스마트폰 USIM 부채널 분석 방법에 대한 연구†

권근°, 정재욱*, 원동호*††
°*성균관대학교 정보보호연구소
e-mail:{kkwon, jwjung, dhwon}@security.re.kr

A Study on Side-channel Analysis for Smartphone USIM

Keun Kwon°, Jaewook Jung*, Dongho Won*††
°*Information Security Group, Sungkyunkwan University

● 요 약 ●

스마트폰의 USIM은 사용자가 별도로 인증정보를 입력할 필요가 없는 매우 편리한 인증 방법을 제공한다. 그러나 USIM에 저장된 정보가 외부로 유출될 경우 공격자가 손쉽게 정당한 사용자로 위장할 수 있는 문제점이 있다. 특히 USIM은 스마트카드에서 실행되는 어플리케이션이므로 기존에 스마트카드에 적용되었던 부채널 분석 공격 기법들이 USIM에도 적용 가능할 것으로 예상된다. 이에 본 논문에서는 스마트폰 USIM에 대한 부채널 분석 공격 가능성에 대해서 분석하고 스마트폰 USIM에 적용될 수 있는 부채널 분석 환경을 제안한다.

키워드: USIM(Universal Subscriber Identification Module), 부채널 분석 공격(Side-channel analysis attack), UMTS, WCDMA, GSM

I. 서론

스마트폰 사용이 활성화됨에 따라 스마트폰의 USIM(Universal Subscriber Identification Module)을 이용한 이동통신 서비스 사용자 인증 기법이 활용되고 있다. USIM을 이용한 사용자 인증은 별도로 아이디나 패스워드를 입력할 필요가 없으므로 매우 편리한 인증 방법 중 하나이다.

그러나 USIM에 저장된 정보가 해커와 같은 악의적인 공격자에 의해 공격을 받아 USIM 외부로 유출될 경우 공격자는 손쉽게 정당한 사용자로 위장할 수 있다는 문제점이 있다. 따라서 이러한 취약점을 개선하기 위해 USIM에 대한 공격방법 및 정보 유출 가능성에 대한 연구가 활발히 진행되고 있는데 특히 부채널 분석 공격과 관련된 연구가 최근 주목 받고 있다.

USIM은 일종의 스마트카드에서 실행되는 어플리케이션이므로 기존에 스마트카드에 대해 시도되었던 많은 부채널 분석들이 이론적으로 USIM에 적용 가능할 것으로 예상되어 관련 연구가 진행되고 있다. 이러한 연구를 통해서 2G 통신의 인증 프로토콜에서 사용되었던 COMP128과 같은 암호 알고리즘에 사용되는 키를 부채널 분석을 통해 찾아낼 수 있다는 것이 발표되었으며 이를 바탕으로 3G 통신에서 사용하고 있는 암호 알고리즘 역시 부채널 분석에 취약할 가능성이 있음을 알 수 있다[1].

이에 본 논문에서는 스마트 카드에 적용 가능한 부채널 분석 공격법을 분석하고 스마트폰 USIM에 적용할 수 있는 부채널 분석 환경을 제안한다.

† "본 연구는 방송통신위원회의 방송통신융합미디어원천기술개발사업의 연구결과로 수행되었음" (KCA-2012-12-912-06-003)

†† 교신저자: 원동호(dhwon@security.re.kr)

II. 관련 연구

1. 배경이론

1.1 이동통신 기술과 사용자 인증 기법

이동통신기술은 크게 GSM(Global System for Mobile Communications)계열과 CDMA(Code Division Multiple Access)계열로 구분할 수 있고, 각 통신기술의 속도 별로 통신기술의 세대를 구분한다. 그림 1은 통신 세대 별로 GSM 계열과 CDMA 계열의 통신 기술을 나타낸 것이다.

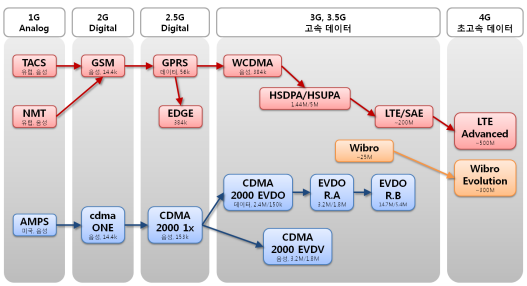

그림 1. GSM 계열과 CDMA 계열의 통신기술
Fig 1. GSM and CDMA mobile communication technology

본 논문에서는 USIM 부채널 분석 환경에 대한 연구를 목적으로 하므로 서비스 종료절차가 진행 중인 CDMA2000과 서비스 보급이 진행 중인 LTE 대신 현재 가장 보급률이 높은 3G 통신 기술인 UMTS와 UMTS의 전신인 GSM에 대해 분석하며 특히 서비스 가입자 인증을 위한 인증 프로토콜을 중점적으로 분석한다.

1.2 GSM 인증 프로토콜과 가상기지국

1.2.1 GSM 인증 프로토콜

GSM은 유럽통신표준협회(ETSI, European Telecommunications Standard Institute)에서 시분할다중접속(TDMA, Time Division Multiple Access)을 기반으로 개발한 2세대 이동통신기술이다. 사용자의 인증정보를 SIM(Subscriber Identity Module)카드라 불리는 소형의 스마트카드에 저장하여, 휴대전화에 SIM카드를 삽입하여 사용한다.

GSM의 사용자 인증 프로토콜은 그림 2와 같이 동작한다[2].

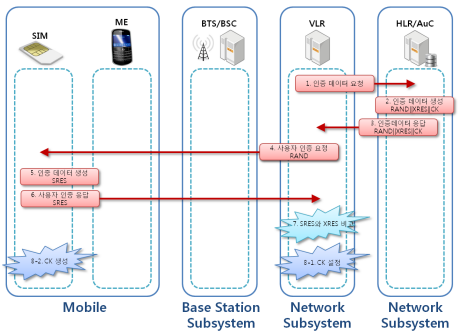

그림 2. GSM 인증 프로토콜
Fig 2. GSM authentication protocol

1.2.2 가상기지국을 통한 GSM 인증 프로토콜 우회

GSM 인증 프로토콜에는 사용자 단말기와 VLR 사이에서 가상기지국을 사용하여 인증과정을 우회할 수 있는 취약점이 있다. 그림 3은 이러한 인증 우회과정을 나타낸다.

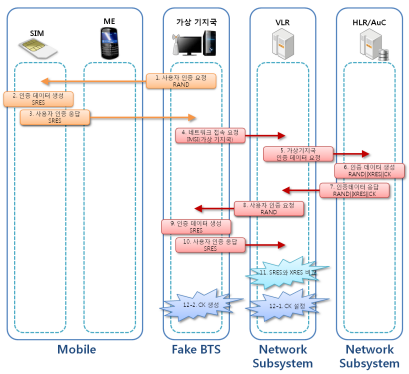

그림 3. GSM 인증 우회
Fig 3. Circumventing GSM authentication

가상 기지국은 자신의 SIM카드를 가지고 있는 정상적인 사용자이며, SIM카드의 K, IMSI(International Mobile Subscriber Identity)등의 모든 정보를 알고 있다. 따라서 위와 같은 과정을 통해 가상기지국은 일반 단말기인 것처럼 작동할 수 있으며 가상기지국과 연결된 사용자 단말기(ME)는 네트워크에 대한 인증을 수행하지 않으므로 진짜 기지국에 연결되었는지 아닌지 구분할 수 없다. 그리고 GSM에서의 음성메시지 암호화 여부는 기지국이 결정하므로 가상기지국은 ME와 CK를 설정하지 않고 비 암호화 통신 모드를 통해 ME의 통화 내용을 도청할 수 있다.

1.3 UMTS 인증 프로토콜

UMTS는 GSM계열의 3세대 통신기술이며 스마트카드의 일종인 USIM을 이용하여 사용자 인증을 수행한다. UMTS는 GSM에서 발전한 통신기술이며 GSM의 사용자 인증 취약점을 개선하였다. 그림 4는 UMTS 인증 프로토콜의 과정을 나타낸다[3].

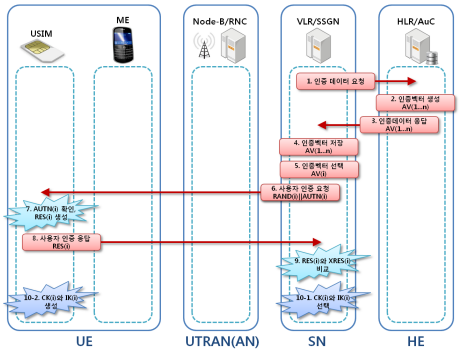

그림 4. UMTS 인증 프로토콜
Fig 4. UMTS authentication protocol

UTMS 인증프로콜은 사용자 단말기(ME)와 VLR이 상호인증 과정을 거치기 때문에 가상기지국을 사용한 인증우회는 불가능하지만 사용자 단말기(ME)에 원격으로 가짜 인증 데이터를 전송하는 것은 가능하다.

1.4 UTMS MILENAGE 알고리즘

UMTS 인증 프로토콜 과정에서의 인증 데이터 생성을 위해서 f 함수가 필요한데 유럽 표준화 기구인 ETSI 산하 SAGE(Security Algorithm Group of Experts)가 설계한 MILENAGE가 f함수의 생성에 적합한 알고리즘으로 권고되고 있다. 그림 5는 MILENAGE 알고리즘의 동작과정을 보여준다[4].

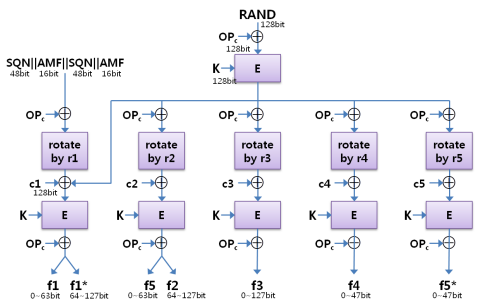

그림 5. MILENAGE 알고리즘
Fig 5. MILENAGE Algorithm

III. USIM 카드에 대한 부채널 분석 방법 및 환경

1. USIM 카드에 적합한 부채널 분석 방법

1.1 USIM 카드 획득시의 부채널 분석 방법

USIM카드에 대한 부채널 공격은 MILENAGE 알고리즘에 사용되는 AES 암호 알고리즘의 키 값을 알아내는 것을 목표로 한다. USIM 카드는 스마트카드의 일종인 UICC에 탑재되어 구동되므로 스마트카드에 적용 가능한 부채널 분석 공격을 적용할 수 있다. 특히 상관전력분석 기법을 사용하여 스마트폰 USIM에 적용된 MILENAGE 알고리즘에서 인증키를 생성하는데 사용된 마스터 키를 찾아낼 수 있음이 밝혀졌다[5]. 하지만 이러한 방법은 USIM을 획득했을 경우에만 공격 시도가 가능하다는 한계점이 있다.

1.2 USIM 카드 비 획득시의 부채널 분석 방법

USIM카드를 획득하지 못하였을 경우 원격 부채널 분석 방법을 적용할 수 있으며 전력 등 기타 부채널 정보에 대한 획득이 불가능하므로 시차 분석을 적용해야 한다. 하지만 일반적인 스마트카드의 경우 네트워크 경로를 고정시킬 수 있는 방법이 있으나 무선 통신을 하는 휴대전화에서 이용되는 USIM카드는 네트워크 경로를 고정시키기 어렵다. 무선 통신에서는 휴대전화의 위치와 기지국의 상태에 따라 무선 통신의 경로가 변경되기 때문이다. 통신경로의 변경은 특정한 시차의 측정을 어렵게 만들기 때문에 시차 측정을 통한 원격 부채널 공격의 적용이 불가능하다. 그림 6은 이러한 네트워크 간섭 발생을 나타낸다.

그림 6. 네트워크 간섭
Fig 6. Network interference

이와 같은 문제를 해결하기 위해 본 논문에서는 GSM 인증 프로토콜을 우회하기 위해 사용할 수 있는 가상기지국을 UMTS 인증 과정에 적용하여 네트워크 경로를 단일화 시키는 방법을 제안한다.

2. USIM 카드 원격 부채널 분석 환경

2.1 가상기지국 구성 요소

GSM 네트워크에 적용되는 가상기지국은 UMTS 네트워크에도 유사하게 사용될 수 있다. 따라서 본 논문에서는 GSM 네트워크에 적용되는 가상기지국 구성 방법을 통해 USIM 카드에 대한 원격 부채널 분석 환경을 구성한다. 그림 7은 USRP와 OpenBTS를 사용한 가상 기지국 구성 환경을 나타낸다[6].

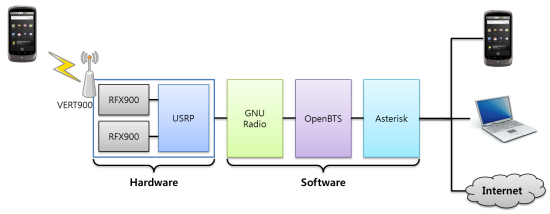

그림 7. 가상기지국 환경 구성
Fig 7. Construction of Fake BTS

2.2 USIM 카드 원격 부채널 시차 분석 환경 구성

가상 기지국을 설치하여 분석대상 USIM에 접근하면 USIM과 가상 기지국 간의 네트워크 간섭을 최소화 할 수 있다. 따라서 USIM의 MILENAGE 알고리즘에서 사용되는 암호 알고리즘의 암, 복호화 과정 시간을 비교적 정확하게 측정할 수 있으므로 원격에서의 부채널 시차 분석이 가능해진다. 그림 8은 일반적인 원격 부채널 분석 환경에 가상기지국을 추가하여 네트워크 간섭을 최소화한 환경을 나타낸다.

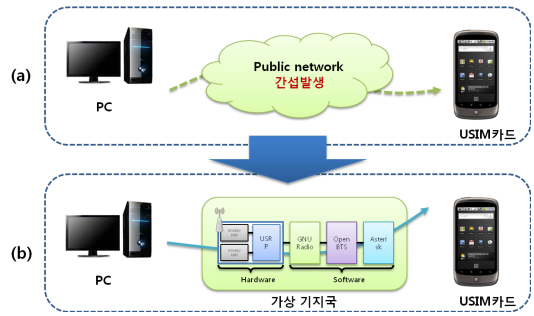

그림 8. USIM 원격 부채널 분석 환경 구성
Fig 8. Construction of remote side-channel analysis environment for USIM

이와 같은 환경을 구성하여 스마트폰 USIM의 킷값을 알아내기 위해서는 Joseph Bonneau 등이 제안한 시차분석 방법을 적용할 수 있을 것이다[7]. 이 시차분석 방법은 AES의 속도 향상을 위해 사용하는 룩업 테이블(lookup table)을 이용할 때, AES 첫 번째 라운드 혹은 마지막 라운드의 수행시간에 대한 통계적인 시차를 측정하는 방법이다. 표 1은 AES에 대한 시차분석 공격방법의 비교를 보여준다.

표 1. AES에 대한 시차 분석법
Table 1. Timing analysis for AES

구분	샘플 데이터 수	샘플 데이터 타입	복구 가능 키 길이
Bernstein	227.5	평문	전체
Tsunoo et al.	226	평문	전체
Joseph Bonneau et al.	214.58	평문	60bit
	215	암호문	전체
	213	암호문	전체

Ⅳ. 결론

본 논문에서는 USIM카드 부채널 분석 환경 구성에 앞서 이동통신기술을 분석하였고, USIM카드에 대한 공격 사례를 분석하였다, 그리고 분석 결과를 바탕으로 USIM카드를 획득하지 못하였을 경우의 부채널 분석 환경 구성 방법을 제안하였다. 특히 가상기지국을 활용하여 네트워크 간섭을 제거한 원격 부채널 분석 환경 구성 방법을 제안하였다.

본 연구 결과를 바탕으로 스마트폰의 USIM 부채널 분석 환경을 구성하면 실제 USIM의 비밀정보에 대한 공격을 원격으로 시도할 수 있다. 그리고 공격 수행 결과를 바탕으로 스마트폰 사용 환경에서 발생할 수 있는 새로운 보안 취약점을 예측하여 사전에 대응방안을 마련할 수 있을 것이다.

참고문헌

[1] K. H. Boey., Y. Lu., M. O'Neill & R. Woods., "Differential Power Analysis of CAST-128", IEEE Annual Symposium on VLSI, 2010

[2] Jeremy Quirke., "Security in the GSM sysetm", 2004

[3] 3GPP TS 23.002 V8.7.0., "Network architecture", 2010

[4] 3GPP TS 35.205 V10.0.0., "3G Security; Specification of the MILENAGE Algorithm Set", 2011

[5] HoSung Jeon., Ji Sun Choi., Dong-Guk Han. & Okyeon Yi., "Correlation Power Analysis of the AES-Milenage", summer conference on KSII, 2011

[6] OpenBTS, Retrieved from http://openbts.sourceforge.net

[7] Joseph Bonneau, Ilya Mironov., "Cache-Collision Timing Attacks Against AES", 2007