정보학연구 제12권 제2호 2009년 6월(pp.1-12)
The Journal of Information Technology. Vol.12. No.2

중국 2G(GSM) SIM카드 복제로 인한 보안 취약성 연구

김 완 수* · 김 식**

목 차

Ⅰ. 서 론

GSM은 전세계 이동통신 시스템에서 가장 많이 사용되고 있는 시스템이다. 1980년대 유럽은 7가지 상호 호환성이 없는 기술을 가지고 서로 다른 9가지 아날로그 이동통신 시스템을 각 국가들이 사용하였다. 1982년에는 유럽전기통신주관청회의(CEPT : European Conference of Postal and Telecommunications Administrations)에서 범유럽 셀룰러 통신망의 개발목적으로 GSM(Group Special Mobile)을 구성하였다. 그러나 1991년 GSM 서비스가 시작되었을 때 Global System for Mobile Communication으로 개명되었다. 1990년 GSM Phase1 모습을 갖추었고, 1992년 유럽지역에서 GSM서비스 상업화가 착수되었다.[1] 유럽의 이동통신은 1990년 GSM으로 통합되었고, 이동전화기에 사용자 식별 모듈(SIM : Subscriber Identity Module)을 내장하여 A3, A5, A8 등 3개의 암호화 알고리즘으로 통화 내용을

* 세명대학교 전산정보학과 박사과정
** 세명대학교 정보통신학부 교수

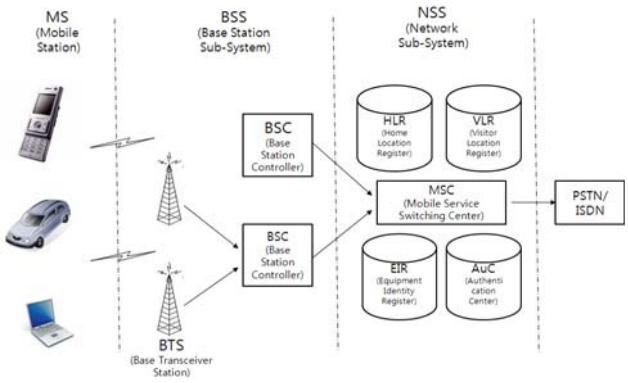
암호화시킬 수 있도록 SIM카드를 설계하였다. GSM 협회의 보도 자료에 따르면 GSM은 2002년 9월에 184개국에서 사용하였고,[2] 2003년에는 200개국에서 사용하였다.[3] 현재 GSM은 전 세계 이동통신 사용자의 약 80% 이상을 차지하고 있는 가장 영향력 있는 이동통신시스템이며, 219개국 40억 이상이 사용하고 있다.[4] GSM협회(GSMA)에는 현재 219개국 750개 이상의 GSM 이동전화사업자가 가입하고 있으며, 200개 이상의 제조업체와 공급업체들이 핵심 파트너로 활동하고 있다.[5] 많은 국가에서 GSM을 사용하고 있는 반면 한국은 CDMA 방식의 이동전화서비스가 사용되고 있다. CDMA가 동기식인 반면 GSM은 비동기식 이동통신방식으로 두 방식은 미국의 GPS (Global Positioning System) 위성시스템 이용 여부에 따라 구분이 된다. 이동통신서비스 시장에서 한국은 CDMA 시장 형성에 큰 역할을 수행하였고, GSM 이동통신서비스 시장은 중국이 큰 역할을 하였다. 1987년 중국은 GSM을 선택하였고, GSM 기술은 중국시장을 발판으로 세계적으로 발전하는 계기가 되었다. CDMA 이동전화기는 GSM의 SIM카드가 아닌 이동전화기 내부메모리에 ESN (Electronic Serial Number)을 기록하여 복제 이동전화기를 만들 수 있다. 하지만 GSM은 전화번호 복제 자체를 원천적으로 봉쇄한 SIM카드를 도입했다.[6]

본 연구는 CDMA의 복제이동전화기를 만들 수 있는 것과 같이 GSM의 SIM카드 복제를 수행하여 GSM 복제이동전화기 제작 가능성을 살펴보고 복제된 이동전화기로 인한 문제점을 확인하고 싶었다. 연구를 위해 GSM 네트워크 구조, 인증절차, SIM카드 특징 및 취약점을 이해하였다. 연구 대상 국가는 전 세계에서 가장 많은 GSM 사용자가 있는 중국을 선택했고, 중국의 이동전화시장을 이해하기 위한 조사와 Ki해독 및 SIM카드 복제 실험을 수행하였다. 그리고 복제된 SIM카드를 이용한 착발신 실험으로 중국 GSM의 다양한 취약점을 발견하였다.

II. GSM의 특징 및 인증절차

1. GSM 네트워크 구조

GSM 네트워크는 <그림 1>과 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.



<그림 1> GSM 네트워크 구조

MS에는 IMEI(International Mobile Equipment Identity)가 들어 있고, SIM카드에는 IMSI (International Mobile Subscriber Identity)가 들어 있다. 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,

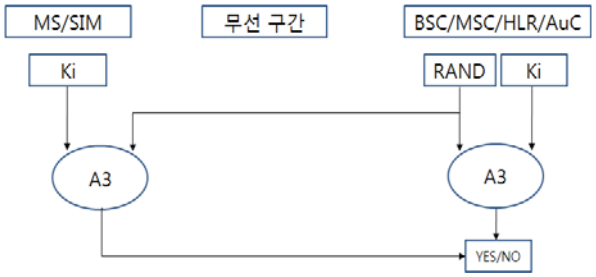
BTS의 셀은 3개의 섹터로 구성된다. 하나의 특정 BSC는 현재 진행 중인 트랙픽 채널의 호(call)를 유지한다. NSS에서 핵심 역할을 수행하는 MSC(Mobile Switching Center)는 Mobility Control, 위치 등록 및 관리, 인증, 위치 갱신, 핸드오버처리, 로밍을 담당한다. 또한 다른 네트워크와의 통신을 위하여 게이트웨이 역할을 할 수 있는데 이러한 MSC는 GMSC(Gateway MSC)라 한다. HLR(Home Location Register)은 사용자의 각종 정보와 단말의 위치정보를 저장하고 관리하는 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 수행하는 것이다. VLR은 자신의 영역에 있는 이동전화기의 위치 정보를 저장하고 있다. EIR(Equipment Identity Register)은 GSM망 내 유효한 모든 이동전화기의 목록을 보관하고 있다. EIR에는 IMEI를 저장하고 있으며, IMEI는 이동전화기에 저장되어 있는 전화기 고유 정보이다. IMEI 정보를 활용하여 이동전화기의 도난여부 및 유효성을 확인할 수 있다. AuC(Authentication Center)는 이동전화기의 SIM에 저장된 암호화 키 값(Kc)의 복사본을 가지고 있으며, 암호화 키 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.

GSM 보안의 특성은 크게 세 가지로 볼 수 있다. 첫째, 익명성(Anonymity)을 보장하기 위해 이동전화기 패킷을 감시하여 송신자를 식별하는 것을 방지하며, 최초 송신자 식별을 위해 IMSI를 사용하고, TMSI(Temporary Mobile Subscriber Identity)가 송신자에게 할당된다. 이때 TMSI는 암호화되어 전송되고, 수시로 변경된다. 이때 TMSI로 인해 동일 이동전화가 GSM 네트워크상에 존재할 수 없게 된다. 둘째, 통화요금 부과를 수행하기 위해 인증(Authentication)을 명확히 수행한다. 인증과정의 특징으로 이동전화기에서 기지국을 인증하지 않고 단지 기지국에서 사용자를 인증하는 단방향 인증을 사용하고 있다. 이 문제는 정보 탈취를 위한 가짜 기지국을 만들었을 경우 보안에 매우 취약해 진다는 점이다. 셋째, 통화에 대한 비밀성(Confidentiality)을 보장하기위해 스트림 암호화 기법을 사용한다.[7]

2. GSM 인증절차

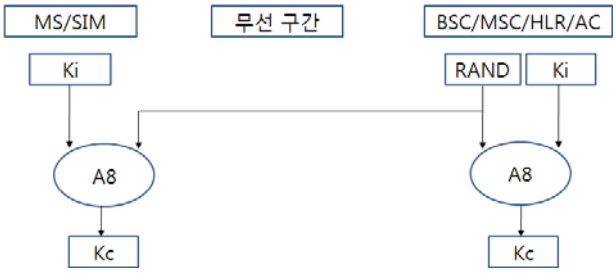
GSM 설계당시 보안 목표는 일반 전화와 같은 수준의 보안성과 이동전화기의 복제 방지였다. 설계 당시에는 능동적 공격이 불가능할 것으로 예상했으나 실험을 통해 현재는 SIM카드 복제가 일부 가능하다는 것을 확인하였다. GSM에서는 「사용자 인증」,「사용자 익명성」,「무선 통신선로의 암호」 서비스를 제공하고 있다. SIM카드에는 개별 사용자 인증키인 Ki(Individual Subscriber Authentication Key), 인증 알고리즘 A3[8]와 암호 키 생성 알고리즘 A8, IMSI 등의 정보가 저장되어 있다. Ki는 사용자의 홈 네트워크의 MS와 HLR 사이에 공유되어지는 고도로 보호된 비밀키로, AuC에 동일한 정보가 저장되어 있으므로 Ki는 전송할 필요가 없다. 이동전화기는 전화를 사용하기위해 최초 IMSI를 AuC까지 전달한다. AuC는 IMSI, Ki, RAND를 가지고 A3 알고리즘을 이용하여 SRES(Signed Response)[9]를 만

들고, SRES와 RAND를 HLR, VLR, MSC에 전달하고, RAND 값은 <그림 2>와 같이 BSS와 MS에 전달한다. MS는 전달받은 RAND 값, IMSI, Ki를 이용하여 A3알고리즘을 이용하여 SRES를 만들고 MSC에 전송한다. MSC는 AuC로부터 전달받은 SRES와 MS에서 전달받은 SRES를 비교하여 일치여부를 확인한다. SRES가 일치하면 MS 인증을 성공시키고 MS에게 TMSI를 할당한다.



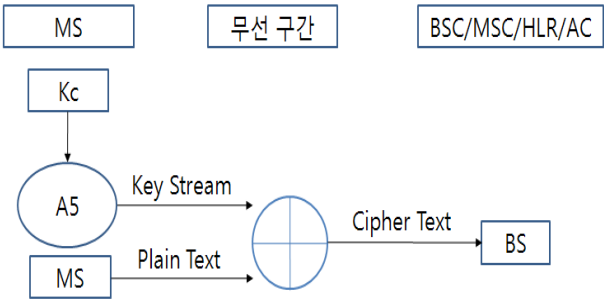
<그림 2> GSM 인증절차

인증에 성공하면 <그림 3>과 같이 RAND 값과 Ki를 이용해 A8알고리즘을 이용하여 암호키 Kc(Cipher Key)를 생성하고 네트워크센터에서도 같은 과정을 통해 암호키 Kc를 생성한다.



<그림 3> GSM 세션키 공유 절차

GSM네트워크는 사용자의 고유ID인 TMSI를 사용하여 사용자의 네트워크 접근을 제어한다. TMSI[10]는 로컬시스템에서 운용되며 이동전화기를 식별하는데 사용하는 일시적인 숫자이다. 이 TMSI는 IMSI또는 MDN (Mobile Directory Number) 대신에 사용된다. A5 암호 알고리즘 수행은 MS에서 이루어지며, 사용자 정보를 일시 저장한다. 그리고 TMSI를 생성/저장 및 인증의 성공 여부를 결정하는 것은 VLR이 수행하며, 암호키 값(Kc), 랜덤값(RAND), 인증 서명값(SRES)의 저장 및 관리는 HLR이 수행한다.[11] <그림 4>는 무선 구간에서의 메시지 암호 통신 절차이다.



<그림 4> GSM 무선구간 메시지 암호 통신 절차

3. GSM SIM카드

SIM카드는 마이크로칩이 내장된 작은 스마트카드이며 GSM 이동전화기에 삽입되어 GSM 네트워크 접속에 필요한 정보를 제공한다. GSM 이동통신서비스의 가장 큰 편의성은 SIM 카드를 사용한다는 점이다. 다양한 GSM 이동전화기에 SIM카드만 삽입하면 사용이 가능하다는 점은 자유롭게 신제품을 구매하여 사용하거나 기존에 사용하던 SIM카드를 다른 이동전화기에 삽입하여 사용할 수 있는 장점이 된다. 또한 기존에 사용하고 있는 이동전화의 번호 변경도 SIM카드만으로 쉽게 변경할 수 있다. GSM 이동전화기에는 IMEI가 들어있고, SIM 카드에는 IMSI등 많은 정보가 저장되어 있다. 결국 실제 사용자의 전화번호는 SIM 카드에 들어 있는 것이다. SIM 카드에 들어 있는

IMSI는 HLR/VLR에서 관할하고, IMEI는 EIR에 저장되어, 이동전화가 도용된 것인지 여부를 알리게 된다.[12] SIM 카드에는 전화번호, 요금 내역 및 자주 이용하는 전화번호 등 사용자정보 및 이동전화 보안 관련 정보가 내장된다. SIM카드는 CPU, ROM, RAM, EEPROM, I/O 회로로 구성되며, 이동전화기에 사용되고 있는 사이즈는 25×15mm이다. ROM에는 A3와 A8 알고리즘을 포함하고 있으며, EEPROM은 IMSI와 Ki(Authentication Key)를 포함한다. IMSI는 15개의 숫자 코드로 되어있으며, 모바일 국가코드(MCC), 모바일 네트워크 코드(MNC), 모바일 사용자 식별번호(MSIN) 세 가지 요소로 구성되며, GSM 네트워크에 각각의 MS를 식별하는데 사용된다. IMSI를 사람들의 ID카드와 같은 개념으로 이해할 수 있다. IMEI는 이동전화기에 저장되어 있는 이동전화기의 국제기기식별번호이다.[13] IMEI는 제조업체에 의해 이동전화기 제작 과정 중에 할당되며, 최대 15자리로 형태는 AABBBB-CC-DDDDDD-E의 형식으로 <표 1>과 같다.

<표 1> IMEI의 형식

구 분	내 용
AA	Country Code
BBBB	Final Assembly Code
CC	Manufacturer Code
DDDDDD	Serial Number
E	Unused

4. GSM SIM카드의 보안 취약점

Ki는 사용자의 인증을 위한 비밀키로 HLR이 관리하는 AuC와 SIM카드 내부에만 보관된다. AuC는 사용자의 SIM에 저장된 Ki의 복사본을 가지고 있으며 이것은 외부에 노출이 되지 않도록 관리되고 있다. 그러나 SIM카드 내부에 보관된 Ki를 알아 낼 수 있다면 동일한 SIM카드를 만들 수 있다는 말이 된다. 이러한 Ki 해독을 위한 연구는 지속적으로 연구되고 있다. SDA(Smart card Developer Association)와 ISSAC(Internet Security, Applications, Authentication and Cryptography)는 SIM카드로부터 Ki를 효과적으로 검색할 수 있는 COMP128 알고리즘의 결함을 발견했다. SIM카드를 물리적으로 접속하여 공격을 수행할 수 있으며, 공격은 chosen-challenge attack을 기반으로 하였다. 이러한 이유는 A8알고리즘에 인수와 RAND를 주었을 때 Ki에 대한 정보를 나타내고 이와 같은 방법으로 COMP128 알고리즘은 깨지게 되기 때문이다. SIM카드는 PC에 연결된 스마트카드 리더기를 통해 접속하고, 150,000번의 시도로 해독될 수 있다. Ki는 차분암호해독기법(Differential Cryptanalysis)을 이용하여 SRES의 응답에서 추론 될 수 있으며, 스마트카드 리더기를 사용하여 공격을 구현하면 SIM카드로부터 초당 6.25번 질문을 만드는 것이 가능하다. 따라서 공격에 필요한 시간은 8시간 정도가 필요하다. COMP128의 패치 버전은 COMP128V2로 불리어지고 있고 현재 이용가능하다.[14] SIM카드의 Ki를 해독하기 위한 방법으로 일반 섬광전구를 이용하여 SIM카드의 Ki를 노출시키는 방법인 광학적 결함 유도(Optical Fault Induction[15])방법과 타이밍 및 전력소모를 분석해서 적응식 선택 평문으로 Ki를 복원하는 방법인 분할(Partitioning) 공격 방법이 사용되고 있다. 분할 공격은 기본 선형분석에서 입력 비트와 출력 비트간의 선형식을 이용하여 공격하는 방법이다. 입력과 출력을 몇 개의 부분으로 분할하여 입력의 특정부분이 출력의 특정 부분으로 가장 많이 가는 특성을 이용하여 키를 찾는 방법이다.

III. 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 기하급수적으로 사용자가 늘어나고 있다.[16] 중국 이동통신 시장은 차이나 모바일(Chana Mobile, 连瑛), 차이나 유니콤(China Unicom, 移通), 차이나 텔레콤(China Telecom)의 3개 사업자가 이끌어 가고 있다. 중국 이동통신 사용자 수는 <표 2>와 같이 2008년 5억 8천8 백만 명, 2009년에는 6억 8천 7백만 명이 사용하고 있으며, 2010년에는 7억 9천 4백만 명이 될 것으로 예상하고 있다.[17]

또한 중국정부는 2009년 1월 7일 3G 이동통신서비스 사업자로 차이나 모바일(China Mobile), 차이나 텔레콤(China Telecom), 차이나 유니콤(China Unicom)을 선정했다. 이들은 각각 중국 독자 기술규격인 TD-SCDMA (Time- Division Synchronous CDMA), 북미방식인 CDMA2000, 유럽방식인 WCDMA에 대한 서비스 허가권을 받았다.[18] 차이나 모바일과 차이나 유니콤은 3세대 이동통신 표준규격인 TD-SCDMA를 서비스하고 있으며 차이나 텔레콤은 CDMA2000 1X EV-DO를 서비스하고 있다.[19] 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.

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

<표 2> 중국 이동통신 사용자 현황 및 전망

Ⅳ. SIM카드 복제로 인한 중국 2G(GSM)의 취약점

1. 중국 GSM SIM카드 복제

SIM카드에 저장되어 있는 정보를 읽기 위해 GOODSUN사의 SUN-500, Verition사의 V608, COMODOW사의 PD822U, 천우(川宇)사의 C205등 많은 제품들이 판매되고 있다. 본 연구에서는 시중에 판매되고 있는 다양한 SIM카드 리더기 중 중국 GOODSUN ELECTRONICS의 SUN-500[20] 모델을 사용하였다. SIM카드 복제에 사용한 카드는 <그림 5>와 같이 차이나 모바일 2개, 차이나 유니콤 3개 제품으로 2009년 6월 구매한 제품이며 ICCID코드 분석 결과 <표 3>와 같이 2008년 및 2009년 제조 제품이었다. 실험에 사용된 SIM카드의 ICCID를 분석 결과 차이나 모바일과 차이나 유니콤은 고유 형식을 사용하고 있었다. 실험에 사용된 차이나 모바일과 차이나 유니콤의 ICCID분석 결과는 <표 4>와 같다.

<그림 5> 복제에 사용된 SIM카드

<표 3> 복제에 사용된 SIM카드 정보

이동 통신사	생산년도	전화번호	ICCID	IMSI
차이나 모바일	2008년	13510593442	8986005719081056668	084906005002xxxxxx
	2009년	15112463940	8986003119091715394 0	084906201142xxxxxx
차이나 유니콤	2008년	13148863236	8986010816755540628	084906107864xxxxxx
	2008년	13243740901	8986010824753534060	084906107341xxxxxx
	2008년	13149988065	8986010814755735457	084906108349xxxxxx

<표 4> 차이나 모바일, 차이나 유니콤의 ICCID 분석

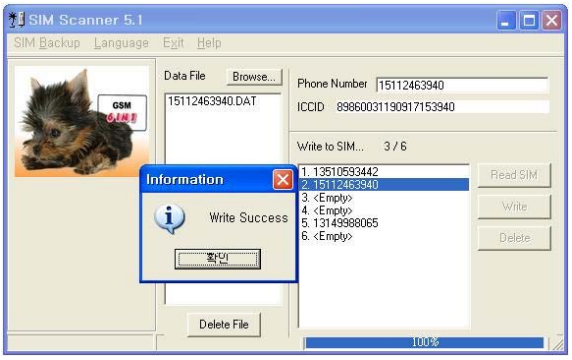
차이나 모바일	ICCID	8986	00	57	19	08	1	0056668
	의미	국가 식별 번호 (86 중국)	00 (차이나 모바일)	전화 번호 국번 (135)	성지역 번호 (19 廣東)	2008년 생산	생산 회사명 (1,프랑스GEMPLUS)	
차이나 유니콤	ICCID	8986	01	08	24	755	324060	Y
	의미	국가 식별 번호	01 (차이나 유니콤)	2008년 생산	전화 번호 국번 (132)	카드 발행 지역 번호	카드 발행 상세 지역	생산 회사 (武漢天喻)

SIM카드 복제를 위해서는 전화번호, IMSI, ICCID, Ki를 기록해야 한다. 따라서 SIM카드 복제를 위해서 Ki 해독은 반드시 수행되어야 하는 작업이다. 앞서 GSM 암호화알고리즘으로 A3, A5, A8이 사용되고 있음을 알 수 있었다. Ki 해독의 시작은 1998년에 유

출된 A3 알고리즘의 유출로부터 시작되었다. 유출된 A3 알고리즘을 미국의 캘리포니아 버클리 대학의 몇몇 교수들에 의해 분석되었고 COMP128이라 불리게 되었다. 많은 사람들이 COMP128 알고리즘에 대해 공격을 시도하였고 Ki 해독에 성공하였다. 이후 COMP128 알고리즘의 취약점을 해결한 COMP128V2알고리즘이 탄생하였다. 그러나 중국의 이동통신사업자는 COMP128 V2알고리즘을 사용하지 않았다. COMP128 V2는 복제 취약점은 해결했지만 호환성과 안정성에서 미흡한 것으로 이야기되고 있다. 이러한 이유로 차이나 모바일은 COMP128V1을 수정하여 COMP128 V0라 불리는 자체 알고리즘을 설계하였다. 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 있다. 현재 Ki 해독을 위해 사용되고 있는 대표적인 프로그램은 QuickScan, FD, WoronScan, SimonScan, SimSearchKi, SimScan 등이 있다. 본 연구에서는 중국 이동통신사들의 SIM카드로부터 Ki 해독을 위해 두 종류의 Ki 해독 프로그램을 병행하여 사용하였다. Ki 해독과정과 절차는 SIM카드 복제로 인한 피해를 예방하는 차원에서 자세히 설명하지 않겠다. 실험을 통해 해독한 결과는 <표 5>와 같다. 획득된 정보를 사용하여 <그림 5>의 좌측 하단에 있는 SIM카드에 기록할 수 있다. <그림 5>의 좌측 하단에 있는 SIM카드는 한 장에 6개의 GSM SIM카드 정보를 기록할 수 있으며, <그림 6>은 <표 6>에서 확인된 정보를 이용하여 SIM카드 복제를 수행한 화면이다.

<표 5> 차이나 모바일, 차이나 유니콤 SIM카드 Ki 해독결과

이동통신사	생산년도	전화번호	ICCID	IMSI	Ki	해독시간
China Mobile	2008년	13510593442	89860057190810056668	084906005002xxxxxx	F2C21F7A61D6A12717 이하 생략	2시간 30분
	2009년	15112463940	89860031190917153940	084906201142xxxxxx	BDF4767ACDE83C17 이하 생략	11시간
China Unicom	2008년	13148863236	89860108167555406288	084906107864xxxxxx	BF77BED120C8FC9F1 이하 생략	8시간 40분
	2008년	13243740601	89860108247553240606	084906107341xxxxxx	89F12E9F156883C644 이하 생략	4시간 30분
	2008년	13149988065	89860108147557354579	084906108349xxxxxx	DC3BA43706423CCEF 이하 생략	1시간 45분



<그림 6> 복제에 사용된 SIM카드

2. 복제 SIM카드를 이용한 착발신 실험

복제한 SIM카드를 이동전화기에 삽입한 결과 <그림 7>과 같이 2대의 전화기 모두 인증에 성공하였다.

<그림 7> 원본 SIM카드와 복제 SIM카드를 삽입한 이동전화기

음성전화, SMS 착신의 경우 마지막에 기지국과 연결된 이동전화기(정상 이동전화기 또는 복제 이동전화기)에서만 정상 착신서비스가 이루어짐을 확인하였다. 음성, SMS 발신시 정상이동전화기 및 복제 이동전화기 모두 발신이 가능했다. 하지만 VLR로부터 생성된 TMSI는 마지막 발신한 이동전화기에 전송되므로 두 개의 이동전화기중 마지막 발신한 이동전화기만 정상적으로 음성전화 및 SMS를 착신할 수 있다. 이러한 문제점은 정상적인 이동전화기를 소유한 사용자가 자신도 모르는 사이에 수신이 불가능한 상태에 놓일 수 있게 된다. 전화기의 신호 및 인증상태는 정상적이지만 복제 SIM카드를 사용한 이동전화기가 마지막으로 발신을 수행했거나 핸드폰 전원을 ON 시켰다면 자신이 발신하기 전까지는 수신이 불가능한 상태에 빠지게 된다. 이러한 복제이동전화기 사용을 알리기 위해 한국의 경우 복제된 이동전화기가 사용되어도 정상 이용자가 이동전화를 사용할 때 "인증에 실패하였습니다. 고객센터로 연락하시기 바랍니다." 와 같은 안내 문구를 전송해 줌으로써 이동전화 복제여부를 확인할 수 있다. 그러나 중국의 경우는 아무런 문구가 전송되지 않았다. 한국은 불법복제탐지시스템(FMS : Fraud Management System)의 도입으로 일정시간 통화시간이 겹치는 중복통화를 체크하는 중복통화 검색기능과 연속된 두 통화의 발신위치를 비교하여 물리적으로 이동이 불가능한 발신통화를 점검하는 통화간 발신위치 비교기능, 단기간 내에 일정량이상 통화가 발생한 경우 불법 복제 의심 건으로 파악하는 통화량 임계치 분석기능, 이통통신사에 등록된 모델명과 무선인터넷에 접속하는 이동전화 모델명이 불일치할 경우도 검색하여 불법복제 가능성을 탐지할 수 있다.[21]

3. SIM카드 복제로 인한 중국 2G(GSM)의 취약점

중국에서 판매되고 있는 SIM카드의 Ki해독 및 복제 실험을 통해 SIM카드 복제가 가능하다는 사실을 확인하였다. 이러한 문제로 인해 이동전화기를 습득하여 SIM카드를 복제할 수 도 있고, SIM카드를 판매하는 악의적 상인들에 의해 복제도 가능하다. 만약 SIM카드가 복제된다면

1) 정상사용자의 착신 방해
2) 착신 및 SMS 가로채기
3) 요금증가
4) 이동전화 부가서비스 악용

등이 발생할 수 있다. 이러한 문제점은 이동통신사업자에 의해 긴급히 해결되어야 할 사항이다. 또한 불법 복제된 SIM카드를 식별하기 위한 노력이 필요하다. 한국의 경우 2005년 8월 16일 정보통신부에의해 이동전화 불

법복제 방지를 골자로 '이동전화 안전성 제고 대책' 을 수립하고 지속적으로 개선방안을 추진해 왔다. 복제에 성공된 이동전화기가 사용되어도 정상 이용자가 이동전화기를 사용할 때 안내 문구를 전송해 줌으로써 이동전화기 복제여부를 확인할 수 있으며, 불법복제탐지시스템(FMS : Fraud Management System)의 도입, 2006년 3월부터 이동전화기 불법복제 신고포상금제도 시행, 이동전화 불법복제에 관한 다양한 처벌 법규 마련 등 다양한 이동전화기 불법복제 대책이 시행되고 있다. 중국과 한국의 이동통신서비스 방식이 상이하지만 한국과 같은 다양한 이동전화기 복제방지 대책이 중국에서도 반드시 필요하다. SIM카드 복제 방지를 위해 COMP128 V2 알고리즘 적용 또는 복제 방지 대책을 적용한 SIM카드 제작이 시급하며 정상사용자에게 복제된 SIM카드의 사용여부에 대한 알림서비스가 필요할 것이다.

Ⅴ. 결론

본 연구는 중국에서 사용되고 있는 2G(GSM)의 SIM카드 복제가능성에 대하여 실험을 통해 복제가 가능하다는 것을 검증했고, 복제된 SIM카드로 인한 취약점을 식별하였다. 또한 시판되고 있는 중국 이동통신사의 Ki 저장에 대한 안전성 문제, 네트워크에 중복된 SIM카드가 사용될 경우 발생될 수 있는 문제점을 확인하였다. 2009년부터 중국에서는 3G서비스가 본격화 되었다. 3G는 GSM 보안 모델을 바탕으로 보안 취약성을 개선하기 위해 상호인증, "시작암호" 지시, 모든 신호에 대한 무결성 보호, 키의 재사용 금지, RAND/XRES/Kc에 대한 재연 불가능, KASUMI 암호 알고리즘 적용, 기지국 제어기까지 암호화 확장 등의 기능을 포함하였다. 그러나 3G 이동통신서비스의 시장 확대에 앞서 2009년 현재 중국에서 95%이상이 사용하고 있는 2G(GSM) SIM카드의 보안대책이 먼저 강구되어야 할 것이다. 이와 같은 이유로 2G(GSM) Ki 공격에 대한 방어기술 연구를 지속 수행하고자 한다.

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] Li, Yong, Chen, Yin, and Ma, Tie-Jun. "Security in GSM". 2002.2, pp.2

[4] Scott Fox Chairman & CEO, Jeffrey Walkenhorst Vice President-Research, "Report Prepared for the GSM Association", 2009.5, pp.31

[5] gsmworld.com/membership/our_members.htm 2009.8

[6] 탁승호, "스마트카드 보안기술은 S I M·S A M·E M V카드로 자리매김했다", Hi-Tech Information, 2007. 4, pp.86-87

[7] "Security Aspects", European Telecommunications Standards Institute, Recommendation GSM 02.09

[8] Jeremy Quirke, "Security in the GSM system", 2004.5

[9] www.gsm-security.net/faq/gsm-ki-kc-rand-sres.shtml

[10] Lawrence Harte, "Inc Introduction to Global

System for Mobile Communication(GSM)", ALTHOS, 2005, pp.75

[11] 박정현, "차세대 디지털 이동통신을 위한 키분배 및 인증 방안 연구", 한국전자통신연구원, 1998.8, pp.52-59

[12] 김성환, 여운영, "미래를 지배하는 모바일 네트워크", 야스미디어, 2003.9.10, pp.313

[13] www.gsm-security.net/faq/imei-international-mobile-equipment-identity-gsm.shtml

[14] “SM Cloning”, www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.Internet Security, Applications, Authentication and Cryptography, University of California,Berkeley.

[15] Sergei Skorobogatov, Ross Anderson, "Optical Fault Induction Attacks", University of Cambridge, 2002.5

[16] "중국 - 이동통신 산업 발전과 20년간의 혁신", Techno Leaders' Digest, 한국과학기술정보연구원 2007.12.25, Vol.184, pp.2

[17] "China Mobile to remain dominant as China begins 3G rollout", Wireless Intelligence WI SNAPSHOT Issue#26, 2009.1.8

[18] 이은민, “중국의 3G 서비스 도입 현황과 전망“, 정보통신정책 제21 권3호, pp.68

[19] Ovum(2009), “3G licences coming to China and India”, 2009.1.7

[20] goodsun.en.china.cn, SUN-500 SIM card Reader

[21] 정보통신부 통신이용제도팀장 이상진, “정보통신부 보도자료, 이동전화 불법복제 방지 대책 추진결과”, 정보통신부 보도자료, 2006.12.12

A Study of Security Vulnerability by Cloning 2G(GSM) SIM Card in China

Wan Soo Kim, Shik Kim

Abstract

China first started its mobile phone services in 1987, and the number of users has exponentially increased so that it reached 700 millions in January 2009. Currently China's 2G(GSM) users is 650 millions. These 2G (GSM) services have an advantage of the capability to use the mobile phone with a SIM (Subscriber Identity Modul) card, one kind of smart cards, inserted into it. However, due to the security vulnerability of SIM cards being used within China's 2G (GSM) services, SIM cards cloning. Problems concerning mobile phone surveillance towards a designated person by illegal cloning ESN and IMSI have recently risen to be a massive social issue within Korea as well. These studies have experimented the possibility of SIM cards clone in various mobile communication corporations using 2G (GSM) in China, and hence discovered the security vulnerability such as the incoming outgoing, SMS service and additional services on mobile phones using clone SIM cards.

Key Words: GSM, SIM, MS(Mobile Station), BSS(Base Station Sub-System), NSS(Network Sub-System)