UMTS 3세대 이동망 보안 아키텍처의 인증 토큰을 이용한 IEEE 802.1X 프레임워크의 보완

송창열[0] 조기환
전북대학교 컴퓨터 정보학과, 전북대학교 전자정보공학부
{crsong[0], ghcho}@dcs.chonbuk.ac.kr

Supplement IEEE 802.1X with UMTS 3G Security Architecture Authentication Token

Chang-Ryeol Song[0] Gi-Hwan Cho
Dept. of Computer Science, Chonbuk National University

요 약

인증(Authentication)과 암호화 키(Key) 운용 방법론은 통신 서비스 고려시 소홀할 수 없는 중요한 문제이다. 현재 가장 널리 보급되어 사용중인 IEEE 802.11 기술에서도 이와 같은 보안 지원에 문제가 있음이 명백히 드러나고 있다. 포트 컨트롤을 통하여 접속 지점에서부터 통신을 제어하는 IEEE 802.1X는 이를 위한 적절한 보안 해결책이 되고 있고, IEEE 802.11 WGi는 802.1X를 기초로하는 RSN(Robust Security Network)을 위한 표준화가 진행중이다. 그러나 IEEE 802.1X 프레임워크에서 상호 인증과, 키 분배 및 갱신 정책은 채택하는 인증 프로토콜에 강하게 의존하는 약점을 가지고 있다. 따라서 본 논문에서는 UMTS 보안 아키텍처의 인증 토큰(Authentication Token)을 추가하여 IEEE 802.1X 프레임워크에 상호 인증 및 키 갱신 구조를 포함하도록 하였다.

1. 서 론

제 3세대 이동통신망의 상용화가 늦어짐에 따라, 휴대용 컴퓨터의 보급 증가와 더불어 무선 LAN을 이용하여 이동 인터넷 서비스를 이용하려는 인식이 급속도로 확산되고 있다. 인터넷 사업자들은 Hot-Spot 지역에 무선 LAN을 설치하여 무선인터넷 서비스를 제공하고 있으며, 가입자들은 이를 이용해서 전자 상거래, E-mail등 많은 정보 서비스를 이용하고 있다.

무선 통신에서 데이터는 전파를 통해 브로드캐스트되기 때문에 일정 범위 안에 있는 모든 무선 LAN 사용자들은 이를 수신할 수 있게 된다. 이는 무선 매체의 공개성에 따른 해킹의 용이성과 단말의 이동에 따른 보안 체계의 복잡성에 기인하므로 무선 LAN의 보안성 제공은 절대적이라고 할 수 있다.

그러나 IEEE 802.11 표준에서 제공하는 보안메커니즘의 핵심인 WEP(Wired Equivalent Protocol) 알고리즘은 암호키가 상수이고 IV(Initialization Vector)가 너무 작다. 24bit 길이인 IV는 재사용이 가능해서 동일한 키 시퀀스(Key Sequence)의 생성이 빈번하게 되고, 따라서 WEP 프로토콜의 크랙이 쉽고 무선 데이터 정보 전송시 위험성이 심각하다.

이에 대한 대안으로 IEEE 802.11 WGi에서는 IEEE 802.1X를 중심으로 RSN을 위한 표준화를 진행중이다. 포트 기반 네트워크 접속 제어 프레임워크인 802.1X 표준은 강력한 인증, 접속 통제, 키 분배 기능을 제공한다.

IEEE 802.1X는 일종의 프레임워크이므로 인증 프로토콜에 따라 좌우되는 것이 당연하지만, 선택되는 인증 프로토콜에 따라서 상호 인증을 수행하지 못하거나, 키 분배를 보다 섬세하게 할 수 없는 단점이 있다. 802.1X의 기본 프로토콜 동작에서 시도/응답 프로토콜을 통한 단방향의 인증만을 정의해 놓기 때문이다.

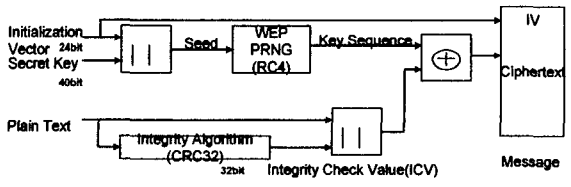
따라서 이를 보완하기 위해서 3세대 통신 시스템인 UMTS(Universal Mobile Telecommunication System) 보안 아키텍처의 AKA(Authentication and Key Agreement)를 적용하여 양방향 인증 및 자유로운 세션키 분배를 지원할 수 있도록 프레임워크 수정 보완 구조를 제시하였다.

2장에서는 먼저 IEEE 802.11 무선랜 보안구조를 설명하고, 이를 위한 견고한 보안(RSN)을 제공하는 방법론으로써 802.1X 프레임워크를 살펴보겠다. 3장에서는 IEEE 802.11을 위한 802.1X 프레임워크 사용에서의 문제점에 대한 보완책으로써 Authenticity 속성을 추가한 제안을 살펴본 뒤, 본 논문에서 참고한 UMTS 보안 아키텍처의 AKA를 살펴본다. 4장에서는 인증 토큰을 이용하여 상호 인증 및 키 갱신부분을 보완한 802.1X 구조를 제안하고, 5장에서 결론 및 향후 연구 과제를 살펴본다.

2. 관련연구

2.1 IEEE 802.11 보안 구조[1]

IEEE 802.11계열 기술의 보안 구조는 크게 데이터 비밀성(data privacy)과 인증으로 나누어 볼 수 있다. WEP프로토콜을 이용한 데이터의 비밀성 제공과, 개방형 인증과 공용키 인증의 두 가지 인증 방식을 이용한 AP와 스테이션 사이의 인증을 제공한다. WEP은 불록 암호화 알고리즘인 RC4를 이용하여 무선상에 전송되는 패킷을 암호화한다. IV와 비밀키를 이용하여 키 시퀀스를 만들고, CRC-32를 이용하여 평문의 무결성을 유지한 뒤 XOR연산을 수행하면 평문이 암호화된다[그림 1]. 복호화는 이를 역순으로 수행한다. 공유키 인증은 WEP 메커니즘을 이용하여 단말의 장치 인증을 수행한다. 그러나 64bit의 작은 키 시퀀스, IV의 재사용 등으로 인하여 Dictionary 공격, MIM(Man In the Middle) 공격 등 여러 가지 가능성이 드러났다.

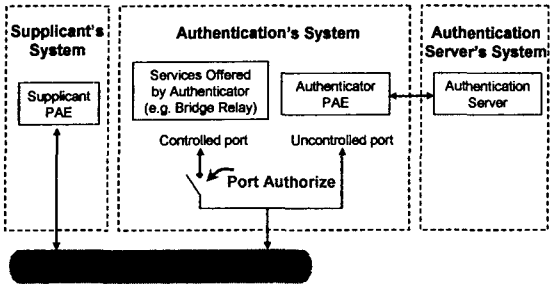


[그림 1] WEP encapsulation block diagram

2.2 IEEE 802.1X 프레임워크[2]

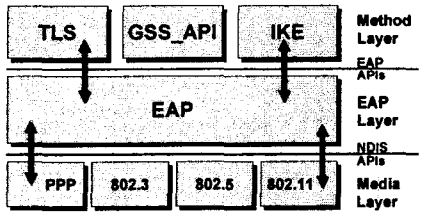
IEEE 802.1X는 논리적 포트 개념을 도입하여 최종단 망시스템인 브릿지 또는 무선 AP에서 인증 수행한 다음에 사용자가 망에 접근할 수 있도록 하는 Port based Network Access Control 메커니즘으로써 EAP(Extensible Authentication Protocol)[3]를 이용하여 여러 가지 인증 프로토콜을 융통성 있

게 사용할 수 있도록 허용한다. [그림 2]는 Supplicant와 Authenticator, Authentication Server 사이의 포트를 이용한 접속 구성도이다. Supplicant(ex. 스테이션)는 Authenticator(ex. AP)를 통해 망 접속을 요청하면 Authenticator는 Uncontrolled Port를 통해 사용자의 인증 정보의 전송을 이용하여 Authentication Server와의 인증 과정을 수행한다. 인증에 성공하면 Controlled Port를 통한 망 접속을 허용하게 된다.



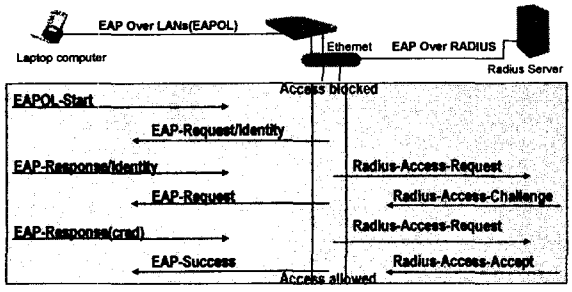
[그림 2] IEEE 802.1X 포트 기반 인증

이러한 인증 과정에서 IEEE 802.1X 에서는 Supplicant와 Authenticator, Authentication Server 사이의 인증 프로토콜로써 EAP를 사용한다. EAP는 다양한 매체 위에서 OPT(One-time password), GSS_API, Public Key, 스마트카드, IKE와 같은 다양한 인증 프로토콜 사용을 지원한다[그림 3].



[그림 3] IETF 표준의 EAP 인증 프로토콜

[그림 4]는 랩탑 사용자, 브릿지, RADIUS 서버 사이의 IEEE 802.1X의 토폴로지와 오퍼레이션 시퀀스를 보여준다. RADIUS는 현재 가장 많이 사용되고 있는 인증 서버 프로토콜이므로 이를 예로 사용한다. 특별히 Supplicant와 Authenticator 사이의 EAP 프레임 전송을 위해서 EAPOL(EAP Over LAN) 이라는 캡슐화 구조를 정의하고 있는데, IETF에서는 현재 802.3/이더넷과 FDDI/토큰링을 EAPOL 캡슐화 기술이 정의되어 있다.



[그림 4] IEEE 802.1X operation

랩탑 컴퓨터를 이용하여 망에 접속하려는 사용자가 먼저 initiate하면 브릿지는 사용자의 신원을 요청한다. 사용자는 자신의 아이디를 포함한 메시지를 보내고 브릿지는 EAPOL에 실려온 EAP부분을 추출하여 RADIUS 패킷에 넣어(EAP over RADIUS) RADIUS 서버로 전송한다. 서버는 적절한 인증 프로토콜을 이용하여 사용자 확인 과정을 수행하여 브릿지에게 접속 허용여부를 알려준다. 만일 인증에 성공할 경우 브릿지는 Controlled Port를 Authorize하여 사용자에게 망 서비스 접근을 허용한다.

3. 802.1X의 보완 방안

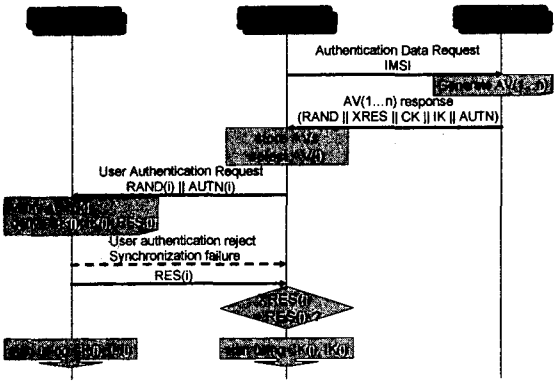
RSN에서 IEEE 802.11의 보안성 제공을 위하여 802.1X 프레임워크를 사용할 때에 강력한 접속 통제와 만족할 만한 인증을 제공하지는 못한다.

3.1 메시지 authenticity 추가[4]

802.11, 802.1X, EAP 프로토콜에서 메시지에 대한 인증 부족으로 인해서 세션 하이젝킹과 MIM공격이 가능하다. 예를 들어 합법적인 사용자와 AP 사이에 EAP 메시지 교환을 통한 인증이 이루어진 후, 임의의 시점에서 공격자가 AP로 위장하여 사용자에게 disassociate 메시지를 보내 사용자 연결이 끊어진 것처럼 하고 자신이 그 세션을 이용한 트래픽 도청이 가능하다. 이는 IEEE 802.11표준에서 관리 프레임에 대한 무결성 보호를 하지 않기 때문이다. 또한 802.1X 프레임워크는 사용자가 AP를 인증하지 않는 단방향 인증만을 제공하므로 상호 인증 결여로 인한 잠재적인 MIM 공격 가능성이 있다. 예를 들어 위의 [그림 4]에서 차용하는 인증 프로토콜을 고려하지 않는다면, EAP-Success 메시지는 무결성이 보호되지 못하므로 공격자가 이 패킷을 날조할 수 있다. 이를 위해 EAP-Success 메시지에 EAP-Authenticator 어트리뷰트를 추가하는 방법이 있다.

3.2 UMTS 보안 아키텍처 AKA 적용[5]

UMTS 보안 아키텍처의 인증 및 키 분배 프로토콜인 AKA의 인증 토큰을 이용하여 802.1X를 이용한 인증 및 키 분배를 보다 강력하게 지원하도록 하기 위하여 AKA의 동작 원리를 살펴보자.



[그림 5] Authentication and Key Agreement 동작

VLR(AP측)은 USIM(사용자측)의 아이디(IMSI)를 가지고 HLR/AuC(인증서버)에게 인증을 요청한다. 인증 서버는 해당 사용자의 인증 정보를 이용하여 난수, 시퀀스, 세션키 등의 정보를 포함하는 인증 벡터(AV)를 만들어 AP에게 보낸다. AP는 이를 저장하고, 사용자를 인증하기 위해 그 중 하나의 인증 벡터의 난수값과 인증 토큰을 포함하여 challenge를 보낸다. 사용자는 자신의 비밀키를 이용하여 인증 서버측에 대한 인증을 수행하고, 세션키를 도출한 후, RES를 만들어 AP에 전송한다. AP는 사용자

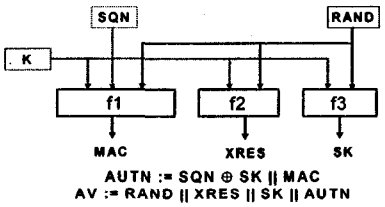
의 RES와 인증 벡터의 해당 값(XRES)을 확인하여 사용자측을 인증하고 해당 세션키를 이용해 사용자와 암호화된 통신을 수행한다. 이와 같이 AKA 프로토콜은 사용자측과 인증 서버측의 상호 인증을 제공하고, 여러 개의 인증 벡터를 이용하여 수시로 세션키 분배를 수행할 수 있도록 하는 장점이 있다.

4. 추가된 802.1X 인증 프레임워크

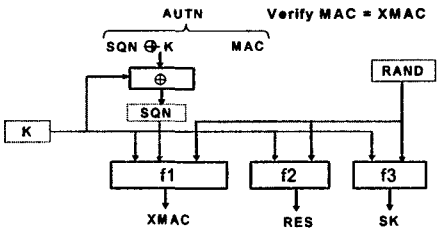
유럽식 제 3세대 이동 통신망 보안 아키텍처의 AKA 프로토콜을 802.1X에 적용하면 프레임워크 내에서 상호 인증을 꾀할 수 있고, 보다 능동적인 세션키 분배를 수행할 수 있게된다.

4.1 requirements

인증 토큰을 생성하기 위해서는 사용자와 인증 서버에 몇 가지 함수와 인수들이 필요한데, 공통적으로 비밀키(K)와 세션키 유도 함수 f3, 양끝단 각각에서 상호 인증시 필요한 함수 f1, f2가 필요하다. 인증 서버는 난수와 시퀀스 넘버를 생성하므로 이를 위한 적절한 모듈이 필요하다. 이를 이용해 인증 서버는 인증 토큰을 생성하고[그림 6], 사용자도 이를 검증하고 응답메시지를 만든다[그림 7].



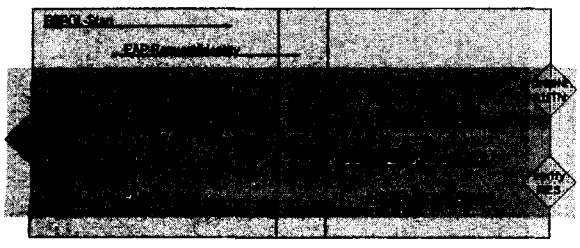
[그림 6] 인증 서버측에서의 함수 수행



[그림 7] Supplicant에서의 함수 수행

4.2 상호 인증 및 메시지 무결성

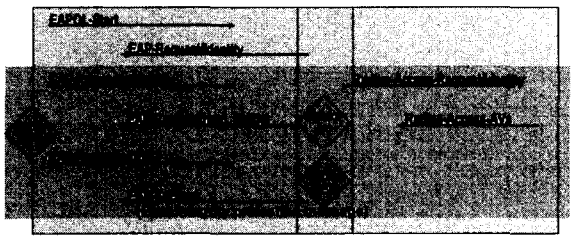
[그림 8]은 802.1X의 시도/응답 프로토콜 기반에 인증 토큰을 추가하여 사용자가 인증 서버에 대한 인증을 수행할 수 있도록 하였다. 상호 인증과 함께 또한 세션 키 일치가 이루어지므로 세션키와 메시지 무결성 알고리즘을 이용하여 EAP-Success 메시지에 대한 무결성 보호를 수행할 수 있다.



[그림 8] 인증 토큰을 결합한 802.1X operation

4.3 능동적 세션키 분배

802.1X에 AKA의 수행과정을 수정 없이 그대로 적용시키면 더욱 능동적인 세션키 분배를 수행할 수 있다[그림 9]. 사용자의 인증 요청시 인증 서버는 난수, 세션키, 인증 토큰, 계산된 응답(XRES)를 포함하는 일련의 인증 벡터들을 생성하여 AP에 전송한다. AP는 인증 벡터중 하나를 선택하여 사용자에게 challenge를 보내고 응답을 받아 인증을 수행한다. 일정 시간이 지나고 세션키를 변경하고 싶을 때, 또는 사용자가 적법한지를 확인하고 싶을 때 AP는 또 다른 인증 벡터를 이용하여 키 분배 및 인증을 수행할 수 있다. 802.11과 802.1X을 이용한 보안 서비스에서 인증 서버와의 거리가 먼 경우, 이처럼 인증 벡터를 이용한다면 AP 자체에서 빠르게 키 분배 또는 인증을 수행할 수 있는 장점이 있겠다.



[그림 9] 능동적 세션키 분배 operation

5. 결론 및 향후 연구과제

IEEE 802.1X 프레임워크는 포트를 정점으로 상위 계층 인증인 사용자에 대한 인증을 수행함으로써 802.11의 단말 인증의 한계를 극복할 수 있도록 한다. 그리고 EAP라는 캡슐화 프로토콜을 이용하여 여러 매체 위에서 여러 가지 인증 프로토콜을 이용하여 융통성 있는 인증 및 키 분배를 수행할 수 있도록 하는 프레임워크이다. 그러나 OTP나 MD5(Message Digest)와 같은 단방향 인증 프로토콜을 이용할 경우 상호 인증을 수행하지 못하게 된다. 이처럼 상호 인증 및 키 분배 수행이 채용되는 인증 프로토콜에 강하게 의존하는 점을 프레임워크 자체에서 보완하고자 UMTS AKA의 인증 토큰을 이용하여 오퍼레이션을 구성하였다. 이로써 상호 인증을 제공토록 하고 키 분배를 보다 효율적으로 수행할 수 있도록 함으로써 세션 하이잭킹에 대해 보호할 수 있다. 또한 세션키와 무결성 알고리즘을 이용해서 EAP 메시지 또는 제어 메시지의 무결성을 보호할 수 있도록 함으로써 MIM 공격에 대해서 방어할 수 있다.

향후 연구과제로써 TLS, IKE, GSS-API와 같은 채택 가능한 인증 프로토콜들에 대한 구체적인 적용 및 구현 평가가 필요하겠다.

6. 참고문헌

[1] IEEE, "IEEE P802.11 Wireless LANs: Proposed TGi D1.8 Clause 8 Editing Changes," IEEE 802.11-02/178r0, March 2002.

[2] IEEE, "Standard for Local and metropolitan area networks : Port-Based Network Access Control," IEEE Std 802.1X, June 2001.

[3] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol(EAP)," RFC 2284, March 1998.

[4] A. Mishra, W. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard," CS-TR-4328, Feb. 2002.

[5] ETSI, "UMTS; 3G security; Security architecture," ETSI TS 133 102 v5.0.0, June 2002.