홈 네트워크 환경에서 EAP-AKA 기반 디바이스 인증 메커니즘 구현

김제윤*, 이진홍*, 신상욱*

*부경대학교 정보보호 협동과정

The Implementation of Device Authentication Mechanism in Home Network based on EAP-AKA

Je-Yoon Kim*, Jin-Hung Lee*, Sang-Uk Shin*

* Department of Information Security, Pukyong National University

요 약

홈 네트워크 보안기술은 안전한 홈 네트워크를 보장하고, 다양한 홈 네트워크 디바이스를 대상으로 안전한 서비스를 위해 필수적이다. 이러한 환경에서 안전하게 디바이스를 인증하고 서비스를 제공하기 위하여 표준화된 보안기술이 요구되고 있다. 본 논문에서는 3GPP UMTS 환경의 표준인 AKA 메커니즘에 기반한 EAP-AKA 인증 방식을 사용하여 디바이스와 네트워크가 상호 인증하고, 디바이스간 보안통신을 컨트롤하는 시스템을 설계하고 구현한다.

I. 서론

향후 홈 네트워크를 위한 다양한 제품 출시가 기하급수적으로 증가될 것으로 예상되는 상황에서 이들 디바이스간의 보안이 이슈화되고 있다. 정부와 통신사업자가 가전 및 건설업계 등과 함께 의욕적으로 진행하고 있는 홈 네트워크 사업이 시범사업을 마치고 본격적인 상용 서비스를 시작함에 따라 홈 네트워크 보안 문제가 뜨거운 관심을 불러일으킬 것이다. 계획에 의하면 오는 2007년까지 국내 총 가구의 60%에 달하는 1000만 가구에 홈 네트워크 시스템이 도입됨으로 인하여 모든 정보가전기기가 연결되어 지능화되는 홈 네트워크 시대가 열릴 것으로 예상된다. 하지만 정보가전기기가 내·외부망과 연동되는 홈 네트워크상에서 디바이스들은 다양한 해킹과 바이러스 등의 사이버 공격을 받을 것으로 예상되면서 홈 네트워크 사업 성공의 필수요소로 보안기술이 요구되고 있다.

홈 네트워크 보안기술은 안전한 홈 네트워크를 보장하고 다양한 홈 네트워크 디바이스를 대상으로 안전한 서비스를 위해 필수적이다. 또한 기존의 네트워크에서 존재하는 보안 취약성의 문제는 홈 네트워크에서도 나타나며, 안전성 확보를 위하여 기존의 인터넷 보안기술이 필수적으로 요소기술 내에 포함되어야 한다.

하지만 국내 보안기술의 현황은 홈 네트워크의 하부계층의 다양한 하드웨어와, 상위계층의 유비쿼터스 홈 네트워크 서비스 및 어플리케이션을 통합하는 기술을 개발하는데 중점을 두고 있다. 아직 미들웨어 상에서 지원되는 보안기술 개발은 그 진행이 미비하며, 홈 네트워크의 다양한 구성요소들 간의 이기종 상호연동을 위한 기술개발은 초기단계이다.

본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었음

한편 802.1x 와 같은 무선 환경에서는 무선 보안 취약성이 많이 나타나고 있다. 때문에 각각의 표준을 지원할 수 있는 EAP[4](Extensible Authentication Protocol)를 사용한 인증이 요구되고 있다.

본 논문에서는 EAP와 DIAMETER[2] AAA Server에 대한 기본사항을 알아보고 3GPP(3rd Generation Partnership Project)에서 사용된 AKA(Authentication and Key Agreement) 인증방식을 무선랜 환경에서 사용한 EAP-AKA인증방식의 진행과정을 알아본다. 그리고 디바이스와 홈 게이트웨이와 홈 서버가 EAP-AKA 와 DIAMETER AAA를 사용하여 상호인증하고 보안 통신하는 시스템을 구현한다. 3GPP UMTS(Universal Mobile Telecommunications System) 환경의 표준인 AKA에 기반한 EAP-AKA[5]방식을 사용하여 사용자가 홈 게이트웨이를 통하여 댁내의 디바이스를 안전하게 제어할 수 있다.

II. EAP 와 DIAMETER AAA

2.1 EAP

EAP(Extensible Authentication Protocol) 프로토콜은 원래 PPP(Point-to-Point Protocol) 접속 환경에서 인증/키 설정을 하기 위해 IETF (Internet Engineering Task Force)에서 표준화되었다[1]. IEEE (Institute of Electrical and Electronics Engineers) 802.1x 규격이 완성됨에 따라 IEEE 802.11등의 WLAN(Wireless local area network) 환경에도 적용될 수 있게 되었다. EAP 프로토콜은 특정 인증 프로토콜이 아니라 이름 그대로 임의의 인증 프로토콜을 확장할 수 있는 메커니즘이다. 따라서 기존 또는 미래의 인증 프로토콜을 EAP 규격에 맞추면 EAP용 인증 프로토콜로 이용할 수 있게 된다.

2.2 DIAMETER AAA

무선 환경에서 IEEE 802.1x 표준을 이용한 인증을 하기 위해 Supplicant, Authenticator, Authentication Server가 필요하다.

DIAMETER AAA 프로토콜은 유무선 이동 인터넷 환경에서 가입자에 대한 인증(Authentication), 권한검증(Authorization) 그리고 과금(Accounting)의 서비스를 제공한다[2]. 또한 안전하고 신뢰성 있는 이동성 지원, 로밍 및 보안 등의 요구를 충족할 수 있다.

휴대인터넷 네트워크 액세스 서비스를 위한 인증시 DIAMETER EAP 응용 프로토콜이 적용되며 DIAMETER의 DER(DIAMETER EAP Request) 메시지를 이용해 EAP Payload를 전달한다[3].

2.3 EAP-AKA

EAP-AKA 인증은 UMTS AKA 메커니즘을 사용하는 EAP (Extensible Authentication Protocol)[4]이다. UMTS AKA는 대칭키 기반으로 Challenge-Response 메커니즘을 사용하며, 상호 인증을 제공한다.

EAP-AKA 인증은 IETF 표준으로 3세대 이동통신망의 사용자가 AKA 메커니즘을 이용하여 WLAN 망에서 동일하게 인증될 수 있다[5].

EAP-AKA 프로토콜은 다음과 같이 진행된다[6][7].

먼저 UE(User Equipment)와 WLAN 사이에 연결이 성립하고 WLAN은 UE의 신원을 요구하는 EAP-Request/Identity를 UE에게 송신한다. 이때, UE는 자신의 신원을 포함한 EAP-Response/Identity로 응답하고 WLAN은 신원을 확인하여 3GPP AAA서버로 UE로부터 수신한 패킷을 재전송한다. AAA서버는 사용자에 대한 AV(Authentication Vector)가 존재하는지 확인하고 존재하지 않으면 HLR(Home Location Register)에서 검색한다. AAA 서버는 RAND, AUTN, 익명 신원이 포함된 EAP-Request/AKA-Challenge를 UE에게 송신한다. UE는 AUTN 검증으로 네트워크를 인증하고 SQN으로 동기를 확인한다. SQN, AUTN 검증에 성공하면 RES, CK, IK를 계산하고, SQN 검증에 실패하면 재동기화를 실행하고 AUTN 검증에

실패하면 프로토콜을 종료한다. UE는 계산한 RES를 포함한 EAP-Response/AKA-Challenge를 AAA 서버에게 송신한다. AAA 서버는 XRES와 RES를 비교하여 UE를 인증한다. 이때, 인증이 성공하면 AAA 서버는 WLAN에게 EAP-Success 메시지와 함께 KEY들을 송신한다. WLAN은 KEY들을 저장하고 UE에게 EAP-Success 메시지를 송신한다. 이러한 과정을 통하여 네트워크와 디바이스 각각의 상호인증이 진행되게 된다[8][9].

III. 시스템 설계 및 구현

3.1 전체 시스템 설계 구성도

전체 시스템 구성은 그림 1과 같다. 각각의 디바이스들은 홈 게이트웨이를 통하여 상호 통신이 가능한 상태이다. 그림 1과 같이 EAP-AKA와 DIAMETER EAP Procotol을 이용하여 홈 네트워크에 적용 가능한 모델을 구성하였다. 디바이스2는 홈 네트워크 기기에 대응하는 컨트롤 가능한 PC카메라를 이용하였고 디바이스1은 디바이스2와 통신하는 또 하나의 디바이스로 PDA와 PC로 구성하였다. 디바이스1은 디바이스2를 제어할 수 있는 메시지를 EAP-AKA를 이용하여 생성한 키를 사용하여 보호하여 통신하게 된다.

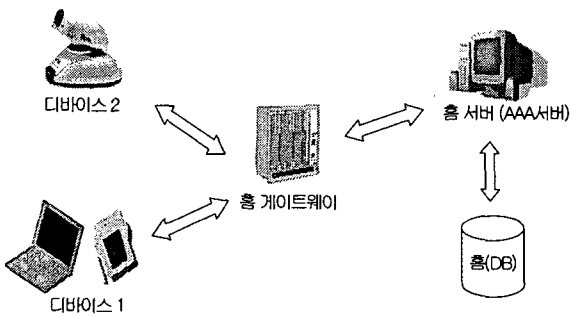

그림 1. 전체 시스템 구성

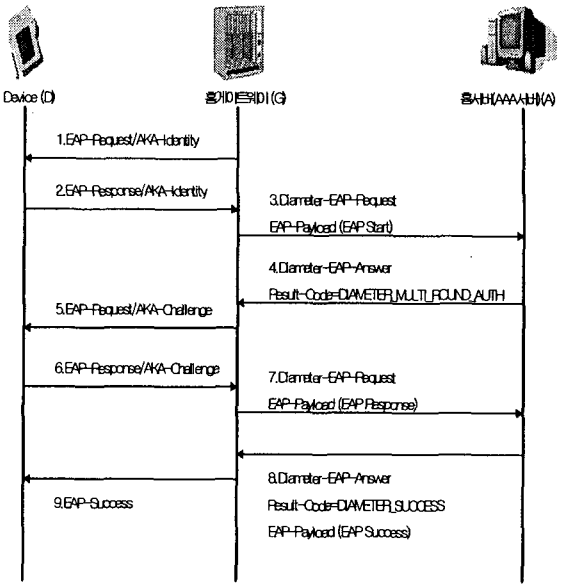

그림2. 디바이스 인증과정

3.2 EAP-AKA 기반 디바이스 인증 프로토콜

EAP-AKA의 인증과정은 그림 2와 같이 이루어진다.

1. 홈 게이트웨이는 디바이스에게 신원을 요구하는 EAP-Request/AKA-Identity 메시지를 보낸다.

2. 디바이스는 자신의 신원을 포함하여 EAP-Response/AKA-Identity 로 응답한다.

3. 홈 게이트웨이는 디바이스의 신원을 확인한 후 메시지를 캡슐화하고 EAP-Payload(EAP Start) 의 DIAMETER-EAP-Request 메시지를 생성하여 홈 서버로 전송한다.

4. 홈 서버는 디바이스의 신원을 데이터베이스에서 확인한다. 그리고 128비트의 인증을 위한 값 RAND를 생성하고 네트워크 인증을 위한 AUTN(SQN, AMF, MAC)을 구성하여, MAC(Message Authentication Code)을 다음과 같이 MAC = f1(PSK, SQN, AMF, RAND)

계산하고 이를 캡슐화 하여 Result-Code = DIAMETER_MULTI_ROUND_AUTH 값을 갖는 DIAMETER-EAP-Answer로 응답한다. 여기서 PSK는 디바이스와 DIAMETER AAA간의 공유 마스터키이다.

5. 홈 게이트웨이는 이 값들을 EAP-Request/AKA-Challenge 메시지를 사용하여 디바이스로 전송한다. 디바이스는 MAC을 검증하여 네트워크를 인증하게 된다. 그리고 디바이스 인증을 위해 서버로 전송할 128비트의 RES를 다음과 같이 RES = f2(PSK, RAND)계산하고 이후에 사용될 128비트의 암호화키 CK(Confidentiality Key)와 무결성키 IK(Integrity Key)를 계산한다. 한편, MAC 검증에 실패하면 프로토콜을 종료한다.

6. 디바이스는 계산한 RES를 포함한 EAP-Response/AKA-Challenge를 홈 게이트웨이로 전송한다.

7. 홈 게이트웨이는 EAP-Payload(EAP Response)인 DIAMETER-EAP-Request로 캡슐화 하여 홈 서버로 전송한다.

8. 홈 서버는 디바이스로부터 받은 RES와 계산한 XRES를 비교하여 디바이스를 인증하고 인증에 성공하면 Result-Code=DIAMETER_SUCCESS, EAP-Payload(EAP Success)를 가지는 DIAMETER-EAP-Answer 메시지로 응답하고 함께 CK, IK를 전송한다. RES 인증 실패시에는 EAP-Payload(EAP Failure)를 송신하고 프로토콜을 종료하게 된다.

9. 홈 게이트웨이는 CK, IK를 저장하고 인증 성공의 EAP-Success 메시지를 디바이스에게 전송하게 된다. CK, IK는 디바이스에도 존재하므로 디바이스와 홈 게이트웨이 사이에 공통된 키를 갖게 되고, 이 키는 보안통신에 사용된다.

3.3 시스템 구현

그림 1에서 설명한 시스템을 다음과 같이 구현하였다.

① 디바이스 1

화상 카메라 컨트롤러로서 일반 Window용 프로그램과 PDA용 EVC 에뮬레이터를 이용하여 구현하였다. 컨트롤 버튼을 이용해서 카메라를 원격 제어하는 디바이스이다.

② 디바이스 2

화상 카메라 서버로서 제어 가능한 화상카메라가 부착되어 있다. 디바이스1 으로부터 데이터를 받아 화상 카메라를 제어하고 영상을 압축 전송하는 디바이스이다.

③ 홈 게이트웨이

각각의 디바이스의 통신을 연결한다. 리눅스에서 구현하였으며 EAP-AKA 를 이용 디바이스와 통신하고 DIAMETER EAP Protocol을 이용하여 AAA서버와 통신한다. 디바이스와의 통신에 기반이 되는 각 디바이스의 비밀키를 저장하고 각각의 디바이스의 통신을 연결하고 암복호화를 수행한다.

④ 홈 서버(DIAMETER AAA서버)

인증에 필요한 정보를 생성하고 디바이스를 인증하는 AAA서버이다. 인증에 관련된 값을 생성하고 디바이스를 인증하고 데이터베이스의 디바이스 정보를 관리한다.

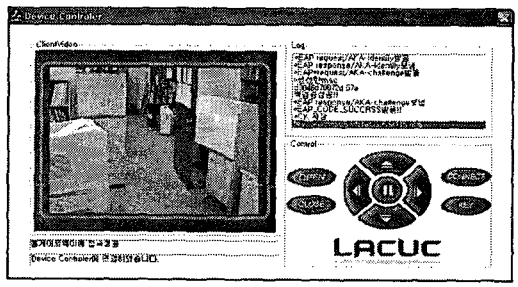

그림 3. 디바이스1 인증화면

3.4 인증과 보안통신

그림 3과 그림 4는 디바이스1이 인증을 요청할 때 디바이스와 홈 서버의 화면이다. 그림 1과 같이 디바이스와 홈 서버는 홈 게이트웨이를 통하여 통신하게 된다. 디바이스는 홈 게이트웨이로부터 EAP-Request/AKA-Challenge

메시지를 받아 RAND, AUTN 으로 XMAC을 생성하고 생성한 XMAC과 서버로부터 받은 MAC을 비교한다.

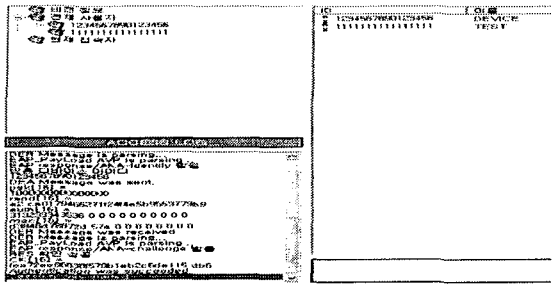

그림 4. 홈 서버

홈 서버는 디바이스로부터 Identity를 받고 키를 검색하여 RAND, AUTN을 디바이스로 전송하고 디바이스로부터 RES를 받아 생성한 XRES와 확인한다. 그림 5와 같이 홈 게이트웨이는 홈 서버와 디바이스간의 통신을 처리하고 각 디바이스의 CK를 저장한다.

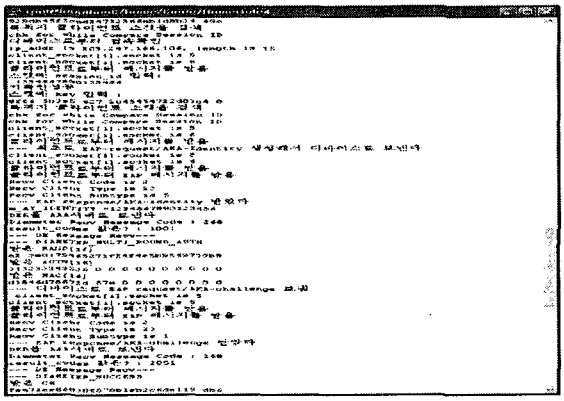

그림 5. 홈 게이트웨이

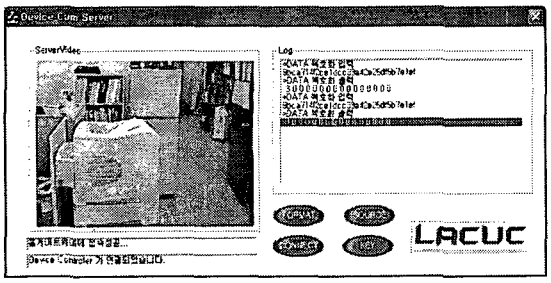

그림 6. 디바이스2

그림 7. EVC 디바이스1

홈 게이트웨이는 각각의 디바이스에 대하여 EAP-AKA 인증과정을 통한 CK를 저장하고 있다. 따라서 디바이스1이 제어 메시지를 CK_D1G로 암호화하여 홈 게이트웨이로 보낸다. 이에 홈 게이트는 패킷의 Send_ID에 대한 CK를 찾아 DATA를 복호화 하고 다시 Recv_ID의 CK로 암호화하여 디바이스2로 전송한다. 그림 6과 같이 디바이스2는 홈 게이트웨이로부터 받은 패킷을 CK_D2G로 복호화 하여 카메라를 컨트롤한다. 또한 PDA에서 사용 가능하도록 그림 7과 같이 WinCE를 기반으로한 EVC 에뮬레이터를 이용하여 디바이스 1을 구현하였다. 디바이스간 메시지 보호는 Rijndael AES(Advanced Encryption Standard) 알고리즘을 사용하였다.

IV. 결론

본 논문에서는 3GPP UMTS와 WLAN환경에서 연동 가능한 EAP-AKA와 DIAMETER EAP 프로토콜을 사용하여 디바이스와 네트워크가 상호 인증하는 시스템을 구현하였다. 또한 홈 네트워크의 환경에 근접하기 위해 각각의 기능을 가진 디바이스를 실제로 구현하였다. 그리고 메시지를 통해 디바이스를 컨트롤하였다.

향후 디바이스간의 단대단 보안채널 설정 메커니즘에 관한 설계 및 구현을 진행할 것이며, 이기종 상호연동 보안 프로토콜에 관해 연구할 것이다.

[참고문헌]

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

[2] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko "Diameter Base Protocol", IETF RFC 3588, sep. 2003

[3] P. Eronen, T. Hiller, G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", IETF RFC 4072, August 2005

[4] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson , H. Levkowetz, "Extensible Authentication Protocol (EAP)", IETF RFC 3748, June 2004

[5] J. Arkko and H. Haverinen "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", IETF RFC 4187, January 2006

[6] 3GPP TR 22.934 "Feasibility study on 3GPP system to Wireless Local Area Network(WLAN) Interworking (release 6)" sep. 2003

[7] 김영세, 이정우, 한진희, 신진아, 전성익, "무선 네트워크 연동 보안 기술 동향", 전자통신동향 분석, 제20권, 제1호, 2005년, 2월

[8] 3GPP TS 35.205-208 "Specification of the MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5, and f5*;(Release 5)" June 2002

[9] 박미애, 김용희, 이창범, 이옥연, "3GPP-WLAN 연동을 위한 EAP-AKA에서의 키 생성에 관한 연구", 한국정보보호학회 동계 정보보호학술대회 논문집 Vol.13, No.2