SIM Card Security

Sheng He
108005239797

Seminar Work

at

Chair for Communication Security
Prof. Dr.-Ing. Christof Paar

advised through Thomas Eisenbarth

12.07.2007

Ruhr-University of Bochum

Contents

1 Overview

Since the GSM communication system has been designed by the Standardization Committee composed of the European leading telecommunication operators and manufacturers, this system concentrates much more on the interests of consumers and operators. Thus, it made great effort to improve its functions including security, convenience etc.

In fact, wireless communication will be tapped more easily than fixed communication. If we do not provide any special countermeasures, it could not be difficult to tap or fake a registered user. In the 1980's, the system of simulation was suffered from the bug of wireless communication so deeply, that the interests of customers were impaired. Therefore, at first, introduction of SIM card technology into the GSM system raises the security level of GSM greatly. It is able to prevent from unauthorized accessing with authentication for protection of the network operators and the interests of users. Moreover, in order to protect the user's privacy, the transmission can be also encrypted to avoid eavesdropping on the wireless channel. Furthermore, it's replaced by a temporary user identification code, that third parties can not track the wireless channel on GSM users. In addition, all of these confidential mechanisms are controlled by the operators, so it seems to be much safer without participating of those users.

As the introduction of the SIM card technology into the GSM communication, the wireless communication has been no long restricted by encryption. As long as the customers bring a card, they could travel all around the world.

SIM cards have many characteristics as below:

Feature 1, separation of the client & equipment. In GSM communication, SIM cards and mobile equipment have been installed in an open interface to the public, so that users and their equipment lie on the interdependent relationship. Because SIM cards stored cardholder's customer data, security data, authentication encryption algorithm, etc. As long as customers holding this card, he or she can borrow and hire different mobile stations from different ISPs and obtain different services in the card. Then, it enhances the flexibility of the GSM mobile communication greatly as well as shares equipments among different manufacturers.

Feature 2, communications are secure. The SIM card has a permanent memory storage and capacity of calculation. Therefore, it belongs to smart cards. When the cell phone is switched on, customer should enter personal identification numbers (PIN), this code is composed by 4 ~ 8 figures and accessed by keyboard typing. If import three incorrect PIN code, PIN codes are locked, communications terminated, this is one way against the misappropriation pseudo-client communication. If customers forget the code or import by mistake three times, the 0 ~ 9-digit personal unlocking key (PUK) stored in the SIM card can be used to unlock PIN codes, recover it back to normal. However, we should also pay special attention to the importation of 10 PUK wrong, the entire SIM cards abandoned. Only Through the purchase of a new SIM cards can we recover our communication. In the process of calling, if we import the correct PIN code, the Internet start a customer identity authentication, using A3, A8 algorithm stored in the SIM card to compare the results of mobile and Internet calculation and same authentication success. This is the second line of defence to prevent misappropriation Communication. After successful Authentication, in order to protect the confidentiality of client information been transmitted to the other the other side of transmission. Another set of encryption methods also been introduced - the use of the A5 algorithm to prevent the illegal customer theft. In addition, in the process of Authentication and decryption, parameters of key (Kc) and authentication key (Ki) on the interface will not be transmitted. Only the International Mobile customer identification code (IMSI) will be transmitted once. After that, the changing temporary code (TMSI) instead, therefore GSM communications are securer than the analog mobile communications.

Feature 3, low cost. Their costs are lower than telephone cards. Furthermore, they are solid and durable and easily to be promoted.

2 SIM Card Introduction

2.1 Structure and type

SIM card is a smart card with a microprocessor and it consists of the following modules:

--- CPU

--- Program memory (ROM)

--- Working memory (RAM)

--- Data memory (EPROM or E2PROM)

--- Serial communication module

These five modules must be integrated into an Integrated Circuit (IC), otherwise their safety would be threatened. This is because the chip connections may become illegal access and misappropriation of SIM cards important clues.

In practice, there are two different forms of SIM cards with the same functions:

(A) Full-size SIM card (commonly known as big card), this form of SIM cards with the IC cards of the ISO 7816 Standard [ISO7816], similar to IC card. The card has since been shrunk to the standard size of 25mm × 15mm.

(B) Embedded SIM card (commonly known as small card), the size of only 25 mm × 15 mm, is a semi-permanent packed to the cards in the mobile station equipment.

Two cards have installed waterproof, wear-resistant, anti-static contact with high accuracy and reliability characteristics.

2.2 Cryptographic algorithm and secret key in SIM card

The most sensitive information of SIM card is the cryptographic algorithm A3, A8, secret Ki, PIN, PUK and Kc. A3, A8 algorithm were written into the SIM card in the producing process, and most people could not read A3, A8 algorithm. HN code could be settled by the phone owners. PUK code is held by the operator. Kc was derived in the process of encryption from Ki.

PIN and PUK:

--- PIN –Personal Identification Number

--- 2 PINs exist (PIN 1 and PIN2)

--- Limited attempts on PIN access

--- PUK –PIN Unblocking Code

--- Resetting PUK, resets PIN and the attempt counter

--- Too many attempts on PUK blocks use permanently

2.3 SIM File System

Let's have a look at the Figure 2-1, the file system of a SIM is organized in a hierarchical tree structure, it consists of the following three types of elements:

- Master File (MF) - the root of the file system that contains dedicated and elementary files.
- Dedicated File (DF) - a subordinate directory to the master file that contains dedicated and elementary files.
- Elementary File (EF) - a file that contains various types of formatted data, structures as either a sequence of data bytes, a sequence of fixed size records, or a fixed set of fixed size records used cyclically.

In the other side, the GSM standards define several important dedicated files immediately under the MF: DFGSM, DFDCS1800, and DFTELECOM. For the MF and these DFs, several EFs are defined, including many that are mandatory. The EFs under DFGSM and DFDCS1800 contain mainly network related information respectively for GSM 900 MHz and DCS (Digital Cellular System) 1800 MHz band operation. EFs for U.S. 850 MHz and 1900 MHz bands are found respectively under those DFs as well.

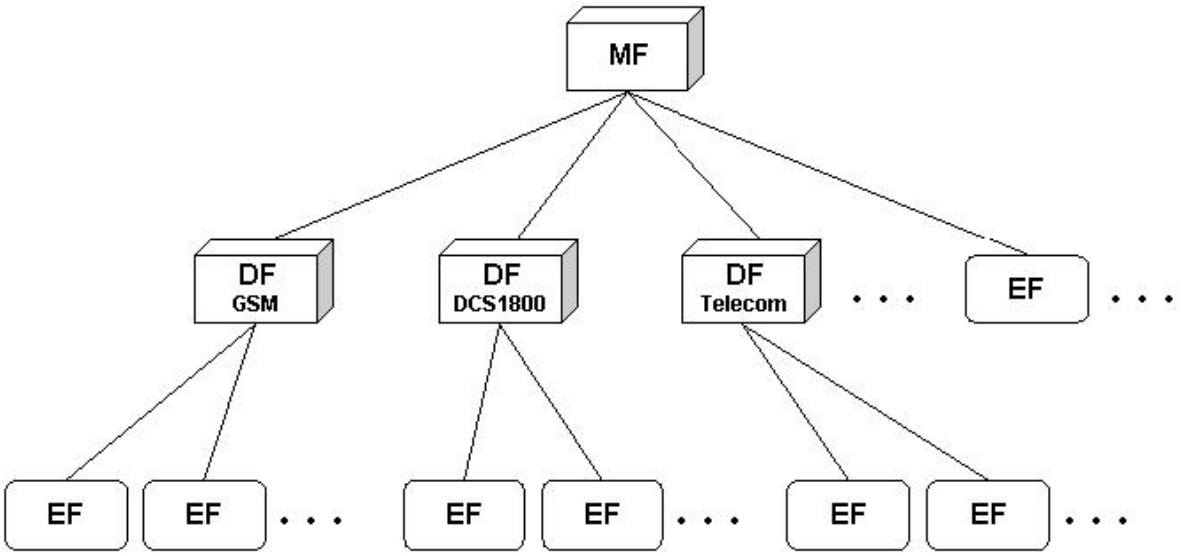

Figure 2-1 SIM File System

In spite of SIM file systems are highly standardized, the standards allow flexibility such that their content can vary among network operators and service providers. For example, a network operator might not use an optional file system element, might create an additional element on the SIM for use in its operations, or might install a built-in function to provide a specialized service.

2.4 Data and Parameter

The following data are stored in the SIM card: ISDN, Ki, PIN, PUK, TMSI, LAI and ICCID (SIM card number): 898600 9F SS YY G xxxxxX Chk

898600	fixed
9	the last digit of Mobile Access No.
F	functional spaces, tentatively 0
SS	the province's No.
YY	the year (last 2 digits) of ICCID establishment
G	SIM card vendor's No.
XXXXXX	random definition by operator
Chk	Parity

The following tables describe the two Phases of SIM card in GSM:

(1) Phase 1

① GSM system parameters

Table 2-1 system parameter data options in phase 1

Identifier	Name	Length
6FAD	Administrative	3
6F38	Service Table	4
6F07	IMSI	9
6F7B	Forbidden PLMN	12
6F7E	TMSI LAI	11
6F20	Kc, n	9
6F30	PLMN Selector	24
6F74	BCCH Information	16
6F78	Access Control	2

Service 1: PIN Disabling
Service 2: Abbreviated Dialling Numbers
Service 4: Short Message Storage
Service 6: Capability Configuration Parameters
Service 7: PLMN Selector

② Telecommunication business parameters

Table 2-2 Telecommunication business options in phase 1

Identifier	Name	Length
6F3A	Abbreviated Dialling Numbers	50*22
6F3D	Capability Config Parameters	1*14
6F3C	Short Message Storage	5*176
6F39	Carging Counter	2

(2) Phase 2

① GSM system parameters

Table 2-3 system parameter data options in phase 2

Identifier	Name	Length
6F05	Language Preferernce	4
6F07	IMSI	9
6F20	Kc,n	9
6F30	PLMN Selector	42
6F31	HPLMN Search	1
6F38	Service Table	4
6F45	Cell Broad Message ID	8
6F74	BCCH Information	16
6F78	Access Control	2
6F7B	Forbidden PLMN	12
6F7E	TMSI LAI	11
6FAD	Admin Data	3
6FAE	Phase Ident	2

Service 9: MSISDN
Service 10: Extension 1 file
Service 12: SMS parameters
Service 13: Last Number Dialled
Service 14: cell Broadcasting Message Identifier file

② telecommunication business parameters

Table 2-4 Telecommunication business options in phase 2

Identifier	Name
6F3A	Abbreviated Dialling
6F3C	Short Message Storage
6F3D	Capability Configuration
6F40	MSISDN
6F42	SMS Paramters
6F43	SMS Status
6F44	Last Number Dialled
6F4A	Extension 1 file

2.5 The files on the SIM-card

The evidence on the SIM card is stored in the following files: [FGM03]

Phase	Phase ID	1 byte
SST	SIM Service table	5 bytes
ICCID	Serial Number	10 bytes
LP	Preferred languages	variable
SPN	Service Provider name	17 bytes
MSISDN	Subscriber phone number	variable
AND	Short Dial Number	variable
FDN	Fixed Numbers	variable
LND	Last Dialled numbers	variable
EXT1	Dialling Extension 1	variable
EXT2	Dialling Extension 2	variable
GID1	Groups 1	variable
GID2	Groups 2	variable
SMS	Text Messages	n * 176 bytes
SMSP	Text Message parameters	variable
SMSS	Text message status	variable
CBMI	Preferred network messages	variable
PUCT	Charges per unit	5 bytes
ACM	Charge counter	3 bytes
ACMmax	Charge limit	3 bytes
HPLMNSP	HPLMN search period	variable
PLMNsel	PLMN selector	variable
FPLMN	Forbidden PLMNs	12 bytes
CCP	Capability configuration parameter	14 bytes
ACC	Access control class	2 bytes
IMSI	IMSI	9 bytes
LOCI	Location information	11 bytes
BCCH	Broadcast control channels	16 bytes
Kc	Ciphering key	
AD	Administrative data variable	

All of the stored data can potentially have evidential value. However, most of the files refer to network internals that the user never see, and therefore does not represent evidence on the usage of the telephone as such. We therefore limit the

discussion here to the files that typical represent relevant evidence on phone usage [GSM1111].

3 Threats to SIM Data

3.1 Attacks to the COMP128

COMP128 is a popular algorithm and a published standard. COMP128 design was completely private. The algorithm was not released to the public, therefore it lacks much needed peer general study. In 1997, a leaked document led to publication of COMP128. That document produced the majority of the code, and what was missing (about 4-6 lines) and was reverse engineered. [COMP128]

In April of 1998, the Smartcard Developer Association along with 2 UC Berkeley researchers (Wagner/Goldberg) produced the first publicized attack on COMP128. It exploits the weakness in diffusion of the second round in the compression function. This is commonly referred to as a 'Narrow Pipe.'

The following examples are two simple attacks to the COMP128:

(1) black box attack against the GSM-MoU example algorithm

- This does not utilise any hardware or software property of the SIM.
- attack against just one card, not against the system itself.

(2) chosen plaintext / ciphertext attack

- approximately 160.000 - 200.000 very specific challenges were then required to calculate the secret, subscription specific key Ki.
- PIN has to be known or PIN-check disabled.

3.2 SIM cloning

SIM cloning consists of duplicating the GSM Subscriber Identity Module identification and placing calls or using other charged services using the account of

the cloned SIM [SIMCLO]. In the early several years, because of poor security features, cloning was more common than it is today. People can fake the SIM card with the SIM cloning technique. Cloning has now been rendered more challenging technically, it is as physical approach to the SIM card is required as opposed to simply being within radio reach.

SIM cloning is nowadays more difficult to perform, as copying the contents of the SIM does not enable a duplicate SIM to operate, as the SIM itself performs security operations on the data contained inside to avoid such copying. In order to function, the cloned SIM needs to perform security operations on the data comprised, just like the old one. SIM cloning is also a great concern of security services because of its GSM location-based service undependable if more than one handset is using the same SIM card.

Cloning SIM data for illicit use – Two key pieces of data: IMSI, Data Encryption Key (Ki). IMSI can be obtained:

– From SIM using scanning software

– Eaves-dropping on networks for unencrypted transmission of the IMSI

Ki can not normally be obtained directly as it is derived from encryption algorithm stored on SIM.

4 Security features

This clause defines the security attributes to be supported by the SIM, which are:

- authentication algorithm (A3);
- subscriber authentication key (Ki);
- cipher key generation algorithm (A8);
- cipher key (Kc);
- control of access to data stored, and functions performed, in the SIM.

An algorithm A38 may perform the combined functions of A3 and A8.

4.1 Algorithms and subscriber authentication key

All reasonable steps shall be taken to ensure that the algorithms (A3 and A8) and subscriber authentication key (Ki) cannot be read, altered, manipulated or bypassed in such a way as to reveal secret information.

All MS processes that require the use of the subscriber authentication key shall be performed internally by the SIM.

4.2 Authentication

Authentication involves two functional entities:

- the SIM Card in mobile device
- the Authentication Center (AC)

Each subscriber has a secret key, one copy of which is stored in the SIM card and the other is stored in the AC. During authentication, AC generates a random number that sends to the mobile. Both mobile and AC use the random number, in conjunction with subscriber's secret key and a ciphering algorithm called A3, to generate a number that is sent back to the AC. If number sent by mobile matches number calculated by AC, then subscriber is authenticated. A list of IMEIs in the network is stored in the Equipment Identity Register (EIR).

The status returned in response to an IMEI query to the EIR is one of the following:

- White-listed: Terminal is allowed to connect to the network
- Grey-listed: Under observation from the network, possible problems
- Black-listed: Terminal has either been reported as stolen, or it is not type approved (the correct type of terminal for a GSM network). The terminal is not allowed to connect to the network.

4.3 Encryption

A stream cipher known as the A5 algorithm. Multiple versions with various levels of encryption.

- A5/0: no encryption.
- A5/1: original A5 algorithm used in Europe.
- A5/2: weaker encryption algorithm created for export, in removal.
- A5/3: strong encryption algorithm created as part of the 3rd Generation Partnership Project (3GPP).

Stream cipher is initialised with the Session Key (Kc) and the number of each frame. The same Kc is used throughout the call, but the 22-bit frame number changes during the call, thus generating a unique key stream for every frame. The

same Session Key (Kc) is used as long as the Mobile Services Switching Center (MSC) does not authenticate the Mobile Station again. The same Session Key (Kc) may be in use for days. Authentication is an optional procedure in the beginning of a call, but it is usually not performed. The A5 algorithm is implemented in the Mobile Station (MS).

PIN locks the SIM card until correct code is entered. Each phone network sets the PIN of SIM to a standard default number.

- Can be changed via handset
- Protects account, even if SIM is inserted into another phone

If PIN protection enabled, PIN will need to be entered each time phone is switched on. If PIN entered incorrectly 3 times in a row, SIM will be blocked requiring a PUK from network/service provider.

PIN code 2 included with new SIM cards (GSM phase 2). Code controls access to advanced features of phone, i.e. fixed dialling list. A restricted list of numbers the phone can call. Default code is set by Service Provider, but editable. PIN entered incorrectly3 times-SIM blocked. Unable to make and receive calls/texts. PUK needed from network provider, or possibly GSM cell phone manual. Caution: if PUK entered 10 times incorrectly, SIM is permanently disabled and the SIM must be exchanged. Performs same function as the PUK, but for PIN Code 2. Service Provider has this code when needed.

4.4 Key Generation

A8 algorithm generates 64-bit Session Key (Kc). From 128-bit random challenge (RAND) received from Mobile Services Switching Center (MSC) and from 128-bit Individual Subscriber Authentication Key (Ki) from Mobile Station's SIM or Home Location Register (HLR).

One Session Key (Kc) is used until the MSC decides to authenticate the MS again. This might take days. A8 actually generates 128 bits of output. The last 54 bits of those 128 bits form the Session Key (Kc). Ten zero-bits are appended to this key before it is given as input to the A5 algorithm. The A8 algorithm is implemented in the Subscriber Identity Module (SIM).

4.5 Subscriber data stored in ME

All subscribers related information conveyed into the ME during GSM network operations should be deleted from the ME after removal of the SIM, deactivation of the MS, or following an electrical reset of the SIM. This includes any data that was transferred to the ME by SIM Application Toolkit commands [SIMME].

The Subscriber related security codes might be kept inside the ME during the enforcement of the appropriate SIM/ME interface procedure. They should be deleted from the ME immediately after completion of the procedure. But in fact, an ME may retain some less security critical data at SIM removal or MS switch-off. Such data are SMS, LND etc. These data, when stored in the ME, shall only be readable or retrievable if the same SIM card is reactivated as determined by the IMSI.

If the IMSI is retained in the ME for this purpose it shall be stored securely and shall not be able to be read out. Storage for other data such as SMS, LND etc., storage may also exist in the ME. These data stored in the ME, which have not been transferred from a SIM during a card session, are not subject to the above security restriction.

5 Future Evolution

5.1 UMTS

UMTS means Universal Mobile Telecommunications System. UMTS is one of the emerging mobile phone technologies known as third-generation, or called 3G. Third-generation systems are designed to include such traditional phone tasks as calls, voice mail, and paging, but also new technology tasks such as Internet access, video, and SMS, or text messaging, its speed will be much faster than the system nowadays (GSM) [WIUMTS].

The speed is one of the main benefits of UMTS. Current rates of transfer for broadband information are 2 Mbits a second. This speed makes possible the kind of streaming video that can support movie downloads and video conferencing. In a sense, UMTS makes it possible for the cell phone owner to enjoy all of the functionality of his home computer while he is roaming. By combining wireless

and satellite cellular technologies, UMTS takes advantage of all existing options to result in the Holy Grail of 3G presentation: seamless transitions between WiFi and satellite.

It was in Japan in 2001, UMTS went live as a network for the first time. Austria had its own network two years later (2003). A handful of other European countries joined the UMTS bandwagon in the next two years, with South Africa and a few other African countries soon following suit. The U.S. has employed UMTS networks in several large cities, and the number is steadily growing. UMTS is based on the Global System for Mobile (GSM) standard, which is the gold standard in Europe and more than 120 countries worldwide.

In fact, UMTS is sometimes referred to as 3GSM. The two systems are not compatible, however. UMTS is incompatible with GSM. Some phones are dual GSM/UMTS phones, but unless that exciting new mobile phone or handset that you can't wait to get your hands on has that kind of duality built in, you will only be able to utilize one mode, the one that came with the device.

As UMTS gains in credibility and functionality, experts believe it will overtake GSM as the industry standard. UMTS is already able to operate at a higher frequency than GSM.

5.2 WCDMA

WCDMA stands for “Wideband Code Division Multiple Access". It is a worldwide communications standard offering a superior ability to handle multimedia communication, including high-speed data, voice, moving and still image transmission.

Type	CDMA			TDMA
Name	W-CDMA	cdma2000	TD-CDMA	EDGE/UWC-136
Committee	3GPP	3GPP2	3GPP (with TD-SCDMA)	ETSI and UWCC
Multiple access	Direct Sequence CDMA	Multicarrier CDMA	TD-CDMA	TDMA
Duplex	FDD	FDD	TDD	FDD

Table 5-1 The 3rd Generation mobile communication network [GGSFMC]

5.3 USIM Card

The Universal Subscriber Identity Module or named USIM card is the logical extension of the SIM card into the 3G environment. The USIM card is an evolution of the SIM card still under the control of the ETSI. The USIM card is also the heart of the mobile phone that enables people to communicate with ease. The computer chip inside stores people's phone number, address book (up to 50 entries) and other information.

Compare with the SIM card: Simply put, this is the world standard. GSM mobile phones used mainly in Europe utilize SIM card. The USIM card is a more sophisticated type that allows you to send and receive calls using your regular phone number in Japan and other major countries around the world.

	Data Rates	Multi-Subscription	Java-Based USAT	Backwards Compatibility
SIM card	low	-	-	lack
USIM card	high	×	×	full

Table 5-2 Comparison of SIM and USIM

6 Conclusion

In this seminar work, we have presented the basic information and structure of the SIM card, also several attacks on the SIM card, e.g. the attack against COMP128 algorithm. So this means, SIM card have been broken?

The answer is: No. The SIM card has successfully stood the test of time and we have shown that SIM card security is susceptible to certain attacks. We also have two most important security parts to protect it. However, with high costs involved to patch SIM cards globally, providers ignore the threats.

Meanwhile, we are looking forward to the future evolution, the UMTS and USIM card. The new mobile system will be much faster and safer than the system GSM nowadays. We think, UMTS will be used commonly instead of GSM in the very near future.

References

[ISO7816] ISO: “Identification Cards - Integrated circuit cards with contacts”, International Standard, Parts 1-15.

[GSM1111] GSM 11.11, December 1995, GSM TECHNICAL SPECIFICATION

[FGM03] Willassen, S., 2003, Forensics and the GSM Mobile Telephone System, International Journal of Digital Evidence, Volume 2, Issue 1.

[COMP128] Billy Brumley, A3/A8 & COMP128, T-79.514 Special Course in Cryptology, 2004

[SIMCLO] SIM cloning, http://en.wikipedia.org/wiki/SIM_cloning

[SIMME] 3GPP, 2005a, Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, 3rd Generation Partnership Project, TS 11.11 V8.13.0 (Release 1999), Technical Specification, (2005-06).

[WIUMTS] What is UMTS? , http://www.wisegeek.com/what-is-umts.htm

[GGSFMC] J. Eberspaecher / H.-J.Vorgel / C.Bettstetter, GSM Global System for Mobile Communication, 3. Edition, page 369