SIP Call Signaling을 위한 사용자 인증 기법

최경호O 임을규
한양대학교
beltre@hanyang.ac.kr, imeg@hanyang.ac.kr

User Authentication Mechanism for SIP Call Signaling

Kyoung Ho ChoiO Eul Gyu Im
Hanyang University

요 약

음성 데이터를 IP기반의 패킷망을 통해 전송하는 기술인 VoIP(Voice over Internet Protocol) 기술은 음성 데이터를 기존의 PSTN(Public Switched Telephone Network)망을 통해 전송하는 방식에 비해 비용 절감 등의 장점을 가지고 있다. 그러나 VoIP가 기존의 PSTN망을 대체하기 위해서는 QoS(Quality of Service)의 보장과 보안이 제공되어야 한다는 문제점을 가지고 있다.

VoIP망에서 보안을 위해서는 사용자간에 전송되는 음성 데이터에 대한 보안과 초기의 세션 연결 시 사용자를 인증하는 과정이 고려되어져야 한다. 실질적인 대화 내용인 음성 데이터의 보안도 중요한 부분이지만 대화에 참여하는 사용자를 인증 하는 과정이 선행되어야 한다.

VoIP에서는 세션 연결 설정을 위해 H.323과 SIP를 사용하고 있으며, 최근에는 H.323에 비해 간단한 SIP가 주목을 받고 있다. RFC3261에서는 SIP를 이용해 세션 연결을 하는 과정에서 사용자를 인증하기 위한 몇 가지 인증 메커니즘을 제시하고 있다. 본 논문에서는 SIP를 이용하여 세션을 연결하는 과정에서 사용자의 인증을 위해 사용되는 인증 메커니즘 중 한 가지인 HTTP Digest Authentication의 취약점을 분석하고, 이를 보완하기 위한 새로운 인증 메커니즘을 제시한다.

1. 서 론

VoIP(Voice over Internet Protocol) 프로토콜은 음성 데이터의 통신에 있어서 기존의 PSTN(Public Switched Telephone Network)망을 사용하지 않고, IP 기반의 패킷망을 사용하여 음성 데이터를 전송하는 기술을 말한다. VoIP의 사용으로 기존의 인터넷망을 사용하여 음성 전화 서비스를 구현할 수 있게 되면서 기존에 사용되던 회선 비용을 크게 절감할 수 있게 되었다. 또한 인터넷 전화 서비스 이외에도 웹 콜 센터, 통합 메시징 서비스 등의 각종 부가 서비스와 영상회의 등 인터넷상에서의 멀티미디어 서비스에 대한 핵심 기술이라는 점에서 VoIP 프로토콜의 중요성은 크다고 할 수 있다.

이러한 VoIP가 기존의 PSTN망을 대체하여 음성 통신의 주류로 발전하기 위해서는 해결해야하는 몇 가지 문제점이 있다. 그 중 하나가 바로 VoIP 보안에 대한 문제이다. 기존의 PSTN망에서 사용되던 음성통신과 달리 모든 사람들에게 공개되어 있는 인터넷망을 사용하여 음성 통신을 하게 되면서 그에 따른 여러 가지 보안상 취약점들이 발생하게 되었다. 따라서 VoIP를 통한 안전한 음성 통신의 전송을 위해서는 보안요소가 필수적으로 고려되어야 한다. VoIP망에서 보안을 위해서는 사용자간에 전송되는 음성 데이터에 대한 보안과 초기의 세션 연결 시 사용자를 인증하는 과정이 고려되어져야 한다. 실질적인 대화 내용인 음성 데이터의 보안도 중요한 부분이지만 대화에 참여하는 사용자를 인증 하는 과정이 선행되어야 한다. 즉, 두 사용자간에 음성 데이터를 안전하게 주고받기 위해서는 두 사용자간의 call을 위한 세션을 연결하는 과정에서 각 사용자의 인증은 필수적이라고 할 수 있다.

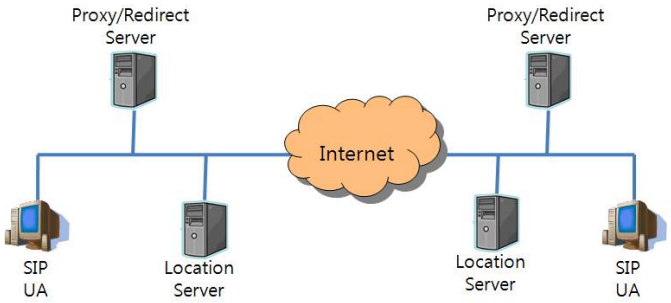
VoIP 프로토콜에서 call을 위한 세션 연결 설정에 사용되는 대표적인 프로토콜에는 ITU-T에서 개발한 H.323 프로토콜과 IETF에서 개발한 SIP(Session Initiation Protocol) 프로토콜이 있다.[1] 최근에는 H.323에 비해 간단하고 확장성이 큰 SIP 프로토콜이 주로 사용되고 있으며, RFC3261에서는 SIP 세션 연결 설정 과정에서 사용자 인증을 위하여 HTTP Basic Authentication, HTTP Digest Authentication, PGP(Pretty Good Privacy), S/MIME, TLS(Transport Layer Security), IPSec 등의 기법들을 제시하고 있다.[2] 본 논문에서는 SIP 세션 연결 설정 과정에서 인증을 위해 주로 사용되는 메커니즘인 HTTP Digest Authentication의 취약점을 분석하고, 이를 보안하기 위한 새로운 인증 메커니즘을 제시한다.

본 논문은 2장에서 VoIP call signaling 프로토콜 중 하나인 SIP 프로토콜에 대한 간단한 설명을 하고, 3장에서 SIP에서 사용자 인증을 위한 메커니즘 중 하나인 HTTP Digest Authentication의 동작 과정을 설명하고, 그 취약점을 분석한다. 그리고 4장에서 HTTP Digest

Authentication의 취약점을 보안하기 위한 새로운 인증 메커니즘을 제안하고, 5장에서 결론 및 향후 계획을 제시하겠다.

2. SIP(Session Initiation Protocol)

SIP 프로토콜은 사용자의 세션을 생성하고, 수정하고, 종료하기 위한 응용 계층의 call signaling 프로토콜이다. Call signaling을 위해 SIP 프로토콜을 사용하는 전체적인 망구성도는 [그림 1]과 같다.



[그림 1] SIP 망 구성도

SIP를 이용하여 세션 연결 설정을 하기위해 필요한 각 구성요소들에 대해 간단히 설명하면 다음과 같다.[3]

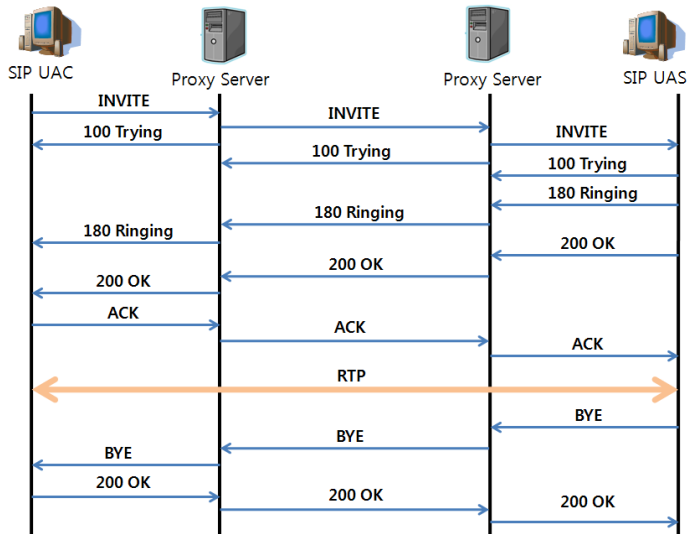
■ SIP UA(User Agent)
통신의 주체로 SIP 요청 메시지를 생성하는 UAC(User Agent Client)와 수신된 요청 메시지에 응답하는 UAS(User Agent Server)로 동작한다.

■ Proxy/Redirect Server
UAC가 call을 요청하는 INVITE 메시지를 UAS에게 전달해 주는 기능을 한다. Proxy server는 요청받은 INVITE 메시지를 목적지까지 포워딩 해주는 역할을 하며, redirect server는 UAS에 대한 정보를 UAC에게 전달해 주어 UAC가 UAS에게 직접 INVITE 메시지를 보낼 수 있도록 해주는 역할을 한다.

■ Registrar Server
사용자는 registrar server에 REGISTER 메시지를 전송함으로 자신의 위치정보를 location server에 등록할 수 있다.

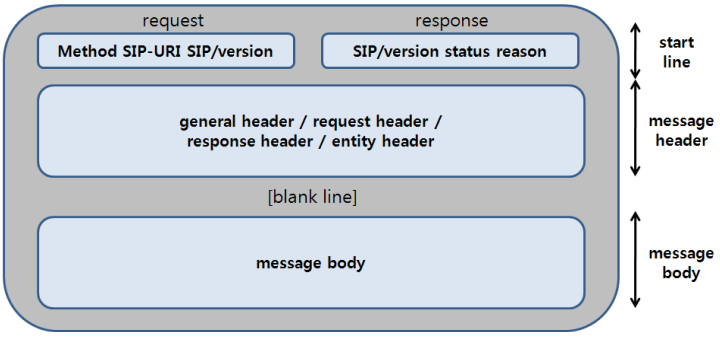
■ Location Server
UA의 실질적인 위치를 저장하고 있는 서버이다.

두 단말간의 음성 통신을 위하여 SIP 프로토콜을 사용하여 사용자간의 세션을 설정하고, 종료하는 과정은 [그림 2]와 같은 절차에 의해 이루어진다.



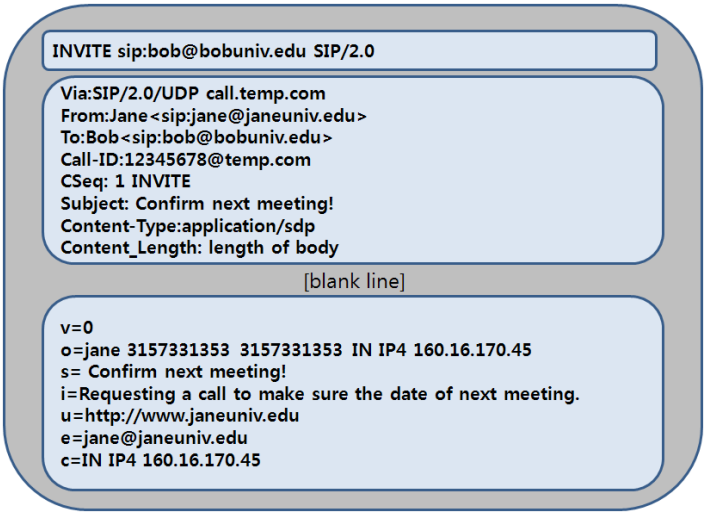
[그림 2] 세션 설정 및 종료

UAC는 UAS와 통신하기 위하여 UAS를 목적지로 하는 INVITE 메시지를 생성하여 전송하게 된다. UAC가 위치하고 있는 도메인의 proxy server는 이 INVITE 메시지를 받고 UAS가 위치하고 있는 proxy server로 INVITE 메시지를 포워딩한다. 그리고 INVITE 메시지를 포워딩 했다는 것을 UAC에게 알리기 위하여 100 Trying 메시지를 UAC에게 전송한다. UAS의 proxy server는 location server를 통해 UAS의 위치를 확인하고, 수신된 INVITE 메시지를 UAS에게 전달한다. INVITE 메시지를 전달받은 UAS는 수신을 받았다는 200 OK 메시지를 UAC에게 전송하고, 200 OK 메시지를 수신한 UAC는 ACK 메시지를 UAS에 보냄으로서 세션이 연결되게 된다. 세션의 종료 시에는 한쪽이 BYE 메시지를 보내고, 그에 대한 응답으로 200 OK 메시지를 수신하게 되면 세션이 종료되게 된다.



[그림 3] SIP 메시지 구조

SIP 프로토콜에서 call signaling을 위해 주고받는 메시지 구조는 [그림 3]과 같다. Start line에는 요청할 method와 SIP URI가 위치하고, 요청에 대한 응답으로 status code가 들어가게 된다. Message header에는 세션을 제어하기 위한 값들이 들어간다. [그림 4]는 실제적인 SIP INVITE 메시지의 예를 보여주고 있다.

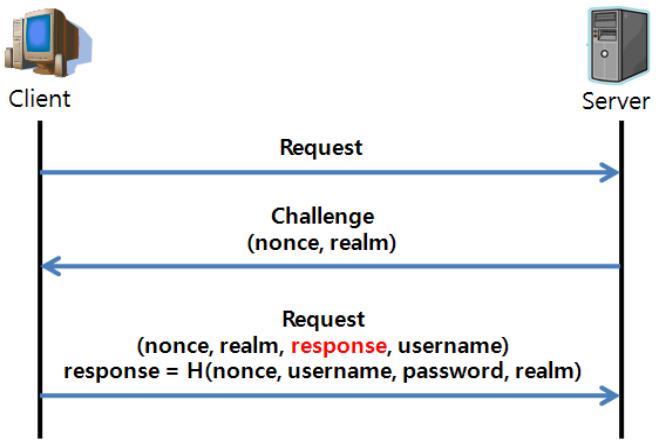


[그림 4] INVITE 메시지

3. HTTP Digest Authentication 기법

3.1. 동작 과정

HTTP Digest Authentication은 HTTP Basic Authentication이 인증을 위해 사용자 이름과 패스워드를 암호화하지 않고 전송하는 문제점을 보안하기 위하여 고안된 메커니즘이다. 이 방식은 사용자의 인증을 위해 사용자와 프록시간에 미리 공유하고 있는 비밀 패스워드와 임의의 값을 해시한 MD5나 SHA-1 digest를 전송한다.[4]

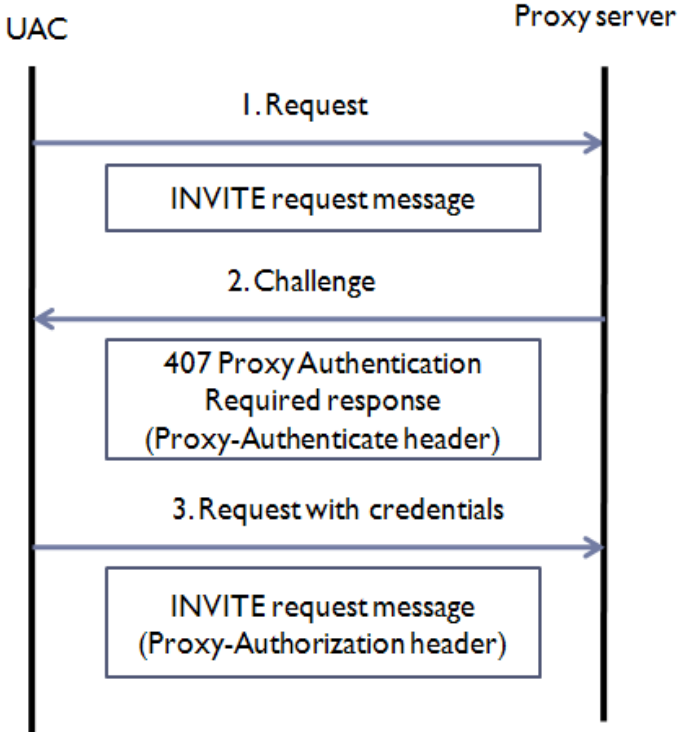


[그림 5] HTTP Digest Authentication

HTTP Digest Authentication은 challenge-response 기반으로 동작하며 [그림 5]에 전체적인 동작과정이 나타나 있다. 클라이언트가 서버에 요청을 하게 되면 서버는 이 요청을 받아들이지 않고, 클라이언트에 nonce와 realm을 포함하는 challenge를 보낸다. Challenge를 받은 클라이언트는 nonce, username, 서버와 공유하고 있는 password, realm을 MD5나 SHA-1 해시함수를 사용하여 해시한 값인 response 값과 nonce, realm, username을 함께 서버로 보내게 된다. 서버는 nonce, username, 클라이언트와 공유하고 있는 password, realm을 해시하여 얻은 값과 클라이언트로부터 전달받은 response의 값을 비교하여 클라이언트를 인증하게 된다.

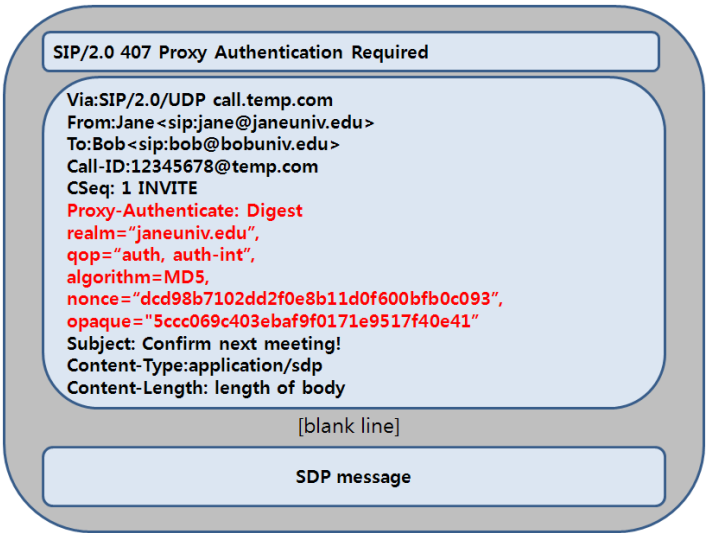
3.2. SIP Call Signaling의 인증

SIP call signaling 과정에서 사용자의 인증에 HTTP Digest Authentication 기법을 사용하기 위하여 SIP 응답 메시지인 401 Unauthorized response와 407 Proxy Authentication Required 메시지를 추가로 정의하고 있으며, 각 메시지 내의 특정 헤더 필드에 인증을 위한 challenge를 담아 전송하게 된다. 401 Unauthorized response 응답 메시지는 registrar, redirect server 또는 UAS가 UAC의 인증을 요구하기 위하여 전송하며, 407 Proxy Authentication Required 메시지는 proxy server가 UAC의 인증을 요구하기 위하여 전송한다. [그림 6]은 인증을 위한 대략적인 동작방법을 나타낸다.

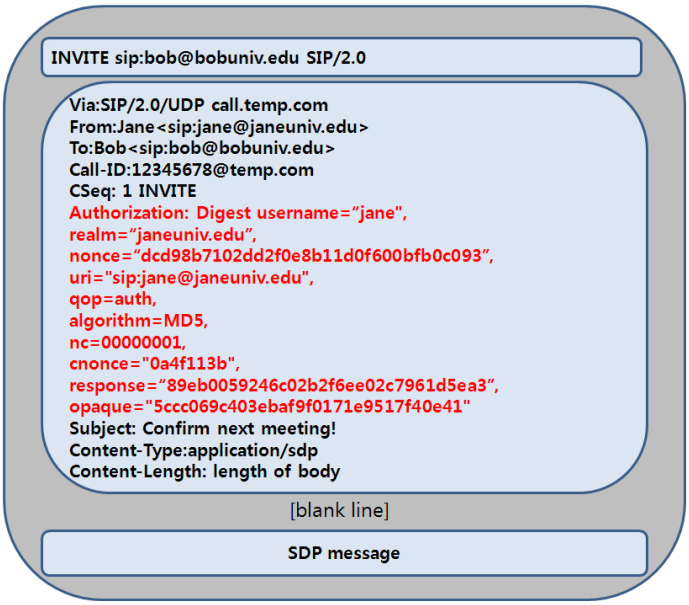


[그림 6] 407 Proxy Authentication의 사용

SIP UAC가 INVITE 요청 메시지를 전송하면 proxy server는 인증이 필요하다는 407 Proxy Authentication Required 에러 메시지를 SIP UAC에게 전송한다. 이 때 nonce와 realm이 전송되게 된다. SIP UAC는 nonce, realm, username, 서버와 공유된 password를 해시한 값인 response 값을 INVITE 요청 메시지에 포함하여 재전송하게 된다. Proxy server는 response 값을 판단하여 UAC를 인증 한다. 이 과정에서 전송되는 실질적인 메시지의 예시가 [그림 7]과 [그림 8]에 나타나 있다.



[그림 7] 407 Proxy Authentication Required 메시지

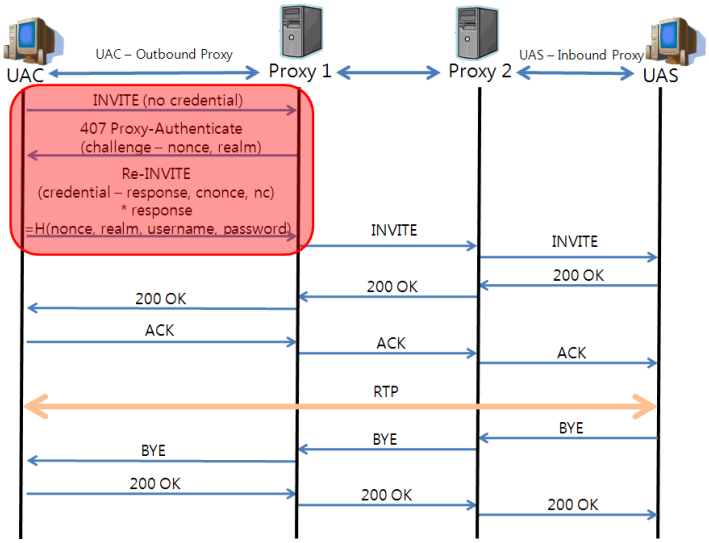


[그림 8] Response를 포함한 INVITE 메시지

407 Proxy Authentication Required 메시지에 사용되는 헤더에 대해 간략히 설명하면 다음과 같다.[5]

- Digest : 인증 기법을 나타냄.
- realm : 인증되는 도메인을 지정.
- qop : auth면 digest의 생성 시 username과 password만을 해시하고, auth-int면 SIP 메시지까지 해시.
- algorithm : 해시에 사용되는 알고리즘을 지정.
- nonce : replay 공격의 방지를 위해 서버 측에서 생성.

[그림 9]는 SIP call signaling 과정에서 사용자의 인증을 위해 HTTP Digest Authentication 기법을 적용 했을 시 세션을 설정하고, 종료하는 과정을 보여준다.



[그림 9] 인증이 적용된 세션 연결 설정

3.3. HTTP Digest Authentication의 취약점

HTTP Digest Authentication 기법을 사용하면 SIP call signaling 과정에서 사용자를 인증할 수 있다. 그러나 HTTP Digest Authentication 기법은 몇 가지 취약점을 가지고 있으며, 이러한 취약점으로 인하여 안전한 사용자 인증을 제공해 주지 못 한다. 이번 절에서는 HTTP Digest Authentication 기법의 몇 가지 취약점을 분석하였다.

① SIP 헤더의 기밀성과 무결성을 제공하지 못한다.

HTTP Digest Authentication 기법은 헤더를 암호화하지 않고, 평문인 상태로 전송을 하기 때문에 헤더의 기밀성과 무결성을 제공하지 못한다. SIP를 사용하여 세션 연결 설정을 하기 위해서는 세션 연결 설정에 앞서 registrar에 UA를 등록하는 과정이 필요하며, UA는 REGISTER 요청 메시지를 사용하여 자신을 registrar에 등록하게 된다. 이 과정에서 UA의 인증을 위하여 HTTP Digest Authentication 기법을 사용하게 될 경우 메시지의 헤더는 평문으로 전송되기 때문에 악의적인 공격자가 헤더의 내용을 수정하여 UA의 올바른 등록을 방해할 수 있다. 또한 악의적인 공격자가 네트워크 도청을 통하여 누가 누구와 세션을 연결했는지 알 수 있게 되어 사용자의 privacy가 노출되는 문제가 발생 할 수 있다.

② Off-line password guessing 공격에 취약하다.
HTTP Digest Authentication 인증 기법은 클라이언트와 서버가 사전에 비밀 패스워드를 공유하고 있다는 전제하에 동작을 한다. 공격자가 이 패스워드를 알 수 있다면 정당한 사용자로 위장하여 인증을 받을 수 있다. [그림 7]과 [그림 8]에서 보는 바와 같이 공격자는 도청을 통해 response의 계산에 사용되는 값인 nonce, username, realm과 response 값 자체를 얻을 수 있다. 공격자가 여러 가지의 패스워드를 추측하면서 response 값을 계산해본 결과 일치하는 response 값이 나오면 공격자는 패스워드를 얻을 수 있게 되고, 정당한 사용자로 위장하여 인증을 받을 수 있다.

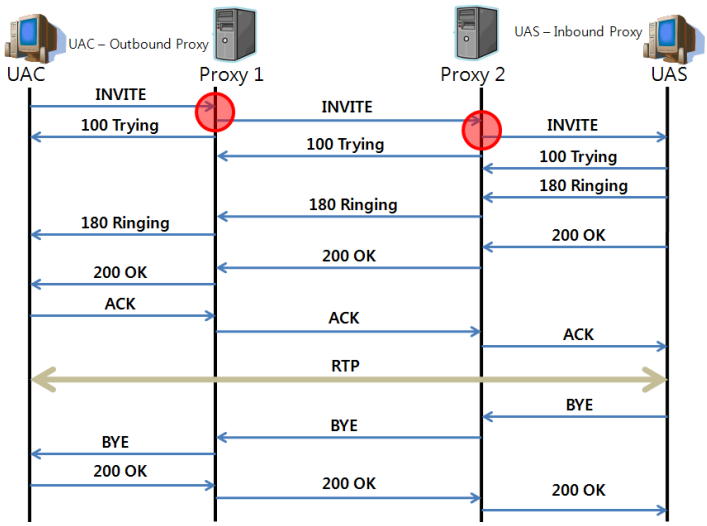
③ Server spoofing 공격에 취약하다.
HTTP Digest Authentication 인증 기법은 상호인증을 제공하지 않는다. 즉, [그림 9]에서 보는 바와 같이 proxy server가 UAC를 인증할 수는 있지만 UAC가 proxy server를 인증할 수는 없다. 이로 인해 공격자가 proxy server로 위장하여 UA로부터의 세션 연결 요청을 악의적인 사용자와 연결되도록 할 수 있다.

④ Inbound proxy와 UAS간 인증은 정의하지 않는다.
RFC3261에서는 SIP call signaling 시 사용자를 인증하기 위하여 HTTP Digest Authentication을 적용하는데 있어서 UAC와 outbound proxy간에만 적용을 하고, inbound proxy와 UAS간에는 적용을 하지 않고 있다. UAS가 inbound proxy로부터 세션 연결 요청 메시지인 INVITE 메시지를 수신하는 과정에서 inbound proxy의 인증 없이 수신하게 되는 경우 여러 가지 공격을 받을 수 있게 된다.

4. 제안하는 기법

3.2절에서 본바와 같이 SIP call signaling 프로토콜을 이용하여 세션 연결 설정을 하는 과정에서 사용자의 인증을 위하여 HTTP Digest Authentication 기법을 사용할 수 있다. 그러나 3.3절에 나와 있는 바와 같이 세션 연결 설정 시 인증을 위해 HTTP Digest Authentication 기법의 사용은 몇 가지 취약점을 가지고 있어 안전한 사용자 인증을 제공해 주지 못 한다. 이번 장 에서는 HTTP Digest Authentication 기법이 가지고 있는 취약점을 보완하여 세션 연결 설정 시 사용자 인증을 안전하게 해줄 수 있는 인증 메커니즘을 제시한다. 본 인증 기법은 세션 연결 설정 시의 인증 기법이며, UA가 registrar에 등록하는 과정에서 서로 간의 비밀 패스워드를 공유하는 것을 가정으로 한다.

[그림 10]은 제안하는 방식이 적용되는 범위를 보여주고 있다. 즉, UAC와 inbound proxy간의 인증과 UAS와 outbound proxy 간의 인증을 제공해주게 된다.



[그림 10] 인증의 적용 범위

4.1. UAC와 Outbound Proxy 간의 인증

UAC와 outbound proxy 간의 인증 시 HTTP Digest authentication 기법이 가지고 있는 취약점인 off-line password guessing 공격이나 server spoofing 공격에 대응할 수 있는 인증 기법이 필요하다. 이를 위해서는 상호 인증 기법이 필요하다.

제안하는 방식의 절차는 다음과 같다.

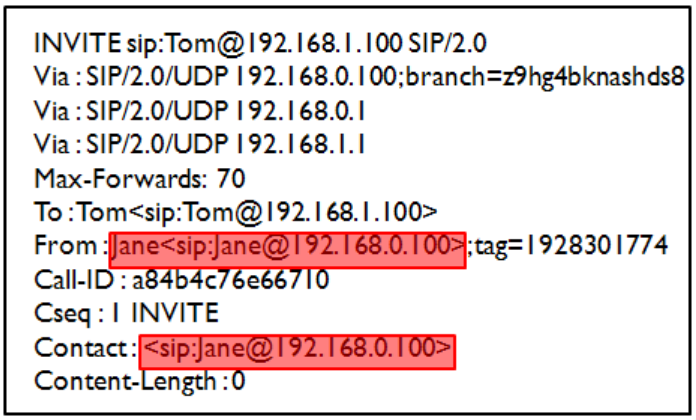
- UAC가 outbound proxy에 INVITE 메시지를 전송할 시 [그림 11]에 나타나 있는 특정 헤더 값을 서로 공유하고 있는 비밀 패스워드를 해시한 값을 키로 대칭키 암호화 알고리즘을 사용하여 암호화된 내용을 전송한다.
- INVITE 메시지를 수신한 outbound proxy는 암호화된 헤더 값을 공유하고 있는 비밀 패스워드를 해시한 값을 키로 대칭키 암호화 알고리즘을 사용하여 복호화 한다. 정상적으로 복호화가 이루어지면 UAC를 인증한다.
- UAC를 인증한 outbound proxy는 INVITE 메시지를 전송하고, 복호화한 헤더 값을 사용하여 100 Trying 응답 메시지를 UAC에 전송한다.
- 100 Trying 메시지를 수신한 UAC는 특정 헤더 값을 비교하여 일치하는 경우 outbound proxy를 인증한다.

```
INVITE sip:Tom@192.168.1.100 SIP/2.0
Via : SIP/2.0/UDP 192.168.0.100;branch=z9hg4bknashds8
Max-Forwards: 70
To : Tom<sip:Tom@192.168.1.100>
From : Jane<sip:Jane@192.168.0.100>;tag=1928301774
Call-ID : a84b4c76e66710
Cseq : 1 INVITE
Contact : <sip:Jane@192.168.0.100>
Content-Length : 0
```

[그 림 11] 인증을 위한 헤더 값 암호화

4.2. UAS와 Inbount Proxy 간의 인증

UAS와 inbound proxy 간의 인증 시에도 안전한 인증을 위해 상호 인증 기법이 필요하다. 제안하는 방식은 UAC와 outbound proxy 간의 인증 절차와 유사하며 인증을 위해 [그림 12]와 같은 헤더 값을 암호화하여 전송한다.



[그림 12] 인증을 위한 헤더 값 암호화

5. 결론 및 향후 연구 계획

VoIP 기술은 음성 통신에 있어서 기존의 PSTN망을 대체하는 새로운 기술로 자리 잡고 있다. 그러나 VoIP가 기존의 PSTN망을 대체하는 음성 통신 기술로 완전히 자리매김하기 위해서는 보안성의 제공이 필수적인 요소로 고려되어야 하며, 이 중 통신의 주체인 사용자가 정당한 사용자 인지를 판단하는 사용자 인증 기법은 VoIP 통신에서 필수적이라 할 수 있다.

VoIP 통신에서 call signaling에 사용되는 프로토콜 중 한 가지인 SIP 프로토콜은 사용자의 인증을 위하여 HTTP Digest Authentication 기법의 사용을 권고 하고 있다. 그러나 이 인증 기법은 off-line password guessing 공격과 server spoofing 공격에 취약점을 보이는 등 몇 가지 문제점을 가지고 있다. 본 논문에서는 이러한 취약점을 보완하는 새로운 인증 메커니즘을 제안하였다. 그러나 제안한 기법은 세션 연결 설정 단계에서의 사용자 인증 기법으로 보다 완전한 사용자 인증을 제공해 주기 위해서는 UA가 registrar에 자신을 등록하는 과정에서 사용자를 인증해 주는 기법이 필요하며, 향후 이 부분에 대한 연구의 진행이 필요하다고 하겠다.

<Acknowledgements>

본 연구는 한국과학재단 특정기초연구(R01200600011196020008) 지원으로 수행되었음.

<참고문헌>

[1] U.Black, "Internet Telephony Call Processing Protocol", Prentice Hall, 2001

[2] J.Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", IETF RFC 3261, 2002

[3] D.Richard Kuhn, Thomas J.Walsh, Steffen Fries, "Security Considerations for Voice Over IP Systems", NIST SP 800-58, 2005

[4] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", IETF RFC 2617, 1999

[5] Paul D.Smith, Ian Clarkson, "Digest Authentication Examples for Session Initiation Protocol(SIP)", Internet Draft, 2004