Journal of Korea Multimedia Society Vol. 10, No. 7, July 2007(pp. 902-911)

SIM 카드 기반 보안 취약성을 개선한 고성능 GSM 보안 프로토콜

김희정[†], 전하용[††], 이주화[†††], 정민수[††††]

요 약

GSM 플랫폼은 전 세계적으로 선례가 없는 아주 성공한 무선기술이다. 처음 GSM이 발표된 후 최근 10년 동안 200여 개 국가 10억 이상의 가입자가 사용하고 있으며, 지금도 빠르게 성장하는 모바일 표준으로 세계 모바일 시장을 리드하고 있다. 기존의 모바일 서비스인 음성통화 서비스 이외에 다양한 멀티미디어 서비스 및 국제 로밍이 가능한 3세대 이동통신으로 진화하고 있어 서비스를 제공하는 동안 개인의 사생활 보호 및 안전한 데이터 송수신 기술이 필수적인 구성요소이다. 그러나 현재 GSM을 이용한 안전한 데이터 통신을 위한 보안 알고리즘 및 프로토콜에 대한 문제점이 여러 번 지적되고 있다. 본 논문에서 우리는 2세대/2.5세대 GSM 네트워크 보안의 문제점을 제시 및 분석하여 2세대뿐만 아니라 3세대 네트워크 환경에서도 보다 안전한 서비스를 제공하는 보안 프로토콜을 제안하고자 한다. 이 보안 프로토콜은 SIM/ME 간 SIM 사용자 검증, SIM/ME/AuC 간 인증 및 키 일치 단계 단축으로 강화된 기밀성을 제공한다.

An Improved High-Performance Protocol for Security Vulnerability of GSM based on SIM Card

Hee-Jung Kim[†], Ha-Yong Jeon[††], Ju-Hwa Lee[†††], Min-Soo Jung[††††]

ABSTRACT

GSM platform is a hugely successful wireless technology and an unprecedented story of global achievement. In less than ten years since the first GSM network was commercially launched, it became the world's leading and fastest growing mobile standard, using over 1 billion GSM subscribers across more than 200 countries of the world. GSM platform evolved into 3th generation mobile communication which includes not only voice call services but also the international roaming and various kinds of the multimedia services. GSM is an essential element techniques a safe data transmission and a personal private protection while support services. However, a crypto algorithm and a secure protocol for a safe data communication using GSM are indicating various kinds of problems. In this paper, we propose a more safer and more efficient authentication protocol in 3th generation network through analysis of GSM security mechanism of 2th/2.5th generation. This security protocol offers enforced security efficiency by using user verification between SIM/ME and reduction of authentication and key agreement step between SIM/ME/AuC.

Key words: Mutual Authentication(상호인증), GSM, SIM 카드

※ 교신저자(Corresponding Author) : 정민수, 주소 : 경남 마산시 월영동 449번지(630-011), 전화 : 055)249-2217, FAX : 055)248-2554, E-mail : msjung@kyungnam.ac.kr
접수일 : 2007년 3월 5일, 완료일 : 2007년 7월 16일
[†] 준회원, 경남대학교 컴퓨터공학과
(E-mail : eunyeop@naver.com)
[††] 준회원, 경남대학교 컴퓨터공학과
(E-mail : hayongj1@nate.com)
[†††] 경남대학교 컴퓨터공학과
(E-mail : f13310@kyungnam.ac.kr)
[††††] 종신회원, 경남대학교 컴퓨터공학과
※ 본 연구는 BK 21의 지원을 받고 있습니다.

1. 서 론

유럽의 디지털 셀룰러 이동통신 시스템인 GSM은 무선을 통하여 전달되는 음성 및 데이터의 비밀성의 보장과 정당한 단말기 사용자의 시스템에서 안전한 접속을 가능하게 하는 여러 가지 보안 서비스를 제공하고 있다. SIM(Subscriber Identity Module) 기반의 GSM 인증 및 세션 키 일치 설정 프로토콜은 이동통신 시스템에서 메시지 기밀성 유지, 가입자 인증 및 가입자 위치 정보의 비밀성 등을 제공하도록 설계되었지만 암호 알고리즘의 운영정책 취약성, 각 장치별 인증 데이터 관리의 문제점과 TMSI를 이용한 가입자 위치 정보가 노출되는 등에 대한 문제점을 가지고 있다.

따라서 본 논문에서는 현재 GSM 방식을 이용한 안전한 데이터 통신을 제공하기 위한 보안 알고리즘 및 보안 메커니즘에 위와 같은 여러 가지 문제점을 지적하고, 2세대 및 2.5세대 GSM 네트워크 보안 취약성 분석을 토대로 앞으로 전 세계적으로 사용될 3세대 무선네트워크 환경을 고려하여 보다 안전하고 효율적인 보안 프로토콜을 제안하고자 한다.

2. 스마트 카드 및 GSM 보안 기술

2.1 스마트 카드 인증 메커니즘

스마트 카드는 데이터의 저장성, 보안성 및 휴대성의 특성을 가지고 있으며, 이중 가장 중요한 기능은 데이터 보안성이다. 독립된 COS(Chip Operating System)와 보안 메커니즘을 기반으로 연산기능을 가진 스마트 카드는 내부에 탑재된 마이크로 프로세스를 이용하여 데이터 암호, 전자서명 등의 암호 및 데이터 접근 제한 기능을 제공함으로써 기밀성, 무결성, 부인봉쇄 및 인증 등의 보안 요구사항을 충족시켜준다[1].

스마트 카드와 터미널간에 데이터의 안전한 송수신을 위해 요구되는 보안 요구사항 중 가장 중요한 것은 Terminal 인증, Smart Card 인증 및 키 일치 메커니즘으로 그림 1과 같은 절차로 수행된다[2].

2.2 SIM 카드 기반 GSM 인증 메커니즘

SIM 기반의 GSM 인증 메커니즘은 크게 2 부분으로 구성되어 있다. 하나는 f 함수 및 A3 암호 알고리즘을 이용하여 초기 키 일치와 단방향 사용자 인증을 수행하는 부분이고 나머지 하나는 A8 암호 알고리즘을 이용하여 세션 키 일치를 수행하며, 이 키를 A5 암호 알고리즘에 사용하여 ME/MSC간의 무선통신 상에서 SMS를 통하여 안전하게 응용 데이터를 송수신하는 부분으로 구성되어 있으며 그림 2와 같은 절차로 수행된다[3-5].

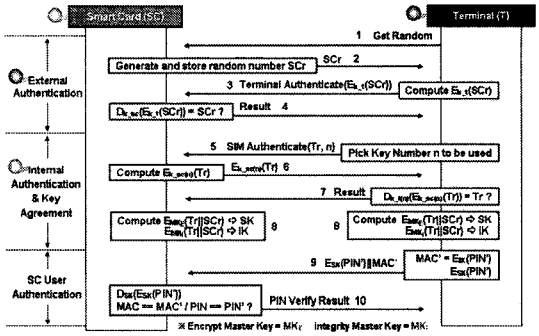

그림 1. Smart Card와 Terminal 간 인증 및 키 일치 프로토콜

2.3 스마트 카드 및 GSM 인증 메커니즘의 문제점

SIM 카드 기반의 GSM 인증방식의 취약성은 SIM/ME간에 SIM이 탑재된 ME 사용자가 SIM 카드를 사용할 권한을 가진 사용자를 인증하는 부분과 SIM/ME/AuC간 무선통신 경로상에서 안전하게 데이터를 송수신하는 인증 및 키 일치를 수행하는 부분으로 나누어 생각할 수 있다.

2.3.1 스마트 카드 인증 메커니즘에 대한 문제점[3]

- 초기 난수 미 암호화 상태에서 전송 : 난수를 암호화하지 않고 전송하기 때문에 해커가 해당 정

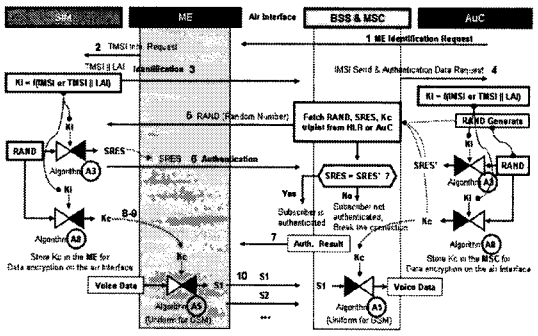

그림 2. SIM 기반 GSM 가입자 인증 및 키 일치 프로토콜

보에 대하여 Brute force, 컷 앤 페이스트(Cut and Paste), 재전송(Replay), 변조(Modification), 위장(Fabrication) 공격 등이 가능하다.

- 한 시점을 기반으로 한 단방향 인증 수행 : 인증 수행 시 한 시점을 기준으로 단 방향 인증 수행으로 스마트 카드 혹은 터미널 장치에 대한 위장 공격이 가능하다.
- 상호인증, 키 일치 및 사용자 인증 단계는 10회를 통하여 수행 : 자원 제한 요소가 큰 스마트 카드 인증 수행 Step 수가 많아 효율성 및 수행속도가 저하된다.

2.3.2 GSM 인증 메커니즘에 대한 문제점[4-8]

- MSC(VLR)/AuC(HLR) 간 인증 데이터 미 보호 : MSC(VLR)/AuC 간 교환 되는 인증 및 세션 키 관련 변수에 대해서 보안 조치가 이루어지고 있지 않기 때문에 이 정보들을 무선 통신상 도청하는 가로채기 공격을 할 경우 시스템의 안전성이 깨지게 된다.
- SIM/ME 간 인터페이스 보안 미 제공 : GSM 인증 메커니즘에는 SIM/ME 간 인터페이스를 제공하지만 보안 메커니즘에 대한 명확한 규격이 없어 재전송 공격(Replay Attack)에 노출되어 있다
- 사용자 인증 시 단방향 인증만을 제공 : BS/MSC 기준의 단 방향 인증만을 제공하기 때문에 해커가 BS로 위장하여 공격하는 방법에 대한 대응 방법이 없다.
- A3, A8, A5 암호 알고리즘의 미공개로 안전성 미검증 : 암호 알고리즘 미 검증으로 안전성 확보가 곤란하고, 시스템 내부 관리자의 정보 유출로 인한 암호 해독이 가능하므로 충분한 안전성 검증이 필요하고 암호 알고리즘 자체의 취약성이 계속 보고되고 있다.
- TMSI를 이용한 가입자 위치정보 보호 곤란 : 잦은 신호 간섭과 다른 시스템의 고장으로 인하여 TMSI의 동기가 깨지면 MS는 자신의 실제 신원인 IMSI를 MSC(VLR)에 평문 형태로 전송해야 하는 문제가 발생하여 해커에게 노출된다.
- GSM과 3GPP 인증 및 키 일치 단계는 10회를 통하여 수행 : 자원 제한 요소가 큰 SIM 기반의 인증 수행 Step 수가 많아 효율성 및 수행속도가 저하된다.

3. 제안된 보안 프로토콜

본 논문에서 제안하는 SIM 카드 기반 보안 취약성을 개선한 고성능 GSM 보안 프로토콜은 스마트 카드 및 GSM 인증 메커니즘의 취약성을 분석하여 보다 효율적인 인증 프로토콜과 3세대 네트워크에서 나타난 문제점도 해결할 수 있는 보안 프로토콜을 설계하였다.

3.1 시스템 개요

SIM 카드 기반 보안 취약성을 개선한 고성능 GSM 보안 프로토콜은 그림 3과 같이 SIM 카드, ME 및 AuC 3부분으로 나누어져 있다. 2세대/2.5세대 및 3세대 네트워크에서 필수적인 보안기능은 인증, 키 일치와 접근제어 기술이다.

인증 기술 설계는 2단계로 나누어 생각할 수 있는데, 1단계는 3DES-ECB/CBC 알고리즘 기반 SIM/ME간에 SIM을 탑재하고 있는 ME 장치 사용자가 SIM 카드를 사용할 수 있는 정당한 권한 가진 사용자를 검증하는 것이고 2단계는 SIM/ME/AuC간에 안전한 통신경로를 형성하기 위한 3DES-ECB/CBC 암호 알고리즘, 3DES-ECB/CBC 기반의 MAC, ReTriDES 알고리즘, 안전한 SMS 및 APDU 통신을 통하여 인증 및 키 일치를 수행한 후 무선 네트워크 상에서 안전하게 데이터를 송수신하는 부분이다.

3.2 보안 프로토콜 설계

제안된 보안 프로토콜은 그림 3과 같이 크게 2단계로 나누어져 수행한다. 1단계는 SIM /ME 간의 SIM 카드 사용자를 인증하는 과정이고, 2단계는 SIM/ME/AuC간 상호인증 및 키 일치를 수행하는 과정이다. SIM/ME/AuC간의 2단계에서 동기화된

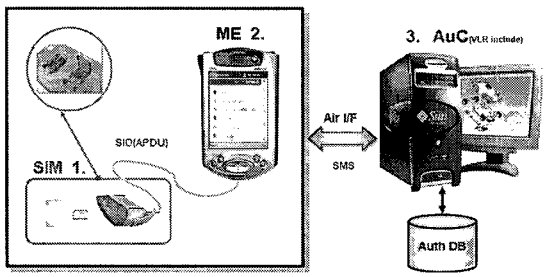

그림 3. 제안된 보안 프로토콜 시스템

세션 키와 안전한 SMS 통신(GSM 03.48/3GPP 23.048)을 사용하여 안전하게 데이터를 송수신한다. 표 1은 제안된 프로토콜에서 사용하는 표기법을 나타낸다.

실제로 2세대와 3세대 네트워크에서는 (U)SIM, ME, BSS, RNC, MSC, VLR, HLR 및 AuC 등의 많은 장치들을 통하여 통신이 이루어지나 본 논문에서는 SIM/ME/AuC 3가지 장치만을 고려하여 보안 프로토콜을 설계하였다.

3.2.1 AuC에서 ME/SIM으로 SecureMessage 전송 방식

ME/AuC간의 무선통신망을 고려하여 안전하게 정보를 송수신하기 위하여 GSM 03.483 이나 3GPP TS 23.048 규격에 명시된 'Implementation for SMS(Secure SMS)'을 기반으로 설계하였고, 모바일 단말기와 SIM 카드 간의 통신은 ISO-7816 APDU (Application Protocol Data Unit) 통신을 기반으로 설계하였다[9].

3.2.2 SIM 사용자 인증 절차 (1단계)

1단계는 ME(GSM 무선단말기) 사용자가 단말기에 탑재되어 있는 SIM 카드를 사용할 권한을 가진 사용자의 정당성을 검증하는 단계로 3DES-ECB/CBC 및 ISO/IEC 9797 페딩방식을 사용하여 설계하였다.

ME는 SIM 카드를 기본적으로 탑재하여 개인정보보호 및 데이터 보호 등의 보안 관련 각종 서비스를 제공하므로, ME를 분실하였거나 도난당한 경우 제 3자가 SIM 기반의 보안서비스를 사용하지 못하도록 하는 SIM 사용자 인증 절차가 필요하다. SIM/ME 간 SIM 사용자 인증은 그림 4와 같은 절차로 수행된다.

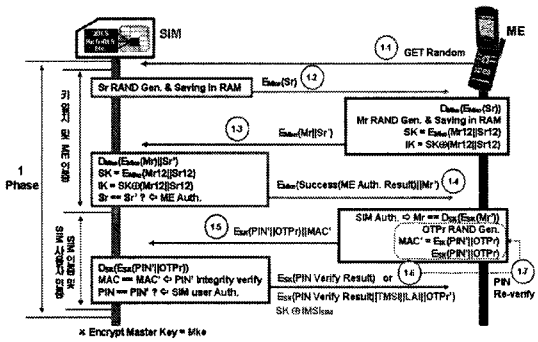

그림 4. SIM/ME간 SIM 사용자 인증 프로토콜

- Step 1-1 (SIM ◀ ME) : 난수 생성을 요청.
- Step 1-2 (SIM ▶ ME) : 난수 Sr를 생성 및 전송.
- Step 1-3 (SIM ◀ ME) : E_{MKE}(Mr), E_{SK}(Sr') 전송.
  - ○ $D_{MK_E}(E_{MK_E}(\mathrm{Sr}))$ 복호화.
  - ○ SK = E_{MK_E}(Mr12 ‖ Sr12) 계산. IK = SK ⊕ (Mr12 ‖ Sr12) 계산.
- Step 1-4 (SIM ▶ ME) : E_{SK}(Success(ME Auth. Result)||Mr')를 전송.
  - ○ $D_{MK_E}(E_{MK_E}(\mathrm{Mr} \| \mathrm{Sr}'))$ 복호화.
  - ○ SK = E_{MK_E}(Mr12 ‖ Sr12) 계산. IK = SK ⊕ (Mr12 ‖ Sr12) 계산.
  - ○ Sr과 $D_{SK}(E_{SK}(\mathrm{Sr}'))$를 비교해서 ME를 인증.
- Step 1-5 (SIM ◀ ME) : E_{SK}(PIN' ‖ OTPr)|| MAC'를 전송.
  - ○ Mr과 $D_{SK}(E_{SK}(\mathrm{Mr}'))$ 비교하여 SIM을 인증.
  - ○ OTPr 생성, 입력된 PIN'이용(E_{SK}(PIN' ‖ OTPr))계산. MAC'=(E_{IK}(PIN' ‖ OTPr))생성.
- Step 1-6 (SIM ▶ ME) : E_{SK}(IMSI or TMSI

표 1. 1, 2단계 인증프로토콜 표기(계수)

표 기	의 미	표 기	의 미
AUTN	인증 토큰	Mke	암호화 마스터 키
IK	무결성 키	Mr	모바일 생성 난수
$IMSI_{AuC}$	AuC 관리 가입자식별번호	OTPr	일회용 패스워드 검증난수
$IMSI_{SIM}$	SIM 관리 가입자식별번호	RAND	AuC 생성 난수
Kc	SIM/AuC 공유 암호 키	RES	SIM 생성 인증정보
Ki	망 식별자	ROP	역 운영자 설정 값
MAC_{AuC}	AuC 네트워크검증코드	SK	세션 키
MAC_{SIM}	SIM 네트워크검증코드	Sr	카드 생성 난수
		XRES	AuC 생성 인증정보

‖ LAI) 전송.

- ○ $D_{SK}(E_{SK}(PIN' \| OTPr))$ 복호화.
- ○ MAC == MAC' 비교 PIN'의 무결성 검증. PIN == PIN'를 비교 SIM 사용자 인증.

• Step 1-7 (SIM ◀ ME) : PIN, OTP 실패한 경우 재인증을 시도.

- ○ E_{SK}(PIN Verify Result||TMSI||LAI||OTPr') 복호화.
- ○ OTPr' == OTPr 비교 패스워드 일회성 검증 성공 시 SK⊕$IMSI_{SIM}$ 정보 메모리 적재.
- ○ PIN 검증 실패 시 3번까지 재인증 허용.

3.2.3 인증 및 키 일치 절차 (2단계)

2단계는 SIM 카드가 탑재되어 있는 ME/AuC간 보안 및 응용 프로그램 등을 유무선 통신 경로상에서 안전하게 전송할 수 있는 보안 경로를 설정하는 단계로 실제로는 많은 장치들 사이에서 이루어지나 구현상 3 장치만을 고려하였다. SIM/AuC에서는 인증 데이터를 생성 및 검증할 수 있는 보안 알고리즘이 필요하다.

(1) ReTriDES 알고리즘

GSM의 암호알고리즘 및 보안 메커니즘이 지닌 문제점을 해결하기 위하여 본 논문은 3DES-ECB/CBC 기반의 알고리즘을 제안한다.

그림 5는 ReTriDES 인증 구조로 이들 함수의 입출력으로 사용되는 값을 3DES-ECB/CBC 알고리즘의 특성을 고려하여 표 2와 같이 설계하였다.

OPC와 ROPC는 아래 수식과 같이 가입자의 비밀키 Ki를 가지고 사업자 의존 코드 값 OP와 ROP (Reverse OP)를 암호화하여 생성한다.

$$OPC = OP \oplus EKi(OP)$$
$$ROPC = ROP \oplus EKi(ROP)$$

여기에서 r1, r2, r3은 고정된 상수로 각각 16, 8, 16번의 자리를 이동하며, ReTriDES의 핵심 함수 E_{Ki}와 E_{ID}에는 3DES-ECB/CBC 암호 알고리즘 및 ISO/IEC 9797(data ‖ n x '00') 패딩 방법을 사용하였다.

(2) AuC/SIM 인증 및 키 정보 생성

AuC는 TMSI||LAI(혹은 $IMSI_{SIM}$) 정보를 수신 받아 AuC에서 관리하는 인증 데이터베이스에서 TMSI와 매핑(Mapping)되는 IMSI를 검색한다. 그림 6은 매핑되는 $IMSI_{AuC}$ 정보를 ReTriDES 알고리즘의 f1 함수 사용하여 Ki, SQN을 생성하고 f0 함수를 사용하여 RAND를 생성한다. 생성된 Ki, SQN, RAND, OP 값을 f2 함수에 사용하여 MAC_{AuC}를 생성하고, f3 함수에 사용하여 XRES 값을 생성하며, f4 함수 세션 키 Kc를 생성한다.

SIM은 RAND ‖ AUTN 정보를 수신 받아 AUNT에 암호화된 정보를 $IMSI_{SIM}$과 XOR 연산으로 SQN ‖ MAC_{AuC}정보를 얻는다. 그림 7은 SIM 카드에서 저장하고 있는 IMSI 정보를 읽어 ReTriDES 알고리즘의 f1 함수를 사용하여 Ki를 생성한다. SIM에서 생성된 Ki, 전송된 SQN과 RAND, SIM의 OP 값을 f2 함수에 사용하여 MAC_{SIM} 값을 생성하고 Ki, RAND, OP 값을 f3 함수를 사용하여 RES 정보를 생성하며, f4 함수에 사용하여 세션 키 Kc를 생성한다.

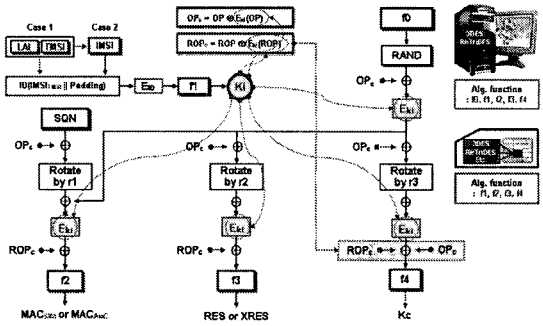

그림 5. 3DES-ECB/CBC 기반 ReTriDES 암호 알고리즘

표 2. ReTriDES 알고리즘 입력 및 출력 값과 길이

함수명	함수 기능	입력 및 길이	출력 및 길이
f0	난수 생성 함수	내부 상태	RAND 64bit(8Byte)
f1	초기 키 유도함수	IMSI or TMSI||LAI 192bit	Ki 192bit(24Byte)
f2	네트워크 인증함수	Ki 192, SQN 64, RAND 64, OP 64bit	$MAC_{AuC/SIM}$ 64bit(8Byte)
f3	사용자 인증 함수	Ki 192, RAND 64, OP 64bit	XRES/RES 64bit(8Byte)
f4	세션 키 유도함수	Ki 192, RAND 64, OP 64bit	Kc 128bit(16Byte)

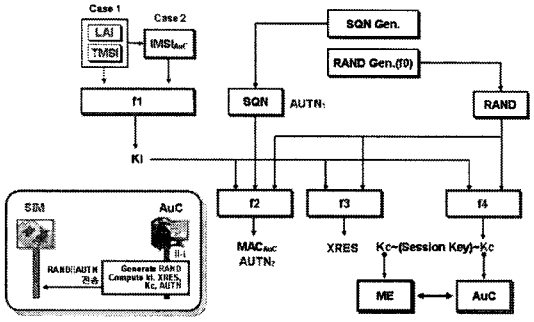

그림 6. AuC에서 인증 및 키 정보 유도 과정

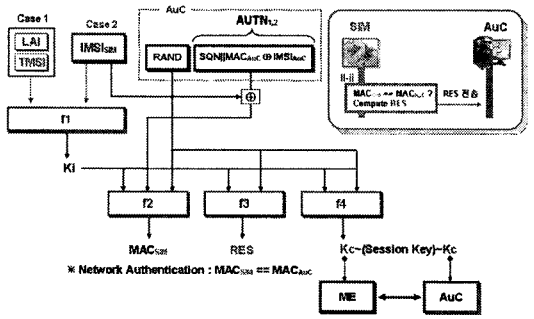

그림 7. SIM에서 인증 및 키 유도 과정

(3) SIM/ME/AuC 간 인증 및 키 일치 절차

SIM/ME/AuC 간의 유무선 통신 경로상에서 다양한 보안 서비스를 제공하므로 유무선 통신상에서 전송되는 정보를 제 3자가 도청, 가로채기, 수정 등의 공격에 대한 대응방법인 인증 및 키 일치 절차가 필요하다. SIM/ME/AuC 간 인증 및 키 일치는 그림 8과 같은 절차로 수행된다.

- Step 2-1 (ME ◀ AuC) : ME 식별 정보 요청.
- Step 2-2 (ME ▶ AuC) : SK⊕IMSI$_{SIM}$ or TMSI 정보 전송.

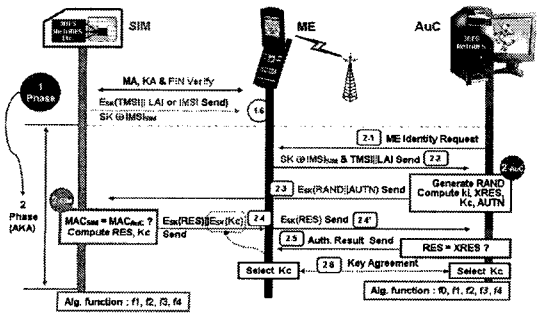

그림 8. SIM/ME/AuC 간 인증 및 키 일치프로토콜

- Step 2-3 (SIM ◀ ME ◀ AuC) : RAND ‖ AUTN 전송.
  - ○ OPc = OPc(ki, OP) 계산.
  - ○ RAND = f0() 함수 사용해서 난수 생성.
  - ○ ki = f1(IMSI, lenIMSI).
  - ○ MAC_{AuC}= f2(ki, RAND, SQN, OPc, ROPc)
  - ○ XRES = f3(ki, RAND, OPc, ROPc).
  - ○ Kc = f4(ki, RAND, OPc, ROPc)
  - ○ AUTN = SQN ‖ MAC_{AuC}.
- Step 2-4 (SIM ▶ ME ▶ AuC) : E_{SK}(RES) 전송.
  - ○ OPc = OPc(ki, OP_{SIM}) 계산.
  - ○ ki = f1($IMSI_{SIM}$, $lenIMSI_{SIM}$).
  - ○ RES = f3(ki, RAND, OPc, ROPc).
  - ○ Kc = f4(ki, RAND, OPc, ROPc)
  - ○ MAC_{SIM}= f2(ki, RAND, SQN, OPc, ROPc)
  - ○ MAC_{SIM}과 MAC_{AuC}비교, 네트워크 검증.
- Step 2-5 (ME ◀ AuC) : 인증 결과 전송.
  - ○ RES와 XRES 비교, 사용자 인증.
- Step 2-6 (ME, AuC) : 암호 키 일치.
  - ○ AuC는 Kc 선택
  - ○ ME는 E_{SK}(Kc)를 복호화 후 Kc 선택

4. 구현 테스트와 안전성 분석

본 논문에서 제안한 보안 프로토콜의 설계를 토대로 구현 테스트와 안전성을 분석하였다. SIM 카드 기반 보안 취약성을 개선한 고성능 GSM 보안 프로토콜은 호스트 환경에서 크게 3부분으로 나누어 구현하였다. 제안한 보안 프로토콜의 안전성은 스마트카드, GSM 표준문서, 3GPP 표준문서 그리고 관련 논문에 제시된 보안 취약성 분석을 토대로 효율적인 대응방법을 제시하였다.

4.1 개발 도구 및 환경

SIM 카드 기반 보안 취약성을 개선한 고성능 GSM 보안 프로토콜 구현 및 실행 환경은 그림 9와 같이 SIM 카드, ME(무선단말기) 및 AuC(인증센터) 각각의 역할에 맞는 자바와 C언어로 구현하였다.

- JDK1.4 이상 : 자바 응용프로그램을 컴파일하여 클래스 파일(.class)을 생성하는 개발 도구이다.

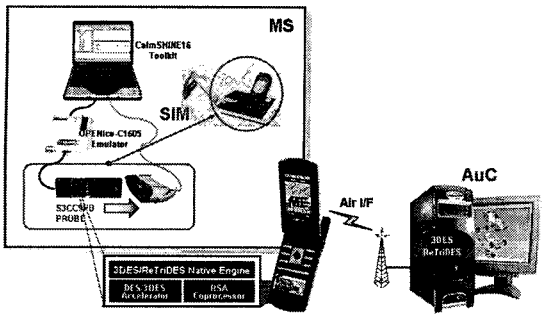

그림 9. SIM/ME/AuC 간 보안 프로토콜 개발 환경

- J2ME Wireless Toolkit 2.2 이상 : 모바일 단말기용 응용 프로그램을 개발하기 위해 SUN 사에서 제공하는 개발 도구이다.
- Visual C/C++ IDE 6.0 이상 : C/C++ 언어를 사용하여 암호 및 통신 모듈의 개발과 테스트를 위해 사용한 마이크로소프트사에서 제공하는 통합 개발 툴이다.
- CalmSHINE16 Toolkit : OPENice-C1600 Emulator는 CalmRISC16 Core를 개발하기 위한 통합 개발 툴이다.
- OPENice-C1605 Emulator : CamlRISC16 용 Emulator로서 고급 디버깅 기능을 지원하는 디바이스이다.
- S3CC9PB PROBE : 에뮬레이터와 특정 디바이스를 사용하는 타켓 시스템을 연결시켜주는 역할을 함으로써 노이즈 (Noise) 없이 프로그램 수행 및 디버깅이 용이한 디바이스이다.

4.2 인증 및 키 일치 테스트

제안한 보안 프로토콜은 크게 SIM Emulator, 모바일 단말기 ME 및 인증센터 AuC 부분으로 나누어져있다.

SIM Emulator는 1단계에서 ME와 상호인증, 암호 및 무결성 키 일치를 통하여 안전한 통신 경로를 설정하여 ME에서 입력한 PIN을 검증하는 역할을 수행하고, 2단계에서는 ME, AuC간 네트워크 검증, 가입자 인증 및 세션 키 정보를 생성하는 역할을 수행한다.

그림 10은 1단계에서 SIM/ME간 상호인증, 키 일치 및 PIN 검증을 통하여 SIM 사용자 인증 수행을 성공시키는 화면이고, 2단계는 SIM 카드가 발급되어 ME에 탑재된 상태에서 ReTriDES 암호 알고리즘을 통하여 SIM/ME/AuC간 인증 및 키 일치(Kc)를 수행한 후 AuC에서 암호 키 Kc를 이용해서 애플릿을 암호화하여 ME를 경유해서 SIM으로 다운로드(Post-Issuance)하기위한 화면이다.

4.3 기존 기술과의 제안 기술의 비교 분석

기존 스마트 카드, SIM 카드 기반의 GSM 및 3GPP 인증 메커니즘에는 여러 가지 보안 취약성이 존재한다. 표 3, 4는 기존 인증 방법 및 절차의 취약성

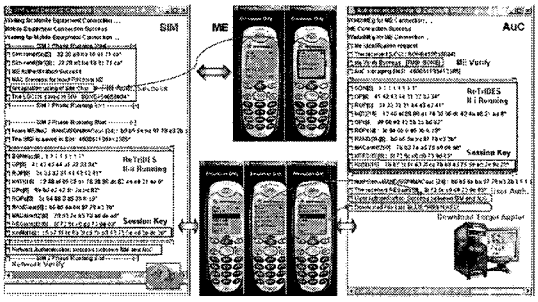

그림 10. SIM/ME/AuC 간 1, 2단계 인증 및 키 일치 수행 화면

표 3. 1단계 SIM과 ME 간의 보안취약성 및 대응방법 비교분석

구 분	스마트 카드 인증 방식 취약성	본 논문의 제안기술의 대응방법	비고
기밀성	초기 난수를 암호화 하지 않은 상태로 전송 신뢰할 수 없는 세션키 생성	MKE을 사용하여 초기 난수 보호 신뢰할 수 있는 세션키 생성	GSM 3GPP
인증방식	한 시점을 기반으로 한 단방향 인증만 수행	시도-응답기반 상호인증을 통시에 수행	GSM
인증 및 키 일치 수행 단계	상호 인증 및 키 일치 PIN검증 Step 수가 10회	상호인증, 키 일치 및 OTP PIN 검증 Step 수가 6회	GSM 3GPP
일회용패스워드	일회용패스워드 검증 모듈을 지원하지 않음	일회용패스워드 검증 모듈을 지원	GSM 3GPP

표 4. 2단계 SIM, ME 및 AuC 간의보안 취약성 및 대응방법 비교분석

구 분	SIM 카드 기반 GSM 인증 방식 취약성	본 논문의 제안기술의 대응방법	비고
암호알고리즘 제공 방식	A3, A8, A5 암호알고리즘을 공개하지 않은 정책으로 암호 알고리즘에 대한검증 필요	국제적으로 검증된 3DES 암호를 사용 안전한 ReTriDES 알고리즘 지원	GSM
인증방식	사용자 인증시 단방향 인증	ReTriDES 기반 상호인증 지원	GSM
SIM/ME/AuC 데이터 전송	SIM/ME/AuC간 인증 데이터가 해킹에 노출	1단계에서 SK 사용한 인증 데이터의 안전한 전송 지원	GSM 3GPP
인증 및 키 일치 수행 단계	인증 및 키 일치 수행완료 단계 수가 10 Step	인증 및 키 일치 수행 완료가 6 Step으로 단축	GSM 3GPP

과 본 논문에서 제안한 방식의 효율성 및 대응방법을 비교 분석한 자료이다.

4.4 제안 방식에 대한 성능 분석

기존 Smart Card, GSM및 3GPP 인증 방식의 성능을 분석할 경우 핵심은 H/W적으로 사양이 가장 떨어지는 (U)SIM 카드의 성능과 (U)SIM 카드에 탑재되어 있는 암호 보조프로세서 및 암호 가속기의 성능에 좌우된다. 표 5의 3.5MHz의 H/W의 성능을 가진 Smart Card의 성능을 토대로 제안한 1, 2단계 인증 메커니즘0의 성능을 분석하였다.

(1) 제안한 SIM/ME 간 SIM 사용자 인증 프로토콜 성능분석

Enc/Dec 사용횟수, Data 전송횟수, 난수 RAND 생성 횟수 등을 고려하여 기존 Smart Card 방식과 제안한 방식(1단계)에 대한 총 수행 시간과 성능 향상 비율을 표 6과 같이 분석하였다.

표 5에서 분석한 자료를 토대로 기존 Smart Card 인증 방식과제안한 SIM 사용자 인증 방식(1단계)에 총 수행 시간과 성능 비율을 그림 11과 같이 그래프로 효율성을 분석하였다.

표 5. 3.5MHz의 Smart Card경우 정보처리 속도

구분	대상	속도(ms)
암호 Alg. 계산속도	3DES Accelerator	0.24
데이터 전송 속도	스마트 카드와 터미널 사이	28.75
데이터 생성 속도	난수 생성	0.08

표 6. Smart Card와 제안방식(1단계)의 정보처리 성능

구 분	기존 Smart Card	제안방식 (1단계)
Enc/Dec 사용 횟수	12	13
Data 전송 횟수	5	3
RAND 생성 횟수	2	2
총 수행 시간(ms)	146.79	89.53
성능향상 비율(%)	0	39.01

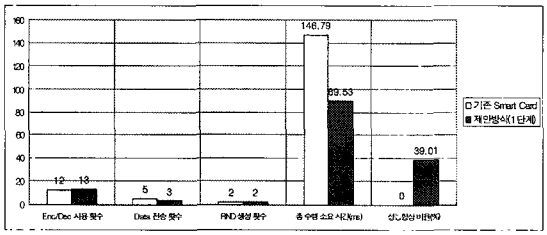

그림 11. 스마트 카드와 제안방식 성능 비교(1단계)

Enc/Dec 사용횟수, Data 전송횟수, 난수 RAND 생성 횟수 등을 고려하여 기존 GSM/3GPP 방식과 제안 방식(1단계)에 대한 오버헤드 비율(Overhead Rate)을 1단계 전체와 1단계의 PIN 검증 시 점으로 나누어 표 7과 같이 분석하였다.

(2) 제안한 SIM/ME/AuC 간 AKA 프로토콜 성능 분석

Enc/Dec 사용횟수, 추가 Data 전송횟수, 등을 고려하여 기존 GSM/3GPP AKA 방식과 제안한AKA 방식(2단계)에 대한 성능향상 비율을 표 8과 같이 분석하였다.

표 7. GSM/3GPP에 대한 제안방식의 오버헤드 비율

구 분	속도(ms) 오버헤드 비율(%)
기존 GSM/3GPP PIN 검증 소요시간	28.75 ms
제안방식의 PIN 검증 시점의 소요시간	29.47 ms
제안방식의 1단계 전체 소요시간	89.53 ms
기존 GSM/3GPP방식에 대한 제안방식의 오버헤드 비율 (1단계 전체)	67.89 %
기존 GSM/3GPP방식에 대한 제안방식의 오버헤드 비율 (1단계 PIN 검증)	2.44 %

표 8. GSM/3GPP와 제안방식(2단계)의 정보처리 성능

구분	기존 GSM/3GPP 방식	제안방식
Enc/Dec 사용 횟수	0	6
추가 Data 전송 횟수	2	0
Enc, Dec 및 전송 총 소요시간(ms)	57.50	1.44
성능향상 비율(%)	0	97.50

표 7에서 분석한 자료를 토대로 기존 GSM/3GPP AKA 방식과 제안한AKA 방식(2단계)에 대한 Enc/Dec 사용횟수, 추가 Data 전송횟수의 총 수행 소요시간 및 성능향상 비율을 그림 12와 같이 그래프로 분석 하였다.

5. 결론 및 연구결과의 활용방안

현재 유럽 중심의 GSM을 이용한 안전한 데이터 통신을 위한 보안 알고리즘 및 프로토콜에 대한 문제점이 여러 번 지적되고 있어 보안 메커니즘에 표준 문서를 개정하고 있으며 필요한 보안 메커니즘을 3GPP 표준 문서에도 적용하고 있다.

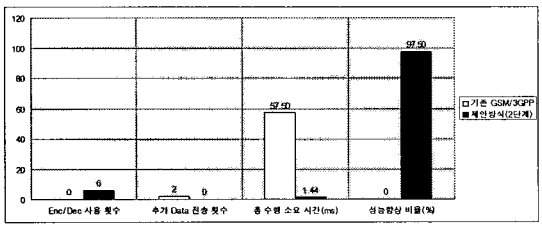

그림 12. GSM/3GPP와 제안방식 성능 비교(2단계)

본 논문에서는 SIM 카드와 동일한 역할을 수행하는 하드웨어 조건인 SIM Emulator 환경에서 GSM 표준 문서, 3GPP 표준 문서 및 관련 논문을 통하여 SIM 기반 GSM 인증 메커니즘을 연구하였고, 국제 표준 암호알고리즘인 3DES-ECB/CBC 모드, MAC, 새로운ReTriDES 알고리즘, ISO 9797 페딩방식을 사용하여 1단계의 GSM 뿐만 아니라 3GPP 인증 메커니즘에 명확하게 표기되지 않은 SIM 사용자 인증의 취약성과 2단계의 SIM 기반 GSM 인증 및 키 일치 메커니즘에 대한 취약성 분석을 토대로 USIM 기반의 3GPP 인증 및 키 일치 메커니즘에 나타난 취약성도 부분 해결할 수 있는 효율적인 보안 프로토콜을 설계 및 구현하였다.

SIM/ME 간 SIM 사용자 인증 기술은 기존 GSM과 3GPP 방식의 표준문서에 안전한 카드 인증 방식을 제공하고 있지 않으므로 스마트 카드 인증 방식을 비교 분석하여 안전한 상호인증 및 키 일치와 One-Time PIN 검증 기능 구현으로 안전성이 강화되었고 인증 단계를 10회에서 6회로 단축하여 처리 속도를 39% 향상시켰다. SIM/ME/AuC 간 인증 및 키 일치 프로토콜은 기존 GSM/3GPP 방식의 인증 데이터 노출 문제를 해결하여 안전성을 보장하였으며, 인증 단계를 10회에서 6회로 단축시켜 처리 속도가 97.5% 향상되었다.

앞으로 접촉식(Contact) 및 비접촉식(Contactless) (U)SIM 카드가 모두 탑재되어 보안 서비스를 제공할 수 있는 모바일 단말기를 고려하여 (U)SIM 카드 설계 및 통신 프로토콜 연구를 통하여 원격지에서 안전하게 홈 네트워크 장비를 제어, 출입통제 및 가전제품 제어를 모두 지원할 수 있는 지능형 홈 인증 플랫폼과 유비쿼터스 컴퓨팅 환경에서 적용 가능한 효율적인 보안 프로토콜에 대한 연구와 개발이 필요하다.

참 고 문 헌

[1] Young Seol Son and Dong Hoon Lee, "The Key Management System using the Secret

Sharing Scheme Applicable to Smart Card," *KIPS Transaction*, Vol. 11-C, No. 5, pp. 373-378, 2004.

[2] Uwe Hansmann, Martin S.Nicklous, Thomas Schäck, Achim Schneider, and Fank Seliger, "Smart Card Application Development Using Java(Second Edition)," *Springer*, pp. 51-67, 2002.

[3] Wolfgang Rankl and Wolfganf Effing, "Smart Card Handbook(Third Edition)," *WILEY*, pp. 735-802, 2003.

[4] Paulo S. Pagliusi, "A Contemporary Foreword on GSM Security," InfraSec 2002, *LNCS 2437*, pp. 129-144, 2002.

[5] Young Jae Choi and Soon Ja Kim, "An Improvement on Privacy and Authentication in GSM," WISA 2004, *LNCS 3325*, pp. 14-26, 2004.

[6] Jesudoss Venkatra, Vijay Raghavan, Debabrata Das, and Asoke K. Talukder, "Trust and Security Realization for Mobile Users in GSM Cellular Networks," AACC 2004, *LNCS 3285*, pp. 302-309, 2004.

[7] Keon-woo Kim, Bae-eun Jung, Ku-young Chang, and Heui-su Ryu, "A study on the authentication mechanism of WCDMA IMT-2000 system," *KIISC*, Vol. 11, No. 6, pp. 53-65, 2001.

[8] 박창섭, "암호이론과 보안," 대영사, pp. 361-383, 2002.

[9] 박미옥, 김상근, "강력한 개체인증 특성을 가지는 GSM 사용자 인증 프로토콜," 한국멀티미디어 학회지, 9권, 제10호, pp. 1314-1321, 2006.

김 희 정

2006년 경남대학교 컴퓨터공학부 졸업(공학사)
2006년~현재 경남대학교 대학원 컴퓨터 공학부 석사과정
관심분야 : 정보보안, 스마트 카드

전 하 용

2003년 경남대학교 정보통신공학부 졸업(공학사)
2005년 경남대학교 대학원 컴퓨터공학부 졸업(공학석사)
2007년 경남대학교 대학원 컴퓨터공학부 박사 수료
관심분야 : 정보보호, 자바카드, 인증 프로토콜

이 주 화

1996년 경일대학교 컴퓨터공학과(공학사)
2000년 경남대학교 대학원 컴퓨터공학과(공학석사)
2007년 경남대학교 대학원 컴퓨터공학과(공학박사)
2000년 7월~2002년 8월 (주)데이타게이트인터내셔널 부설 보안기술연구소 주임연구원
2004년 3월~2006년 4월 경남대학교 컴퓨터공학부 강의전담교수
2006년 5월~2007년 1월 (주)디지탈홈네트 기술연구소 책임연구원
관심분야 : 암호학, 정보보안, SIM/USIM/R-UIM 보안, 모바일 보안, 유비쿼터스 보안

정 민 수

1986년 서울 대학교 컴퓨터공학과(공학사)
1988년 한국과학기술원 전산학과 (공학석사)
1994년 한국과학기술원 전산학과 (공학박사)
1990년~현재 경남대학교 교수
관심분야 : 자바기술, 홈네트워킹, 이동단말기 프로그래밍, USIM기술