PKMv2 RSA 기반 인증에서의 DH키 분배를 적용한 WiBro 무선네트워크의 인증 및 TEK 생성

이형섭, 조치현, 김경태, 윤희용
성균관대학교 컴퓨터공학과
e-mail:ratm@skku.edu

WiBro Network Authentication and TEK establishment using DH key distribution on PKMv2 RSA based authentication

Hyoung Seob Lee, Chi Hyun Cho, Kyung Tae Kim, Hee Yong Youn
Dept of Computer Engineering, SungKyunKwan University

요 약

와이브로 서비스는 고속 이동 인터넷 환경 속에서 고속으로 무선 인터넷 서비스를 제공하는 기술이다. 기존의 무선인터넷 서비스와 달리 이동성을 제공한다는 점에서 차별화를 제공한다. 이렇게 이동하는 단말에게 양질의 데이터를 안전하게 전송하기 위해서는 보안기술이 중요한 요소로 작용한다. 서비스를 제공하기 전에 단말(Mobile Station)과 RAS(Radio Access Stations)간의 인증을 바탕으로 상호 키(TEK:Traffic Encryption Key)를 분배하고 TEK를 바탕으로 데이터를 암호화해서 전송하게 된다. 기존의 인증 프로토콜에서는 RAS에서 단독으로 키를 생성하는 방식이지만, 본 논문에서는 기존의 프로토콜의 문제점으로 지적된 Replay Attack에 대해 DH(Diffie-Hellman) 키 분배(Key Distribution) 방식을 적용하는 프로토콜을 제안함으로써 취약점에 대비 하였다. 이를 통해 RAS에 집중되는 키 생성에 대한 오버헤드를 단말에 분산 시킬 수 있다. 이로써 제안된 프로토콜을 사용해서 기존의 프로토콜을 사용했을 때보다 보안강도를 높일 수 있다.

1. 서 론

국내 이동통신 시장은 2세대 이동통신 기술(CDMA)을 넘어 3.5세대 이동통신 기술을 바탕으로 사용자로 하여금 음성은 물론 양질의 콘텐츠를 제공하고 있다. 3.5세대 이동통신에 사용되는 기술은 기존의 WCDMA기술을 이용한 HSDPA(High Speed Downlink Packet Access)와 OFDM기술을 이용한 WiBro(Wireless Broad-band)가 있는데, 이 기술들의 공통점은 이동성을 제공한다는 점이다. 사용자들은 이동 환경 중에서도 고속으로 인터넷에 접속해 여러 서비스를 제공 받을 수 있다. 이런 강점을 바탕으로 HSDPA나 WiBro는 3.5세대 이동통신 기술로서 이동통신 시장을 빠르게 점유해 나가고 있는 상태이다. 이러한 휴대인터넷의 안전한 서비스를 위해 중요한 기술 요소 중 하나가 보안이다.[1]

기본적인 구조에서는 단말, RAS, 콘텐츠 서버 간의 인증을 시작으로 암호화된 트래픽으로 통신함으로써 외부 침입자로부터 데이터를 보호 한다. 하지만 실제 데이터를 암호화 하는 키를 RAS에서 일방적으로 생성하는데, 이는 RAS가 단일 실패지점으로써 공격 시 와이브로 서비스에 큰 손실을 입히게 된다. 본 논문에서는 PKMv2에서 두 가지 인증 방법 중 PKMv2 RSA기반 인증 프로토콜에서 사용되고 있는 기존의 키 생성 방식을 DH(Diffie-Hellman) 키 분배 방식으로 교체하여 기존의 암호 강도는 유지한 채 Replay Attack을 대비 하며 단일 실패 지점을 보완하는 방법을 제안한다. 본 논문의 구성은 2장에서는 현재 PKMv1, PKMv2 RSA 기반 인증에 대한 설명과 DH 키 분배 방식에 대해 설명하고, 3장에서는 제안하는 프로토콜을 설명 및 개선 사항을 다룬다. 마지막으로 4장은 이 글의 결론을 맺는다.

2. 기존 와이브로 인증 프로토콜 분석

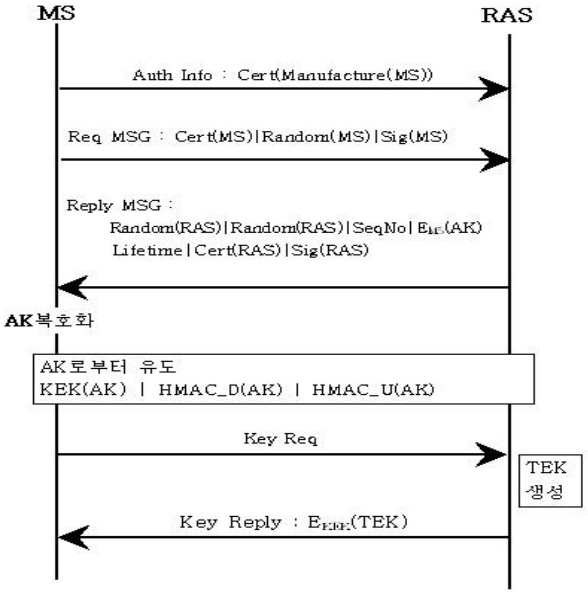
와이브로의 MAC 보안구조는 IEEE 802.16e Privacy계층을 기반으로 정의한다.[1] 이 구조는 인증 및 키 관리를 위한 PKM(Privacy Key Management) 프로토콜과 패킷 데이터에 대한 암호화를 위한 Encryption 프로토콜로 구성된다. PKMv1은 RAS에서 단말을 인증하는 일방향성을 가지고 있다. 그래서 위장 공격에 취약 하다는 점이 지적 되었다. PKMv2는 PKMv1에서의 이러한 문제점을 보완하고자 양방향 상호 인증을 제공 하였다. PKMv2 RSA기반 인증은 단말인증과 RAS인증을 제공하고, PKMv2 EAP기반 인증은 AAA(Authentication, Authorization, Accounting), RAS, 단말 간의 상호 인증을 바탕으로 단말을 사용하는 사용자 인증을 제공한다.

<표 1> PKMv1과 PKMv2 비교[2]

구 분	PKMv1	PKMv2
인증속성	단방향 인증	상호인증
인증방식	RSA (Mandatory)	RSA(Option), EAP(Option)
인증내용	단말기 인증	단말기, 사용자 인증
TEK 암호화	3DES	3DES-EDE, RSA, AES-EBC/KEY-WRAP
데이터 암호화	No Encryption DES	No Encryption DES-CBC,3DES,RSA, AES-CCM/CBC/CTR
데이터 무결성	No MAC, HMAC	No MAC, HMAC.CMAC

2.1 PKMv1에서의 TEK생성 과정

PKMv1에서는 단말의 제조업체로부터 발급 받은 X.509인증서를 통해 단말 인증을 한다. 이 인증서를 RAS에게 전송하면 RAS는 AK(Authorization Key)를 단말의 공개키로 암호화해서 단말에게 전송한다. 단말은 자신의 개인키로 메시지를 복호화 하여서 얻은 AK를 바탕으로 KEK(Key Encryption Key), Downlink에 사용되는 HMAC_D와 Uplink에 사용되는 HMAC_U를 유도 한다. AK를 유도 한 뒤 단말이 RAS에게 Key Request를 전송하면 RAS에서는 TEK를 생성한 뒤 KEK로 암호화 하여서 단말에게 전송한다.



(그림 1) PKMv1 RSA기반 인증 및 TEK생성 과정

2.1.1 보안상 취약점

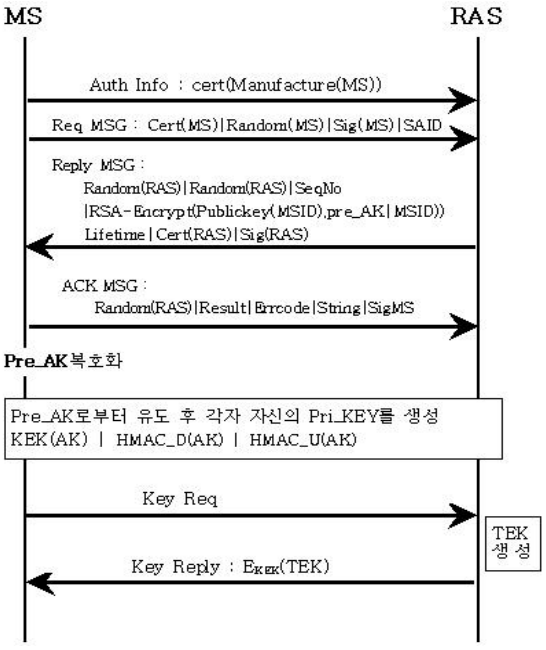
TEK는 단말(MS)에서 Key Request 메시지를 RAS에게 전송하면 RAS가 일방적으로 생성하여 전송하는 키 분배방식이다. 이 부분은 무선네트워크 인정 절차 없이 네트워크에서 생성한 키로 서비스를 하는 점에서 보안상 문제점이 존재 한다.[1] 이러한 서비스가 가능하기 위해서는 우선 무선 네트워크에 대한 신뢰성이 필요하다. 하지만 와이브로 서비스의 환경 특성상 빠르게 이동하는 단말에게 신뢰할 수 있는 무선 네트워크를 생성하는 것은 단말과 RAS간 오버헤드를 가져오게 된다. 따라서 이를 해결하기 위해 상위 계층에서의 보완이 필요하다.[1]

2.2 PKMv2 RSA기반 인증의 TEK생성과정

PKMv2에서는 두 가지 인증 메카니즘을 제공한다. RSA 기반 인증, EAP(Extensible Authentication-Protocol) 기반 인증. 두 메카니즘은 기본적으로 단말 인증과 RAS 인증을 제공한다. 본 논문에서는 PKMv2 RSA기반 인증만을 다루도록 하겠다.

PKMv1과 마찬가지로 단말의 제조업체로부터 발급 받은 X.509인증서를 RAS에게 전송한다. 단말은 Authentication Information을 보낸 뒤 PKMv2 RSA Request 메시지를 보낸다. 이를 통해 RAS가 요청 메시지를 보낸 단말이 인증 받은 단말인지를 결정 한다. RAS가 Sig(MS) 검증을 성공적으로 마치면 단말은 RSA로부터 자기 자신과 자신의 인증서에 대한 인증을 얻게 된다.[3] RAS는 이를 PKMv2 RSA Reply 메시지를 통해 보낸다. Random(MS)와 Random(RAS)는 Replay Attack으로부터 메시지를 보호하기 위해 사용된다. RAS가 Sig(MS)를 검증 했던 것처럼 MS가 Sig(RAS)검증하고 나면 RAS에게 PKMv2 RSA Acknowledgement 메시지를 전송한다.[3]

TEK생성은 PKMv1에서의 방식과 마찬가지로 단말이 Key Request를 보내면 RAS에서 이루어지며 이는 KEK로 암호화한 형태로 전송한다.



(그림 2) PKMv2 RSA기반 인증 및 TEK생성 과정

2.2.1 보안상 취약점

PKMv1의 취약점으로 지적 되었던 단방향 인증 메커니즘이 PKMv2에서는 양방향 인증 메커니즘으로 사용되었다. AK생성 방식 또한 Pre-AK를 통해 RAS와 단말이 각각 AK를 유도하는

방식으로 보다 안전한 키 분배 방식이 적용되었다. 하지만 여전히 TEK는 RAS에서 일방적으로 생성하여서 인증을 마친 뒤 Key Request가 있을 시에 단말에게 전송 하는 방식을 취하고 있다. 이는 RAS가 단일 실패 지점으로 공격 시 세션 키를 노출시킬 위험이 있으며, TEK 길이는 802.16-2004에서 사용 되었던 키 길이와 같은 길이로서 Replay Attack에 취약하다.[3]

2.3 DH 키 분배 방식

DH 키 분배 방식은 계산적 Diffie-Hellman 가정을 바탕을 두고 있다. g ∈ G 이고, a, b ∈ Z_p, a, b ∈ 0,1,2, ... ,p-1 일 때, g^a와 g^b로부터 g^{ab}를 계산하는데 이때 계산한 결과 값에 각각 Modular연산을 취하면 g, g^a, g^b이 주어 졌어도 g^{ab}를 계산하는 것이 어렵다는 것이다.[4]

이를 이용한 DH 키 분배 방식은 A가 난수 생성기를 통해 a ∈ Z_{p-1}인 난수 a를 생성하면 자신의 개인키를 $y_A \equiv g^a \bmod p$으로 계산한다. B도 같은 방식으로 b ∈ Z_{p-1}인 난수를 생성하여 자신의 개인키를 $y_B \equiv g^b \bmod p$으로 계산 한다. A와 B가 성공적으로 자신의 키를 성공했으면 KDC(Key Distribution Center)에게 자신의 식별정보와 함께 제출하여 자신의 공개정보임을 확인하는 인증서를 발급 받아 공개 목록에 등록한다.[5] 비밀 통신을 원하는 A와 B는 상대방의 인증서를 KDC에 있는 공개목록으로부터 제공 받아 각자 세션 키 SK를 생성한다.

$$SK \equiv g^{ab} \bmod p$$

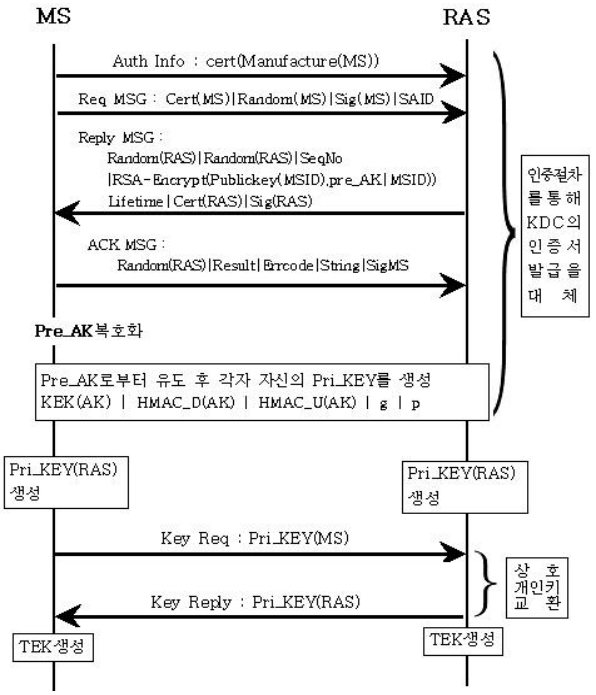
키를 생성 할 때 난수생성기를 견고하게 설계 하는지, Seed 값으로 어떤 것을 선택할 것인지 주의해야 한다. 이에 따라 키의 강도가 정해진다. 또한 난수생성기는 난수성의 충분히 확장 할 수 있어야 되고, Seed 값은 예측 불가능 하며 충분한 길이를 가져야 한다.

3 제안하는 프로토콜

Replay Attack을 방지하는 일반적인 방법은 이전에 사용되었던 메시지와 현재 사용되는 메시지를 구별 할 수 있는 정보를 메시지에 첨부함으로써 공격을 방지하는 것이다. 현재 Replay Attack을 방지하기 위해 OTP(One-Time-Password)방식이나 Time-Stamp를 추가하는 메커니즘이 사용된다. 제안하는 방식에서는 TEK 생성을 일방적으로 RAS에서의 생성이 아닌 단말과의 DH키 분배 방식으로 키를 생성하는데 단말의 상태 정보를 이용해 Time-Stamp 를 구현하는 방식을 제안한다. 또한 상호 키 분배를 이용해 단일 실패 지점을 보완한다.

3.1 제안하는 방식을 적용한 프로토콜

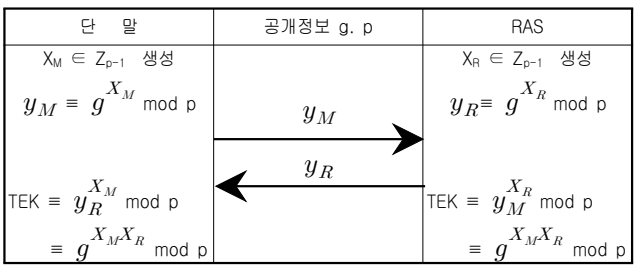
DH키 분배 방식에서 장점은 둘 중 한쪽만 난수를 적절하게 생성해도 안전한 SK를 생성할 수 있다는 점이다. 이 점을 이용해 RAS에 집중되는 부하를 줄이기 위해 단말에서 적절한 난수를 생성하고 RAS에서는 상대적으로 단순한 난수를 생성해도 SK는 안전하다. 제안하는 방식에서는 PKMv2 RSA기반 인증 프로토콜에서 Pre-AK를 통해 AK를 유도한 것으로 DH 키 분배 방식에서 KDC의 인증서 발급 받는 과정을 대체 한다. 이때 Pre-AK에 RAS에서 생성한 공개정보 g와 p값을 같이 포함 하여 전송함으로써 단말이 복호화 하면 공개정보 g와 p를 얻을 수 있게 한다. 이를 이용해 단말과 RAS가 각자 Private Key y_M, y_R을 생성한다. 인증 절차를 마쳤으면 단말이 Key Request를 RAS에게 보낼 때 y_M를 포함해서 전송하고 RAS는 Key Reply 메시지에 y_R 포함해서 전송한다.



(그림 3) 제안 방식을 적용한 인증 및 키 분배 과정

3.2. TEK 생성과정

단말과 RAS는 공통적으로 난수 생성기를 FIPS 186-2 표준의 PRNG 또는 KO-12.0001 KCDSA 표준의 PRNG(Psuedo-Random Number Generator)으로 사용한다.[5] 단말의 PRNG의 Seed 값 X_M는 단말의 일일 상태정보를 이용함으로써 매 세션마다 서로 다른 난수를 생성 한다. 단말과 RAS가 서로 Key Request와 Key Reply메시지 교환을 통해 상대방 개인키를 얻게 되면, 그림 4와 같은 과정을 거쳐서 TEK를 생성한다.



(그림 4) 제안하는 프로토콜에서의 TEK생성과정

3.3 제안한 프로토콜의 안전성 분석

단말에서 난수를 생성 할 때 사용되는 Seed 값을 단말의 상태 정보 즉, 시간정보, 배터리 잔여량, 통화기록 등 일일 상태 정보들을 조합해서 사용한다. 이러한 정보로 이뤄진 Seed 값은 매 세션마다 다르게 되므로 PRNG 특성상 난수 생성 시 매번 서로 다른 난수 값이 생성된다. 이렇게 생성된 난수가 Time-Stamp 역할을 하게 된다. 즉, 이전 메시지와 현재 메시지를 구별 해주는 역할을 하게 된다. 따라서 RAS에서 생성된 난수가 단순하고 일정하더라도 단말에서 생성된 매번 다른 난수로 인해 세션 키는 매번 다르게 되므로 Replay Attack에 견딜 수 있다. 설사 한 쪽의 개인키가 노출 되었다 하더라도 세션 키를 유도 할 수 없다는 장점이 있다. 이로써 RAS의 단일 실패 지점이 단말과 상호 키 분배 과정으로 인해 사라지게 된다.

4. 결 론

본 논문은 RAS에서 일방적으로 생성하는 TEK에 대한 취약점을 대비하기 위해 DH 키 분배 방식을 제안하였다. DH 키 분배 방식에서 한 쪽만 난수가 적절하게 생성 되면 안전한 세션 키가 생성된다는 점을 이용하여 단말의 일일 상태 정보를 Seed 값을 선택하여 매 세션 마다 서로 다른 키의 조합이 이뤄지도록 하였다. 이를 통해 취약점인 Replay Attack을 방지할 수 있다. 또한 단말에 보다 강력한 난수 생성기를 설치함으로써 1:n으로 여러 단말을 상대해야 하는 RAS의 난수생성에 대한 과부하를 줄일 수 있다. DH 키 분배 방식에서 자신의 개인 키 생성 시와 키 조합 시 각각 2번의 지수 승 연산과 modular연산이 필요한데 이는 많은 연산 소요 시간을 요구 하게 된다. 최근에 기존의 지수 승 연산과 modular 연산을 빨리 수행하는 알고리즘(Montgomery Algorithm, Common-Multiplicand modular multiplication Algorithm)에 대한 개발이 활발하게 이뤄지고 있는 상태 이고, 단말 시스템의 향상으로 인해 연산에 소요 되는 시간이 줄어 들 것으로 전망한다.

참고문헌

[1] Sun Hee Lim, Okyeon Yi, Sungik Jun, Jin-hee Han, “A Study on EAP-AKA Authentication Architecture for WiBro Wireless Network”, Korea Information Processing Society, Vol 31 4c, Apr. 2006

[2] 이석래, “인터넷보안 관련 융합기술 및 국제 표준화 동향”, 한국정보보호진흥원, 2007. 4

[3] Di Pang, Lin Tian, Jinlong Hu, Jihua Zhou, Jinglin Shi, "Overview and Analysis of IEEE 802.16e Security", Mar. 2007

[4] Computational DIffie Hellman Assumption, http://en.wikipedia.org/wiki/Computational_Diffie-Hellman_assumption

[5] 원동호, “현대 암호학” 그린 출판, 2004. 2