임베디드 환경에서의 H.235 기반 VoIP 보안 단말 구현 및 안전성 분석에 관한 연구

정회원 김 덕 우, 홍 기 훈, 이 상 학, 정 수 환*

An implementation and security analysis on H.235 for VoIP security on embedded environments

Deok Wu Kim, Kihun Hong, Sang-hak Lee, Souhwan Jung* *Regular Members*

요 약

본 논문에서는 ITU-T에서 제안한 VoIP 표준인 H.323 시스템의 보안 프로토콜인 H.235에 대하여 연구하고 이를 임베디드 환경의 IP phone에 구현하여 VoIP 보안 프로토콜의 구현 요구사항 및 구현 결과에 따른 분석을 실시하였다. 특히 annex D에서 제안하고 있는 VoIP 단말에서의 보안 기능을 분석하여 구현하였는데, annex D에서는 HMAC-SHA1-96을 이용하여 인증과 무결성을 제공하고 Diffie-Hellman을 이용해서 음성 데이터 암호화에 사용되는 세션 키를 암호화해서 전달하며 음성 데이터의 암호화를 위한 RC2, DES, 3DES 등을 지원하고 있다. 또한 annex D의 안전성 및 상호 연동 문제점을 분석하여 취약점을 발견하고 보안을 강화하는 개선 방안을 제시하였다.

Key Words : VoIP; Security; H.235; Embedded system.

ABSTRACT

In this paper, H.235 based security mechanism for H.323 multimedia applications was implemented in embedded environment. H.235 covers authentication using HMAC-SHA1-96, authenticated Diffie-Hellman key exchange, security capability exchange, session key management for voice encryption, and encryption functions such as DES, 3DES, RC2. H.235-based mechanisms were also analyzed in terms of its security and possible attacks.

Ⅰ. 서 론

컴퓨터 기술의 발전과 인터넷의 보급 확산으로 기존 문자 기반의 인터넷을 벗어나 문자 이외에도 음성, 도형, 영상 등으로 이루어진 다양한 매체를 처리할 수 있는 멀티미디어 인터넷으로 발전해왔다. 새롭게 등장한 멀티미디어 서비스는 전 국가 산업에 큰 영향을 미치고 있으며, 새로운 문화생활의 출현과 새로운 비즈니스를 창출하고 있다. 이러한 멀티미디어 서비스 중 네트워크에서 표준 프로토콜인 IP를 이용해 데이터뿐만 아니라 음성까지 함께 실어 보내는 VoIP 기술은 기존에 전화망을 통해 전송했던 음성 신호를 데이터망을 통해 전송하는 전화 서비스로 기존 유선 전화보다 저렴한 가격과 각종 부가 서비스 지원으로 기업과 사용자로 하여금 많은 기대와 호응을 얻고 있다. 하지만, VoIP 기술은 기존 IP 프로토콜을 기반으로 하고 있는 서비스이므로 IP 네트워크가 가지고 있는 특성을 따라 IP 네트워크의 보안 취약점 역시 가지고 있다. 이로 인해 네트워크 상에서 불법 도청, 비인가자의 불법 전

* 숭실대학교 정보통신전자공학부 통신망보안 연구실
(thenine@cns.ssu.ac.kr, kihun@cns.ssu.ac.kr, lsh815@cns.ssu.ac.kr, souhwanj@ssu.ac.kr)
논문번호 : 030086-0306, 접수일자 : 2003년 4월 22일
※본 연구는 숭실대학교 교내 연구 지원에 의해 수행되었습니다.

화 사용 및 전화 서비스 거부 공격 등이 가능해 이러한 공격에 대한 방어와 안전한 VoIP 서비스를 위해서 보안 시스템을 적용할 필요가 있다.

Ⅱ. H.235 보안 관련 기술

H.235[1]는 ITU-T의 VoIP 프로토콜인 H.323[2]의 보안 표준안을 말한다. H.235에서는 기존 IPsec, TLS 등의 낮은 계층의 보안 프로토콜뿐만 아니라 H.235 보안 시그널링을 통해서도 보안을 지원할 수 있기 때문에 VoIP 보안에 있어서 융통성을 가진다.

다음 표 1은 H.235 annex D에서 제안하고 있는 보안 프로파일(기본 보안 프로파일과 음성 암호화 프로파일)로써 RAS, H.225.0[3], H.245[4] 메시지에 대해 HMAC-SHA1[5]을 사용하여 인증과 무결성을 제공하며 H.225.0 메시지 중 Setup과 Connect 메시지 교환시 Diffie-Hellman 키 교환[6]과 암호 알고리즘이 교환되고 음성 데이터에 대해 비밀성을 제공하기 위해 협상된 암호 알고리즘에 의해 세션 키가 전달되어 RTP 페이로드를 암/복호화한다.

Ⅲ. H.235 기반 IP phone 단말기 구현

본 논문에서는 H.235 annex D에서 제안하고 있는 보안 프로파일을 기반으로 하여 H.323 단말과

표 1. H.235 annex D 보안 프로파일.

보안 서비스	호 기능			
	RAS	H.225.0	H.245	RTP
인증	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	·
부인 방지	·	·	·	·
무결성	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	·
비밀성	·	·	·	DES, RC2, 3DES
접근 제어	·	·	·	·
키 관리	사용자 가입 기반 패스워드	Diffie-Hellman 키 교환	세션 키 교환	·

게이트키퍼간의 RAS, H.323 단말간의 H.225.0 메시지 교환시 인증과 무결성 제공, Diffie-Hellman 키 교환, 세션 키 교환, 보안 능력 교환 및 음성 데이터 암호화를 구현하였다.

1. 시스템 구현 환경

구현 환경은 임베디드 리눅스 환경에서 VoIP 보안 시스템을 구현하기 위하여 ARM7TDMI 프로세서와 uClinux 운영체제로 동작하는 IP phone 단말기를 이용하였고, 개발 환경으로 리눅스 PC에서 uClinux 크로스 컴파일을 사용하여 구현하였으며, 사용되는 암호 알고리즘은 Openssl 프로젝트[7]를 사용해서 구현하였다.

2. 구현 요구사항

본 논문 구현시 필요한 요구사항은 다음과 같다. 현재 ITU-T에서 제안하고 있는 H.235 버전 2를 엄격히 지원해 H.235를 지원하는 게이트키퍼, 단말기간 상호 운용성을 보장해야 하겠다.

H.323 시그널링에 있어서 호 연결간 음성 채널을 빠르게 열기 위해 Setup 메시지에 OpenLogicalChannel 필드를 입력하는 Fast start와 GK-routed 모델을 지원해야 한다. 특히 H.245 메시지에 대해 인증과 무결성을 제공하기 위해 H.245 시그널링시 별도의 H.245 채널을 열지 않고 기존 H.225.0 채널로 터널링하는 방법을 지원해야 한다. 또한 H.235의 국내 표준에 따라 국내 표준의 블럭 암호 알고리즘인 SEED를 지원해야 하겠다.

본 논문에서 사용한 임베디드 시스템은 ARM7TDMI 프로세서 특성상 MMU를 지원하지 않기 때문에 메모리 누수와 같은 메모리 관리 문제를 고려해야 한다. 임베디드 시스템의 계산 능력은 일반 PC의 계산 능력에 미치지 못하지만, H.323 시스템간 RAS, H.225.0 메시지 교환시 사용되는 HMAC-SHA1-96 알고리즘 수행, Diffie-Hellman 키 교환과 음성 데이터 암호화에 사용되는 각종 암호알고리즘을 수행함에 따라 호 연결 지연 및 음성 지연이 발생해서는 안 된다.

3. 구현 내용

3.1 RAS 시그널링

RAS 시그널링에 있어서 보안 메커니즘은 게이트키퍼와 GRQ, GCF 메시지 교환시 xRQ, xCF 메시지의 인증과 무결성에 사용될 보안 방법을 설정하고 설정된 보안 방법으로 xRQ, xCF 메시지에 대해 보안을 적용하는 구조로 되어 있다.

3.1.1 보안 방법 설정

게이트키퍼와의 RAS 메시지 교환시 인증과 무결성 제공을 위한 보안 방법을 먼저 설정해야 한다. 그림 1은 게이트키퍼와 보안 방법을 설정하는 것으로 단말은 GRQ 메시지를 통해 RAS 메시지에 대해 지원하는 보안 방법과 알고리즘을 보내는데, 보안 방법에는 Diffie-Hellman 키 교환을 통한 인증, 사용자 가입 기반 인증 방법으로 대칭 키 암호화, 해시, 서명을 통한 인증 방법이 있다. H.235 annex D에서는 사용자 가입 기반의 해시 인증 방법을 채택하고 있다. 따라서 게이트키퍼는 GCF 메시지를 통해 RAS 메시지의 보안 방법을 결정해서 단말 쪽으로 전송한다. 이로써, GRQ, GCF 메시지 이후의 xRQ, xCF는 선택된 방법으로 보안이 이루어지게 된다.

3.1.2 메시지 인증과 무결성

xRQ, xCF의 보안 방법은 GRQ, GCF에 의해 선택된 보안 방법으로 이루어지는데, H.235 annex D에서는 사용자 가입 기반의 해시 인증 방법을 채택함에 따라 RAS 메시지에 대해 사용자가 입력한 패스워드를 키 값으로 HMAC-SHA1-96을 수행한 인증값으로 메시지 인증과 무결성을 제공한다. 다음 그림 2는 HMAC-SHA1-96 절차이다.

구현에서 송신측 처리는 후킹 함수에서 cryptoHashedToken의 hash 필드에 '0' 비트를 입력하고 인코딩 함수를 통해 메시지를 HMAC-SHA1-96한 후 다시 디코딩 함수를 통해 hash 필드에 입력했다. 또한 수신측 처리 또한 후킹 함수에서 디코딩 함수를 통해 메시지에서 hash 필드를 읽어오고 다시 '0' 비트를 입력한 후 인코딩 함수를 통해 메시지에서 HMAC-SHA1-96을 수행해 나온 결과 값을 비교해 구현하였다. 따라서 디폴트 패턴과 hash 필드 값을 검색하는 절차를 생략할 수 있다.

3.2 H.225.0 시그널링

H.225.0의 시그널링은 메시지에 대한 인증과 무결성 제공, Setup-Connect 메시지 교환시 Diffie-Hellman 키 교환, 보안 능력 교환 및 세션 키 교환을 수행하는 절차로 나눌 수 있는데, 메시지에 대한 인증과 무결성을 제공하는 메커니즘은 RAS 시그널링과 동일하게 사용자 패스워드 기반 HMAC-SHA1-96을 수행한다.

3.2.1 Diffie-Hellman 키 교환

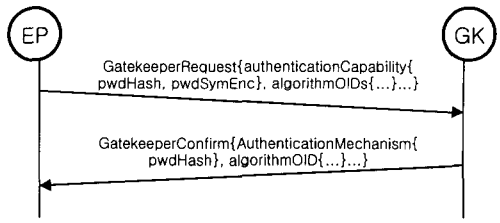


그림 1. RAS 메시지에 대해 보안 방법 설정

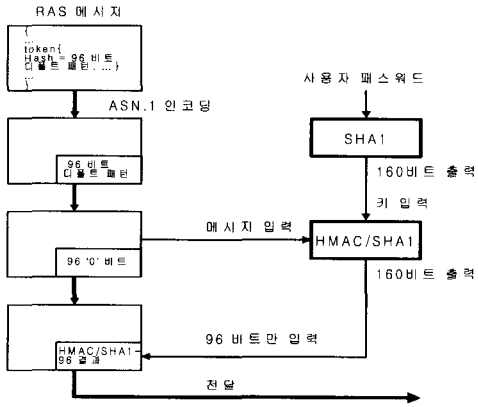


그림 2. RAS 메시지의 HMAC-SHA-96 절차

Diffie-Hellman 키 교환 알고리즘은 두 사용자가 사전에 어떠한 비밀 교환 없이 안전하지 않은 매체상에서 키를 교환하는 알고리즘으로 이산대수 문제를 기반으로 한다.

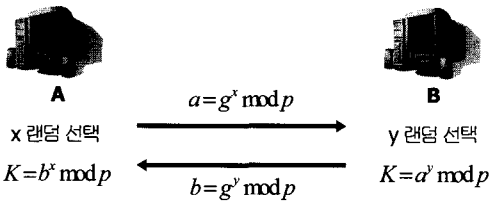


그림 3. Diffie-Hellman 키 교환 절차

그림 3과 같이 Diffie-Hellman 키 교환은 교환된 공개 파라미터(a, b, g, p)와 비밀 파라미터(x, y)의 연산으로 사용자간의 동일한 키를 가지게 되는데, 공격자는 공개 파라미터를 가로챘다고 하더라도 비밀 파라미터를 모르기 때문에 동일한 키(K)를 계산할 수 없게된다.

H.235 annex D에서는 Diffie-Hellman 키 교환에 사용되는 파라미터는 암호화에 사용되는 알고리즘에 따라 분류하고 있는데, RC2, DES인 경우는 적당한

512 비트 소수를 생성해서 사용하고 3DES인 경우는 표준에 정의된 고정 1024 비트 소수를 사용하도록 되어있다.

3.2.2 보안 능력 교환 및 세션 키 교환

보안 능력 협상을 위해 Fast start된 Setup 메시지의 EncryptionCapapbility 필드가 교환되면서 각 단말이 지원하는 보안 능력이 교환된다. 이 때 교환되는 보안 능력은 지원하는 암호 알고리즘이며 세션 키 암호화에 사용되고 음성 데이터 교환시 사용되는 암호화에도 동일하게 사용된다. H.235 표준에서는 RC2, DES, 3DES를 기본으로 하고 있으며 본 논문에서는 H.235 국내 표준을 위해 국내 표준의 블록 암호 알고리즘인 SEED를 추가하였다.

세션 키 교환은 보안 능력 교환시 협상된 암호 알고리즘으로 암호 알고리즘에 맞게 생성된 세션 키를 암호화하는데, 이 때 사용되는 키 값이 Setup-Connect 메시지간에 Diffie-Hellman 키 교환 알고리즘으로 교환된 키이다. 그림 4와 같이 보안 능력은 EncryptionCapability 필드, 세션 키는 h235key 필드, Diffie-Hellman 파라미터는dhkey 필드를 사용해서 교환된다.

3.3 H.245 시그널링

H.235 표준에서 H.245 메시지는 H.225.0 메시지에 터널링되는 것을 가정하고 있는데, 이것은 H.245 메시지의 인증과 무결성을 위한 별도의 보안 필드를 사용하지 않고 기존 H.225.0 메시지의 cryptoHashedToken의 hash 필드를 사용해 HMAC-SHA1-96으로 H.245 메시지의 인증과 무결성을 제공한다.

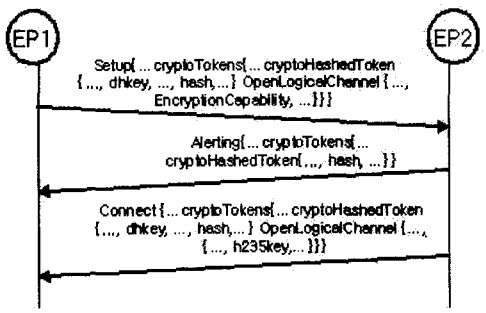


그림 4. 세션 키 생성 및 교환

3.4 음성 데이터 암호화

음성 데이터 암호화는 그림 5와 같이 RTP 패킷의 페이로드를 대상으로 암호화를 수행하는데, 암호화는 음성 코덱을 거쳐 인코딩된 음성 데이터 프레임을 RTP 패킷에 입력할 때 수행되기 때문에 RTP 패킷 생성단에서 음성 코덱의 종류와 무관하게 암호화를 구현할 수 있다. 이 때 블럭 단위의 암호화로 추가적인 패딩이 필요하다. 수신단에서는 수신한 RTP 페이로드를 복호화하여 패딩을 제거한 후 음성 코덱의 디코딩 과정을 수행한다.

Ⅳ. H.235v2 annex D 분석

H.235v2 annex D 기반으로 구현된 IP phone을 다음과 같이 분석하고 해결 방안을 제시하였다. 먼저 안전성은 H.235v2 annex D가 가지는 취약성에 대해 분석하였으며, IP phone에 보안 기능 추가로 인해 발생하는 각종 지연 및 오버헤드를 측정, 분석하였다. 마지막으로 기타에서는 다른 보안 프로토콜과 비교해서 가지는 문제점을 분석하였다.

1. 안전성

1.1 Diffie-Hellman 키 교환

1.1.1 취약한 Diffie-Hellman 파라미터 사용

Diffie-Hellman 키 교환 알고리즘에서 취약한 파라미터를 생성, 교환하게 되면 쉽게 공개 파라미터로부터 비밀 파라미터를 계산하여 공유된 키를 알아낼 수 있는데, 표준에 있어서 교환된 알고리즘이 RC2, DES일 경우, 통신하고자 하는 단말은 랜덤한 512 비트 소수를 생성한다. 이때 취약한 소수가 발생할 수 있다. 따라서, 생성된 소수가 안전한지 확인할 수 있는 Diffie-Hellman 파라미터 확인 함수를 사용해서 안전성을 개선할 수 있다.

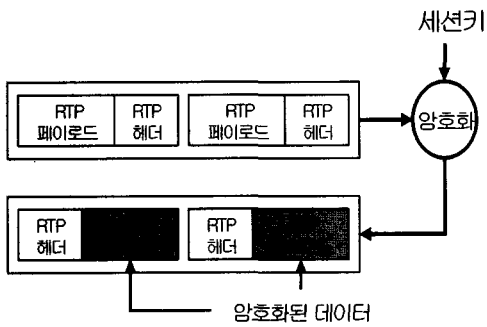


그림 5. 음성 데이터 암호화

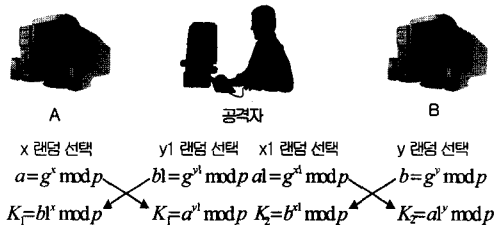


그림 6. Man-in-the-middle attack

1.1.2 Man-in-the-middle attack

Diffie-Hellman 키 교환 알고리즘에는 교환하고자 하는 통신 단말 사이에서 파라미터를 가로채는 공격 방법이 있다. 그림 6에서 공격자는 통신 단말 A, B 사이에 위치해서 A, B가 교환하는 공개 파라미터(a, b, g, p)를 가로챈 후 공격자가 생성한 공개 파라미터(a1, b1, g, p)를 전송해서 A, B간의 키(K1, K2)를 알아낼 수 있다.

H.235 표준에서는 Diffie-Hellman 키 교환 알고리즘을 그대로 사용한 것이 아니라, Authenticated Diffie-Hellman 키 교환 알고리즘으로 두 단말이 Diffie-Hellman 파라미터를 생성한 후 생성한 파라미터에 대해 인증 값을 계산해, 파라미터와 같이 전송함으로써 공격자가 파라미터를 수정하는 man-in-the-middle attack에 안전하다. 이때 사용되는 인증 알고리즘이 HMAC-SHA1-96이다.

1.2 세션 키 전송

세션 키 전송은 협상된 암호 알고리즘에 의해 Connect 메시지의 h235Key의 sharedSecret 필드를 사용해서 전달되는데, 이 sharedSecret 필드는 KeySyncMaterial 필드를 암호화해서 입력한다. KeySyncMaterial 필드는 다음 표 2와 같다.

KeySyncMaterial 필드에서 genereallD 필드는 Connect 메시지를 보내는 사람(callee)의 H.323 ID가 입력되는데, 이 H.323 ID는 공개된 정보이며 평문으로 전송되므로 KeySyncMaterial 필드의 세션 키 정보와 같이 암호화되어 known-plaintext attack에 취약하게 된다. H.235v2 표준에서 이렇게 정의함에 따라, H.235v2에서는 개선할 수 없으며 현재 진행중인 H.235v3 draft에는 V3KeySyncMaterial 필드를 사용하여 개선하였다. V3KeySyncMaterial 필드는 다음 표 3과 같다.

1.3 세션 키, RTP 암/복호화

1.3.1 취약 키, 취약 IV 발생

표 2. KeySyncMaterial 필드

```
KeySyncMaterial ::= SEQUENCE
{
   generalID    Identifier,
   keyMaterial    KeyMaterial,
   ...
}
```

표 3. V3KeySyncMaterial 필드

```
V3KeySyncMaterial   ::= SEQUENCE
{
   generalID    Identifier, -- peer terminal ID
   algorithmOID    OBJECT IDENTIFIER,
                   -- encryption algorithm
   paramS    Params, -- IV
   encryptedSessionKey    OCTET STRING,
                   -- encrypted session key
   encryptedSaltingKey    OCTET STRING OPTIONAL,
                   -- encrypted salting key
   ...
}
```

H.235v2에서 사용하는 암호 알고리즘 중 DES는 취약 키와 취약 IV가 존재함으로, 안전성에 문제가 있다. 따라서 DES 키와 IV를 생성할 때, 취약 키와 취약 IV인지 확인하는 함수를 사용해서 개선할 수 있다.

1.3.2 키 길이 제한

DES 암호 알고리즘은 제한된 키 길이(56 비트)로 brute-force attack에 취약하다. 따라서, 안전성을 갖는 암호 알고리즘의 사용이 요구된다. 참고로, H.235v3 draft에서는 AES 암호 알고리즘이 추가되었다.

1.4 패스워드

H.235v2 annex D에서 사용되는 패스워드는 사용자 가입 기반의 패스워드이나 구현상 H.323 ID를 사용한다. H.323 ID는 공개된 정보이며 평문으로 전송되므로, LAN 상에서 쉽게 스니퍼링 될 수 있다. 따라서, 안전성을 강화하기 위해서는 엄격하게 표준을 따라야 한다.

2. 오버 헤드

2.1 Diffie-Hellman 키 교환

Diffie-Hellman 키 교환 알고리즘은 512 비트 또는 1024 비트의 매우 큰 수를 사용해서, 구현 환경에 따라서 Diffie-Hellman 키 교환 시그널링시(Setup, Connect 메시지) 큰 지연을 발생시킬 수 있다. 따라서, 구현 환경에 맞게 Diffie-Hellman 파리

표 4. 연결에 필요한 시간(ARQ ~ 첫 RTP)

구분	OpenGK			시스코 GK			AnyuserNet GK		
	보안 통화		일반 통화	보안 통화		일반 통화	보안 통화		일반 통화
	DES	3DES		DES	3DES		DES	3DES	
측정 1	2.036	2.768	1.333	2.181	2.825	1.36	2.11	2.933	1.251
측정 2	1.854	2.832	1.158	1.928	2.608	1.207	2.023	2.723	1.189
측정 3	1.890	2.620	1.321	2.155	2.786	1.236	1.991	2.657	1.039
평균 시간(초)	1.93	2.74	1.27	2.09	2.74	1.27	2.04	2.77	1.16

표 5. 암호 알고리즘 수행 속도 (RTP 페이로드 생성 속도 : 24B/초)

구 분	RC2		DES		3DES		SEED	
	암호화	복호화	암호화	복호화	암호화	복호화	암호화	복호화
측정 1	301	256	208	213	73	71	132	134
측정 2	301	256	208	213	73	71	132	134
측정 3	301	256	208	217	73	71	132	134
평 균 처리량 (KB/초)	301	256	208	214	73	71	132	134

미터 크기를 수정해 지연 정도를 수정할 수 있다. 위 표 4는 연결에 필요한 시간을 측정한 것으로, 보안 적용시 약 0.7 ~ 1.6초 정도 추가 지연이 발생하였으며 지연에 영향을 준 요소는 Diffie-Hellam 키 교환이다.

2.2 RTP 암/복호화

미디어 데이터에 비밀성을 보장하기 위해 RTP 페이로드를 대상으로 암/복호화가 수행되는데, 이 암/복호화로 인해 RTP 전송 지연이 발생할 수도 있다. 하지만, 표 5와 같이 암호 알고리즘의 암호화 수행 속도가 RTP 페이로드 생성 속도보다 높으므로 테스트간 지연이 발생하지 않았다.

2.3 보안 시그널링

H.225.0의 보안 시그널링은 메시지에 대한 인증과 무결성 제공, Setup-Connect 메시지 교환시 Diffie-Hellman 키 교환, 보안 능력 교환 및 세션 키 교환을 수행하는 절차로 나눌 수 있는데, 이 절차를 수행하면서 증가된 메시지 크기는 표 6과 같다. 보안 기능 지원으로 인해 메시지는 일반 통화 메시지에 비해 2.49 ~ 3.77 배로 증가됨을 볼 수 있다.

표 6. 메시지 크기(Setup ~ ReleaseComplete)

구분	OpenGK			시스코 GK			AnyuserNet GK		
	보안 통화		일반 통화	보안 통화		일반 통화	보안 통화		일반 통화
	DES	3DES		DES	3DES		DES	3DES	
메시지 크기 (B)	3998	4414	1169	3840	4459	1216	2406	2822	963
증가율	3.42	3.77	·	3.15	3.66	·	2.49	2.93	·

3. 기타

3.1 보안 서비스

H.235 annex D에서는 보안 서비스 중에서 부인방지(Non-repudiation)를 지원하지 않는데 비해, H.235 annex E Signature Profile은 부인 방지 서비스를 제공할 수 있다.

3.2 게이트키퍼간 키 공유

H.235 annex D는 게이트키퍼간 키 공유가 필요한데, 다음 그림과 같이 n개의 게이트키퍼간 $\frac{n(n-1)}{2}$ 개의 키가 필요하다. 그림 7에서는 4개의 게이트키퍼가 존재하기 때문에 게이트키퍼간 필요한 키는 총 6개이다.

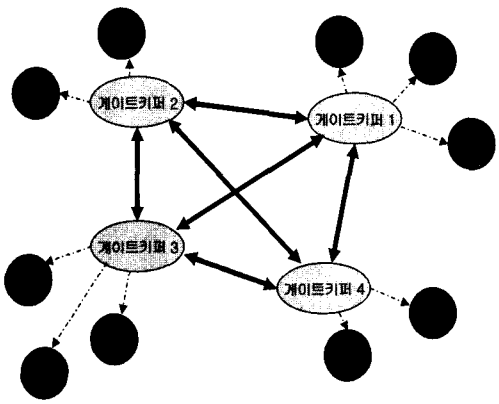


그림 7. 게이트키퍼간 공유

표 7. 에러 코드

에러 코드	내 용
securityWrongSyncTime	잘못된 time stamp
securityReplay	같은 sequence number
securityWrongGeneralID	generalID 불일치
securityWrongSendersID	sendersID 불일치
securityMessage IntegrityFailed	무결성 확인 실패
securityWrongOID	OID 불일치

3.3 에러 시그널링

H.235에서는 2개의 에러 코드가 존재하는데, 단말이 보안 능력 교환 실패나 보안 확인이 실패하면, 단말이 ReleaseComplete 메시지에 SecurityDenied로 응답하며 게이트키퍼간 보안 능력 교환이 실패하면, 게이트키퍼가 RAS 메시지에 securityDenial로 응답한다. 이에 비해, H.235v3 draft에는 표 7과 같이 6개의 에러 코드가 추가되어, 단말에게 정확한 보안 실패 원인을 제공한다.

3.4 NAT/방화벽 통과

H.235 기능이 있는 단말이 NAT/방화벽을 통과해 시그널링이 이루어질 경우, 시그널링 메시지 중 IP 주소와 포트 번호가 변경되므로 보안 시그널링을 수행할 수 없다. H.235v3 draft에서는 Authentication-only 방식을 추가하여 ClearToken만 인증을 실시하여, IP 주소와 포트 번호가 변경되더라도 보안 시그널링이 가능하다. 하지만, 이 방식은 제한적인 인증만 제공한다.

V. 결 론

본 논문에서는 ITU-T에서 제안하는 VoIP 표준 프로토콜인 H.323 시스템의 보안 프로토콜인 H.235에 사용되는 보안 알고리즘을 분석하고 임베디드 환경에서 구현하였으며, H.235 보안 프로토콜이 가지는 안전성에 대해서 분석하였다.

구현상의 어려움으로는 상용 게이트키퍼가 H.235 보안 표준을 따르지 않고 각 회사 별로 별도의 RAS 보안 메커니즘이 존재해 상호 운용성에 문제가 발생하였다. 이에 RAS 시그널링에 여러 가지 경우를 만들어 상호 운용성을 보장하였으나 상용 게이트키퍼에 대한 지속적인 기술 분석과 표준화 동향 분석으로 상호 운용성을 높여 나가야 할 것이다.

H.235 보안 프로토콜에 대한 안전성 측면을 보면, RTP 미디어 암호화를 위한 키 교환에 있어 Diffie-Hellman 키 교환 알고리즘을 수행하지만, Authenticated Diffie-Hellman 키 교환을 수행함으로 man-in-the-middle attack에 안전하다. 또한 취약한 Diffie-Hellman 파라미터를 생성하더라도 파라미터 확인 함수를 통해, 안전성을 개선할 수 있다. KeySyncMaterial 필드를 이용한 세션 키 전송은 공개된 정보와 세션 키를 같이 암호화해 known-plaintext attack의 취약점을 가지므로, 향후 개선 방향에 대한 추가적인 연구가 필요하다. 세션 키 및 RTP 미디어 암호화에 사용되는 암호 알고리즘에서는 DES 암호 알고리즘이 brute-force attack에 취약한 특성을 갖는다. 따라서 향후 적용하는 알고리즘은 3DES 이상의 안전성을 갖는 알고리즘의 사용이 권장되며 새로 개발된 AES 암호 알고리즘의 표준 적용이 요구된다. 또한, 보안 적용으로 인해 시그널링 시간과 메시지 크기가 증가하였는데, 이는 기존 서비스에 대해 추가적인 보안 적용으로 발생하였다. 하지만, 임베디드 환경 특성상 프로세서 성능이 일반 PC에 비해 낮으므로 메시지 증가 등을 발생시키지 않는 알고리즘 도입 등이 요구된다.

참 고 문 헌

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

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

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

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

[5] RFC 2104, "HMAC: Keyed-Hashing for Message Authentication", IETF, 1997.

[6] RFC 2631, "Diffie-Hellman Key Agreement Method," IETF, 1993.

[7] Openssl 프로젝트, http://www.openssl.org.

김 덕 우 (Deok Wu Kim) 정회원

1999년: 숭실대학교 정보통신공학과 학사
2003년: 숭실대학교 정보통신공학과 공학석사
2003년 ~ 현재: ㈜쏠리테크 연구원

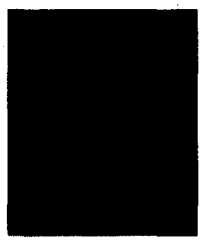
<관심분야> VoIP Security, 네트워크 인증, 무선랜

홍 기 훈 (Kihun Hong) 정회원

2000년 2월: 숭실대학교 정보통신공학과 학사
2002년 2월: 숭실대학교 정보통신공학과 석사
2002년 3월~현재: 숭실대학교 정보통신공학과 박사과정

<관심분야> VoIP 보안, 모바일 보안, 멀티캐스트 보안, IPsec.

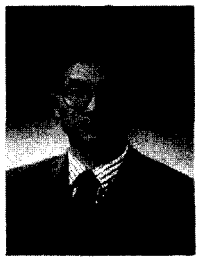
이 상 학 (Sang-hak Lee) 정회원



2002년 2월 : 숭실대학교 정보통신공학과 졸업
2004년 2월 : 숭실대학교 정보통신공학과 석사
2004년 1월~현재 : 시큐아이 닷컴 유넷사업부 PKI팀

<관심분야> PKI, VoIP보안, IDS

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> 모바일 인터넷 보안, NEMO Security, VoIP 보안.