SIP와 DIAMETER의 인증 연동 및 안전성 분석

준회원 박 성 준*, 정회원 정 수 환*, 이 병 길**, 김 현 곤**

Interworking of SIP Authentication with DIAMETER and Security Analysis

Sungjoon Park* *Associate member,*

Souhwan Jung*, Byung-Gil Lee**, Hyun-Gon Kim** *Regular members*

요 약

AAA는 다양한 응용 서비스에 대한 신뢰성을 보장하기 위해 인증, 권한 검증, 과금 등의 기능을 제공하고 있으며, IETF에서는 차세대 AAA 프로토콜로 DIAMETER를 제안하고 있다. 또한 VoIP용 호 설정 프로토콜로서 제안된 SIP(Session Initiation Protocol)[1]는 앞으로의 통신망에서 핵심기능을 담당할 것이며, SIP 서비스에 대한 신뢰성을 보장하기 위해서는 AAA와의 연동이 필요하다. 그러나 SIP에서 사용자 인증을 위한 digest 인증 메커니즘은 man-in-the-middle attack이나 dictionary attack에 취약성을 갖고 있다. 본 논문은 유무선 통합 시그널링 프로토콜로 정착될 SIP와 신뢰성 있는 서비스를 제공하기 위한 AAA 프로토콜인 DIAMETER 간의 인증 연동 방안과 인증 연동에서의 안전성을 분석하였다. 또한 보안상의 취약성 해결을 위해 주소 정보를 포함한 인증 정보의 생성 방안과 패스워드 기반의 상호인증 및 세션키 교환을 위해 AKE-ECC를 적용하는 방법을 제안하였다.

Key Words : SIP; DIAMETER; Authentication.

ABSTRACT

The DIAMETER protocol provides Authentication, Authorization, and Accounting (AAA) transactions across the Internet. SIP(Session Initiation Protocol)[1] will be used for new types of signaling, such as instant messaging and application level mobility across networks. And SIP will be a major signaling protocol for next generation wireless networks. But the Digest authentication scheme is not using a secure method of user authentication in SIP, and it is vulnerable to man-in-the-middle attacks or dictionary attacks. This study focused on designing a SIP proxy for interworking with AAA server with respect to user authentication and security analysis. We compared and analyzed the security aspects of the scenarios and propose two proposals that a response which include the user address and password-based mutual authentication and key agreement protocol. It is claimed to be more secure against common attacks than current scenarios.

Ⅰ. 서 론

IETF에서 제안한 SIP는 텍스트 기반 응용 계층의 접속제어 프로토콜로서 클라이언트/서버 구조를 가지며, 인터넷을 이용한 원격 회의, 인터넷 전화, 인스턴트 메시지 등의 서비스와 같이 음성 통신이 가능한 단말간의 호 설정 기능을 제공한다. 또한 SIP는 인터넷상의 모든 단말기, 응용 서비스에서의 시그널링 프로토콜로 적용이 가능하며, 이러한 특성으로 인하여 소프트 스위치(Softswitch)와 3GPP(3rd

* 숭실대학교 정보통신공학과 통신망보안연구실(sjpark5486@hanmail.net)

논문번호 : 030185-0430, 접수일자 : 2003년 4월 30일

Generation Partnership Project)에서도 SIP를 시그널링 프로토콜로 결정하였다. 그리고 앞으로 유무선 통합 네트워크인 NGN(Next Generation Network)에서의 핵심 시그널링 프로토콜 기능을 담당할 것이다.

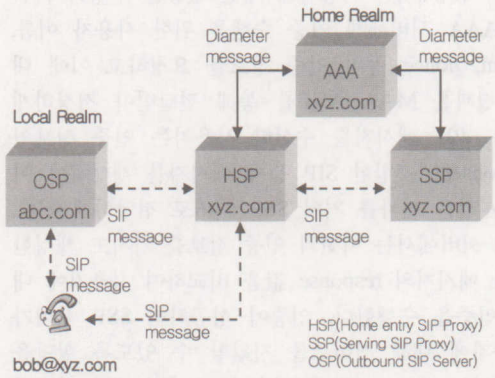
AAA(Authentication, Authorization, Accounting)는 여러 다양한 응용 서비스들에 대한 신뢰성과 안전성을 제공하며, 네트워크 상에서 인증, 권한 검증, 과금 등의 기능을 지원한다. AAA 서버에는 사용자가 제공한 인증 데이터를 저장하고 있으며, AAA 클라이언트와 AAA 서버간의 인증 데이터 전달을 위한 대표적인 프로토콜로 RADIUS (Remote Authentication Dial-In User Service) 프로토콜과 DIAMETER[2][6] 프로토콜이 있다.

SIP가 앞으로의 차세대 통신망에서의 핵심 기능을 수행하기 위해서는 SIP 기반 서비스에 대한 신뢰성과 안전성이 요구되며 이를 위해서는 SIP와 DIAMETER 연동의 중요성이 점점 부각되고 있다. 본 논문에서는 앞으로의 ALL IP 네트워크를 위해 SIP 서버와 AAA 서버에서 사용자 인증을 위한 연동 방법과 보안의 안전성을 분석하고자 한다. Ⅱ장에서는 3GPP와 IETF에서 제시하고 있는 SIP와 DIAMETER간의 연동 방법에 대해 기술하고 있으며, Ⅲ장에서는 기존의 연동 방법들의 보안상의 취약점을 분석하여, 인증정보 생성과 패스워드 기반 프로토콜[9][10]을 이용한 해결 방안을 제시하고 Ⅳ장에서 결론을 기술하고 있다.

Ⅱ. 사용자 인증 연동 방안

1. IETF의 사용자 인증 연동

DIAMETER는 RADIUS와 달리 다양한 응용 서비스의 지원을 위한 확장성과 유연성을 가지고 있으며, SIP와의 연동을 위해서 AVP(Attribute Value Pairs)에 대한 확장이 진행 중이다. 또한 무선 기반의 로밍 서비스 지원하는 3GPP에서도 AAA 서버와 AAA클라이언트간의 프로토콜로 DIAMETER를 선택하고 있다. SIP와 DIAMETER의 인증 연동을 지원하기 위해서는 DIAMETER 메시지와 SIP 메시지간의 변환이 필요하며, 이를 위해서는 SIP 연동을 위한 AVP와 메시지 처리에 대한 정의가 필요하다. SIP 기반의 서비스 사용자는 자신의 위치 정보를 SIP 서버인 REGISTRAR에 등록해야 하며, 이 과정에서 AAA 서버와 DIAMETER를 통한 연동이 필요하다. (그림 1)에서는 SIP와 DIAMETER의 연동을 위한 네트워크 구조를 보여주고 있다[4]. (그림 1)에서 OSP(Outbound SIP Server)는 다른 도메인에 있는 SIP 서버를 나타내며, HSP(Home entry SIP Proxy)는 홈 도메인에 있는 SIP 서버를 말한다. 또한 SSP(Serving SIP Proxy)는 사용자에 대해 SIP 서비스를 제공하는 SIP 서버를 나타내고 있다.



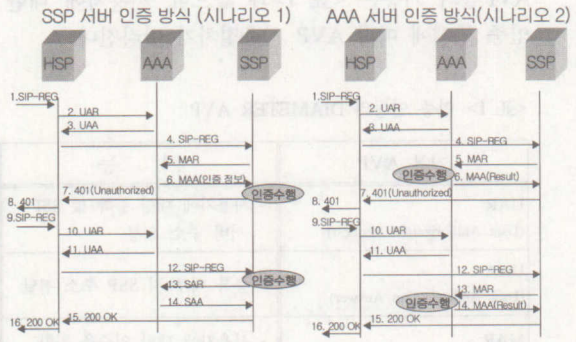
(그림 5) SIP와 DIAMETER의 연동 구조

IETF에서 제안하고 있는 연동 방법은 사용자 인증의 주체에 따라 SIP 서버에서 인증 연동 방법과 AAA 서버에서의 인증 연동방법을 제시하고 있으며, 기본적 구조는 SIP와 AAA의 연동을 위해서 DIAMETER 프로토콜에 UAR/UAA, MAR/MAA등과 같은 새로운 AVP(Attribute Value Pairs)를 정의하고, SIP 메시지의 인증정보를 DIAMETER 메시지로 변환하게 된다. 인증 연동을 위해 정의한 AVP들의 기능은 <표 1>과 같으며, 사용자에 대한 인증 주체에 따라 AVP 사용절차가 달라진다.

<표 1> 인증 연동의 DIAMETER AVP

기본 AVP	기 능
UAR (User Authorization Request)	- 사용자에 대한 등록 및 SSP 서버 주소 요청
UAA (User Authorization Answer)	- 등록 여부 및 SSP 주소 전달
MAR (Multimedia Auth Request)	- 사용자에 대한 인증을 위한 인증 정보 요청
MAA (Multimedia Auth Answer)	- 사용자 인증 정보 전달
SAR (Registration Termination Request)	- 서비스 지원을 위해 SSP 서버의 할당 요청
SAA (Registration Termination Answer)	- SSP 서버의 할당을 응답

(그림 2)는 IETF에서 제안되고 있는 두 가지 인증 연동 방안의 절차를 나타내고 있다.[5] 사용자의 SIP 등록 메시지를 수신한 HSP 서버는 사용자의 등록 여부를 AAA 서버에 요청하고, 이에 대한 결과와 할당된 SSP 서버의 주소 정보를 획득하여, 해당 SSP 서버로 SIP 등록 메시지를 전달하게 된다. SSP 서버에서는 사용자에 대한 인증을 수행하기 위해 AAA 서버에게 인증 수행을 위한 사용자 이름, realm, nonce 등의 인증 정보를 요청하고 이에 대한 결과를 MAA AVP를 통해 전달받아 저장하게 된다. 401 메시지를 수신한 사용자는 인증 정보인 response를 포함한 SIP 등록 메시지를 생성하여 이전과 같은 절차를 거쳐 SSP 서버로 전달하게 된다. SSP 서버에서는 이전의 인증 정보를 가지고 생성한 값과 메시지의 response 값을 비교하여 사용자에 대한 인증을 수행한다. 인증이 성공하면 SSP 서버가 사용자에 대해 서비스를 지원할 수 있도록 할당을 요청하는 SAR AVP를 전송하고, 이에 대한 결과로 SAA AVP를 수신하여 인증 절차가 완료된다. 반면 AAA 서버에서의 인증을 통한 연동 방법에서는 모든 사용자에 대한 인증을 AAA 서버에서 담당하게 되며, SSP 서버에서는 SIP 메시지의 인증 헤더인 Authorization 헤더나 Authentication 관련 헤더 정보를 MAR/MAA AVP에 포함하여 전달하게 된다. SSP 서버는 SIP 메시지 안에 있는 헤더관련 정보를 그대로 MAR/MAA AVP를 통해 전달하는 기능을 담당하고 있다.



(그림 6) IETF 인증 연동 절차

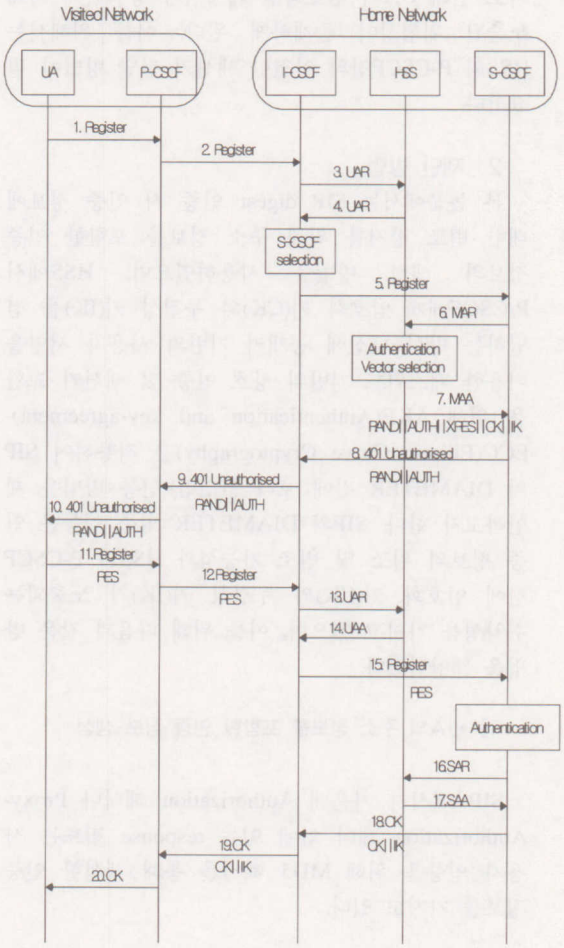
이와 같은 두 가지의 연동 방안 중 AAA에서의 인증 연동 방안이 연동의 기본 모델이라 할 수 있으며, 이는 AAA 서버를 통한 중앙 집중형 인증 구조라 할 수 있다. 이와 같은 연동 방안은 SIP 서비스 사용자 수의 증가에 따라 AAA 서버를 별도로 증설해야 하는 단점을 가지고 있다. 반면 SIP 서버에서 인증 연동 방안은 AAA의 인증 기능을 SIP 서버에서 담당하여 AAA 서버에 대한 부하를 줄일 수 있고 확장성도 용이한 장점을 가지고 있다. SIP 기반 서비스의 활성화와 사용자 수의 증가에 따른 네트워크의 확장성 측면에서 보면, 앞으로 AAA 서버를 통한 인증 연동 방안에서 SIP 서버에서의 인증 방안 형태로 변화해 나갈 것이다. 그리고 네트워크 보안 측면에 있어서 AAA 서버를 통한 인증 방안에서는 AAA 서버에서의 보안이 가장 중요하며, SIP 서버에서의 인증 연동 방안은 AAA 서버와 모든 SIP 서버에 대한 보안을 충분히 고려해야 한다. SIP에서의 인증 방안은 SIP의 REGISTRAR 서버 인증 기능을 그대로 사용할 수 있는 특징을 가지고 있어 SIP에서 별도의 확장이 필요 없다는 장점이 있다. AAA 서버를 통한 인증방법에서는 AAA 서버가 SIP 서버에 대한 지원 및 관리 기능이 필요하며 SIP 서버에서는 사용자 인증 정보 관리에 대한 보안 기능이 요구되어진다.

2. 3GPP에서의 사용자 인증 연동

3GPP에서는 IM(IP-based Multimedia) 서비스 제공을 위해 ALL IP 기반의 네트워크를 표준화하고 있으며, SIP 서버와 AAA 서버간을 Cx 인터페이스로 정의하고, 이를 위한 프로토콜로 DIAMETER를 선택하고 있다. 3GPP에서는 무선 사용자의 이동성과 확장성을 보장하기 위해 SIP 사용자에 대한 인증 벡터를 AAA 서버로부터 획득하여 SIP 서버에서 인증을 수행하는 연동 방안을 선택하고 있다. 그리고 HTTP digest 인증을 확장한 HTTP digest AKA(Authentication and Key Agreement) 인증 방법을 적용하며, 사용자 단말과 AAA 서버간에 AKA 알고리즘을 통해 무선 구간에서 사용할 암호화 및 무결성 키를 생성한다. 또한 3GPP에서는 SIP 서버 기능을 담당하는 논리적 개념으로 CSCF(Call Session Control Function)를 정의하고, 서버의 위치 및 기능에 따라서 P-CSCF(Proxy-CSCF), I-CSCF (Interrogating CSCF), S-CSCF(Serving CSCF)로 나누고 있다. 그리고 AAA 서버 기능을 담당하는 개념으로 HSS(Home Subscriber Server)를 정의하고 있으나, 기본적인 연동 구성은 IETF에서 제시하는 SIP에서의 인증 연동 방안과 같은 구조를 가진다[7].

전체적인 인증 연동 절차는 (그림 3)에서 보여주고 있다. 사용자는 SIP 등록 메시지를 P-CSCF로

전송하며 P-CSCF는 홈 도메인 이름을 알아내어 홈 도메인의 I-CSCF로 메시지를 전달하게 된다. I-CSCF는 수신한 SIP 등록 메시지를 바탕으로 생성한 UAR AVP를 HSS 서버에게 전달하여 사용자에 대한 권한 검증을 요청하며, HSS 서버에는 UAA AVP를 통하여 등록 여부와 결과를 I-CSCF로 전달하게 된다. I-CSCF는 UAA AVP를 수신받은 후, S-CSCF에게 SIP 등록 메시지를 전달하게 된다. 사용자의 등록 메시지를 수신한 S-CSCF는 사용자 인증을 수행하기 위해 MAR AVP를 HSS 서버에 전송하여 인증 벡터를 요구하게 된다. MAA AVP를 통해 HSS 서버로부터 인증 벡터를 수신한 S-CSCF는 SIP 401 Unauthorized 메시지를 통해 인증 challenge인 RAND와 인증 token인 AUTN를 사용자에게 전송하게 된다.



(그림 7) 3GPP의 인증 연동 절차

사용자는 수신한 challenge를 이용하여 Expected Message Authentication Code(XMAC)를 생성하고, AUTN에 포함된 MAC과 비교하여 홈 망에 대한 인증을 수행한다. 이때 인증이 실패하면 AUTS를 전송하고, 인증이 성공하면 RES를 생성하여 전송하게 된다. 사용자의 등록 메시지를 수신한 S-CSCF는 XRES와 사용자가 전달한 RES를 비교하여 인증을 수행한다. 인증이 성공하면 S-CSCF는 SAR 메시지를 통하여 사용자의 등록 요청과 사용자 프로파일 정보를 요청하게 된다. 또한 200 OK 메시지에 무선 구간의 안전성을 위한 암호화 키(CK)와 무결성 키(IK)를 P-CSCF에게 전달하게 되며 이를 통하여 사용자와 P-CSCF간의 보안을 제공하고 있다.

Ⅲ. 연동 방법의 안전성 및 제안 방법

1. 개요

SIP와 DIAMETER간의 인증 연동은 사용자 인증 기능과 단말기-서버간의 세션키 교환 기능을 제공하고 있으나, 다음의 2가지에 대한 보안 취약성을 내포하고 있다. 첫 번째 보안 취약성은, 공격자가 인증 정보에 대해서 변조 및 위장 공격이 가능하며, SIP와 DIAMETER의 프로토콜 변환과정에서 SIP와 DIAMETER 메시지간의 사용자 인증 정보(SIP response 값)에 대한 신뢰성이 부족하다. 왜냐하면 SIP digest 인증 메커니즘의 인정 정보는 사용자 인증과 제한적인 무결성만을 지원하기 때문에 네트워크 중간에서 메시지에 대한 변조나 가로채기와 같은 공격이 가능하다. SIP와 DIAMETER에서도 이와 같은 문제점으로 인해 TLS나 IPsec과 같은 다른 보안 메커니즘의 사용을 권고하고 있다.

<표 2> SIP와 DIAMETER의 보안 메커니즘

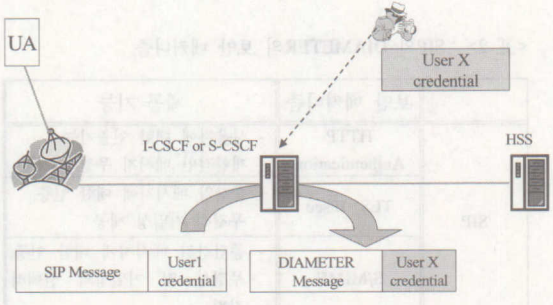
	보안 메커니즘	제공 기능
SIP	HTTP Authentication	- 사용자에 대한 인증기능 - 제한적인 메시지 무결성 기능
	TLS, IPsec	- 홉간의 메시지에 대한 인증, 무결성 기밀성 제공
	S/MIME	- 종단간의 메시지에 대한 인증, 무결성 및 기밀성의 선택적 지원
DIAMETER	TLS, IPsec	- 홉간의 메시지에 대한 인증, 무결성 및 기밀성 제공
	CMS 보안 응용	- 종단간의 메시지 보안 기능

또한 SIP와 DIAMETER의 인증 연동 취약성으로 인해 공격자는 SIP 사용자의 세션을 가로채거나 연결된 세션에 대해 강제 종료를 하는 공격유형이 가능하다. 그리고 사용자의 패스워드를 추측을 통해 공격하는 dictionary 공격에도 취약한 문제점을 가지고 있다. 이와 같이 SIP와 DIAMETER 인증 연동에서 발생할 수 있는 서비스 공격 유형의 형태는 <표 3>과 같이 정리할 수 있다.

<표 3> SIP와 DIAMETER 인증 연동에서의 서비스 공격 유형

서비스 공격 유형	공격 방법
Registration Hijacking	- 공격자가 네트워크 중간에서 다른 사람의 SIP Register 메시지에서 사용자의 주소 정보인 Contact 헤더 필드나 From 헤더 필드를 변경하여 세션을 가로채는 공격 유형
Impersonating Server	- 공격자가 사용자 SIP Register 메시지를 가로챈 후 이에 맞는 SIP response 메시지를 전달하여 서버로 위장하는 공격 유형
Tearing Down Sessions	- 공격자가 세션 초기에 사용자의 모든 SIP 메시지를 캡처한 후 연결되어 있는 세션에 Bye 메시지를 전달하여 강제로 종료하는 공격 유형

SIP와 DIAMETER간의 프로토콜 변환에서 SIP의 인증 정보는 DIAMETER의 인증 필드로 그대로 삽입되기 때문에 이전에서 일어난 인증 정보의 변조에 대해서는 확인할 방법이 없으며, 공격자가 인증 정보를 위조할 경우 정당한 사용자에 대한 인증이 실패하게 된다. 이와 같은 공격에 대한 방지를 위해서는 SIP와 DIAMETER 메시지 변환에서 사용자 인증 정보에 대한 확인이 필요하다.



(그림 4) SIP-DIAMETER 메시지 변환에서 인증 정보 공격 예

또한 dictionary 공격에 의해 사용자의 패스워드 정보가 노출되었을 경우에는, 중간 노드에서 man-in-the-middle 공격이 가능하다. Man-in-the-middle 공격유형은 제 3의 공격자가 사용자와 서버사이에 존재하여, 사용자와 서버의 메시지를 변조해 거짓 정보를 생성하는 공격방법으로 SIP와 DIAMETER간의 프로토콜 변환이 일어나는 I-CSCF나 S-SCSF 서버가 공격자에게 노출 될 경우 UA의 세션키가 노출될 위험성이 있다. 두 번째 취약성은 인증 이후에 사용될 암호화 키(CK)와 무결성 키(IK)가 P-CSCF까지 전달되는 과정에서 발생한다. 암호화 키(CK)와 무결성 키(IK)는 UA와 P-CSCF간의 보안을 위해 사용되는 세션키로 사용되며, UA에서는 자체 계산에 의해 생성되나 P-CSCF는 HSS로부터 생성된 키를 수신해서 사용하고 있다. 그러나 공격자는 HSS와 P-CSCF간에서 스니퍼링을 통해 암호화 키(CK)와 무결성 키(IK)를 획득할 수 있으며, 이로 인해 UA의 암호화된 메시지가 공격자에 의해 노출될 위험성이 존재하게 된다. 이를 위해서는 HSS와 P-CSCF간의 안전한 세션키 전달 방법이 필요하다.

2. 제안 방법

본 논문에서는 SIP digest 인증 시 인증 정보에 대한 변조 방지를 위해 주소 정보를 포함한 인증 정보의 생성 방법을 사용하였으며, HSS에서 P-CSCF에게 암호화 키(CK)와 무결성 키(IK)를 전달하는 방식 대신에 공개키 기반의 사용자 서명을 이용한 패스워드 기반의 상호 인증 및 세션키 교환을 위해 AKE(Authentication and key-agreement)-ECC(Elliptic Curve Cryptography)를 적용하여 SIP와 DIAMETER 간에 보다 안전한 연동 방법을 제안하고자 한다. SIP와 DIAMETER 인증 연동은 인증 정보의 위조 및 변조 가능성과 HSS와 P-CSCF간에 암호화 키(CK)와 무결성 키(IK)가 노출되는 취약성을 가지고 있으며, 이를 위해 다음과 같은 방법을 제안하였다.

1) UA의 주소 정보를 포함한 인증 정보 생성

SIP 메시지 가운데 Authorization 헤더나 Proxy-Authorization 헤더 안에 있는 response 필드는 사용자 인증을 위해 MD5 해시를 통해 생성한 인증 정보를 가지고 있다.

response=H(H(username:realm:password):nonce:
H(method:URI))

안전한 인증을 위해서는 인증 정보인 response 값에 대해 공격자가 메시지를 변조하더라도 중간 노드에서 이를 확인 할 수 있어야 한다. 또한 CSCF에서 발생할 수 있는 Registration Hijacking이나 Tearing Down Sessions와 같은 공격을 막기 위해서는 메시지발신자에 대한 정확한 address 정보가 필요하며, 이를 위해서 인증 정보 생성 시 사용자의 주소 정보를 포함하는 방법을 제안하였다. 제안된 인증 절차는 사용자 주소를 포함한 인증 정보인 response를 생성하여 메시지를 전달하고, 이를 수신한 인증 서버에서는 저장되어 있는 사용자의 이름, realm, 사용자 password, nonce, URI 정보와 메시지 헤더에 있는 사용자 주소 정보를 가지고 해시한 값을 메시지 안에 있는 response 값과 비교하여 사용자 인증을 수행하게 된다.

response = H(H(username:realm:password
:*useraddress*):nonce:H(method:URI))

공격자가 사용자의 메시지에서 사용자 주소 정보인 Contact 헤더나 관련 주소 정보를 변조할지라도 서버에서는 인증 수행 시에 사용자의 주소 정보를 포함하여 인증을 하기 때문에 변조 여부를 확인할 수 있다. 사용자의 주소 정보는 IP 주소나 사용자의 주소 정보인 Contact 헤더를 사용할 수 있으며 이와 같은 방법을 통하여 Registration Hijacking이나 Tearing Down Sessions 등의 공격 유형을 방지 할 수 있다. 그리고 SIP 프로토콜의 특징 중 하나인 사용자 이동성 측면에서는 보면, 사용자 주소가 변경될 경우에는 SIP 프로토콜에서 다시 재등록 절차를 수행하기 때문에 기본 프로토콜의 변경 없이 적용할 수 있다.

2.) 패스워드 기반의 상호 인증 및 세션키 교환을 위한 AKE-ECC의 적용

UA에서 암호화 키(CK)와 무결성 키(IK)는 P-CSCF와 공유되어 무선 구간의 안전성을 제공한다. 그러나 P-CSCF는 HSS로부터 생성된 키를 수신 받아 사용되며, 이때 암호화 키(CK)와 무결성 키(IK)가 완전히 노출되어 전달되기 때문에 전체 시스템의 안전성을 떨어뜨릴 수 있다. 본 논문에서는 이와 같은 문제를 해결하기 위해 UA와 서버간의 키 교환을 위한 방법으로 사용자의 서명을 이용한 스워드 기반의 상호 인증 및 세션키 교환 방법인 AKE(Authentication and key-agreement)-ECC (Elliptic Curve Cryptography)[11]를 적용하였다. AKE-ECC는 공개 키 알고리즘인 ECDSA(EC Digital Signature Algorithm)[8]를 적용하여, 키 교환으로 생성된 세션키에 대해서 서명을 통하여 인증하고, 통신회수는 4회의 절차를 거치게 된다.

● Notation :

π : 공유한 패스워드

SK : A와 B에 의하여 생성된 세션키

α, β : 타원곡선 $y^2 = x^3 + \alpha x + \beta$를 정의하는 계수 $\alpha, \beta \in F_q$ (도메인파라미터)

$\# E$: 타원곡선 위의 점의 개수

q : 유한체의 크기 (도메인파라미터)

n : basepoint G의 위수(order) (도메인파라미터)

h : $\# E/n$ 공통인자 (도메인파라미터)

G : 타원곡선의 basepoint(위수가 n인 그룹의 점의 생성원) (도메인파라미터)

H : 일 방향 해쉬함수

전체적인 AKE-ECC 절차는 다음과 같으며, 이전에 UA와 HSS는 사용자의 패스워드 π와 타원 곡선 도메인 파라미터 $(\alpha, \beta, q, n, h, G)$를 공유해야 한다.

1) UA에서는 우선 임의의 값 a를 선택하고, 자신의 패스워드를 이용하여 $H_1(\pi)$를 계산한 후, 타원곡선의 basepoint G를 이용하여 $(a + H_1(\pi) \cdot G) = (x_a, y_a)$를 계산한다. UA는 이 결과 값을 HSS에게 전송한다.

2) 1)의 메시지를 받은 HSS는 임의의 값 b를 선택하고 자신의 패스워드를 이용하여 $H_1(\pi)$를 계산한다. 그리고 타원곡선의 basepoint G를 이용하여 를 계산한다. 이 결과 값을 UA에게 전송 후 HSS는 ECDH에 의해 $k' = (abG)(x)$를 계산하여 UA의 공개키인 $dG = k'aG$를 계산하고, 401 Unauthorised 메시지를 통해 CSCF에게 UA의 공개키를 전달하게 된다.

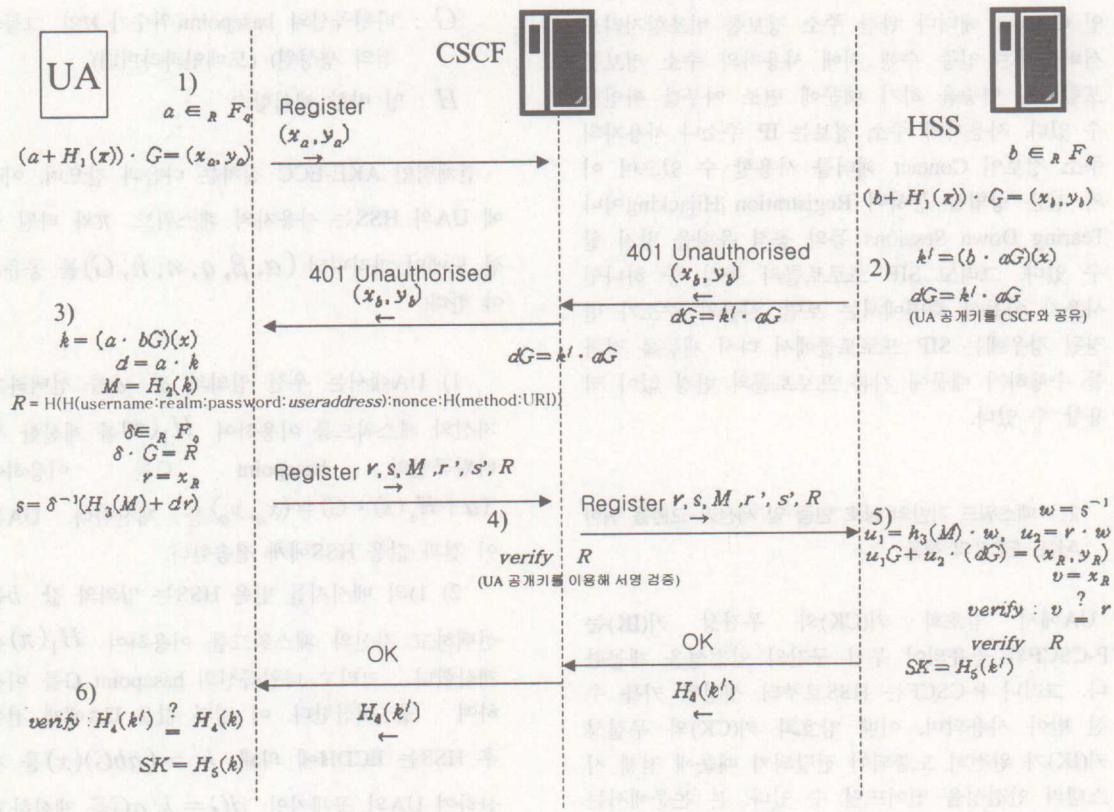
3) 2)의 메시지를 받은 UA는 $k=(abG)(x)$와 비밀키 $d=ka$를 계산한다. 비밀키 d를 이용하여 메시지 M에 대한 서명 (r,s)를 생성한 후 HSS에게 전송한다. 여기서 $M=H_2(k)$이다. 또한 이때 SIP digest 인증을 위해 사용될 response값인 R에 대해서도 서명 (r',s')를 생성한 후 HSS에게 전송하게 된다.

4) CSCF에서는 2)에서 수신한 UA의 공개키 정보를 가지고 사용자 인증 정보인 R과 서명 (r',s')를 확인하여 이상이 없을 경우 HSS로 전달하게 되며, 이때 I-CSCF나 S-CSCF에서는 SIP 메시지의 사용자 인증 정보인 R과 서명 (r',s')를 DIAMETER 메시지에 포함시켜 프로토콜 변환을 하게 된다. 이와 같은 SIP와 DIAMETER의 프로토콜 변환은 인증 정보에 대한 서명을 추가하여 안전한 사용자 인증을 제공한다.

5) 4)의 메시지를 받은 HSS는 UA의 공개키를 $dG=k'aG$를 이용하여 UA의 서명을 검증한다. 또한 사용자 인증 정보인 R 에 대한 서명을 검증하여 인증을 확인한다. 서명이 검증되면, HSS는 UA를 인증을 수행하고, $H_4(k')$를 계산하여 UA에게 전송한다. HSS는 전송 후 세션키 $SK=H_5(k')$를 생성한다.

6) 5)의 메시지를 받은 UA는 받은 메시지와 자신이 계산한 메시지, $H_4(k)=H_4(k')$를 비교하여 일치할 경우 UA는 HSS를 인정한다. 인증 후 UA는 세션키 $SK=H_5(k)$를 생성한다.

상기와 같은 절차를 통해 SIP 메시지의 사용자 인증 정보 R은 서명 값도 같이 포함하여 DIAMETER 메시지로 변환되고, CSCF와 HSS에서는 서명 확인을 통해 정확한 인증을 수행하게 되며,



(그림 5) 제안 방법을 적용한 SIP-DIAMETER 인증 연동 절차

인증 수행이후 UA의 공개키는 CSCF에게 배포되어지고, HSS와 세션키를 공유하게 된다. AKE-ECC는 서명으로 사용자 인증과 사용자의 세션키에 대한 부인 방지를 제공하며, 서명에 사용되는 키 쌍의 생성과 세션키의 생성은 모두 ECDH에 의한 키 교환 알고리즘에 의해 생성된다.

3. 제안 방법의 안전성 분석

본 논문에서는 SIP와 DIAMETER의 인증 연동에서 주소 정보를 포함한 인증 정보의 생성 방안과 패스워드 기반의 상호인증 및 세션키 교환을 위한 AKE-ECC의 적용 방안을 제시하였으며, 이 두 방법을 통해 앞에서 설명하였던 서비스 공격 유형과 SIP와 DIAMETER 인증 연동 프로토콜에 대한 안전성을 분석하였다.

- Registration Hijacking

SIP Authorization 헤더 필드의 response 인증 정보에는 사용자의 주소 정보를 포함시켜 생성하기 때문에 공격자가 SIP 메시지 안의 Contact이나 From 헤더 필드를 변조할 경우에는 사용자 인증이 실패하게 된다. 또한 패스워드 기반의 상호 인증 및 세션키 교환을 위한 AKE-ECC를 이용하여 SIP의 사용자 인증 정보인 response 값에 대한 서명을 같이 보내기 때문에 공격자가 메시지를 변조하더라도 서버에서는 변조 여부를 확인할 수 있다.

- Impersonating Server

패스워드 기반의 상호 인증 및 세션키 교환을 위한 AKE-ECC를 적용할 경우에 프로토콜의 인증 절차의 마지막 단계에서 서버는 세션키를 해시하여 사용자에게 전송함으로써 사용자는 서버에 대한 인증을 확인 할 수 있다. 또한 SIP 프로토콜에서 사용자가 서버에 대한 인증이 가능하다. SIP 메시지의 옵션 헤더 필드 중 하나인 Authentication-Info 헤더를 필수적으로 사용하는 방법이 있을 수 있으며, 이를 통해 SIP에서는 사용자 단말기에서 서버에 대한 인증을 수행할 수 있다.

- Tearing Down Sessions

사용자 인증을 위한 response 값에는 UA의 주소 정보가 들어가 있으며, 세션 종료를 위한 BYE 메시지에도 이 값을 포함해야 한다. 하지만 공격자가 UA의 주소를 알고 있다고 하여도 사용자의 패스워드 값을 모르기 때문에 response 값을 생성할 수 없다. 또한 공격자가 다른 주소 정보를 변경하더라도 response 값과의 주소 정보가 다르기 때문에 인증이 실패하게 된다.

본 논문에서 적용한 AKE-ECC는 ECC, ECDLP (Elliptic curve Discrete Logarithm Problem), ECDH (Elliptic curve DH)의 안전성을 기반으로 하고 있어, ECC의 안전성에 대한 설명은 제외하고, 인증 연동에서 발생할 수 있는 대표적인 프로토콜 공격에 대한 안전성을 설명한다.

- Dictionary attack

Dictionary attack은 공격자가 사용자의 패스워드를 추측하여 실제 메시지에서 드러나는 값에 대입한 후 결과를 비교하여 실제 패스워드를 찾는 공격 방법이다. AKE-ECC에서는 사용자가 자신의 메시지를 전송하고 서버로부터 받는 메시지는 첫 번째 메시지와 상관없는 값을 받게 됨으로 추측한 패스워드로서 생성한 결과 값을 비교할 수 없다. 따라서 dictionary attack은 불가능하며, 세 번째 메시지를 받은 서버는 정당한 패스워드 정보를 사용하는 사용자만이 인증하게 됨으로 더 이상 dictionary attack은 불가능하다.

- Replay attack

Replay attack은 공격자가 사용자의 메시지를 재전송하여 이미 정상적인 사용자에 의해 생성된 이전 키(old session key)를 다시 생성하기 위함이다. 이 공격 방법은 사용자와 서버간에 항상 임의의 값을 사용하기 때문에 불가능하다. AKE-ECC에서는 사용되는 값인 a와 서버에 의해 생성되는 임의의 값인 b가 매 세션마다 새롭게 생성됨으로써 반복(replay)에 의한 이전 키 생성이 불가능하다. 따라서 AKE-ECC는 replay attack으로부터 안전하다.

- PFS(Perfect Forward Secrecy)

PFS는 "현재의 세션키 정보가 알려져도 이전키를 알 수 없다"는 것으로 PFS를 제공하기 위해서는 사용자와 서버간에 주고받는 메시지 내용이 이전 키 생성을 위한 정보와 관련이 없어야 한다. 이를 위해서는 생성되는 세션키값이 항상 임의의 값으로 생성되어야 하고, 메시지에서 임의의 값이 ECDLP에 의해 보호되어야 한다. AKE-ECC의 세션키값은 a, b로서 생성되고, ECDLP에 의해 알려지지 않는다. a, b값이 알려지지 않음으로 AKE-ECC는 PFS를 제공한다.

- Man-in-the-middle attack

AKE-ECC에서는 인증 정보인 패스워드가 사용되고 있으므로 공격이 불가능하다. 또한 세션키는 해쉬값으로 되어 있어 공격자가 세션키를 획득할 수 없다. 그리고 인증 정보와 서명값을 같이 보내 man-in-the-middle attack이 불가능하다.

지금까지 SIP와 DIAMETER의 인증 연동에서 주소 정보를 포함한 인증 정보의 생성 방안과 패스워드 기반의 상호인증 및 세션키 교환을 위한 AKE-ECC의 적용 방안이 기존 방식에 비해 여러 가지 공격방법에 대한 안전성을 제공한다는 것을 확인하였다.

Ⅳ 결 론

본 논문은 유무선 통합 시그널링 프로토콜로 정착될 SIP와 신뢰성 있는 서비스를 제공하기 위한 AAA 프로토콜인 DIAMETER의 인증 연동을 위해 3GPP와 IETF에서 제안하고 있는 인증 연동 방안을 분석하고 SIP와 DIAMETER의 인증 연동에서 발생할 수 있는 보안상 안전성 분석 및 해결 방안을 제안하였다.

SIP와 DIAMETER 인증 연동 방안에 있어서 IETF는 인증의 주체를 SIP 서버나 AAA 서버에서 가능하도록 하여 유연한 연동 방안을 제시하고 있으며, 3GPP에서는 모든 사용자에 대한 인증을 SIP 서버에서 담당하는 분산형 구조를 제시하고 있고, 기존의 digest 인증방법보다는 무선 구간에서 암호화키의 분배를 위해 digest AKA(Authentication and Key Agreement) 인증 방법을 적용하여 무선 환경에 적합한 형태를 제시하고 있다. 그러나 인증 연동의 기본구조는 SIP 서버와 AAA 서버 간에 SIP 메시지의 인증 헤더나 인증 수행을 위한 인증 정보들을 DIAMETER 메시지 변환을 통해 사용자의 인증을 수행하게 된다.

또한 SIP와 DIAMETER의 인증 연동은 Registration Hijacking, Impersonating Server, Tearing Down Sessions 등의 서비스 공격과 dictionary, replay, man-in-the-middle 공격과 같은 프로토콜 공격에 안전성이 노출되어 있으며, 이를 위한 해결방안으로는 사용자의 주소 정보를 포함하여 인증 정보를 생성 방안과 패스워드 기반의 상호 인증 및 세션키 교환을 위한 AKE-ECC의 적용 방안을 제시하였다. 그리고 제안된 방법에 대한 안전성을 분석한 결과 기존의 여러 공격에도 안전한 SIP와 DIAMETER간의 인증 연동임을 확인하였다.

참 고 문 헌

[1] FC 3261, SIP: Session Initiation Protocol, June 2002.

[2] Pat R. Calhoun, John Loughney, "Diameter Base Protocol," draft-ietf-aaa-diameter-12.txt, IETF, July 2002.

[3] RFC 2138, Remote Authentication Dial In User Service (RADIUS), June 2000.

[4] Henrik Basilier, Pat R.Calhoun, "AAA Requirements for IP Telephony/multimedia," draft-calhoun-sip-aaa-reqs-04.txt, IETF, March 2002.

[5] Kevin Purser, Carolina Canales, "Diameter Multimedia Application,"draft-johansson-aaa-diameter-mm-app-02.txt, IETF, November 2002.

[6] Pat R. Calhoun, Glen Zorn, "Diameter Framework Document," draft-ietf-aaa-diameter-framework-01.txt, IETF, March 2001.

[7] 3GPP TS 29.228 Technical Specification Group Services and System Aspects; IP Multimedia(IM) Subsystem Cx and Dx Interface. March 2002.

[8] ANSI X9.62-1998, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)," 1998.

[9] T.Kwon, "Authentication and Key Agreement via Memorable Passwords," NDSS 2001 Symposium Conference Proceedings, February 7-9, 2001.

[10] T. Wu, "The Secure Remote Password Protocol," Proceedings of the 1998 Internet Society Network and Distributed System Security Symposium, San Diego, pp. 97-111. March 1998.

[11] 박호상, 정수환, "패스워드 기반의 상호 인증 및 키 교환 프로토콜," 정보보호학회논문지, 12권, 5호, pp. 37-43, 2002년 10월.

박 성 준(Sungjoon Park) 준회원

1998년 2월: 숭실대학교 정보통신공학과 졸업
2003년 2월: 숭실대학교 정보통신공학과 석사
2003년 3월~현재: 삼성종합기술원 i_Networking LAB

<관심분야> VoIP security, Network Security, Authentication

정 수 환(Souhwan Jung) 정회원

1985년 2월: 서울대학교 전자공학과 졸업
1987년 2월: 서울대학교 전자공학과 석사
1988년~1991년: 한국통신 전임연구원
1996년: 미 워싱턴 주립대 (시애틀) 박사
1996년~1997년: Stellar One SW Engineer
1997년~현재: 숭실대학교 정보통신전자공학부 부교수

<관심분야> VoIP security, Security Protocol, 사용자 인증, Cryptography

이 병 길(Byung-Gil Lee) 정회원

1991년 2월: 경북대학교 전자공학과 졸업
1993년 2월: 경북대학교 전자공학과 석사
2003년 2월: 경북대학교 전자공학과 박사
1993년 1월~2001년 7월 데이콤종합연구소 선임연구원
2001년 7월~현재: 한국전자통신연구원 정보보호연구단 선임연구원

<관심분야> IP기반 이동통신 네트워크 및 정보보호

김 현 곤(Hyun-Gon Kim) 정회원

1992년 2월: 금오공과대학교 전자공학과 졸업
1994년 2월: 금오공과대학교 전자공학과 석사
2003년 8월: 충남대학교 전자공학과 박사
1994년~현재: 한국전자통신연구원 정보보호연구단 AAA정보보호연구팀장

<관심분야> IP기반 이동통신 네트워크 및 정보보호, 무선 인터넷 정보보호