主題

# VoIP 보안 기술

정 수 환, 홍 기 훈, 박 성 준

차 례



## Ⅰ. 개요

VoIP 기술이 발전되고 사용이 일반화되면서 이제 사용자들은 자신의 통화 내용이나 인터넷폰을 통한 사생활 정보가 보호받기를 원하게 되었다. 그러나 인터넷은 개방형의 네트워크로서 누구나 쉽게 접근하여 정보를 공유하거나 확산시킬 수 있고 다른 사용자의 정보를 빼내어 악용할 수 있는 보안상의 약점을 가지고 있다. 따라서 메일이나 파일뿐만 아니라 인터넷 기반의 실시간 통신인 VoIP에 의해 전달되는 정보들도 예외일 수는 없다. 이러한 문제점은 VoIP의 확산에 악영향을 줄 수 있으며 따라서 VoIP에 보안 기능을 추가하는 작업이 반드시 수행되어야 한다.

VoIP 보안 문제는 VoIP를 위한 보안 프로토콜을 정의하고 보안 알고리즘을 사용하여 사용자의 음성 정보를 암호화함으로써 해결할 수 있다. 이러한 VoIP 보안을 위해 H.323과 SIP 프로토콜에 보안 기능을 추가하는 작업이 현재 진행중이다. 우선 ITU-T에서는 H.323을 위한 보안 프로토콜로서 H.235를 정의하여 H.323 시그널링 메시지의 무결성을 보장하고 사용자의 음성 정보를 암호화하여 비밀성을 제공한다. 반면에 SIP(Session Initiation Protocol) 프로토콜은 호 설정 메시지에 대하여 비밀성을 보장하지만 아직까지 사용자의 음성을 보호하는 기능은 정의하고 있지 않다. SIP에서는, IETF에서 주로 제안되어 기존에 사용되고 있는 IPsec(IP Security), TLS(Transport Layer Security), S/MIME(Secure/Multipurpose Internet Mail Extension) 등의 보안 메커니즘을 이용하여 암호화를 권장하고 있다. 그러나 이러한 보안 프로토콜들은 VoIP만을 위한 보안 프로토콜이 아니므로 사용 시 호 설정 시간이 증가하거나 VoIP 프로그램에서 보안을 제어하기 곤란한 문제점들이 있다. IETF에서는 앞으로 발표되는 모든 문서에서 보안을 반드시 고려하도록 규정할 정도로 보안은 모든 인터넷 기반 프로토콜의 핵심 고려사항이 되고 있어 조만간 SIP을 위한 보안 메커니즘 정의도 완료될 것으로 예상된다. 또 다른 문제점은 보안 장비인 방화벽이나

표 1. Baseline security profile

| 보안 서비스 | 기능 | | | |
|---|---|---|---|---|
| | RAS | H.225 | H.245 | RTP |
| 인 증 | Password HMAC-SHA1-96 | Password HMAC-SHA1-96 | Password HMAC-SHA1-96 | |
| 무결성 | Password HMAC-SHA1-96 | Password HMAC-SHA1-96 | Password HMAC-SHA1-96 | |
| 비 밀 성 | | | | 56-bit DES / 56-bit RC2-Compatible / 168-bit 3DES |
| 키 관 리 | 가입자 정보기반의 패스워드 할당 | Diffie-Hellman 를 이용한 키 교환, 패스워드 할당 | Security Capability 교환, H.225 세션키의 암호화 전송 | |

NAT (Network Address Translator) 등의 장비를 사용하는 경우 기존 VoIP 프로토콜이 이런 장비들을 통과하지 못하는 문제가 발생하고 있다. 이러한 문제를 해결하기 위해 IETF에서는 Transport Area에 MIDCOM (Middlebox Communication) 워킹 그룹을 구성하여 문제 해결 방안을 모색하고 있다. 따라서 본 고에서는 VoIP 보안에 관련된 H.235와 SIP 보안 그리고 MIDCOM에 대하여 알아보도록 하겠다.

## Ⅱ. H.235

H.323 프로토콜의 보안을 고려하여 ITU-T에서 발표한 H.235는 메시지의 인증과 무결성을 지원하며 미디어 암호화와 게이트키퍼, 게이트웨이 인증 등을 포함하여 H.323 시스템의 모든 부분에 대하여 보안 기능을 규정하고 있다.

### 1. 기술 개요

Baseline Security는 일반적인 H.323에서의 보안 적용을 다루고 있고 SET(Simple Endpoint Type)에서의 보안에 대한 기본 방향을 제시하고 있으며 표 1에서 전반적인 구성을 보여주고 있다. H.235 에서는 RAS를 통해 패스워드 기반의 인증을 사용하고 H.225 연결 설정에서 Diffie-Hellman 키 교환 알고리즘을 사용하여 두 단말간에 대칭키를 공유하게 된다. 이 키는 H.245에서 RTP 채널을 암호화하는데 사용되어진다. H.245에서는 양 단말간에 Security capability를 교환하고 RTP 채널을 암호화하기 위한 대칭키를 생성한 후 H.225에서 공유한 키를 사용하여 암호화하여 전송한다. 실제 음성이 전달되는 RTP 채널은 H.245에서 전달된 대칭키를 사용하여 암·복호화된다. 이 때 사용 가능한 암호 알고리즘은 56-bit DES, 56-bit RC2-compatible 그리고 168-bit 3DES 등이 있다[1].

### 2. RAS 보안

RAS메시지에서는 메시지 인증과 무결성 보장 기능을 제공하며 메시지의 암호화는 제공하지 않는다. RAS 메시지를 위한 인증 방법의 결정은 GRQ/GCF 메시지에서 결정하며 결정된 인증 방법을 통하여 xRQ, xCF, xRJ 메시지를 인증하고 무결성을 보장하게 된다. RAS 메시지 교환 중 첫 단계인 GRQ 메시지에서는 단말기가 지원하는 인증 알고리즘을 authentication- Capability 메시지에 첨부하여 전송한다. GRQ 메시지를 받은 게이트키퍼는 받은 capability 중 지원하는 capability를 정책 결정에

맞게 선택하여 GCF 메시지의 authentication Mode에 첨부하여 전송한다. 이 과정은 단말기와 게이트키퍼 간의 인증 및 무결성 보장보다는 차후 교환될 메시지에 대한 인증 및 무결성 검사 방법을 설정하는 단계로 볼 수 있다. H.235 annex D에서는 기본적으로 표 1과 같이 HMAC-SHA1-96을 사용하도록 권고하고 있으며 기타 인증 및 무결성 알고리즘은 nonStandard로 개발자 정의 하에 사용하도록 하고 있다. GRQ/GCF 이후 사용되는 모든 xRQ, xCF 메시지는 선택된 알고리즘에 의해 인증 및 무결성 보장 데이터를 생성하여 메시지에 첨부시켜서 전송한다.

### 3. H.225 보안

H.225.0에서는 메시지 인증, 무결성 보장 및 세션키 암호화를 위한 Diffie-Hellman 키 생성의 세 가지의 보안 기능을 갖는다. 메시지 인증과 무결성 보장은 RAS와 동일한 방법으로 사용되며 이 때 사용되는 인증 알고리즘은 HMAC-SHA1-96을 이용하며 무결성도 동시에 보장된다. Diffie-Hellman 키 생성은 음성 채널 암호화에 사용될 키를 암호화하기 위하여 생성된다[3].

### 4. H.245 보안

H.245에서는 음성 데이터의 암호화에 사용될 암호화 알고리즘의 단말 지원 여부(capability)를 교환한다. H.235 security capability는 H.323에서 교환하는 audio, video capability 등과 동일한 방법으로 전송 및 처리된다. H.245 terminal CapabilitySet 메시지에 모든 음성, 영상 알고리즘 및 암호화 알고리즘을 같이 삽입하여 서로 전송하게 되면 양 단말은 각각 지원하는 보안 알고리즘을 선택해서 이를 이용하여 암호화를 하게 된다. H.235 annex D에서는 DES, 3DES, RC2를 지원하도록 하고 있으며 이들 모두 CBC모드로 IV(Initialization Vector)를 필요로 한다. Capability 교환 후 H.245 에서는 마스터/슬래이브 결정 과정을 거치게 된다. 이 과정을 거치고 나면 마스터로 결정된 단말이 음성 데이터 암호화에 쓰일 키를 생성하게 되고 이 세션키는 H.245 메시지에서 암호화되어 전달하게 된다[4].

### 5. 음성 데이터 보안

상기의 과정을 거쳐 호 설정에 대한 인증을 수행하고 음성 통신에 사용될 암호화 알고리즘이 설정되었으며 암호화에 사용될 키와 IV를 결정하였다. 이러한 정보를 이용하여 실제 음성 데이터를 암호화하게 되는데 RTP 패킷의 헤더는 제외하고 RTP 페이로드만을 암호화하게 된다. 페이로드만을 암호화하게 되면 헤더까지 암호화하지 않으므로 암호화 지연시간을 줄일 수 있으며 수신이 잘못되거나 시간이 지난 RTP 패킷을 헤더정보만을 해석함으로써 복호화하지 않고 바로 삭제할 수 있기 때문에 CPU 자원의 낭비를 막을 수 있는 장점을 갖고 있다. 음성 데이터 보안에 사용되는 또 다른 기능은 Anti-spamming 알고리즘으로 이 알고리즘은 RTP 패킷의 Replay 공격을 방지하기 위한 메커니즘이다. Replay 공격이란 공격자가 암호화된 RTP 패킷을 도청할 수 없다 하더라도 표적 시스템의 통신을 방해하기 위해서 암호화되어 있지 않는 IP , UDP와 RTP 헤더 등을 변조하여 위조된 혹은 전에 받았던 RTP 패킷을 계속 전송함으로써 음성 통신이 불가능하게 만드는 공격법을 말한다. 이러한 공격법을 이용하게 되면 통신 당사자는 음성을 들을 수 없거나 잡음이 섞이게 되어 통신이 불가능하게 된다. 그림 1에서 이를 방지하기 위한 Anti- spamming 알고리즘을 보여주고 있는데, RTP 패킷 헤더의 P는 패딩을 의미하며 이를 1로 설정하여 패딩이 되었음을 알리고 패딩의 마지막 바이트에 인증 코드를 포함한 패딩 길이를 명시한다.

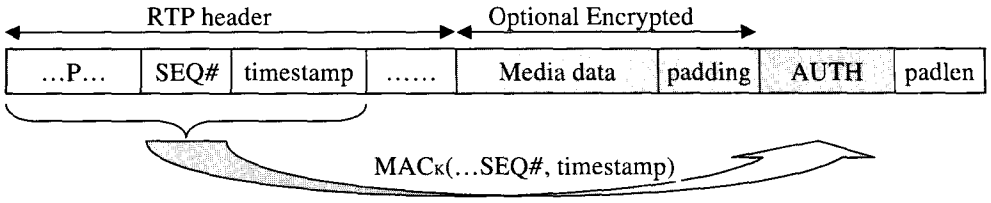



그림 1. Media Anti-spamming

표 2. Signature security profile

| 보안 서비스 | 기 능 | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | RAS | | H.225 | | H.245 | | RTP | |
| 인 증 | SHA1/ | MD5 | SHA1/ | MD5 | SHA1/ | MD5 | | |
| | Digital signature | | Digital signature | | Digital signature | | | |
| 부인 방지 | SHA1/ | MD5 | SHA1/ | MD5 | SHA1/ | MD5 | | |
| | Digital signature | | Digital signature | | Digital signature | | | |
| 무 결 성 | | | | | | | | |
| 키 관 리 | 인증 기관 | | 인증 기관 | | | | | |

세션키로부터 추출된 키를 이용하여 RTP 헤더의 처음 64비트로 인증 코드를 생성하여 AUTH 부분에 삽입하면 수신자는 패킷을 정상적으로 처리하기 전에 인증 절차를 거쳐 패킷의 정당성을 확인한 후에 처리하게 되며 이에 따른 연산 지연이 발생하지만 HMAC 등의 고속 알고리즘을 이용하기 때문에 지연이 크지 않다.

### 6. 인증서 기반 보안

H.235 Annex.E인 Signature profile은 전자서명을 이용한 VoIP 보안방법으로 PKI(Public-Key Infrastructure)을 기반으로 X.509의 인증서를 사용함으로 보다 규모가 큰 광범위(global) VoIP 서비스 구축을 위해서 반드시 필요한 부분이다. 이 부분을 위해서는 반드시 게이트키퍼 경유 모델을 써야 하며 H.245 메시지의 무결성 보장을 위해 H.245 터널링 모드를 지원해야 한다. 이 방법을 이용하면 인증과 무결성 보장 뿐 아니라 부인 방지의 효과도 볼 수 있다. 이 방법은 전자 서명의 검사를 통한 서비스 거부 공격의 대응이 가능하고 인증을 통한 man-in-the-middle 공격을 막을 수 있으며 타임스탬프와 일련번호를 이용해서 Replay 공격을 막을 수 있고 인증을 통하여 신분 위장 및 연결 탈취(session hijacking) 등을 막을 수 있는 장점을 갖는다. 표 2에서 보는 바와 같이 전자 서명을 이용한 보안 서비스는 암호화를 지원하지 않으며 이 서비스는 인증과 무결성 보장 그리고 부인 방지 기능을 인증기관을 이용하여 보장한다. 그러나 이 기능은 PKI 기반의 전자서명을 사용하므로 PKI 시스템이 갖추어지지 않았을 경우 적용이 곤란하다.

## Ⅲ. SIP Security

IETF에서 제안한 SIP(Session Initiation

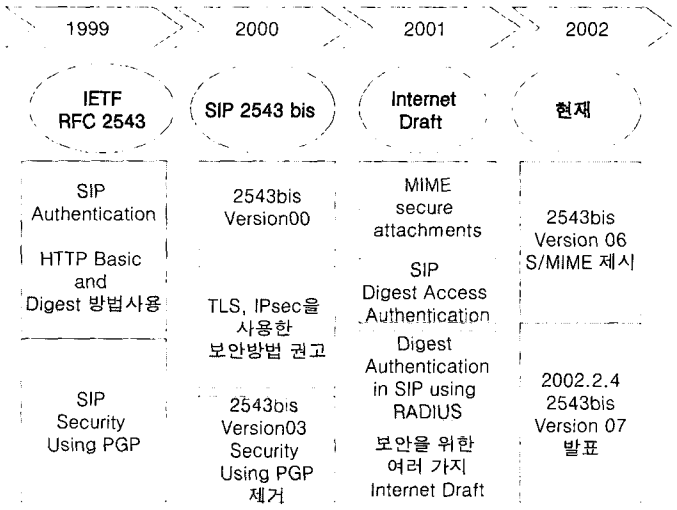



**그림 2. SIP 보안 기술 동향**

Protocol)은 텍스트 기반 응용 계층의 접속제어 프로토콜로 HTTP와 SMTP를 기반으로 클라이언트/서버 구조를 가지며, 앞으로 실시간 미디어 통신을 위한 차세대 인터넷 프로토콜로 주목을 받고 있다. 또한 3GPP(3rd Generation Partnership Project)에서는 SIP를 시그널링 프로토콜로 결정했으며 인터넷을 이용한 원격회의, 인터넷 전화, 인스턴트 메시지 등의 서비스에 적용할 수 있다. 이와 같은 서비스를 위해서는 인터넷에서 발생되는 보안문제 해결이 중요하며 이장에서는 SIP의 보안 문제를 해결하기 위한 SIP 보안 기술 동향에 대해 설명할 것이다.

## 1. SIP 보안 기술 동향

SIP에서는 보안을 위한 새로운 메커니즘을 정의하지 않고 주로 기존에 사용하고 있는 보안 메커니즘을 사용한 보안 모델을 제시하고 있으며 주로 HTTP나 SMTP 같은 프로토콜에서 사용되는 방법을 적용하고 있다. SIP 보안에서 중요한 요구 사항으로는 여러 가지 다양한 환경과 응용 프로그램에 적용할 수 있는 보안 메커니즘으로 복잡성을 최소화하기 위하여 새로운 기반 구조나 알고리즘의 확장은 지양하고 있다. 이는 SIP 보안 기술의 변화에서도 살펴볼 수 있다. IETF에서는 1999년 RFC2543[6]을 발표하고 이를 보완하기 위해 여러 가지 드래프트들을 제안하고 인터넷 드래프트인 2543bis를 만들어 계속 표준화 작업을 진행하고 있으며, 2002년 2월에는 2543bis version 7[7]을 발표했다. RFC 2543에서는 기존의 HTTP에서 사용하고 있는 basic과 digest 인증 방법[8]을 SIP에서 제시하였고 PGP 암호화 방법을 사용하여 end-to-end 메시지 암호화 방법을 제시하였다. 그러나 PGP 암호화 방법은 키 교환 방법, 확장성 등의 문제점으로 인해 2543bis version 3에서는 이를 제거하게 되었다. 또한 2002년 1월에 발표된 2543bis version 6에서는 end-to-end 메시지 암호화를 위한 방법으로 S/MIME을 새롭게 제시하고 있다. 그림 2에서는 SIP 보안 기술의 동향을 나타내고 있다.

## 2. SIP 보안 메커니즘

SIP의 보안을 위해서는 기본적으로 메시지에 대한 비밀성과 무결성을 지원하여 Replay 공격이나

메시지 변조(spoofing)와 같은 공격을 방지하고 메시지에 대한 인증을 통해 DoS(Denial of Service) 같은 공격을 차단해야 한다. 이를 위해 SIP에서는 여러 가지 보안 메커니즘을 적용하고 있다. SIP 메시지 전체에 대한 암호화는 메시지에 대한 비밀성을 완벽하게 보장하여 네트워크 상의 공격자로부터 정보 누출을 방지 할 수 있으나 프락시 서버에서 라우팅을 위한 정보를 나타내는 To, From, Request-URI, Route, Via 등의 헤더를 확인할 수 없어 정확한 메시지 전달이 어렵다. 따라서 프락시 서버와 SIP UA 간에 서로에 대한 신뢰를 할 수 있도록 하기 위한 방법으로 하위-레이어 보안 메커니즘을 적용할 수 있다. 이는 IPsec[9]나 TLS[10]와 같은 네트워크나 트랜스포트 레이어 보안 프로토콜을 적용하는 방법으로 IPsec이나 TLS을 통하여 hop-by-hop 간의 메시지에 대한 비밀성과 무결성을 지원하게 된다. end-to-end 암호화 방법을 사용할 때에는 앞에서 말한 바와 같이 프락시에서 SIP메시지를 변경하거나 분석할 수 있도록 라우팅 관련 헤더는 제외하고 암호화하여 전송하게 된다. 메시지 암호화를 위해 새롭게 제시된 S/MIME은 end- to-end간의 메시지에 대한 비밀성과 무결성을 지원할 뿐만 아니라 인증서를 통한 상호간의 인증도 제공할 수 있다. MIME은 SMTP를 확장하여 오디오, 비디오, 이미지, 응용프로그램, 기타 여러 가지 종류의 데이터 파일들을 주고받을 수 있도록 기능이 확장된 프로토콜로서 보안 메커니즘을 가지고 있지 않으며, 이 때문에 응용계층에서 보안을 제공하기 위해 S/MIME이 제안되었다. S/MIME은 전자 메일뿐만 아니라 MIME 형태를 전송하는 모든 프로토콜에 적용할 수 있고 암호화와 전자서명 기능을 제공하며 사용되는 암호화 알고리즘은 표 3에서 보여주고 있다.

SIP 메시지 또한 텍스트 기반의 MIME 형태로 전송되기 때문에 S/MIME을 사용하여 end-to-end 간의 비밀성과 무결성을 지원할 수 있다. 그림 3는 S/MIME을 이용한 메시지 암호화를 보여주고 있으며, "*"로 표시된 부분이 암호화된 부분을 나타내고 있다[7]. 그림 3에서와 같이 프락시에서 변경되거나 라우팅에 관련된 헤더 정보는 제외하고 SDP와 같은 메시지 바디를 암호화하여 전송한다.

**표 3. S/MIME 보안 서비스**

| 보안 서비스 | 보안 메커니즘 | 암호화 알고리즘 |
|---|---|---|
| 비밀성 | 암호화 | 3DES |
| 무결성 | 전자서명 | SHA-1 |
| 인증 | 전자서명 | X.509v3 인증서 |
| 부인방지 | 전자서명 | DSA |

SIP에서는 메시지 변조를 통한 서비스 방해나 Replay 공격을 방지하기 위해 메시지에 대한 인증

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKnashds8
To: Bob <bob@biloxi.com>
From: Alice <alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Max-Forwards: 70
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
   name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
   handling=required

* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
* Content-Type: application/sdp                                 *
*                                                               *
* v=0                                                           *
* o=alice 53655765 2353687637 IN IP4 pc33.atlanta.com           *
* s=-                                                           *
* t=0 0                                                         *
* c=IN IP4 pc33.atlanta.com                                     *
* m=audio 3456 RTP/AVP 0 1 3 99                                 *
* a=rtpmap:0 PCMU/8000                                          *
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

**그림 3. S/MIME 메시지 암호화**

메커니즘을 지원하고 있으며 이를 위해 HTTP에서 사용하는 인증 방법인 basic 인증과 digest 인증 방법[8]을 적용하고 있다. 그러나 basic 인증 방법은 패스워드가 누출될 수 있어 보안에 상당히 취약하기 때문에 주로 digest 인증 방법의 사용을 권고하고 있다. Digest 인증 방법은 challenge-response 형태로서 UAC에서 request 메시지를 보내면 UAS에서는 nonce와 realm 등과 같은 정보를 보내주게 된다. 이와 같은 정보를 받은 UAC에서는 받은 정보와 자신의 패스워드, username값을 가지고 해쉬하여 UAS에게 response로 보내게 된다. UAS에서는 받은 해쉬 값과 자신이 가지고 있는 UAC에 대한 정보를 가지고 해쉬한 값을 비교하여 값이 같으면 인증이 성공하게 된다. 그림 4는 digest 인증 방법의 절차를 보여주고 있다. 이와 같은 인증 절차는 UAS에서 UAC에 대한 인증이나 Authentication-Info 헤더를 사용하면 UAC와 UAS간의 서로에 대한 상호 인증을 할 수도 있다.

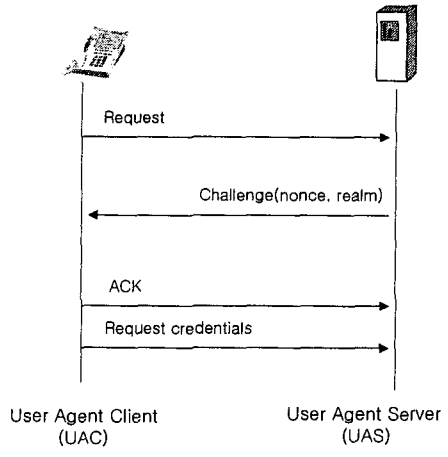



그림 4. Digest 인증 절차 단계

## Ⅳ. MIDCOM

MIDCOM은 IETF에서 네트워크에 방화벽이나 NAT 등의 장비가 설치된 경우 IP 주소나 포트가 바뀔 때 통신이 원활히 수행되지 못하는 문제를 해결하기 위해 구성된 워킹 그룹이다. 특히 현재 VoIP와 같이 시그널링 중에 미디어를 위한 주소나 포트가 할당되어 실제 음성을 전달 시 할당된 주소나 포트를 사용하는 경우 NAT나 방화벽을 지나지 못하는 문제를 해결하는데 도움이 될 것이다. 그러나 이러한 작업은 근본적으로 중간 장비인 방화벽이나 NAT등에서 미디어 채널을 인식하여 통과할 수 있도록 수정하여야 하는데, 문제를 분석하고 해결 방안을 정의한 후, 이를 실제 모든 방화벽과 NAT에 적용하기까지는 많은 시간이 필요하므로 우선 NAT나 방화벽의 수정 없이 해결할 수 있는 방안을 모색중이며 관련된 몇 편의 드래프트가 나와 있다.

### 1. VoIP 채널의 방화벽 및 NAT 통과 문제

방화벽이나 NAT에서 미디어를 위한 프로토콜이 통과하지 못하는 문제점은 방화벽의 경우 내부에서 외부로 세션을 시작하면 1분에서 3분 정도의 시간동안 세션을 열어주고 패킷이 오가지 않으면 닫아 버리기 때문이며, NAT의 경우는 내부 사설 IP 주소와 외부 IP 주소간에 연결 테이블을 구성하고 유지하는 방식이 여러 가지로 분류될 수 있기 때문에 VoIP 프로토콜의 통과 문제 해결을 위한 처리가 곤란하며 따라서 NAT의 네 가지 분류를 살펴보자.

**Full Cone NAT** : 고정 IP 할당 방식으로 외부 IP 주소와 포트 번호가 내부 IP 주소와 포트 번호로 할당되어 외부의 호스트가 세션을 시작할 수 있는 방식이다.

**Restricted Cone NAT** : 동적으로 IP를 할당하는 방식으로 내부와 외부의 IP 주소와 포트 번호가 대응되며 내부에서 외부로의 연결 요청을 받은 IP 주소의 호스트만이 외부에서 내부로 패킷을 전송할 수 있다.

**Port Restricted Cone NAT** : 내부와 외부

의 IP 주소와 포트 번호가 대응되며 Restricted Cone NAT 방식에 IP 주소뿐만 아니라 포트 번호까지 확인하여 내부에서 외부로의 연결을 요청 받은 호스트의 IP 주소와 포트 번호를 가지는 패킷만이 외부에서 내부로 패킷을 전송할 수 있다.

**Symmetric NAT** : 내부 호스트의 패킷을 받은 호스트만이 외부에서 내부로 패킷을 전송할 수 있는 방식으로 하나의 내부 IP를 가지는 호스트가 각각의 다른 외부 호스트에게 접속 시 각각 다른 외부 IP가 할당되는 방식으로 VoIP의 미디어 패킷이 전송되기 가장 곤란한 방식이다.

## 2. 방화벽 및 NAT Traversal

앞에서 살펴본 방화벽과 NAT의 주소 및 포트 대응 방식을 파악하기 위해 STUN(Simple Traversal of UDP through NATs)을 이용하여 알 수 있도록 제안하고 있다. STUN은 클라이언트와 서버로 구성되는데 클라이언트는 사용자의 PC나 내부 네트워크의 요소로서 동작할 수 있고 서버에게 요청 메시지를 생성하여 보낸다. STUN 서버는 외부 네트워크에 존재하며 클라이언트로부터 전송된 요청 메시지를 받아 STUN 응답 메시지를 생성하여 클라이언트에 전송한다. 클라이언트는 수신한 응답 메시지를 통해 현재 내부 네트워크와 외부 네트워크 사이에 NAT가 존재하는지 여부와 어떤 방식의 NAT가 동작하는지를 파악한다.

1) 만일 STUN 클라이언트가 요청 메시지를 보낸 후 응답을 받아서 로컬 주소와 비교하여 다르면 중간에 하나 이상의 NAT가 존재함을 알 수 있다.
2) STUN 클라이언트는 요청 메시지를 두 개의 다른 STUN 서버에게 연속해서 보낸 후 응답을 받아 소스 주소와 포트를 비교하여 다르면 symmetric NAT가 존재함을 알 수 있다.
3) 플래그를 설정하여 요청 메시지의 IP 주소와 포트번호가 대응되지 않는 다른 IP 주소와 포트번호로 응답하도록 하여 응답 메시지를 받으면 Full Cone 방식의 NAT가 있음을 알 수 있다.
4) 플래그를 설정하여 요청 메시지의 포트번호와 대응되지 않는 포트번호로 응답하도록 하여 응답 메시지를 받으면 Restricted Cone 방식의 NAT가 있음을 알 수 있다.

이러한 방법을 사용하여 NAT의 특성을 파악하여 어떤 방법으로 NAT을 통한 미디어 패킷을 전송 할 수 있는지 알 수 있다[11].

방화벽이나 NAT 등을 통과하는 방법으로 어플리케이션 프락시와 PEA(Proxy Extension Agent)를 사용하여 포트를 예약하는 방법이 다른 드래프트에 의해 제안되고 있다. 이 방법은 방화벽과 NAT 등의 장비를 가운데 두고 내부 네트워크 쪽에는 어플리케이션 프락시를 두며 외부 네트워크에서는 PEA를 두어 미디어가 전송될 채널을 예약하도록 하는데, RTP 패킷을 방화벽이나 NAT에 통과시켜 미리 확보한 후 시그널링을 완료하여 통신이 가능하도록 한다. INVITE 메시지를 받은 어플리케이션 프락시는 미디어 채널을 확보하기 위해 PEA에 미디어 채널 요청을 한 후 응답으로 받은 포트와 토큰을 이용하여 PEA에게 RTP 프루브 패킷을 보낸다. 프루브 패킷의 응답이 도착하면 어플리케이션 프락시는 할당된 포트를 이용하여 INVITE 메시지를 통화하고자 하는 상대에게 보낸다. INVITE 메시지를 받은 상대방은 RTP 패킷을 전송한 후 200 OK 메시지를 전송하면 어플리케이션 프락시는 이를 받아 포트를 확인하고 이 포트와 상대방의 주소를 PEA에게 보내 어플리케이션 프락시가 RTP 패킷을 받을 수 있도록 알려주고 200 OK 메시지를 내부 사용자에게 전달한다. 내부 사용자는 RTP 패킷을 전송하고 SIP ACK 메시지를 통화하고자 하는 상대방에게 보내 시그널링을 완료한다[12].

또 다른 IETF 드래프트에서는 실제 방화벽과

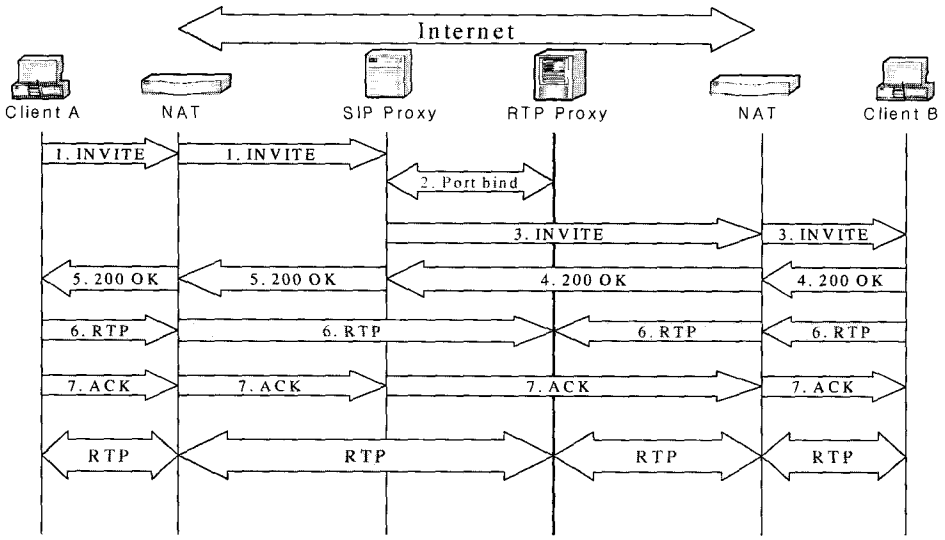



그림 5. Firewall/NAT traversal

NAT를 통과할 수 있는 시스템을 제안하고 있는데 크게 나누어 시그널링 패스와 미디어 패스를 위한 해결 방안으로 나눌 수 있다. 그림 6에서는 SIP에서 RTP 프락시를 이용한 제안된 시스템의 전체 동작을 보여주고 있다. 시그널링 패킷의 통신은 VoIP 프로그램이 Keep-alive 패킷을 이용해 주기적으로 시그널링 세션을 열어 줌으로써 외부에서 내부로의 연결 요청을 가능하게 하고 있다. 이러한 Keep-alive 패킷은 방화벽이나 NAT의 타임아웃 시간이 주로 1분에서 3분이므로 이보다 적은 시간에 주기적으로 프락시에 Keep-alive 패킷을 전송하여 열린 세션을 유지시킨다. 미디어 패스 확보를 위한 방법은 다음과 같다.

1) 클라이언트 A는 INVITE 메시지를 NAT를 통하여 SIP 프락시로 보내어 통화를 요청한다.
2) SIP 프락시는 RTP 프락시에게 IP 주소와 포트번호 쌍을 예약하도록 하고 RTP 프락시는 예약한 내용을 SIP 프락시에 알린다.
3) SIP 프락시는 INVITE 메시지의 SDP를 수정하여 미디어 패킷을 RTP 프락시의 할당된 포트로 전송하도록 클라이언트 B에게 알린다.
4) 클라이언트 B는 미디어 패킷을 받기 위해 자신의 사설 IP 주소와 포트번호 등을 SDP에 명시하여 200 OK 메시지를 SIP 프락시에게 보낸다.
5) SIP 프락시는 200 OK 메시지의 SDP 내용을 수정하여 클라이언트가 미디어 패킷을 클라이언트 B가 아닌 RTP 프락시의 할당된 포트로 보내도록 한다.
6) 각각의 클라이언트는 RTP 패킷(잡음)을 RTP 프락시에게 보내고 RTP 프락시는 패킷을 수신하여 각각의 소스 IP 주소와 포트 번호를 기억하여 연결할 대상의 외부 IP 주소와 포트 번호를 대응시킨다.
7) 마지막으로 클라이언트 A는 ACK 메시지를 SIP 프락시를 경유하여 클라이언트 B에게 전송한다.
8) 이후 전송되는 미디어 패킷은 RTP 프락시로 전송되어 목적지 주소와 포트번호가 변경되어 각각의 클라이언트에게 전송된다.

이와 같은 방법을 사용하는 이유는 Symmetric NAT의 경우 할당되는 목적지에 따라 NAT가 다른 외부 IP 주소를 할당하기 때문이다. 그러나 이러한

방법은 RTP 프락시가 많은 패킷에 대하여 주소 변환을 시켜주어야 하기 때문에 과부하와 지연시간의 증가를 유발할 수 있다[13].

## V. 결론

지금까지 VoIP의 보안에 관련된 사항들에 대하여 알아보았다. H.235는 현재 VoIP을 위한 보안 요소들에 대하여 많은 부분들이 잘 정의되어 있으며 인증서를 사용한 전자 서명으로 사용자의 인증과 부인 방지 등을 제공한다. 또한 기존에 정의된 암호 알고리즘과 운영 모드에 새로운 운영 모드와 알고리즘이 추가 될 것으로 예상된다. 반면에 SIP에서는 현재 보안을 위한 추가적인 작업이 한창 진행 중으로 주로 시그널링 메시지의 암호화에 중점을 두어 연구하고 있으며 아직까지 음성 채널의 암호화를 위한 보안은 제공하지 못하고 있다. 물론 기존의 범용 보안 프로토콜을 이용하는 방안이 있지만 VoIP 프로그램과 범용 보안 프로토콜과의 인터페이스가 정의되어 있지 않아 접목이 그리 간단히 진행되지는 않을 것으로 예상된다. MIDCOM 워킹 그룹이 구성됨으로써 방화벽 및 NAT 통과 문제 해결을 위한 근본적인 노력이 시작되었지만 VoIP 입장에서는 몇 년 후의 해결책보다는 현재 빠르게 문제를 해결 할 수 있는 방안이 필요한 시점이다. 따라서 현재 이런 문제들을 해결하기 위해 사용되는 방법을 정리하고 드래프트로 제안하여 토론함으로써 해결책을 찾는 작업이 진행 중이다.

### 참고 문헌


[1] ITU-T, "Security and encryption for H-Series(H.323 and other H.245-based) multimedia terminals", H.235 v2, Nov. 2000

[2] ITU-T, "Packet-based multimedia communications systems", H.323 v4, 2000

[3] ITU-T, "Call signaling protocols and media stream packetization for packet-based multimedia communication systems", H.225.0, 2000

[4] ITU-T, "Control Protocol for Multimedia Communication", H.245, 2000

[5] RSA lab., "Diffie-Hellman Key Agreement Standards version 1.4", PKCS #3, 1993

[6] RFC 2543, "SIP : Session Initiation Protocol", IETF SIP WG., 1999

[7] Internet Draft, "SIP: Session Initiation Protocol RFC 2543 bis-07", IETF SIP WG., 2002

[8] RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication", IETF , 1999

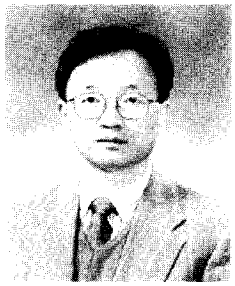
[9] RFC 2402, "IP Authentication Header", IETF IPsec WG., 1998

[10] RFC 2246, "The TLS Protocol Version 1.0", IETF TLS WG., 1999

[11] Internet Draft, "STUN - Simple Traversal of UDP Through NATs", IETF MIDCOM WG., Oct. 2001

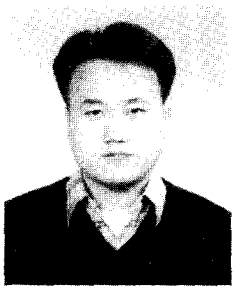
[12] Internet Draft, "Traversal of non-Protocol Aware Firewalls & NATS", IETF MIDCOM WG., Oct. 2001

[13] Internet Draft, "Midcom-unaware NAT/Firewall Traversal", IETF MIDCOM WG., Sept. 2001



**정 수 환**

1985년 2월 : 서울대학교 전자공학과 학사, 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 조교수 〈관심분야〉 VoIP security, Security Protocol, 사용자 인증, Cryptography



**홍 기 훈**

2000년 2월 : 숭실대학교 정보통신공학과 졸업 학사, 2002년 2월 : 숭실대학교 대학원 정보통신공학과 석사, 2002년 현재 : 숭실대학교 대학원 정보통신공학과 박사 과정 〈관심분야〉 VoIP 보안, 보안 프로토콜, 컴퓨터 네트워크

**박 성 준**

1997년 2월 : 숭실대학교 정보통신공학과 학사
1998년~현재 : 숭실대학교 정보통신공학과 석사 과정
〈관심분야〉 VoIP 보안, 보안 프로토콜