자바카드 기반 무선단말기용 보안 프로토콜 연구

황철준°, 이주화, 정민수
경남대학교 컴퓨터공학과

A Study of Security Protocol for Wireless Devices based on Java Card

CheulJun Hwang, JuHwa Lee, MinSoo Jung
Dept. of Computer Engineering, Kyungnam University

요 약

자바카드는 스마트카드와 같은 작은 메모리를 가진 임베디드 장치를 위한 프로그램으로 국제 표준인 ISO-7816 과 산업 표준인 EMV 와 호환되며, 무선단말기 보안 표준화를 진행하고 있다. 그러나, 기존 3GPP 의 인증 및 키 일치 프로토콜에는 해킹에 대한 취약성이 존재한다. 그래서 본 논문에서는 표준 3GPP 보안 메커니즘의 취약성을 방지 및 극복할 수 있는 자바카드 기반 무선단말기용(IMT-2000) 보안 프로토콜에 대하여 연구하였다. 이 기술은 무선상거래, 무선 보안, 전자지불시스템, 모바일 인터넷, 위치추적 서비스 그리고 유비쿼터스 컴퓨팅 환경 등에 널리 사용 될 수 있다.

1. 서론

IMT2000 은 제 3 세대 이동통신서비스로 전세계적으로 표준화 및 동일 주파수를 활용하여 세계적인 로밍이되고 무선 인터넷과 같은 다양한 데이터 통신과 무선상 거래가 가능하다. 이와 같이 IMT2000에서 제공하는 다양한 부가 서비스를 제공 받기 위해서는 가입자 인증과 결재 방식이 필요하다. 이에 따라 ETSI나 3GPP/3GPP2 같은 표준화 기구들은 UICC/USIM을 IMT-2000의 UIM(User Identification Module) 표준 규격으로 정하였다.

기존 3GPP 네트워크 표준 문서에는 보안에 대한 취약성이 내포되어 있다. 그래서 본 연구진은 이 보안 취약성을 분석하고, 이 취약성을 개선하기 위하여 표준화된 보안 기술을 적용함으로써 보다 효율적인 무선단말기용(IMT-2000) 보안 프로토콜을 연구하고자 한다.

2. 관련연구

2.1 자바카드

자바카드란 스마트카드 기술을 기반으로 하여 자바의 기술을 접목시킨 것으로 COS(Card Operating System) 위에 JCVM(Java Card Virtual Machine)이 랩핑(Wrapping)되어 있는 구조의 IC 카드를 말한다.

자바카드는 스마트카드 기술에 자바의 기술을 접목 시켰기 때문에 플랫폼 독립성, 복수의 응용프로그램, 응용프로그램의 갱신, 융통성, 호환성 등의 특징들을 제공한다.

2.2 자바카드 애플릿

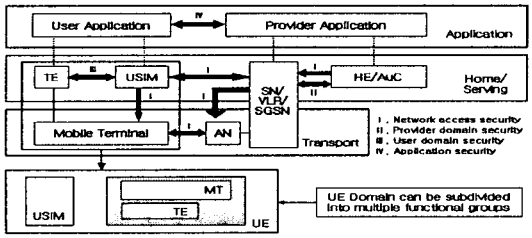
자바카드 애플릿은 자바카드 상에서 실행될 수 있는 자바 프로그램이다. 자바 응용프로그램과 달리 애플릿은 카드의 ROM에 설치될 필요가 없고, 단지 카드상에 다운로드 함으로써 사용이 가능하게 된다. 자바카드 애플릿의 특징은 다음과 같다.

- 자바카드 런타임 환경에서 수행
- APDU(Application Program Data Unit) 교환을 통해 JCRE(Java Card Run-time Environment)와 통신
- AID(Application IDentifier)에 의해 식별
- 자바카드상에 동적으로 다운로드

3. 3GPP 보안

3.1 3GPP 보안 구조

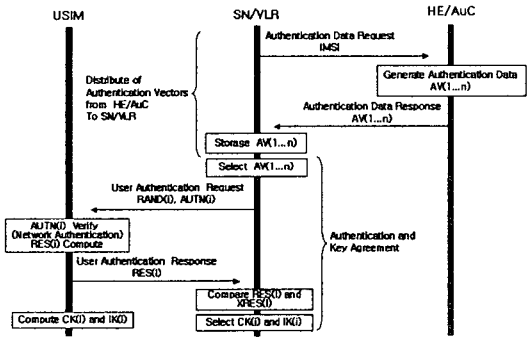
IMT-2000같은 무선단말기에서 보안 기능을 제공하기 위한 3G 보안 구조는 그림 1 과 같다. 그림 1 에는 5 가지의 보안 관련(네트워크 접근 보안, 네트워크 도메인 보안, 사용자 도메인 보안, 응용 도메인 보안 및 보안의 가시성과 구성) 정보를 정의하고 있으며, 각각의 부분은 다음과 같다.



[그림 1] 3GPP 보안 구조

3.2 3GPP 인증 메커니즘

3GPP 인증 메커니즘은 그림 2 와 같이 가입자와 네트워크 사이의 상호인증을 실시하며, 각각 USIM과 AuC가 공유한 비밀키의 지식을 보유함으로써 이루어진다.



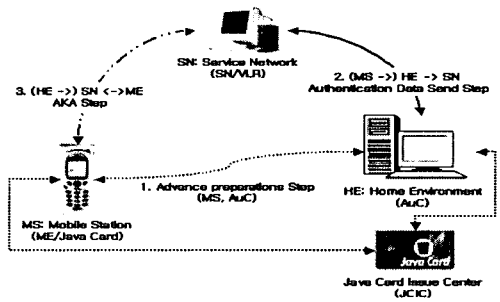
[그림 2] 3GPP 보안 메커니즘

4. 구현 및 고찰

본 논문에서 제안하는 자바카드 기반 무선단말기용 인증 및 키 일치 프로토콜은 정보보호 모델의 설계(세션 키 설정 및 가입자 인증)와 각 프로토콜별 사용되는 표준화된 암호 알고리즘 및 3GPP/3GPP2의 안전한 수행절차 그리고 SSL(Secure Socket Layer) 매커니즘을 사용하여 설계 및 구현하였다.

4.1 시스템의 개요

자바카드 기반 무선통신용 인증 및 키 일치 시스템은 그림 3 과 같이 크게 4 부분(AuC, SN, ME/JavaCard 및 JCIC)으로 나누어져 있다.



[그림 3] 제안된 보안 시스템 전체 구성도

4.2 보안 프로토콜 설계

제안된 보안 프로토콜은 크게 3 부분으로 나누어져 있다. 첫째는 서버에서 SN으로 안전한 보안 프로토콜을 이용하여 인증 속성정보를 전송하는 프로토콜이고 SN과 ME 사이에 3GPP의 SMS 패킷을 이용하여 안전하게 정보를 전송하는 방식이며, 그리고 마지막으로 인증서버와 자바카드간 키 일치 및 사용자 인증하는 프로토콜이다. 표1은 본 프로토콜에 사용되는 계수를 나타낸다.

표1. 인증 및 키 일치 프로토콜 계수

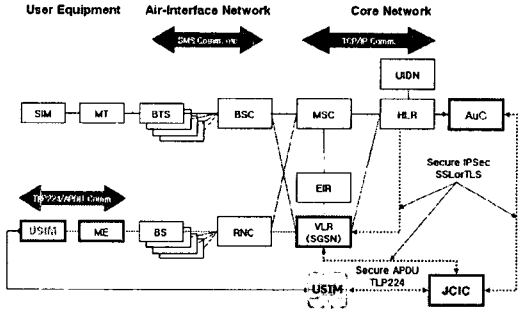
계 수	의 미	계 수	의 미
||	연접	MAC	메시지인증코드
⊕	XOR	MacKey	AuC/JC공유무결성키
AD	인증 데이터	RES	JC 생성 인증정보
AK	익명성 키	SALT	사용자별 인증속성값
AUC_RAND	AuC 생성 난수	SK	AuC/JC 공유 세션키
AUTN	인증토큰	SQN	순차번호
CAF	인증실패횟수	SN_RAND	SN 생성 난수
IMSI	이동가입자식별번호	TMSI	임시가입자식별번호
K	AuC/JC초기공유키	XRES	AuC생성 인증정보

4.2.1 SN과 자바카드간 안전한 메시지 전송방식

무선통신망(SN[AuC]에서 MS간의 통신)에서 안전하게 정보를 송수신 위해서 3GPP TS 23.048에 명시된 "Implementation for SMS"을 기반으로 설계하였으며, 단말기와 자바카드 간은 APDU 통신은 ISO7816을 기반으로 설계하였다.

4.2.2 자바카드 발급센터

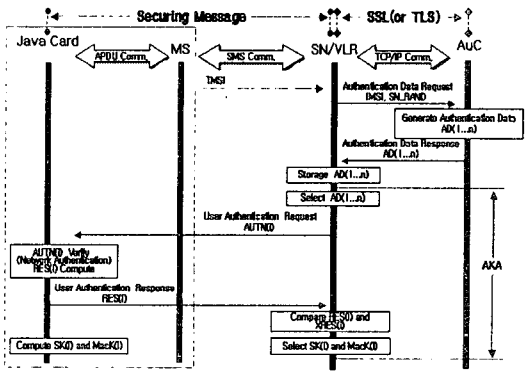
자바카드 발급센터(JCIC; Java Card Issuance Center)는 그림 4 와 같이 3 가지 시스템(AuC, SN, USIM[or Java Card])에서 보유해야 하는 정보를 생성하여 동일한 시간에 분배한다.



[그림 4] JCIC 인증 인자 분배 구성도

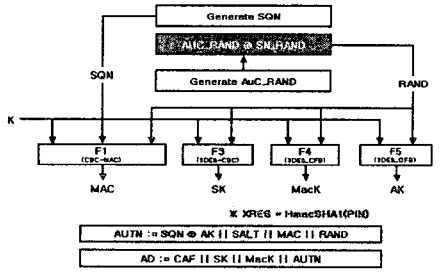
4.2.3 인증 및 키 일치 수행 절차

자바카드기반 무선단말기용 인증 및 키 일치 수행절차는 그림 5 와 같이 유무선 통신상에서 2 가지 보안 메커니즘 즉, 안전한 메시지(Secure Message)와 안전한 소켓(Secure Socket Layer)의해 보호되어 동작한다.



[그림 5] 인증 및 키 일치 수행 절차

Step 1 : SN -> AuC 에게 인증 데이터를 요구(SSL)



[AuC 의 인증벡터 구성요소]

Step 2 : AuC 는 MS 인증 인자를 생성(SSL)

- MAC(i)=f1{K(i):SQN(i):RAND(i)}
- SK(i)=f3{K(i):RAND(i)}
- MacK(i)=f4{K(i):RAND(i)}
- AK(i)=f5{K(i):RAND(i)}
- AUTN=[SQN(i)⊕AK(i)|SALT(i)|MAC(i)|RAND(i)]
- XRES=HmacSHA1(PIN_i)

Step 3 : AuC-> SN 로 생성한 인증 데이터 전달(SSL)

- Secure SMS Type : AUTN(i), XRES(i)
- General Type : SK(i), MacK(i), CAF(i)

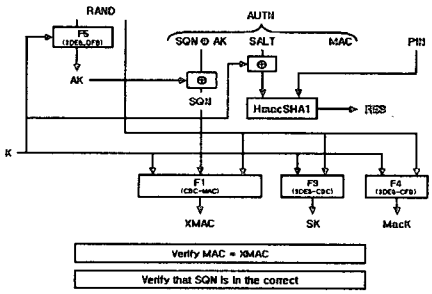
Step 4 : SN 은 인증인자를 자신의 DB 에 저장(SSL)

Step 5 : SN -> MS 로 n 개의 인증토큰 중에서 하나를 선택하여 MS 에게 전달(SM)

- Secure SMS Type : AUTN(i)

Step 6 : MS 은 인증토큰으로부터 XRES(i)를 계산(SM)

- AK(i)=f5{K(i):RAND(i)}
- XMAC(i)=f1{K(i):SQN(i)[(SQN⊕AK)⊕AK]:RAND(i)}
- SK(i)=f3{K(i):RAND(i)}
- MacK(i)=f4{K(i):RAND(i)}
- RES(i)=HmacSHA1([SALT⊕K],PIN_i)



[자바카드내에서 인증 및 키 일치 수행절차]

Step 7 : MS 는 RES(i)를 SN 으로 전송(SM)

- Secure SMS Type : RES(i)

Step 8 : SN 은 RES(i)와 XRES(i) 동일성 검증(SSL)

- ifRES(i)=XRES(i), Step 9 Execution
- ifRES(i)=XRES(i), CAF++ {ifCAF<=5, 반복 else 계정차단}

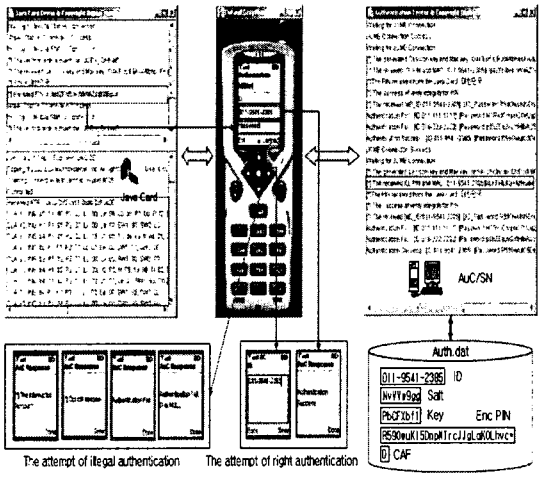
Step 9 : SN 은 SK(i)와 MacK(i)를 선택하여 안전하게 응용서비스를 지원한다.

5. 테스트 결과 및 분석

자바카드 기반 무선단말기용 인증 및 키 일치 시스템은 호스트 환경에서 크게 3 부분으로 나누어 구현하였다. 또한, 이 설계 기술은 기존 3GPP 표준 문서에 제시하는 보안에 대한 취약성을 방지하는 대안을 제시하고 있다.

5.1 사용자 인증 테스트

제안된 보안 프로토콜은 크게 AuC(SN)와 ME 및 Java Card[USIM]로 나누어져 있다. 그림 6 은 AuC와 Java Card 사이에 효율적인 사용자 인증 과정을 수행하는 화면이다.



[그림 6] AuC와 자바카드간 인증 수행화면

5.2 기존 인증 방식에 대한 취약성과 대응방안

3GPP에 대한 표준 문서에 나타난 인증 방식에 취약성이 존재한다. 표2는 기존 3GPP 인증 방식과 제안 방식을 비교 분석한 자료이다.

표 2. 3GPP 보안 취약성 및 대응방안

구 분	기존 3GPP 표준 문서 내의 취약성	본 제안기술의 대응 방안
SQN 동기화 과정 취약성	SQN 동기화 과정에서 도청공격 가능	- MS<-> SN : Secure SMS - SN <-> AuC : SSL(도청 방지)
인증벡터 재사용 불가능	AV(SN/MS) 재사용 불가능	CAF 기능 사용으로 인증실패 허용 횟수 만큼 AV 재사용가능
SN과 AuC 사이의 취약성	SN과 AuC 사이 신뢰할 수 있는 안전한 채널이 존재 하지 않음	SN과 AuC 간에 신뢰할 수 있는 안전한 통신 채널 제공 : SSL(위장공격 방지)

기본 3GPP 인증방식에 존재하는 취약성을 개선하는데 요구되는 보안 요구사항 및 대응기술은 아래와 같다.

- SN 과 AuC 인증 인자를 안전하게 보관 : SN 과 AuC 인증 인자 정보를 저장하고 있는 DB 암호화
- 비밀키 안전한 공유 : JCIC로 사전에 안전하게 공유
- SN과 AuC 안전한 통신 채널 필요 : SSL 지원으로 SN과 AuC간 신뢰성 확보

6. 결론 및 연구결과의 활용 방안

본 논문에서는 USIM 카드가 탑재 가능한 무선단말기에 인증 시스템을 구현하기 위하여 자바카드 기술과 표준화된 안전한 보안 메커니즘들을 이용한 보다 효율적인 사용자 인증 방식을 제안하였다.

본 기술은 무선보안, 무선상거래, 무선 전자지불시스템, 전자화폐, 모바일 인터넷, 위치추적 서비스 등에 활용할 수 있다. 향후 모바일, 자바카드 및 USIM 카드의 하드웨어 제약성이 극복될 것이 예상되기 때문에 자바카드 기반으로 모든 움직이는 매체에 컴퓨터 기술을 적용하는 유비쿼터스 컴퓨팅 보안 기술에 대한 연구가 필요하다.

[참고문헌]

[1] 김충남, 이성준, 최호규, 신상욱 외 10 명 "IMT-2000 이동통신 표준화에 대한 조사", TTA, 2002.

[2] 김성준, 이희규, 조한진, 이재광, "자바카드 상에서의 공개키 암호화를 위한 클래스의 설계와 구현", 한국정보처리학회, VOL. 9-C, NO 2, pp163 ~172, 2002.

[3] 3GPP TS 33.102, "3rd Generation Partnership Project(3GPP) ; Technical Specification Group Services and System Aspects ; 3G Security security Architecture."

[4] 3GPP TS 22.022, "3rd Generation Partnership Project(3GPP) ; Technical Specification Group Services and System Aspects ; Personalisation of UMTS Mobile Equipment(ME) ;Mobile functionality specification"

[5] 3GPP TS 33.103, "3rd Generation Partnership Project(3GPP) ; Technical Specification Group Services and System Aspects ;3G security ; integration Guidelines."

[6] 3GPP TS 33.105, "3rd Generation Partnership Project(3GPP) ; Technical Specification Group Services and System Aspects ; 3G security ; Cryptographic Algorithm Requirements."

[7] 3GPP TS 33.120, "3rd Generation Partnership Project(3GPP) ; Technical Specification Group Services and System Aspects ; 3G security ; Security Principles and Objectives."

[8] 이동규, 이임영, "IMT-2000에서 컨텐츠 서비스를 위한 보안 프로토콜", 한국정보처리학회, VOL. 10-C, NO 2, pp241 ~252, 2003.

[9] Uwe Hansmann and Thomas Schäk, etc"Smart Card Application Development Using Java, Springer, pp49 ~ 65, 2002.