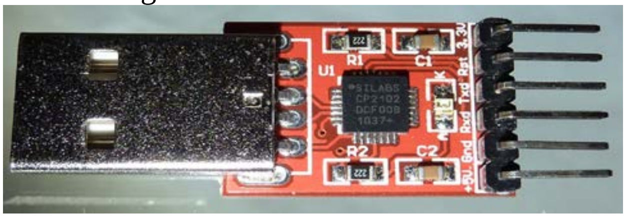

Fig. 1 The motherboard of Moto C118

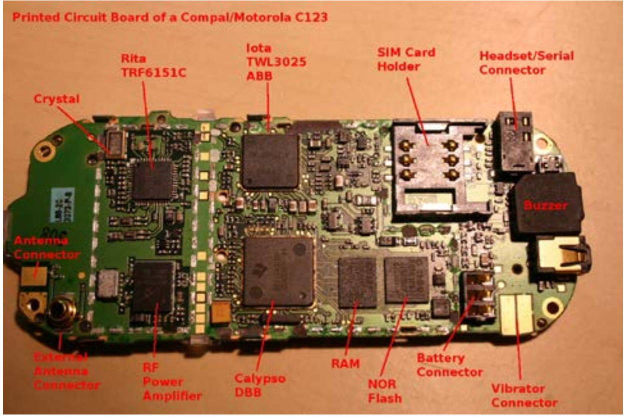

Fig. 2CP2102

OsmocomBB Project.

OsmocomBB is a free software / open source GSM baseband software implementation. It intends to completely replace the need for proprietary GSM baseband software, such as

- drivers for the GSM analog and digital baseband (integrated and external) peripherals
- GSM phone-side protocol stack, from layer 1 up to layer 3.

The project is implemented for several reasons.

- Security

Every mobile device that is connected to a cellular network runs on some kind of baseband processor with highly proprietary and closed-source firmware.

Any reasonably complex software has bugs, and a number of them will be security relevant and might get exploited.

As we know from more than a decade of security nightmares on the Internet: Open Source projects provide a much higher level of security, as more eyes review the code and security related bugs get fixed almost immediately. An update is released, and that particular security issue is closed.

Most people understand that connecting an unprotected PC to a public network like the internet is dangerous. People use personal or dedicated firewalls, application level gateways, virus scanners and other technology to protect their PC.

But what about the mobile phone, particularly the baseband processor? It is permanently attached to a public network, in most cases there is no proper incident response management and not even a clean way how bugs in that software can be updated quickly, as device manufacturers rarely release firmware update, publish security advisories or any of that sort.

The security situation becomes even worse when looking at the software architecture in those baseband chips. They often run the entire software stack in supervisor mode, without any software protection. There are no non-executable pages, there's no stack protection, etc. The UI and the protocol stack run in one shared address space with no privilege separation.

The only companies that have access to the baseband firmware source code have no interest in improving this situation. So the logical conclusion is to form an Open Source project that can try to improve the situation

- Education

Despite GSM being a public standard maintained by the ETSI, there are very few people outside a small group of GSM baseband chip makers who really understand the details of operation in a GSM mobile phone.

Existing books and other publications focus on "user" or "system administrator" topics such as network deployment. Or they are scientific literature about the signal processing involved in GSM and optimizations thereof. Other books explain the layer 3 protocol very well, but only from a theoretical point of view.

Designing and implementing the software that runs in the digital baseband of a GSM mobile phone covers many areas that are currently not publicized much.

One such topic is the layer 1 stack operating synchronous to the TDMA frame clock of the GSM network. Another important practical issue is what software can do for power efficiency, as this directly translates to longer battery life.

Digital Baseband ASICs and their corresponding software are present in billions of mobile phones, but the detailed knowledge on how they work is so far restricted to a small elite of engineers working for the industry.

Compare that with the knowledge of the Internet protocols such as Ethernet, IP, TCP, HTTP, SMTP and others. Virtually every IT professional around the world understands them, the knowledge is wide spread. One of the major reason for that is the existence of no Free Software or Open Source software implementations.

How to write OsmocomBB to Moto C118

We use the Linux Ubuntu 12.04 as our platform. We download this protocol to our computer and deploy a cross compile environment. Then we connect our Moto C118 to the CP2120 chip and then connect the chip to computer using USB port.

GSM Message

If you are using Word, use either the Microsoft Equation Editor or the MathType add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation or MathType Equation). “Float over text” should not be selected. GSM message was first used in Europe since 1991. GSM Protocol 03.40 defined a point-to-point method for GSM message, the most common method people used, Cell-Broadcast (SMS-CB). SMS-CB allows message sender (individuals, companies, advertisers, etc.) can send message to many people in one cell with broadcast. In this way, when there is someone get into the cell, he will get the message.[3]

A piece of message contains 140 Bytes, 160 characters with 7 bits or 140 characters with 8 bits, in other word. Some kinds of characters such Chinese, Korean, Japanese are characters with 2-Byte and it can be contained into one message within 70 characters (Unicode).

Overview of GSM.

The technology behind the Global System for Mobile communication (GSM™) uses Gaussian Minimum Shift Keying (GMSK) modulation a variant of Phase Shift Keying (PSK) with Time Division Multiple Access (TDMA) signaling over Frequency Division Duplex (FDD) carriers. The physical layer is specified in 3GPP™ TS 45.001 and the logical channels in 3GPP™ TS 45.002. The modulation is specified in 3GPP™ TS 45.004.[4]

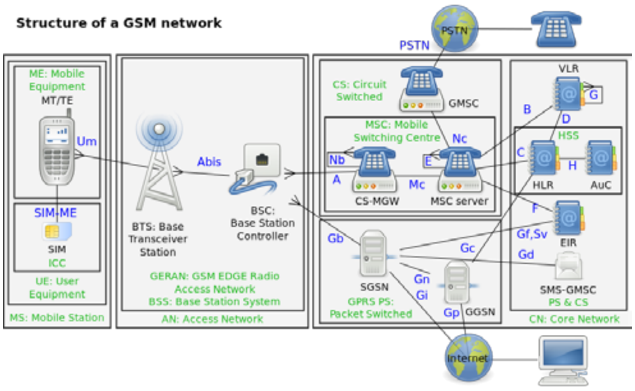

Fig.3 Structure of GSM Network

Principle of GSM message.

In the specification set by the ESTI SMS, there are three ways to send and receive Text messages: Block Mode, Text Mode and PDU Mode. Now in China is PDU mode. PDU string is a string of ASCII code with '0'-'9', 'A'-'F' numbers and letters. They are eight bytes of hexadecimal numbers, or BCD decimal numbers. PDU string contains not only the message itself, also a lot of other information, such as SMS service center number and target number, respond number, encoding and service response time, etc. In the PDU Mode, three types of encoding can be used to send the content of the coding, 7-bit, 8-bit and UCS2 code. 7-bit encoding used to send the ordinary ASCII characters, it will be a 7 - bit string of characters (most significant bit is 0) encoded in 8-bit data, every eight characters can be "compression" into seven. We usually call “ASCII encoding” in the text, actually refers to 7 - bit encoding. [5] Besides, 7-bit encoding can not only represent ordinary ASCII characters, but also some special characters. 7-bit encoding and ASCII code is actually two totally different concepts, they only share the same ordinary ASCII characters code. 8-bit codes are usually used to send data messages such as images and ringtones, etc. UCS2 code is used for sending Unicode characters. PDU string of user information’s (TP-UD) maximum capacity is 140 bytes. As a result, under these three coding mode, individuals can send a short message with the maximum number of characters is 160, 140 and 70 respectively. Here, we see an English letter, Chinese character and a data byte as one character.

Basic Services of GSM Message.

Short Message Mobile Terminated (SMMT) denotes the capability of the GSM/UMTS system to transfer a short message submitted from the SC to one MS, and to provide information about the delivery of the short message either by a delivery report or a failure report with a specific mechanism for later delivery, as shown inFig.1.

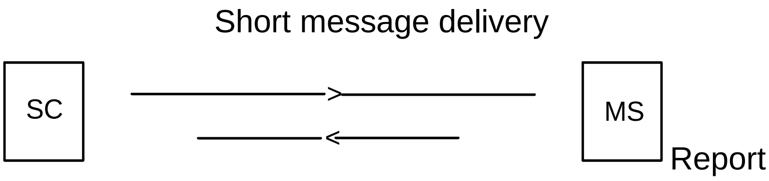

Fig.4 The SMS mobile terminal

Short Message Mobile Originated (SMMO) denotes the capability of the GSM/UMTS system to transfer a short message submitted by the MS to one SME via an SC, and to provide information about the delivery of the short message either by a delivery report or a failure report.[6] The message shall include the address of that SME to which the SC shall eventually attempt to relay the short message, as shown inFig.4.

The text messages to be transferred by means of the SMMT or SMMO contain up to 140 octets.

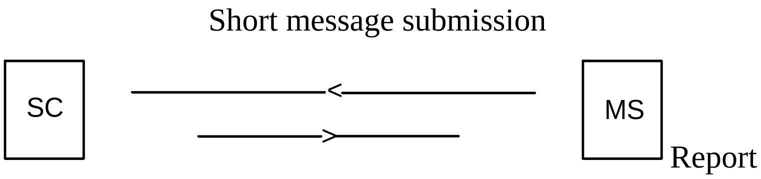

Fig.5 The Short Message Service mobile originated

Eight Elements of SMS.

The SMS comprises 8 elements particular to the submission and reception of messages:

- Validity-Period;
- Service-Centre-Time-Stamp;
- Protocol-Identifier;
- More-Messages-to-Send;
- Priority;
- Messages-Waiting;
- Alert-SC.
- MT Correlation ID.

GSM MessageProtocol Stack.

The basic GSM message architecture is defined as

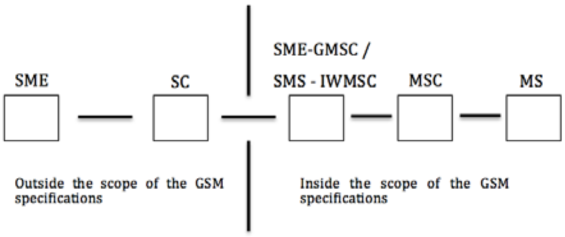
SME-GMSC /
SME
SC
SMS - IWMSC
MSC
MS
Outside the scope of the GSM specifications
Inside the scope of the GSM specifications

Fig.6 GSM message architecture definition

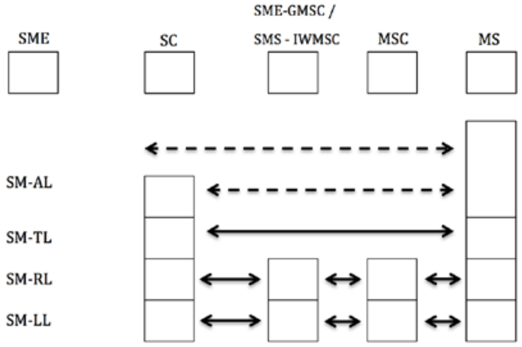

Fig.7 Protocol layer overview for the SMS service

MD5 encryption

Introduction.

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte)hash value, and is also commonly used to verify data integrity. MD5 was designed by Ronald Rivest in 1992 to replace an earlier hash function, MD4. The source code in RFC1321.[7]

In 1996 a flaw was found in the design of MD5. While it was not deemed a fatal weakness at the time, cryptographers began recommending the use of other algorithms, such as SHA-1—which has since been found to be vulnerable as well. In 2004 it was shown that MD5 is not collision resistant. As such, MD5 is not suitable for applications like SSLcertificates or digital signatures that rely on this property for digital security. Also in 2004 more serious flaws were discovered in MD5, making further use of the algorithm for security purposes questionable; specifically, a group of researchers described how to create a pair of files that share the same MD5 checksum. Further advances were made in breaking MD5 in 2005, 2006, and 2007. In December 2008, a group of researchers used this technique to fake SSL certificate validity, and CMU Software Engineering Institute now says that MD5 "should be considered cryptographically broken and unsuitable for further use", and most U.S. government applications now require the SHA-2 family of hash functions. In 2012, the Flame malware exploited the weaknesses in MD5 to fake a Microsoft digital signature.[8]

MD5 Algorithms.

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits fewer than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}.[9]

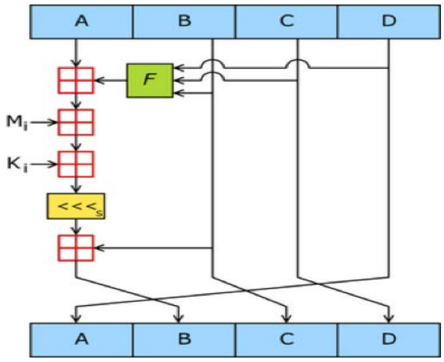

Fig.8. MD5 operation

MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. *F* is a nonlinear function; one function is used in each round.M_i denotes a 32-bit block of the message input, and K_i denotes a 32-bit constant, different for each operation. *s* indicates that a left bit rotation by *s* places; *s* varies for each operation, which denotes addition modulo 2^{32}.[10]

Experiment Process

In our experiment, we use our cellphone sending GSM message to 10086. Our message content is “Michelangelo”. Then we use Wireshark (a packet capture software) and peripheral devices to capture our test GSM packet

From the packet we receive, we can see that the message is transmitted in cleartext.

Our solution to this issue is that applying MD5 encryption to our message. So that the GSM message content will be transmitted in ciphertext. If it is been tapped, the content was encrypted and the real content can only be readable after decryption in cellphone.This is the packet we capture in the experiment.

```
No.    Time          Source              Destination          Protocol
Length Info
    324 9.212320000    127.0.0.1            127.0.0.1              GSM
SMS  81     I, N(R)=0, N(S)=1(DTAP) (SMS) CP-DATA (RP) RP-DATA (MS to
Network)

Frame 324: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
on interface 0
Ethernet  II,  Src:  00:00:00_00:00:00  (00:00:00:00:00:00),  Dst:
00:00:00_00:00:00 (00:00:00:00:00:00)
Internet  Protocol  Version  4,  Src:  127.0.0.1  (127.0.0.1),  Dst:
127.0.0.1 (127.0.0.1)
```

```
User Datagram Protocol, Src Port: 37929 (37929), Dst Port: gsmtap
(4729)
GSM TAP Header, ARFCN: 60 (Uplink), TS: 1, Channel: SDCCH/8 (1)
Link Access Procedure, Channel Dm (LAPDm)
GSM A-I/F DTAP - CP-DATA
GSM A-I/F RP - RP-DATA (MS to Network)
GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
    1 (0... .... = TP-RP: TP Reply Path parameter is not set in this
SMS SUBMIT/DELIVER) putline
    1 (.0.. .... = TP-UDHI: The TP UD field contains only the short
message) putline
    1 (..0. .... = TP-SRR: A status report is not requested) putline
    1 (...0 0... = TP-VPF: TP-VP field not present \(0\)) putline
    1 (.... .0.. = TP-RD: Instruct SC to accept duplicates) putline
    1 (.... ..01 = TP-MTI: SMS-SUBMIT \(1\)) putline
    1 (TP-MR: 1) putline
    1 (TP-Destination-Address - \(10086\)) putline
    1 (TP-PID: 0) putline
    1 (TP-DCS: 8) putline
    1 (TP-User-Data-Length: \(10\) depends on Data-Coding-Scheme)
putline
    1 (TP-User-Data) putline
    2 ([SMS text: Michelangelo]) putline
```

From the packet, we can find the cleartext easily. If MD5 algorithm is applied on GSM SMS, the content will be “29fa7a8c9632590d”.

Application and Conclusion

GSM message is the cheapest and most available way for a second check. And it will be widely used for a couple of years.

SMS security is required in different application at different level, like some people are very less concerned about their SMS security while some organizations have big concern about their SMS security, like banks nowadays. Different banking solution are based on the SMS like password authentication, dual authentication of banking transaction for cash withdrawal, cash transfer, due to high security requirement in banking transactions. There many threats can come to account for m-commerce via SMS. Sometimes the passwords for a bank account need to be sent. If any intruder read the SMS, he or she can gain the password as it is in plaintext. Encryption technique would be required to solve this attack.

Not only the messages sent by banks need this technology, but also every single message need to be protected including Personal information, business plans and deals certificates. Users stand to lose privacy and money if hackers get these unprotected messages. This technology can apply to any service that needs the cell phone as a second check of the users’ identity.

Reference

[1] http://www.freebuf.com/news/30875.html

[2] S. M. Redi, M. K. Weber and M.W. Oliphant, *GSM and PersonalCommunications Handbook*, Artech House, London, 2000.

[3] Hodges, M.R.L., "The GSM Radio Interface," *British TelecomTechnology Journal*, vol. 8, no. 1, Jan. 1990, pp. 31-43.

[4] Williamson, J., "GSM Bids for Global Recognition in a CrowdedCellular World," Telephony, vol. 333, no. 14, April 1992, pp. 36-40.

[5] Scmidt M, “Consistent m-Commerce Security on Top GSM-basesDataprotocols: A security analysis”, University of Siegen, Institute for Datacommunication systems, Siegen, Germany 2001.

[6] Papadiglou, N and Stipide, E. , “Short message service link forautomatic vehicle location reporting”, *Electronic Lett.*, 1999, vol. 35, pp.876-877.

[7] Andrew S. Tanenbaum, “Computer Networks”, fourth edition, Pearsoneducation, 2006.

[8] European Telecommunications Standards Institute, RecommendationGSM 02.09, "Security Aspects".

[9] European Telecommunications Standards Institute, RecommendationGSM 03.20, "Security Related Network Functions".

[10] R. L. Rivest, A. Shamir and L. Adleman, “A method for obtainingdigital signature and public key cryptosystem,” Communication of theACM, vol.21, pp. 120-126, Feb. 1987.