정보학연구 제12권 제4호 2009년 12월(pp.1-10)
The Journal of Information Technology. Vol.12. No.4

통신서비스의 건전성 연구 : 중국 GSM 카드복제를 통한 보안 취약성에 대하여

김 식*

목 차

Ⅰ. 서 론

이동통신이란 이동통신 가입자가 단말기를 사용하여 음성, 영상, 데이터 등을 장소에 구애받지 않고 통신할 수 있도록 이동성을 제공하는 통신 서비스를 말한다. 단말기는 이동전화기(휴대전화)라 불리고 있으며, 최초의 아날로그 방식의 이동통신에서는 음성 송수신을 주된 서비스로 하는 셀룰러폰이 사용되었고, 최근에는 동영상, 문자, 인터넷, 방송, 사진, 전자결재 등 다양한 서비스를 수행할 수 있는 단말기를 사용하고 있다. 2009년 8월 세계의 이동통신 사용자는 40억 명을 넘어섰다. 가장 많은 이동통신 서비스를 이용하는 것은 2세대 이동통신서비스인 GSM으로 <표 1>과 같고 약 34억 명이 사용하고 있다. GSM 다음으로 많이 사용되는 이동통신은 CDMA2000 1X, WCDMA이다. 지역별로 가장 많은 이동통신 사용자가 분포하는 곳은 아시아로 약 19억 명이 사용하고 있으며, 유럽과 미주 지역에서 약 5억 명이 사용하고 있다.

* 세명대학교 정보통신학부 교수

<표 1> 이동통신 기술별 가입자 현경

이동통신 기술	가입자	퍼센트(%)
cdmaOne	2,512,409	0.06%
CDMA2000 1X	309,507,900	7.18%
CDMA2000 1xEV-DO	121,821,983	2.83%
CDMA2000 1xEV-DO Rev. A	13,912,386	0.32%
GSM	3,449,010,903	80.02%
WCDMA	255,773,412	5.93%
WCDMA HSPA	132,079,727	3.06%
TD-SCDMA	825,044	0.02%
TDMA	753,411	0.02%
PDC	2,752,436	0.06%
iDEN	21,361,981	0.50%
합 계	4,310,311,592	

우리는 흔히 이동통신시스템을 1세대, 2세대, 3세대, 4세대 등으로 분류하고 있다. 1세대는 음성, 2세대는 음성과 문자, 3세대는 2세대의 서비스에 영상서비스가 더해졌고, 4세대는 모든 것(everything)을 서비스 한다고 요약할 수 있다. 이러한 세대 구분은 세계 전기·전자 분야의 국제기구인 국제전기통신협회(ITU)가 주관하고 있다.

이동통신은 제어국, 기지국, 단말기로 구성되며, 제어국은 다수의 기지국과 연결 및 통제를 수행하며 고정 통신망과의 접속을 담당하는 역할을 수행한다. 기지국은 단말기와 무선으로 접속할 수 있다. 이동통신을 구성하는 네트워크는 코어망(Core Network)과 엑세스망(Access Network)로 구분되며, 기지국은 CDMA, GSM, WCDMA 등의 이동통신 엑세스 네트워크와 휴대전화를 연결하는 기지국이 대표적이며, WLL(Wireless local loop) 전화, WIFI, WIMAX, WAN 등과 같은 무선통신에서도 사용된다. 기지국은 육상 이동국 등 이동하며 통신을 수행하는 무선국과 고정되어 통신하기 위한 고정 무선국이 있다.

통신서비스의 건정성을 확보하기 위해서는 이동통신의 가입자와 이를 지원하는 법규, 단말기의 통신 형태 및 발전세대 그리고 이동통신서비스를 제공하는 네트워크의 코어망과 엑세스망 그리고 기지국간의 유기적인 결합이 보장되어야 한다. 본 연구는 통신서비스의 건전성에 관하여 연구하기 위하여 세계에서 가장 큰 규모인 중국의 GSM 서비스에 대하여 실제로 SIM카드의 복제 가능성을 실증적으로 실험하고 복제된 SIM 카드 단말기를 중국 현지 통신서비스에 적용해 봄으로써 보안취약성을 검증하고자 했다.

II. 관련 연구

GSM(Global System for Mobile Communications)은 전세계에서 가장 널리 사용되는 개인 휴대통신 시스템으로 시분할다중접속(TDMA, Time Division Multiple Access) 기반의 통신 기술이다. GSM은 1982년에 열린 CEPT에 의해 처음 제시되었다. CEPT(Conference of European Post and Telecommunications Administrations)는 유럽 전역의 공중 셀룰러 전화서비스의 수요가 1980년대와 1990년대에 엄청난 수요가 있을 것으로 예견하고, 유럽의 셀룰러 서비스를 단일화하기 위한 공통의 표준을 설정하기로 결정하였다. 유럽 국가들은 유럽 내의 어느 곳에서나 통화가 가능한 단일 시스템을 구축하기 위해 공동 연구를 추진한 것이 바로 GSM이다. GSM은 표준화 과정을 단계적으로 접근하였기 때문에 GSM 서비스도 단계적으로 제공되었다. GSM의 표준화 단계는 <표 2>와 같으며, 각 단계별 주요 서비스는 <표 2>과 같다

GSM 네트워크는 <그림-1>와 같이 MS

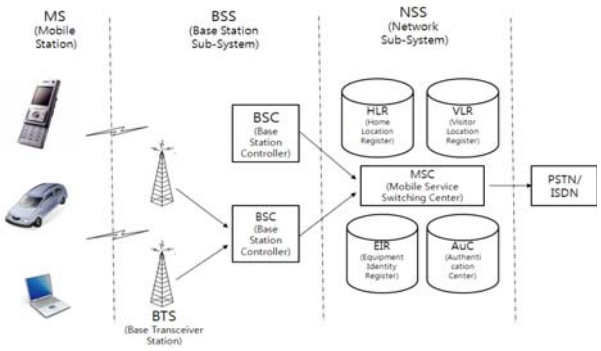
(Mobile Station), BSS(Base Station Sub-System), NSS(Network Sub-System) 3개의 파트로 구성된다. MS는 GSM 이동전화기에 해당하며 ME(Mobile Equipment)라고도 한다.

<표 2> GSM 표준화 단계

단 계	내 용
GSM 1단계 서비스 (GSM phase 1 Service)	- 1992년 이후 사용 - 초기 GSM의 표준으로 추가서비스와 기능들의 호환성을 높임 - Call forwarding, Global Roaming 등
GSM 2단계 서비스 (GSM phase 2 Service)	- 1995년 이후 사용 - 초기에 계획했던 서비스와 망의 모든 특징들을 완전히 구현하기 위한 단계로 최종사용자에게 다향한 부가 서비스 제공 - SMS(Short Message Service) 등
GSM 2+단계 서비스 (GSM phase 2+ Service)	- 1996년 이후 사용 - 시장 수요와 표준 명세의 이용도에 따라 갱신된 추가적인 서비스 - 패킷 데이터 서비스 지원 등 - 두가지 형태의 패킷 데이터 서비스로 발전(GPRS, HSCSD)
GSM 3단계 서비스 (GSM phase 3 Service)	- 진행 중(UMTS 또는 IMT-2000)

MS에는 IMEI(International Mobile Equipment Identity)가 들어 있고, SIM카드 에는 IMSI (International Mobile Subscriber Identity)가 들어있다. 엄밀히 말해 MS는 ME(Mobile Equipment)로 알려진 MS 그 자체와 SIM (Subscriber Identity Module)라는 카드의 두 부분으로 구성되어있다.[1] BSS는 RF 송수신을 처리하는 BTS(Base Transceiver Station)와 무선채널 Setup, Frequency Hopping, 핸드오버를 처리하는 BSC(Base Station Controller)로 구성된다. BTS는 GSM에서 무선 송신기 역할을 수행하며, BTS의 셀은 3개의 섹터로 구성된다. 하나의 특정 BSC는 현재 진행 중인 트랙픽 채널다. (call)를 유지한다. NSS에서 핵심 역할을 수행하는 MSC(Mobile SwitchhhhhCenter)는 Mobility Control, 위치 등록 및 관리, 인증, 위치 갱신, 핸드오버처리, 로밍을 담당한다. 또한 다른 네트워크와다.통신을 위하여 게이트웨이 역할을 할 수 있는데 이러한 MSC는 GMSC (Gat쉥행하y MSC)라 한다. HLR(Home Location Register)은 사용자다.각종 정보와 단말의 위치정보를 저장하고 관리하는 일종의 데이터베이스이다. IMSI, 이동전화기의 ISDN (Integrated Service Digital Network)번호, VLR(Visitor Location Register)주소 등 다양한 정보를 관리한다. HLR의 주요 기능은 사용자의 호를 정확히 설정하기 위한 라우팅 정보를 관리하여 사용자의 위치관리를 수행한다.

AuC(Authentication Center)는 이동전화기의 SIM에 저장된 암호화키 값(Kc)의 복사본을 가지고 있으며, 암호화키 값(Kc)을 이용하여 인증기능과 암호화기능을 수행한다. GSM 이동통신서비스에서 이동전화기가 연결된 네트워크에서 기지국은 하나의 셀(CELL)에 속하며, 기지국제어기(BSC)는 여러 개의 셀을 관리한다.



<그림-1> GSM 네트워크 구조

GSM 설계당시 보안 목표는 일반 전화와 같은 수준의 보안성과 이동전화기의 복제 방지였다. 설계 당시에는 능동적 공격이

불가능할 것으로 예상했으나 실험을 통해 현재는 SIM카드 복제가 일부 가능하다는 것을 확인하였다. GSM에서는「사용자 인증」,「사용자 익명성」,「무선 통신 선로의 암호」 서비스를 제공하고 있다.

III. GSM 보안기능과 A3A8 알고리즘

GSM 보안의 특성은 크게 세 가지로 볼 수 있다. 첫째, 익명성(Anonymity) 보장이다. 이를 위해 이동전화기 패킷을 감시하여 송신자를 식별하는 것을 방지하며, 최초 송신자 식별을 위해 IMSI(International Mobile Subscriber Identity, 국제 이동통신 사용자 정보)를 사용하고, TMSI(Temporary Mobile Subscriber Identity)가 송신자에게 할당한다. 이때 TMSI는 암호화되어 전송되고, 수시로 변경되어, 동일한 이동전화기는 GSM 네트워크상에 존재할 수 없게 된다. 둘째, 통화요금 부과과과과과워크상에해 인증(Authentication)을 명SM 수행한다. 인증 과정의 특징으로 이동 전화기에서 기지국을 인증하지 않고 단지 기지국에서 사용자를 인증하는 단방향 인증 방식을 사용하고 있다. 이 문제는 위장 기지국을 만들었을 경우 사용자의 정보를 해킹할 수 있는 보안 취약점을 가진다. 셋째, 통화에 대한 비밀성(Confidentiality)을 보장하기위해 스트림 암호화 기법을 사용한다. 또한 사용자의 프라이버시를 보호하기 위하여 몇 가지 보안 기능들이 GSM에 구축되었으며, 기능들은 아래와 같은 사항들을 포함하고 있다.[2)3)]

- 등록된 사용자들만 인증
- 암호화를 사용한 안전한 데이터의 전송
- 사용자 정보 보호
- 이동 전화기들은 SIM 없이 사용 불가능함
- 복제된 SIM들은 네트워크에 허용되지 않음
- 보안화되어 저장된 Ki

특히 사용자 정보보호를 위해 IMSI는 SIM 카드에 저장된다. 사용자 정보의 비밀을 보장하기 위해서 임시 이동통신 사용자 정보(TMSI, Temporary Mobile Subscriber Identity)가 사용된다. TMSI는 인증과 암호화 과정들이 발생한 후에 이동통신 기지국으로 송신되며, 기지국은 TMSI의 수신을 확인해줌으로써 응답하고, TMSI는 TMSI가 발행된 지역에서만 유효하다. 해당 지역 외부에서 통신을 수행하기 위해서는 TMSI에 지역 정보(LAI, Location Area Identification)가 추가적으로 필요하다. 또한 SIM카드의 보호를 위해 SIM카드의 ROM을 프로그래밍하여 매우 보안성이 높은 수준으로 민감한 데이터를 저장할 수 있다. 그러므로 SIM카드는 Ki와 IMSI, 그리고 다른 민감한 사용자 데이터를 저장할 수 있다. GSM에서 제공하는 보안 알고리즘들은 수출의 제한으로 인해 공개되지 않는다. GSM에서 사용되는 알고리즘은 세 가지로 A3, A8, A5가 있다. 사용자 인증을 위한 알고리즘 A3와 암호화 키 생성 알고리즘 A8은 MS의 SIM카드 내부와 GSM망의 HLR, VLR의 데이터베이스에 저장되어 있다. GSM 문서에는 이 암호화 알고리즘에 관한 설명이 없다. 그러나 A3, A8 알고리즘에 대한 문서 유출이 발생했고, 이는 COMP128 알고리즘으로 명명되었으며 여러 사람에 의해 분석되고, 취약점이 노출되었다. 통신 채널의 암호화는 A5 알고리즘을 사용한다. A3와 A8 알고리즘은 이동통신사에 의해 수정 및 정의될 수 있다. 음성 암호화 알고리즘 A5는 상호 연동성을 위해 각 나라마다 같아야 하며 엄격한 저작권의 관리하에 ETSI로부터 얻을 수 있다. 망 운영자가 GSM망 서비

스를 시작하고자 할 때 텔레콤 회사로부터 장비를 지급받는다. 이 장비에는 A3와 A8은 지정되어 있지 않고 비어 있게 되며, 운영자는 A3와 A8알고리즘을 결정하고 결정된 알고리즘을 사용자들에게 판매될 SIM카드 내부에 프로그래밍 한다. 이러한 사유로 중국의 이동통신사들은 2005년 COMP128의 보안 취약점을 개선한 COMP128 V0 버전을 개발하였고, 판매하는 SIM카드에 삽입하였다. 신규 구매한 SIM카드를 GSM 이동전화에 삽입한 후 인증을 받게 될 때 Ki는 네트워크상에 송수신되지 않으며, SIM카드 내부의 Ki도 읽을 수 없는 구조로 되어 있다. 네트워크는 128비트의 RAND를 MS에 보내고 SIM은 자신이 가지고 있는 Ki와 전달받은 RAND를 입력 값으로 A3 알고리즘을 실행한다. 실행결과로 32비트의 응답(SRES)을 생성하고 Ki와 RAND의 입력으로 A8알고리즘을 수행하여 64비트의 암호화 키(Kc)를 생성한다. 생성된 암호화 키(Kc)는 A5 알고리즘의 입력으로 사용된다. 네트워크에서도 같은 알고리즘을 수행하여 MS가 보내온 SRES와 비교하여 인증을 수행하게 된다.[4)]

COMP128 알고리즘은 1997년 3월 3일 익명의 문서로 세상에 유출되었다. 유출된 문서[5)]는 <그림-2>과 같으며, COMP128알고리즘의 전체적인 구조를 이해할 수 있었다. 이 문서는 캘리포니아 버클리 대학의 Marc Briceno, Ian Goldberg, and David Wagner 교수에 의해 잘못된 부분이 수정되어 공개되었고 COMP128 알고리즘이라 불리었다. A3A8 알고리즘은 두 입력 값을 받아 8번 for 루프를 실행하고, 내부적으로 5단계의 압축 과정을 수행한다. 수행 후 32비트의 SRES와 64비트의 Kc를 출력한다 .COMP128 알고리즘 소스를 컴파일한 후 실행하면, 16바이트(128비트) RAND와 16바이트(128비트) Ki를 입력하고, 32비트 SRES와 64비트 Kc 총 96비트의 결과를 얻을 수 있다.


CRYPTOME

Donate $25 for two DVDs of the Cryptome collection of files from June 1996 to the present — Natsios Young Architects

20 April 1998
Source: Hardcopy from anonymous 3 March 1997

See related file on GSM cloning: http://cryptome.org/jya/gsm-cloned.htm

[Extracts From]

TECHNICAL INFORMATION

GSM System Security Study

10-1617-01 10th June 1988

RACAL RESEARCH LTD.

WORTON DRIVE, WORTON GRANGE INDUSTRIAL ESTATE,
READING, BERKS, RG2 0SB, ENGLAND.

Telephone: Reading (0734) 868601 Telex: 847152

3 COMMERCIAL IN CONFIDENCE *[Top of each page: omitted hereafter]*

Part 1

Overview of GSM Security Features

The object of this part of the report is to provide an overview of the security features in the GSM system. The description is brief, and focuses on the

<그림-2> 유출된 A3A8 문서

COMP128 알고리즘은 5단계의 압축을 갖는다. 각 압축 단계에서 결과 바이트는 2개의 입력 바이트에 따라 다르며, 두 개의 입력 바이트는 검색 테이블의 인덱스를 결정하고, 결과 바이트를 갱신하는데 사용된다. 따라서 압축 후에 단지 4 비트 값만이 X[] 벡터 안에 남아 있게 된다. 이 압축 방법은 COMP128의 주요 약점이다.[6)]

Ⅳ. SIM카드 복제실험 및 결과고찰

1. 중국 이동통신서비스 현황

중국은 1987년부터 무선이동전화 서비스를 개시하였다. 1997년까지 10년 동안 이동전화 이용자는 1,000만 명이 되었고, 2001년에는 1억 명이 되었다. 2002년 11월 중국 이동전화 사용자 수는 2억 명으로 증가하였고, 2004년 5월 3억 명, 2006년 2월 4억 명에 이르렀고, 2007년 11월말 기준 5억 명에 이르는 등 기하

급수적으로 사용자가 늘어나고 있다.[7] 중국 이동통신 시장은 차이나 모바일(China Mobile, 连瑛), 차이나 유니콤(China Unicom, 移通), 차이나 텔레콤(China Telecom)의 3개 사업자가 이끌어 가고 있다. 중국 이동통신 사용자 수는 <표 3>와 같이 2008년 5억 8천8 백만 명, 2009년에는 6억 8천 7백만 명이 사용하고 있으며, 2010년에는 7억 9천 4백만 명 정도 될 것으로 예상하고 있다. 또한 국정부는 2009년 1월 7일 3G 이동통신서비스 사업자로 차이나 모바일(China Mobile), 차이나 텔레콤(China Telecom), 차이나 유니콤(China Unicom)을 선정하였다.

<표 3> 중국 이동통신 사용자 현황 및 전망

이동통신사	서비스	2008	2009	2010
차이나 모바일	2G(GSM)	457,860,308	538,982,539	615,678,911
	3G(TD-SCDMA)	0	3,038,891	9,390,926
	사용자	457,860,308	542,021,430	625,069,837
	시장 점유율	78%	79%	79%
차이나 유니콤	2G(GSM)	101,835,554	112,344,798	125,561,415
	3G(TD-SCDMA)	0	974,546	3,285,598
	사용자	101,835,554	113,319,344	128,847,013
	시장 점유율	17%	16%	16%
차이나 텔레콤	2G(CDMA)	28,600,000	30,800,929	37,156,549
	3G(EVDO)	0	899,071	3,502,786
	사용자	28,600,000	31,700,000	40,659,335
	시장 점유율	5%	4%	5%
총사용자		588,295,862	687,040,774	794,576,185

이들은 각각 중국 독자 기술규격인 TD-SCDMA (Time-Division Synchronous CDMA), 북미 방식인 CDMA2000, 유럽방식인 WCDMA에 대한 서비스 허가권을 받았다. 차이나 모바일과 차이나 유니콤은 3세대 이동통신 표준규격인 TD-SCDMA를 서비스하고 있으며 차이나 텔레콤은 CDMA2000 1X EV-DO를 서비스하고 있다. 그러나 2009년 통계를 보면 2G (GSM) 사용자가 전체사용자의 95%에 달하고 있다. 다수 사용자가 2G(GSM) 방식을 사용하고 있으므로 현재 중국내 2G(GSM)이 갖고 있는 보안 문제 해결은 시급한 상황이다. 본 논문에서는 중국 통신서비스의 건전성을 검증하기 위해서 중국내의 SIM카드를 누출된 COMP128 알고리즘을 기반으로 하는 카드복제가 가능한지를 확인하고, 복제된 SIM카드를 현지의 통신서비스에 적용해 봄으로써 보안의 취약성을 검증하였다.

2. GSM SIM카드 복제 실험 및 고찰

SIM카드가 발전하면서, SIM카드 제조업체들은 더욱더 안전한 SIM카드 개발에 중점을 두어 Ki가 쉽게 해독되지 않는 수준을 목표로 삼았다. COMP128 V2 알고리즘은 V1이 해독된 뒤, V1을 개선하여 얻어낸 결과이다. V들은알고리즘의 취약점을 해결했다고 하지만 이 알고리즘 역시 V들처럼 대중에 알려지지 않았고 아직까지 공개한 사람은 없다. 따라서 기본적으로 해독이 불가능한 상태이다. 중국의 이동통신사업자 역시 SIM카드 복제 문제를 맞이하게 되었다. 2005년 하반기부터 발행된 카드는 SIMSCAN등의 소프트웨어로 Ki 값을 읽어낼 수 없게 되었다. 그러나 중국에서 판매되고 있는 SIM카드는 진정한 COMP128 V2카드가 아니었다. 중국의 이동통신사업자는 COMP128 V1알고리즘을 수정하여 교묘하게 SIMSCAN 등의 프로그램에 Ki가 해독되지 않도록 SIM카드를 제작하였다. 이런 카드는 중국이동에서 자체 설계한 것으로 KI 세트

규칙을 변경시켜 통상적인 스캔방법으로는 Ki를 해독할 수 없게 만든 방식으로 COMP128 V0라 불리고 있다. 본 연구는 중국내 2009년 현재 판매되고 있는 SIM카드에 대한 Ki 해독 및 복제가능성을 검증하여 이동전화기 복제로 인한 보안 문제를 확인하였다.

중국에서 시판되고 있는 SIM카드 복제 가능성을 실험하기 위해 다음 절차와 같이 실험을 수행하였다.

① 2009년 시판중인 중국 이동전화기 SIM 카드 획득
② SIM카드 리더기 및 SIM카드 Ki해독 프로그램 조사
③ Ki 해독 프로그램을 이용하여 획득한 SIM 카드 Ki 해독
④ SIM카드 복제 프로그램, 복제를 수행할 초기 상태의 SIM카드 확보
⑤ IMSI, ICCID, 해독된 Ki를 이용하여 SIM 카드 복제
⑥ 복제된 SIM카드와 정상 SIM 카드를 이용하여 중국 현지에서 이동전화기 인증 반복 측정실험
⑦ 동일기지국에 있을 때와 다른기지국에 있을 경우 음성전화송수신, 단순문자메시지 송수신, 동시 송수신, 통화 중 다른 이동 전화기를 이용한 송신(수신 방해) 실험
⑧ 실험 결과 분석 및 중국 GSM 보안 취약점 도출

SIM카드 복제에 사용한 카드는 차이나 모바일 2개, 차이나 유니콤 3개 제품으로 <표 4>과 같이 2009년 6월 구매한 제품이다.

<표 4> 복제에 사용된 SIM카드 정보

이동 통신사	생산 년도	전화 번호	ICCID	IMSI
차이나 모바일	2008 년	13510 593442	898600571908 10056668	084906005002 xxxxxx
	2009 년	15112 463940	898600311909 17153940	084906201142 xxxxxx
차이나 유니콤	2008 년	13148 863236	898601081675 55406288	084906107864 xxxxxx
	2008 년	13243 740601	898601082475 53240606	084906107341 xxxxxx
	2008 년	13149 988065	898601081475 57354579	084906108349 xxxxxx

ICCID 코드 분석 결과 <표 16>와 같이 2008년 및 2009년 제조 제품으로 식별되었다. 실험에 사용된 SIM카드의 ICCID를 분석 결과 차이나 모바일과 차이나 유니콤은 고유 형식을 사용하고 있었으며, 실험에 사용된 차이나 모바일과 차이나 유니콤의 ICCID분석 결과는 <표 5>과 같다.

<표 17> 차이나 모바일, 차이나 유니콤의 ICCID 분석

차이나 모바일	ICCID	8986	00	57	19	08	1	0056668
	의미	국가 식별 번호 (86 중국)	00 (차이나 모바일)	전화 번호 국번 (135)	성지역 번호 (19 廣東)	2008년 생산	생산 회사명 (1,프랑스GEMPLUS)	
차이나 유니콤	ICCID	8986	01	08	24	755	324060	Y
	의미	국가 식별 번호	01 (차이나 유니콤)	2008년 생산	전화 번호 국번 (132)	카드 발행 지역 번호	카드발행 상세 지역	생산회사 (武漢天喻)

차이나 모바일은 2000년~2004년까지 SIM카드 암호화 알고리즘으로 COMP128V1 알고리즘을 사용하였고, 2005년부터 COMP128V0 알고리즘을 사용하고 있다. 차이나 유니콤은 2000년~2005년 상반기까지 COMP128V1 알고리즘을 사용하였고, 이후 COMP128V0

알고리즘을 사용하고 있음이 조사되었다. 가능한 영역을 사전에 정하여 실험을 수행하였다. CID, IMSI등을 스캔하고, Ki 해독을 위해 사용되고 있는 대표적인 프로그램은 QuickScan, FD, WoronScan, SimonScan, SimSearchKi, SimScan 등이 있다. 본 연구에서는 중국 이동통신사들의 SIM카드로부터 Ki 해독을 6개의 프로그램을 사용하여 실험하였다. 그러나 실험에 사용된 SIM카드들은 FD와 WoronScan 단 두 종류의 Ki 해독 프로그램에서만 해독되었다.

2. 복제 SIM카드를 이용한 인증 실험

GSM 네크워크 상에는 동일한 SIM카드라 할지라도 VLR로부터 생성된 TMSI는 오직 하나이기 때문에 동일한 이동전화기가 존재할 수 없다. 중국 GSM에서 동일한 SIM카드를 사용하는 단말기가 가능한지를 발생될 수 있는 가를 실험하였다. 두 대의 이동전화기에 정상 SIM카드와 복제된 SIM카드를 삽입하여 두 대의 복제 이동전화기를 만들었다. 각 개체(이동전화기)들이 GSM 네트워크로부터 인증을 받는 환경 변수로는 동일 기지국에 있을 경우와 다른 기지국에 이동전화기가 존재했을 경우 두 가지 상황을 가정하였다. 또한 동일기지국과 다른 기지국에 있을 경우 두 개의 이동전화기가 동시에 GSM 네트워크에 인증을 시도하는 경우, 시간차를 두고 GMS네트워크에 인증을 시도하는 경우를 실험하였다. 실험은 2009년 4월과 6월 에 걸쳐 2회의 반복측정실험을 수행하였다. 반복측정의 반응 값에 영향을 미치는 원인인 반복요인으로는 동일한 시간에 송신 버튼을 누룰 경우 오차를 감안하여 1회 6번을 시행하였다. 실험결과 동일 기지국과 다른 기지국에서 두 개의 이동전화기를 GSM 네트워크에 인증할 경우 최종 GSM네트워크에 접속한 이동전화만이 정상적인 인증 상태임을 확인하였다. 그러나 <그림-3>에서 보는 것과 같이 마지막에 기지국과 연결된 이동전화기 뿐만 아니라 동일 SIM카드를 삽입한 다른 이동전화기도 정상상태(기지국과 인증 성공)인 것처럼 보여 졌다. 아래 <그림-3>에서 좌측 이동전화기는 정상적인 SIM카드를 삽입한 이동전화기이고, 우측 이동전화기는 복제한 SIM카드를 삽입한 이동전화기이다.

<그림-31> 원본 SIM카드와 복제 SIM카드를 삽입한 이동전화기

복제된 SIM카드와 정상 SIM카드를 이용할 경우 발생될 수 있는 문제를 확인하기 위하여 다양한 실험을 추가 시행하였다. 동일 기지국에 있을 때와 다른 기지국에 있을 경우 음성전화 송수신, 단순문자메시지 송수신, 동시 송신, 통화중 다른 이동전화기를 이용한 송신(수신 방해) 실험을 하였다.

복제 SIM카드를 이용한 인증 실험의 다양한 결과에서 중국 2G(GSM)의 많은 보안 취약점을 확인하였다. 실험 과정에서 두 이동전화기에 한국에서와 같은 복제이동전화기의 알림서비스는 없었다. 한국의 통신서비스의 경우 불법복제탐지시스템 (FMS : Fraud Management System)의 도입과 같은 복제탐지시스템을 도입하여야 통신서비스의

건전성을 보장할 수 있음을 확인하였다. 한국의 경우 2005년 8월 16일 정보통신부에 의해 이동전화 불법복제 방지를 골자로 '이동전화 안전성 제고 대책' 을 수립하고 지속적으로 개선방안을 추진해왔다. 또한, 2006년 3월부터 이동전화기 불법복제 신고포상금제도 시행, 이동전화 불법복제에 관한 처벌 법규 마련 등 다양한 이동전화기 불법복제 대책이 시행되고 있다. 이와 같은 통신법규를 정비하여야 중국의 통신서비스에 대한 건전성을 보장할 수 있음을 확인하였다.

Ⅴ. 결론

3G 이동통신서비스의 시장 확대에 앞서 2009년 현재 중국은 95%이상이 2G(GSM) SIM카드를 사용하고 있다. 본 연구수행 결과 중국 2G(GSM) SIM카드는 현행 Ki 해독을 수행하기 위한 다양한 프로그램으로부터 안전하지 않았다. 2005년부터 중국 이동통신사들은 COMP128버전을 수정한 COMP128V0 알고리즘을 적용했지만 이 알고리즘은 실험결과 여전히 Ki 해독 공격에 대한 취약점을 가지고 있었다. 본 연구에서는 2009년 시판되고 있는 차이나모바일과 차이나유니콤의 SIM카드를 대상으로 Ki 해독 및 SIM카드를 복제하는데 성공하였다. 또한 복제된 SIM카드를 이동전화기에 삽입하여 인증에 성공했으며, 복제된 SIM카드를 삽입한 이동전화기를 이용하여 정상 이동전화기의 착발신 방해, 문자메시지 가로채기 등 다양한 보안 취약점이 있음을 확인하였다. 통신서비스의 건전성을 확보하기 위해서는 새로운 기술의 단말기 도입만큼 중요한 것이 기존 단말기에 대한 취약성이 시급함을 확인하였다.

참고문헌

[1] 변태영, "GSM이동통신기술 기초", Jinhan M&B 대구테크노파크 모바일단말상용화센터 공동발행, 2008.3.31, pp.174~179

[2] GSM Association, "2008 Corporate Brochure" 2008.3, pp.34

[3] http://gsmworld.com/membership/our_members.htm 2009. 8

[4] http://www.gsm-security.net/faq/gsm-ki-kc-rand-sres.shtml

[5] http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html. "SM Cloning", Internet Security Applications Authentication and Cryptography, University of California Berkeley

[6] K. Mikolajczyk and C. Schmid. "Indexing based on scale invariant interest points," In Proceedings of International Conference on Computer Vision, pages 525-531, July 2001.

[7] J. Daugman and G.O. Williams, "A proposed standard for biometric decidability," In Card TechSecureTech, pp. 223-224, Atlanta, GA, 1996.

[8] Y. Wang and J. Han, "Iris Recognition Using Independent Component Analysis," Int. Conf. Machine Learning and Cybernetics, 2005, pp. 18-21.

[9] http://www.sinobiometrics.com

Study on Robustness of Communication Service : By theCloning SIM Card in Chinese GSM

Shik Kim

Abstract

The robustness of communication service should be guaranteed to validate its security of the whole sevice not just high performance. One kind of practical test-beds is the chinese communication service based on SIM Card and GSM. In paper, we try to experiment the possibility of SIM cards clone in various mobile communications using 2G in china, and hence discovered the security vulnerabilities such as the incoming outgoing, SMS service and additional services on the mobile phones using clone SIM cards. The experiments show that chinese communication service should be prepared the Fraud Management System against the cloning SIM card. and furthermore, regulations related to the communication service should be tuned the realistic security environments.

Key Words: Biometrics, Iris recognition, Gradient orientation, Orientation histogram, Iris rotation invariance