AVISPA를 이용한 3GPP 네트워크의 EAP-AKA 프로토콜 명세 및 검증

김현수*, 최진영*
*고려대학교 컴퓨터학과
e-mail:hyunsu@formal.korea..ac.kr

The Specification and Verification of EAP-AKA Protocols on 3GPP Network Using AVISPA

Hyun-Su Kim*, Jin-Young Choi*
*Dept. of Computer science, Korea University

요 약

휴대인터넷(WiBro: Wireless Broadband)은 언제 어디서나 고속으로 무선 인터넷 접속이 가능한 서비스를 위한 기술이다. 노트북을 비롯한 휴대가 간편한 PDA, 스마트폰으로 사람이 보행 또는 차량 주행 중에서도 끊김 없이(seamless) 무선 인터넷 서비스가 가능하다. 이동성과 고속 무선 통신이 가능한 서비스에서 중요한 기술 요소 중 하나가 보안이다. 본 논문은 안전한 서비스를 제공하기 위하여 WiBro 무선 네트워크에서의 USIM 기반 EAP-AKA 인증 프로토콜 보안 요구사항 안전성을 정형기법 툴인 AVISPA를 이용하여 명세 및 검증해 본다.

1. 서 론

언제 어디서나 인터넷에 접속하여 필요한 정보를 얻을 수 있는 고속 이동 인터넷 환경을 제공하기 위한 서비스가 2.3GHz 휴대인터넷(WiBro: Wireless Broadband)[1]이다. 사용자가 보행 또는 차량 주행 등의 이동환경에서 고속으로 인터넷에 접속해 필요한 정보나 멀티미디어를 즐길 수 있는 무선 네트워크를 이용한 데이터 서비스로서 이동 멀티미디어 서비스가 가능하다. 고속 이동 중에도 인터넷에 접속할 수 있다는 점에서 기존 핫스팟 공중망 무선랜과 차별화되고 있으며, 고속으로 데이터 통신이 가능한 점에서 기존 이동통신의 데이터 서비스와 차별화되는 강점을 가진다.

이러한 휴대인터넷의 안전한 서비스를 위해 중요한 기술 요소 중 하나가 보안이다. 안전한 고속 이동 무선 네트워크 서비스를 제공하기 위해서는 기본적으로 네트워크 보안, 단말 보안, 사용자 보안을 고려할 수 있고, 더불어 타 망과의 연동 시 망간의 보안 연동 구조도 설계되어야 하며, Mobile IP, 무선 그룹 멀티캐스팅 등의 여러 보안 요소들이 고려되어야 한다. 본 논문에서는 여러 보안 요소들 중에서 IEEE 802.16에서 제안하고 있는 EAP-AKA[2] 인증프로토콜과 정형기법의 적용을 제시한다. 3GPP에서 무선랜과의 연동을 위해 제안한 인증 프로토콜인 EAP-AKA를 WiBro 무선 네트워크에서도 적용하여 사용자와 네트워크간의 상호 인증 및 사용자 인증 정보를 USIM 기반의 스마트 카드에서 관리 및 처리하여 보다 안전한 인증 메커니즘을 설계할 수 있다.

2. EAP-AKA

3GPP[3] 네트워크 접속을 위해서는 USIM에 탑재된 AKA 인증 절차를 수행하여야 한다. AKA 인증은 크게 단말과 네트워크 사이의 인증 벡터 분배 단계와 분배된 인증 벡터와 USIM의 AKA 절차를 통한 인증 및 키 분배 단계로 나눌 수 있다. 위 두 절차가 끝나면 단말과 네트워크는 두 통신 객체 사이에 교환될 메시지의 무결성 및 기밀성 제공이 가능

해진다. 또한 단말과 네트워크의 상호 인증을 통해 두 통신 객체간의 신뢰관계가 형성된다. [그림.1]은 3GPP 네트워크 접속인증을 위한 전체 단계를 보여주며, 다음은 3GPP AKA 인증 절차를 설명한 것이다.

2.1 EAP 프로토콜

EAP[4]는 IEEE 802.1x 포트 기반의 가입자 인증 데이터 전송을 위한 표준 프로토콜이다. 다중 인증 메커니즘을 지원하는 프로토콜로서 스마트 카드, Kerberos, 공용키 암호화, OTP(One Time Password)를 포함한 수많은 인증 방식을 지원한다. 현재 IETF에 EAP 워킹 그룹이 설치되어 ID/Password, 인증서, 스마트 카드 등 다양한 인증 방식을 지원하는 알고리즘과 각 인증 알고리즘을 이용한 세션 키 생성 방법의 표준화를 추진하고 있다.

2.2 AKA(Authentication and Key Agreement)

3GPP(3rd Generation Partnership Project)[5]에서 제안하여 유럽 3G 이동통신에서 사용되는 인증 및 키 일치 메커니즘이다. AKA 인증 및 키 일치 프로토콜은 GSM(Global System for Mobile Communication)인증 메커니즘과의 backward compatibility를 지원하고, GSM과 비교하여 볼 때 키 길이가 충분히 크고, 클라이언트 뿐만 아니라 서버까지 인증하는 상호 인증 방식을 제공한다. 또한 UICC/USIM(UMTS Subscriber Identity Module) 등 스마트 카드 기반으로 하는 인증 및 키 일치 메커니즘이다.

2.3 EAP-AKA

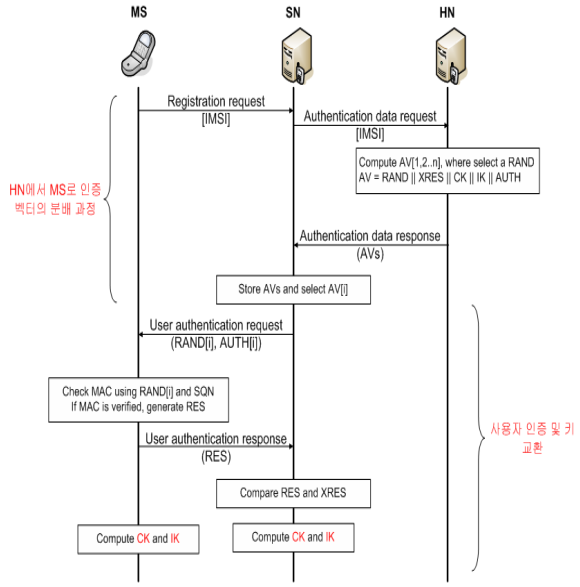
3GPP에서 제안한 AKA 방식을 EAP의 인증 프로토콜에 적용하여 3GPP와 무선랜과의 연동 보안 인증 프로토콜로 EAP-AKA를 3GPP에서 제안하고 있다[6]. 본 논문에서는 EAP-AKA를 WiBro 무선 네트워크 인증 메커니즘 PKMv2 EAP 기반의 인증 절차에 적용하여 사용자와 무선 네트워크간의 상호 인증과 세션 키를 생성한다. 그리고 사용자 인증 정보를 단말이 아닌 UICC에 안전하게 저장, 관리, 처리함으로서 사용자 인증 정보를 보호할 수 있다. EAP-AKA를 적용한 3GPP-WLAN 연동 네트워크에서 EAP-AKA를 적용한 WiBro 무선 네트워크까지도 쉽게 접목시킬 수 있는 연동 보안 인증 메커니즘이 가능하다.

3. EAP-AKA 프로토콜 동작 과정

3.1 인증 벡터 분배 단계

3.1.1) SN에서 새로운 단말의 접근을 확인하면 단말의 ID인 IMSI (International Mobile Subscriber Identifier)를 요청하고 단말은 자신의 IMSI를 등록 요청 메시지에 포함하여 해당 SN에게 전달한다.

3.1.2) 등록 요청 메시지를 수신한 SN은 단말의 IMSI를 인증 요청메시지를 통해 HN 전달한다. IMSI를 수신한 HN은 해당 단말이 자신이 관리하는 단말인지 확인하고 확인 과정을 마치면 SN이 단말을 인증할 파라미터와 SN과 단말의 비밀통신을 위한 키를 생성하여 다수의 인증 벡터를 만든다. HN은 생성된 인증 벡터를 해당 SN에게 전송한다.



[그림.1] EAP-AKA 인증 절차

3.1.3) HN에게 해당 단말에 대한 다수의 인증 벡터를 수신한 SN은 이를 저장하고, 단말을 인증하기 위해 하나의 인증 벡터를 선택한다. 선택한 인증 벡터의 RAND와 AUTH만을 검출하여 단말에게 인증 요청 메시지를 통해 전달한다.

3.2 상호 인증 및 키 교환 단계

3.2.1) 인증 요청 메시지를 수신한 단말은 수신한 RAND 값과 자신의 마스터키를 이용하여 AUTH의 MAC 값을 확인한다. 이것이 확인되면 단말은 HN을 인증하여 수신한 인증 요청 메시지가 정상임을 알 수 있다. 이후 단말은 수신한 AUTH의 SQN 값이 적절한 범위의 값인지 확인 하고 SN으로부터 인증 받기 위한 RES 값을 RAND와 마스터키를

사용하여 생성한다. 생성된 RES 값을 인증 응답 메시지에 포함하여 해당 SN에게 전달한다.

3.2.2) 인증 응답 메시지를 수신한 SN은 HN으로부터 수신한 인증 벡터의 XRES 값과 단말의 RES 값이 일치 하는지 확인하고 두 값이 일치하면 단말의 네트워크 접속을 허용한다.

3.2.3) 이후 단말과 네트워크 사이의 데이터 기밀성 및 무결성 제공을 위한 CK(Cipher Key)와 IK(Integrity Key)를 공유하게 된다. SN은 인증벡터 내에 포함된 CK, IK를 사용하고 단말은 인증 요청 메시지에 포함된 RAND 값과 자신의 마스터키를 사용하여 CK, IK를 생성한다. 정상적인 인증 절차가 완료되면 SN의 CK, IK는 단말과 동일 한 값이 된다.

[표.1] 주요 용어 정리

용 어	내 용
Time Stamp	단말의 현재 시간 값 Ti
SN	Serving Network
HN	Home Network
SK	Session Key, 단말과 SN 간에 생성되는 세션키
CK	Cipher Key, 단말과 네트워크 사이의 데이터 기밀성을 제공하는 키
IK	Integrity Key, 단말과 네트워크 사이의 무결성을 제공하는 키
LAI	Location Area Identity, SN의 지역ID
IMSI	International Mobile Subscriber Identifier로 단말의 ID
RADN	인증 서버에서 생성하는 임의의 수
AUTH	Authentication Value, 인증 서버에서 생성하는 인증 값
f1, f2	암호 알고리즘
f3, f4, fx	키 생성함수

4. EAP-AKA 보안 요구 사항

4.1 기밀성(Confidentiality)

· 암호 알고리즘 동의: MS와 SN은 이후 통신에 사용될 알고리즘을 안전하게 협상한다.
· 암호키 동의: MS와 SN은 이후 사용할 암호키를 협상한다.
· 사용자 데이터의 기밀성: 사용자의 데이터는 통신 인터페이스 상에서 누설되지 않아야 한다.
· 시그널링 데이터의 기밀성: 시그널링 데이터는 통신 인터페이스 상에서 누설되지 않아야 한다.

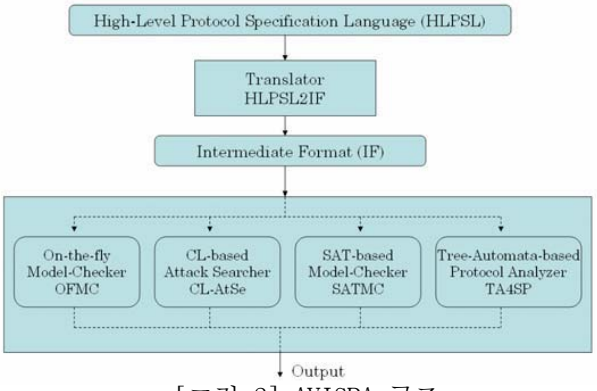
4.2 데이터 무결성(Data integrity)

· 무결성 알고리즘 동의: MS와 SN은 이후 사용될 무결성 알고리즘을 협상한다.
· 무결성 키 동의: MS와 SN은 이후 사용될 무결성 키를 협상한다.
· 데이터 무결성과 시그널링 데이터의 인증: MS또는 SN은 SN과 MS에서 보내진 데이터가 권한 없는 방식으로 수정되지 않았음을 확인할 수 있는 성질을 가지고 있어야 한다.

5. AVISPA와 HLPSL 소개

5.1. AVISPA (Automated Validation of Internet Security Protocols and Applications)

인터넷 프로토콜의 보안성을 정형 검증하는 도구로 상용 프로토콜을 보안의 문제점을 지적하고 있다. AVISPA Tool[7]은 독립적으로 개발된 모듈로 구성되어 있다. 툴의 입력으로 사용되는 High-Level Protocol Specification Language(HLPSL)은 표현력이 뛰어 나고, 모듈로 구성되어 있고, role-based인 정형언어이다. HLPSL은 HLPSL2IF 변환기을 통하여 Intermediate Format(IF)으로 자동 생성되어 OFMC[8], CL-AtSe, SATMC, TA4SP의 입력으로 사용된다.



[그림.2] AVISPA 구조

5.2 HLPSL(High Level Protocols Specification Language)

HLPSL[9]은 role을 기반으로 하는 언어로써, 각각의 role들은 서로 독립되어 구성이 되어있고, channel을 통

해 의사소통을 한다. role은 역할에 따라 두 가지로 나누어 구분할 수 있는데, 프로토콜을 구성하는 각각의 개체들을 기술하는 basic role과 basic role들의 시나리오를 기술하기 위한 composition role로 구성된다. basic role은 각 개체들이 가지고 있는 정보를 표기하고, SND와 RCV 명령어를 이용하여 다른 개체들과 서로의 정보를 교환하여 의사소통을 한다. composition role은 전체 프로토콜의 구성을 나타내는 role로써 각 role들이 가지고 있는 각각의 구조와 공격자(intruder)가 가지고 있는 정보, 프로토콜의 검증 속성을 포함하는 goal들을 표기한다.

5.3 SPAN

SPAN[10]은 AVISPA의 web graphical interface의 local version이다. 범용 적으로 사용되는 컴파일러의 형태를 차용하여 시각적으로 이해하기 쉽게 설계되었고, 아직 툴이 완벽하지는 않지만, 단점을 보완한 새로운 버전이 계속 나오고 있다.

6. EAP-AKA 프로토콜 분석

다음은 EAP-AKA 프로토콜을 HLPSL로 명세한 부분 중에서 서버(server)에 대한 role의 명세부분이다.

```
role server (

  init
    State := 1

  transition
  1. State   = 1
       ∧ RCV(start)
     =|>
     State' := 3
       ∧ SND(request_id)

  2. State   = 3
       ∧ RCV(respond_id.NAI')
     =|>
     State' := 5
       ∧ AT_RAND' := new()
       ∧                  AT_AUTN'                  :=
{SQN}_F5(SK.AT_RAND').F1(SK.SQN.AT_RAND')
       ∧ CK'      := F3(SK.AT_RAND')
       ∧ IK'      := F4(SK.AT_RAND')
       ∧                  AT_MAC1'                  :=
HMAC(PRF_SHA1(NAI'.IK'.CK').AT_RAND'.AT_AUTN')
       ∧ SND(AT_RAND'.AT_AUTN'.AT_MAC1')
       ∧ witness(S,P,at_rand,AT_RAND)
       ∧ secret(CK',sec_ck,{S,P})

  3. State   = 5
       ∧ RCV(AT_RES'.AT_MAC2')
       ∧ AT_RES'  = F2(SK.AT_RAND)
       ∧ AT_MAC2'= HMAC(PRF_SHA1(NAI.IK.CK).AT_RES')
     =|>
     State' := 7
       ∧ SND(success)
       ∧ request(P,S,at_rand,AT_RAND)

end role
```

[그림.3] EAP-AKA 프로토콜의 HLPSL 명세 코드

[그림.3]의 명세를 통해 단말(P)와 서버(S) 사이의 기밀성키(CK)와 무결성키(IK)의 인증 과정을 보였고 프로토콜의 검증 속성인 보안(secrecy)과 인증(authentication)을 검증하기 위하여 secret()과 witness(), request()의 함수를 사용하였다. 위에 명세된 코드에서의 각 함수의 의미는 다음과 같다.

secret(CK',sec_ck,{S,P}) : 단말(P)와 인증서버(S)사이에 암호키(CK')에 대한 보안요구 사항이 만족 되는지를 검증한다. sec_ck은 goal부분에 명세하기 위한 ID값이다.

witness(S,P,at_rand,AT_RAND) : AT_RAND의 값에 대해서 S는 P와 통신하길 원하는 인증(authentication)을 의미 하며, at_rand는 goal에 명세하기 위한 ID값이다.

request(P,S,at_rand,AT_RAND) : P는 AT_RAND의 값을 받아들이고 S의 존재에 대한 인증(authentication)을 의미 하며, at_rand는 goal에 명세하기 위한 ID값이다.

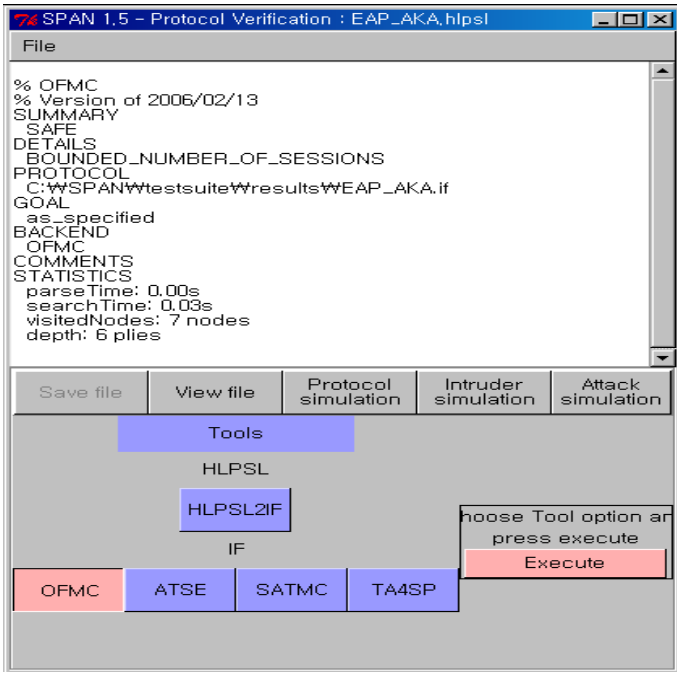
request()는 witness()와 함께 인증을 위한 함수로 사용 된다. 위와 같은 검증 속성을 통해 프로토콜의 보안 요구 사항과 인증 문제의 안전성을 검증하였다.

7. EAP-AKA 프로토콜 검증 결과

[그림.4] EAP-AKA 프로토콜 검증 결과

위의 검증결과는 AVISPA의 4가지 back-ends 중에서 OFMC에 대한 검증결과로서, [그림.4]에서 볼 수 있듯이 SUMMARY 부분이 SAFE 함을 통해 본문의 명세 부분에 대해서는 안전한 프로토콜임을 확인할 수 있고, 이로써 GOAL부분을 통해 명세 된 EAP-AKA 프로토콜의 검증 속성인 보안(secrecy)과 인증(authentication)에 대한 요구사항을 만족함을 확인할 수 있다.

8. 결 론



Ubiquitous 네트워크 환경에서 3G 이동 통신 네트워크는 넓은 사용자 서비스 영역과 Global Roaming을 지원하는 무선망으로 널리 사용되고 있다. 이러한 3G 네트워크를 접속하기 위해서는 USIM 기반의 AKA 인증 절차가 필수적으로 수행되어야 한다.

단말기의 보급과 함께 네트워크에서 관리해야할 사용자 수의 증가로 네트워크에서 관리해야할 사용자 정보가 급격하게 증가하는 네트워크 환경에서는 사용자 인증 및 네트워크 접속 관리를 효율적으로 제공하는 인증 기법이 필수적이다. EAP-AKA 프로토콜의 안전성을 검증하기 위하여 정형 명세 언어인 HLPSL을 이용하여 명세하고, 이를 정형 검증 툴인 AVISPA를 통해 요구된 검증 속성에 대한 안정성을 검증하였다.

향후 연구 방향으로 언제 어디에서든지 기밀성과 무결성이 보장된 서비스를 받을 수 있도록 보다 안전성이 뛰어난 프로토콜 개선에 대해 연구해 보고자 한다.

참고 문헌

[1] 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.

[2] RFC 4187, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement(EAP-AKA)”, January 2006.

[3] 3GPP TS 33.234, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security, Wireless Local Area Network(WLAN) interworking security”, June 2005.

[4] RFC 3748, “Extensible Authentication Protocol(EAP)”, June 2004.

[5] 3GPP TS 33.102, “3rd Generation Patnership Project; Technical Specification Group Services and System Aspects; 3G Security, Security architecture”, June 2003.

[6] Draft-arkko-pppext-eap-aka-12.txt “Extensible Authentication Protocol for UMTS Authentication and Key Agreement(EAP-AKA),” Apr. 2004.

[7] AVISPA. "AVISPA v1.1 User Manual", Available at http://www.avispa-project.org, 2006.

[8] D. Basin, S. M¨odersheim, L. Vigano`, "OFMC : A symbolic model checker for security protocols", International Journal of Information Security, 2004.

[9] AVISPA. "HLPSL Tutorial : A Beginner's Guide to Modelling and Analysing Internet Security Protocols",Available at http://www.avispa-project.org, 2006.

[10] AVISPA. "SPAN : A Security Protocol Animator for AVISPA Version 1.1 User Manual", Available at http://www.avispa-project.org, 2007.