무선 인터넷환경의 USIM 인증취약성과 보안메커니즘

송 유 진*　　이 재 용*

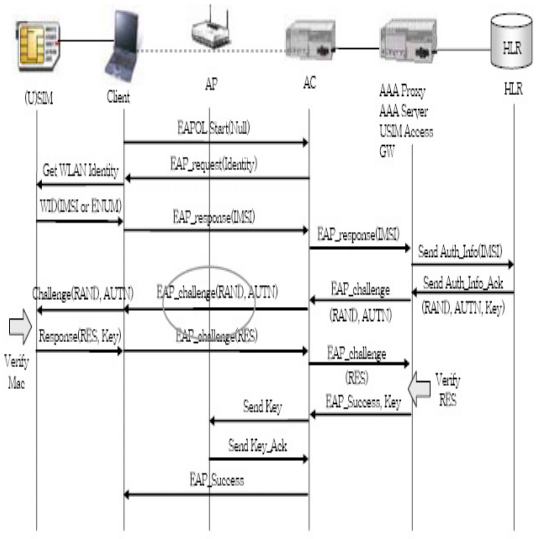
◈ 목 차 ◈

1. 서　론

최근 USIM 칩이 내장돼 있는 3세대 서비스 가입자가 증가하고, 3G USIM 뱅킹이 표준화되면 개인 모바일뱅킹이 활성화 될 것이다. 금융결제원의 발표에 따르면 은행들은 2008년 10월 말부터 표준화된 USIM 뱅킹을 단계적으로 상용화한다. 현재의 USIM 칩은 144KB 칩이지만 앞으로 대용량의 칩이 개발되면 한 곳만의 은행정보가 아닌 여러 은행의 금융정보와 컨텐츠를 넣을 수 있게 될 것이다. 이에 USIM 뱅킹 관련 소프트웨어 및 시스템 개발과 그에 따른 USIM의 보안에 관한 연구의 필요성이 대두되고 있다.

2. USIM 인증

무선 인터넷 환경에서의 USIM의 인증과정은 USIM에서 IMSI(International Mobile Subscriber Identity)의 정보를 AuC(Authentication Center)에 보내어 AuC가 그에 상응하는 Subscriber Authentication Key 값을 선택한 후 난수를 생성한다. AuC는 A3 알고리즘을 이용해 Ciphering Key와 Result를 생성시킨 후, Result는 MSC(Mobile Switching Center)/VLR(Visited Location Register)에, 난수는 MS에 각각 보낸다.



(그림 1) USIM 인증체계

난수를 받은 MS의 USIM카드는 미리 분배한 키와 A3 알고리즘을 사용하여 Ciphering Key와 Result를 생성한 뒤, 이를 MSC/VLR로 보내 HLR(Home Location Register)/ AuC에서 만들어진 Result와 비교해 동일하면 인증에 성공하게 된다. 이와 같은 인증절차가 끝나면 USIM카드의 LOCI에 TMSI(Temporary IMSI)와 위치정보가 저장된다.

* 한서대학교 인터넷공학과

3. 무선인터넷 환경의 인증 메커니즘

3.1 PKMv1 인증메커니즘

PKMv1은 단말이 망에 접속하기 위해 자신의 MAC 주소와 RSA기반 공개키가 결합된 X.509 인증서를 사용한다.

인증과 키 교환절차는 단말이 X.509 인증서를 Base Station에 보내 인증을 요청하고, Base Station은 인증서를 기반으로 단말을 인증한다. Base Station은 인증키(Authorization Key)를 생성한 후 단말의 공개키로 암호화해 단말에 전송한다.

단말은 자신의 비밀키로 복호화해 인증키를 얻게 된다. 단말과 Base Station은 공유하고 있는 인증키로부터 각각 KEK(Key Encryption Key)와 무결성 검사키를 생성한다.

단말은 데이터 암호화키(Traffic Encryption Key)를 Base Station에 요청, Base Station은 데이터 암호화키를 KEK로 암호화해 단말에 분배한다. 이후 사용자의 트래픽은 TEK로 암호화해 단말과 기지국간에 안전하게 전달된다.

PKMv1에서는 기지국이 단말을 인증하지만 단말이 기지국을 인증하지 않는 단방향인증 방식을 사용한다. 만약 악의적인 공격자가 False Base Station을 공격한다면 Base Station으로 위장할 수도 있다. 이때 정상적인 단말이 접속요청을 하면 공격자가 생성한 임의의 인증키를 단말에 주고 단말은 공격자를 통해 인터넷을 사용하게 된다. 이렇게 되면 공격자는 단말의 모든 트래픽을 도청하거나 데이터를 위변조 할 수 있다.

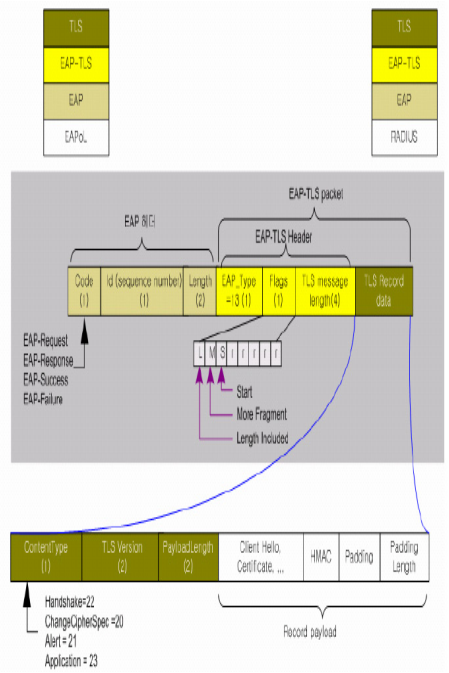
3.2 PKMv2 인증메커니즘

PKMv2는 PKMv1의 단점인 단방향 인증을 단말이 기지국을 인증하고 기지국이 단말을 인증하는 양방향 인증방식으로 개선되어 공격자가 False Base Station으로 위장하는 것을 막을 수 있다.

(표 1) PKMv1과 PKMv2

인증 메커니즘	PKMv1	PKMv2
속 성	단방향	양방향
인 증	RSA 기반	RSA 기반, EAP 기반
내 용	단말인증	단말, 사용자 인증
키	MS의 공개키로 암호화하고 인증키 분배	RSA : Pre-PAK를 MS의 공개키로 암호화하여 전송 EAP : AAA-Key를 인증서버가 BS에게 전송
데이터 암호화	DES	DES-CBC, 3DES, RSA AES-CCM /CBC /CTR

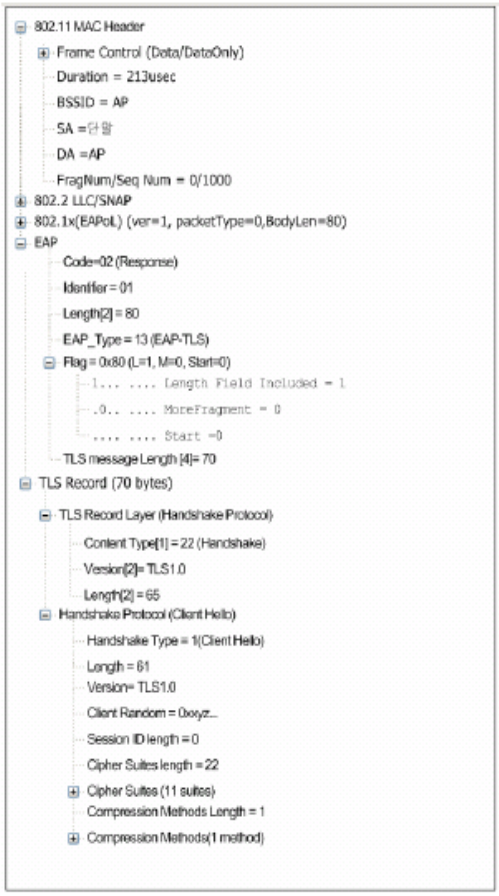
인증 및 키 교환에서 단말과 Base Station은 난수를 생성하여 데이터에 포함시켜 통신한다. 데이터 암호화 방식에서는 DES 알고리즘 대신 암호강도가 높은 128bit AES-CCM 알고리즘으로 전송하기 때문에 보다 안전하며 인증키는 단말과 기지국이 각각 생성하는 방식을 사용함으로써 인증키가 무선구간에 직접 노출되지 않아 보안성이 강하다.



(그림 2) EAP-TLS 인증방식

PKMv2는 RSA 기반인증방식과 EAP(Extensible Authentication Protocol)기반 인증방식을 지원한다. PKMv2 RSA 기반인증 방식은 PKMv1과 같은 RSA 기반의 공개키와 단말의 MAC주소를 결합한 X.509 인증서를 사용하지만 기지국도 단말에 인증서를 제공하는 양방향 인증방식을 사용하며 인증시 메시지 무결성 보장을 위해 전자서명과 난수 등이 추가되어 PKMv1에서 예상됐던 취약성을 개선했다.

PKMv2 EAP기반 인증방식은 IEEE802.1x포트 기반의 가입자 인증데이터 전송을 위한 표준프로토콜로 EAP-MD5, EAP-TLS, EAP-AKA(Authentication and Key Agreement)등 다양한 인증프로토콜을 사용할 수 있으며 사용자 인증 및 단말 그리고, 네트워크간 상호인증이 가능하다.



(그림 3) EAP-TLS 패킷

AAA 인증서버를 통해 인증을 수행하기 때문에 무선인터넷 네트워크의 사용자가 증가해도 기지국에 오버헤드가 발생되지 않는다.

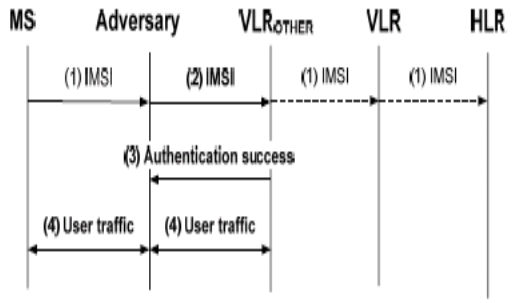
PKMv2 RSA 기반 인증메커니즘은 단말이 제조업체로부터 발급받은 인증서로 인증을 수행하는 방식이다. RSA 인증은 단말 인증은 가능하지만 단말의 사용자 인증은 제공하지 못한다. 사용자 인증을 제공하기 위해 PKMv2에서는 추가적으로 EAP 기반의 인증메커니즘을 선택할 수 있도록 제공하고 있다.

PKMv2 EAP 인증은 RFC 3748에서 정의한 EAP의 EAP-TLS를 사용하여 MS와 AAA의 상호 인증이 가능하다. RAS에서는 AAA 프로토콜을 사용, 인증 서버와 클라이언트 사이의 EAP 메시지를 암·복호화하여 무결성을 확보하고 연계할 수 있다[1].

4. 인증취약성 공격

VLR과 HLR간의 통신과 VLR과 VLR간의 통신에서 암호화 방식을 사용하지 않기 때문에, 공격자는 이를 도청하여 HLR에 연결된 채널을 모니터링하고, IMSI 인증정보를 획득함으로써 인증취약성을 이용한 공격을 시도 할 수 있다. MS의 통신정보를 도청하여 이루어지는 공격인 Redirection Attack(RA)은 MS의 인증세션을 가로채 사용자가 원하는 않는 VLR로 전송하여 정상적인 서비스를 방해하는 공격이다[2].

인증의 취약성을 이용한 공격은 VLR과 VLR의 통신에서 암호화방식을 사용하지 않는다는 것 이외에도, VLR은 MS를 인증할 수 있으나, MS가 인증을 요청한 VLR은 인증할 수 없기 때문에 발생한다.



(그림 4) Redirection Attack

3GPP AKA기반에서의 이러한 문제점을 보완하기 위해 VLR마다 ID를 부여해서 MS가 인증요청시 난수를 발생시켜 MS와의 상호인증을 제안한 방법도 있다.

그러나 이러한 방법도 사용자의 위치정보(Location privacy)를 이용한 공격이 발생할 수 있다. 사용자의 위치정보를 이용한 공격은 VLR과 VLR사이에 인증벡터를 전송하면 공격자가 만든 기지국(False base station)을 이용 VLR과 VLR 사이의 인증요청을 방해하여, MS는 자신이 인증요청을 전송한 VLR이 아닌 공격자의 기지국에 의해 선택된 VLR에 접속하게 되고 MS의 IMSI를 노출하도록 유도하는 공격기법이다.

5. 인증 취약성 보안메커니즘

5.1 EAP-AKA

무선인터넷 환경에서 가입자 인증은 IETF(Internet Engineering Task Force)의 표준인 EAP(Extensible Authentication Protocol)-AKA(Authentication and Key Agreement) 방식을 사용한다.

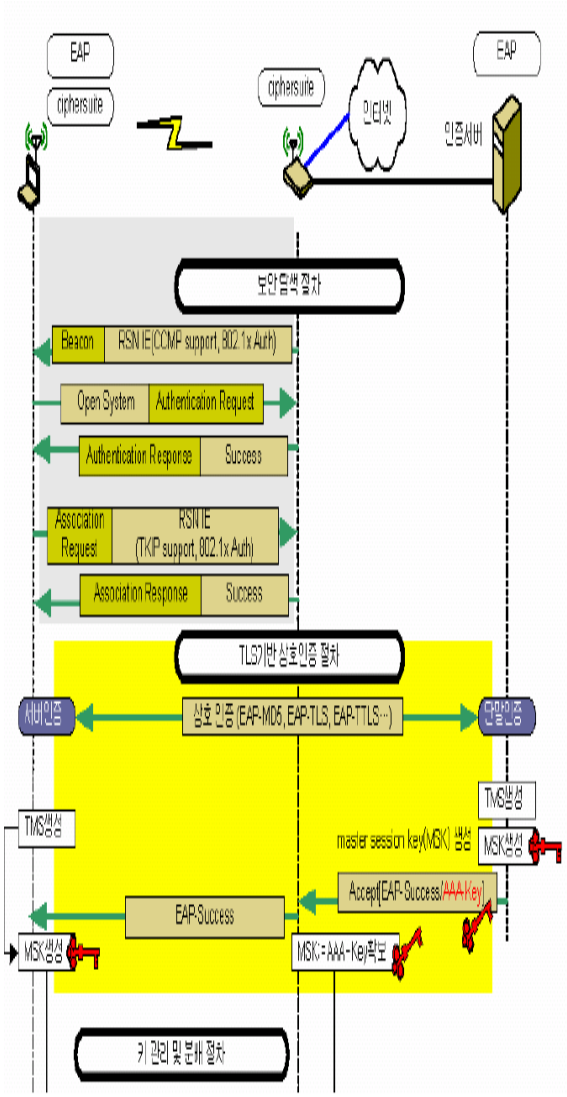
이 방식은 단말과 인증 서버가 동일 인증키를 안전하게 공유한 후 인증 절차를 수행하여 대칭키 기반의 인증을 수행한다. EAP-AKA 인증 방식은 기존 AKA 인증에 EAP 개념을 도입함으로써 사용자의 단일 인증을 통한 편의성 호환성 및 보안이 한층 강화된 인증 절차를 수행할 수 있다. Base Station은 사용자의 Identity를 EAP-Request/AKA-Identity 메시지를 통해 요구하고 단말기 내의 USIM(Universal Subscriber Identity Module)은 자신의 identity를 EAP-Response/AKA-Identity 메시지에 포함하여 전달한다.

인증서버는 해당 메시지를 수신하면 해당 가입자의 권한을 검증하여 인증 벡터를 생성하고 EAP-Request/AKA-
Challenge 메시지를 통해 중간 노드인 Radio Network Controller/Serving General Packet Radio Service Support Node, Access Control Router에게 전달한다.

중간 노드는 인증벡터 중에서 Random Number와 Authentication Token을 USIM에게 전달한다.

USIM은 Authentication Token에 포함된 Message Authentication Code값을 검증하고 Result를 생성하여 중간 노드 또는 인증 서버에게 전송한다. 여기에서 USIM은 데이터의 기밀성과 무결성을 위한 Ciphering Key와 Integrated Key를 생성한다.

중간 노드 또는 인증 서버에서는 저장하고 있는 XRES(Expected Result)와 USIM으로부터 수신한 RES를 비교하여 사용자 인증을 수행한다[6-8].



(그림 5) EAP의 상호인증 및 키 분배

5.2 EAP-TLS

EAP-TLS는 클라이언트 및 네트워크에 대한 인증서 기반 상호 인증 기능을 제공 할 수 있다. 이 방법은 클라이언트 인증서와 서버의 인증서를 통해 인증을 수행하며 WLAN 클라이언트와 액세스 포인트 간 후속 통신에 대한 보안을 강화하기 위해 사용자 기본 WEP 키 및 세션 기반 WEP 키를 동적으로 생성한다.

IMSI가 노출되지 않도록 보안채널을 구성할 수 있으며, 동시에 사용자의 개인정보를 인증센터에 보내어 인증 할 때에 EAP-TLS를 통하여 보다 안전한 채널로의 인증을 가능하게 할 수 있다[3-5].

6. 결 론

무선 인터넷 환경에서 단말과 사용자의 신분을 확인해 줄 유일한 것은 USIM(Universal Subscriber Identity Module)카드의 IMSI(International Mobile Subscriber Identity)이다. MS가 WLAN Identity를 요청했을때 IMSI를 평문으로 MSC/VLR에 전송된다. VLR과 HLR의 통신에는 암호화를 사용하지 않아 IMSI가 노출되고, GSM은 단일 인증(unilateral authentication)방식을 사용하기 때문에 VLR이 검증되지 않았더라도 인증하게 되어 Redirection Attack(RA) 공격에 노출될 수 있다. MS를 이용하여 WLAN을 접근하려 하였을 때, USIM에서 MS에게 IMSI가 평문으로 전달되고 이를 다시 VLR에 암호화 되지 않은 상태로 전달하게 되어 보안에 취약점을 갖고 있었다.

EAP-AKA는 기존의 AKA에 EAP개념을 도입하여 상호 인증과 키 일치를 통한 보안인증을 할 수 있도록 하고 있다. MS가 사용자 VLR에 인증을 요청 할 때, PKMv2 EAP 기반의 개선된 EAP-TLS를 사용한다. 이 때 암호화된 채널을 통해 클라이언트와 네트워크에 대한 인증서기반 상호인증 및 동적인 세션 기반 WEP 키를 생성하여 보안을 할 수 있다.

그러나 인증 연동이 지원되는 망에서는 무결성과 기밀성이 보장되는 통신을 할 수 있지만, 인증연동이 되지 않는 망으로 로밍하여 서비스(데이터통신, 음성통화 등)를 받을 경우 개인 정보가 노출 될 위험이 있다. 이러한 점을 보완하기 위해 모든 이동망에서 인증연동을 제공할 수 있는 보다 강력한 Integrated Mobile Authentication Server를 구축하여 어디에서든지 기밀성과 무결성이 보장된 서비스를 받을 수 있도록 하여야 할 것이다.

참 고 문 헌

[1] 와이브로 인증 키 관리 기술동향, Information Security News, Vol.105 June 2006

[2] Wen-Shenq Juang, Jing-Lin Wu, "Efficient 3GPP Authentication and Key Agreement with Robust User Privacy Protection", IEEE Wireless Communications and Networking Conference (WCNC 2007)

[3] B. Aboba, D. Simon, PPP EAP TLS Authentication Protocol, RFC 2716, IETF, October 1999.

[4] Moby Dick WP4, "AAAC Design", IST-2000-25394 Project Moby Dick, Jan 2002.

[5] IEEE, "Standard for Local and metropolitan area networks-Part16:Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE P802.16e/D12,October 2005.

[6] Yuh-Min Tseng, "USIM-based EAP-TLS authentication protocol for wireless local area networks", CSI-02532; No of Pages 9 Available online at www.sciencedirect.com

[7] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAPAKA)", RFC-4187, IETF, January 200

[8] B. Aboba et al. "Extensible Authentication Protocol (EAP)", RFC-3748, IETF, June 2004.

◐ 저 자 소 개 ◑

송 유 진(Yu-Jin Song)

- 2002년 2월 : 한서대학교 물리학과 (이학사)
- 2006년 2월 : 한서대학교 정보보호공학과 (공학석사)
- 2008년 3월 ~ 현재 : 한서대학교 디지털포렌직학과 박사과정
- 2008년 3월 ~ 현재 : 한서대학교 인터넷공학과 겸임강사

<관심분야> : 정보보호, 디지털포렌식

이 재 용(Jae-yong Lee)

- 1985년 2월 : 인하대학교 전자계산학과 (이학사)
- 1990년 2월 : 인하대학교 전자계산학과 (이학석사)
- 2000년 2월 : 인하대학교 전자계산공학과 (공학박사)
- 1991년 3월 ~ 1993년 3월 : KIST/SERI 연구원
- 1993년 3월 ~ 1999년 8월 : 수원여자대학 컴퓨터응용학부 조교수
- 2000년 3월 ~ 현재 : 한서대학교 인터넷공학과 부교수

<관심분야> : 인터넷관리, 의료정보처리, 디지털포렌직