H.235 기반 VoIP 보안 시스템 구현

임범진*, 홍기훈*, 정수환*

*숭실대학교, 정보통신 전자공학부

Implementation of Secure VoIP System based on H.235

Bumjin Im*, Kihun Hong*, Souhwan Jung*

*School of Electronics Engineering, Soongsil Univ.

요 약

인터넷 서비스와 함께 발달한 멀티미디어 서비스 중 각광받고 있는 VoIP 서비스는 유선 전화보다 저렴한 가격을 바탕으로 하여 호황을 누리고 있다. 그러나 인터넷을 전송망으로 이용하는 VoIP는 개인의 암호화되지 않은 음성데이터의 도청이 쉽게 이루어질 수 있을 뿐만 아니라 사용자 및 서비스 업자에 대한 인증 방법.부재로 인한 불법 이용이 예상되는 등 보안적 문제점을 가지고 있다. 그에 따른 VoIP 서비스의 보안 요구사항은 계속 증가하고 있으며 이에 대한 연구 노력이 시급하다.

본 논문에서는 ITU에서 제안한 H.323 VoIP의 보안 프로토콜인 H.235에 대하여 연구하고 이를 구현한 VoIP 보안 시스템을 구축하여 VoIP 보안 프로토콜의 요구 사항 및 방향을 제시하였다.

I. 서론

정보통신 기술이 발전함에 따라 인터넷 응용 기술을 생활에 접목하고 기존에 사용하고 있는 통신방식을 인터넷에 응용하고자 하는 노력들이 진행되어 왔다. 그 노력의 일환으로 이루어진 VoIP 또한 인터넷 데이터 전송속도가 빨라지고 사용료가 저렴하여 이용자의 수도 늘어나고 있으며 향후에는 공중 전화망(PSTN)의 가입자 수를 능가할 것으로 기대되고 있다. 그러나 현재의 VoIP 기술은 공중 전화망의 서비스에 비추어 볼 때 서비스의 다양성과 서비스 품질이 공중전화망에 미치지 못하는 것이 사실이다. 하지만 계속되는 인터넷 기술의 발전과 VoIP 기술 표준화 노력으로 인하여 서비스 품질의 만족과, 일반 전화망에서 서비스되고 있는 호 전환 등의 서비스 다양화에 대한 노력이 기울여지고 있어서 VoIP 기술의 발전 속도는 점차 가속화 될 것으로 예상된다.

VoIP는 유선전화망과는 달리 인터넷을 기반으로 이루어지고 있는 서비스이다. 따라서 IP 네트워크가 가지고 있는 특징을 그대로 따른다. IP 네트워크의 취약점 중 하나인 보안의 취약성을 VoIP도 가지고 있기 때문에 VoIP는 보안을 위한 고려가 필요하다. 공중전화망보다 발전된 형태의 보안을 제공하려면 데이터의 기밀성과 사용자 인증, 데이터의 무결성 등을 보장해야 하며 기존 VoIP와의 호환성도 유지해야 하고 합법적인 감청(Lawful Interception)도 지원해야 할 것이다.

현재 ITU, IETF, ETSI 등의 통신 표준화 기구에서는 VoIP의 보안 표준화를 서두르고 있으며 VoIP 서비스 업체에서도 속속 보안을 적용한 VoIP 솔루션을 선보이고 있으며 관련 연구를 진행중에 있다.

본 논문에서는 제 I장 서론에 이어 제 II장에서는 VoIP 보안 표준안 중 ITU에서 제안하고 본 논문에서 다루어질 H.235에 대해 서술하고, III장 구현에서는 본 논문에서 중점적으로 다루어지는 H.323 시스템의 보안 표준안인 H.235를 분석, 구현하여 실험한 결과에 대하여 서술하며 제 IV장에서는 구현 및 연구 결과 및 결론을 서술한다.

II. VoIP 보안 관련 기술

1. H.235

H.235[1]는 ITU의 VoIP 표준안인 H.323[2]의 보안 표준안을 말한다. ITU에서는 VoIP만을 위한 보안 표준안을 제안한 것으로 IPSec, TLS 등의 낮은 계층의 프로토콜에 대한 보안을 정의한 기존의 보안 프로토콜과는 달리 VoIP 만을 위한 보안 프로토콜이라는 특징이 있기 때문에 VoIP에 최적화 되어 있다고 할 수 있다.

H.235는 H.225.0[3]의 RAS(Registration, Admission, and Status)에 대한 보안, 호 처리에 대한 보안 및 세션 키의 생성, H.245[4]에서의 security capability 교환, 그리고 음성 데이터의 보안인 미디어 암호화 부분으로 구성되어 있고, 덧붙여진 부록에서는 ASN.1 메시지 정의 및 네트워크의 기반 구성을 다룬 baseline security, 제 3 자 인증을 통한 방법을 제안한 signature security profile, 그리고 무선 VoIP 보안을 위한 security for mobile H.323 system으로 이루어져 있다.

H.235는 먼저 RAS 메시지를 통하여 게이트키퍼와의 인증 과정을 정의하고 있고, 호 설정 시 상대방과의 인증 과정을 포함하며 이 때 세션 키의 암호화 교환을 위한 Diffie-Hellman[7] 키를 교환하고 호 설정 후 H.245 메시지에서는 capability 교환과 같은 양식으로 security capability 교환을 실시한다. 음성 채널을 생성할 때, 이미 교환된 capability 중 한가지를 선택하여 음성 데이터의 암호화 알고리즘으로 이용하고, 동시에 호 설정 시 교환되었던 Diffie-Hellman 키를 이용하여 마스터가 생성한 세션 키를 암호화하여 전송한다.

H.235 Annex D인 Baseline security[5]는 일반적인 H.323 네트워크에서의 보안 적용에 대한 내용을 다루고 있으며 H.225.0 RAS, 호 설정, H.245 capability에 대한 교환 및 media encryption에 대한 보안으로 이루어져 있고 구성 가능한 네트워크의 구성도 다루고 있다. Baseline security는 H.235가 수행되어야 할 가장 기본적이고 필수적인 부분을 다루고 있으며 SET(Simple Endpoint Type)에서의 보안에 대한 기본 방향을 제시하고 있다.

H.235 Annex.E인 Signature profile[6]은 전자서명을 이용한 VoIP 보안방법으로 이를 이용하여 보다 스케일이 큰 광범위(global) VoIP 서비스 구축을 위해서 반드시 필요한 부분이다. 이 부분을 위해서는 반드시 게이트키퍼 routed 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 timestamp와 sequence number를 이용해서 replay 공격을 막을 수 있고, 인증을 통하여 신분 위장 및 연결 탈취(session hijacking) 등을 막을 수 있는 장점을 갖는다.

III. H.235 기반 VoIP 보안 시스템 구현

본 논문에서는 annex D[5]에서 권고하고 있는 보안 사항과 SASET(Secure Audio Simple Endpoint Type)[8]에서 권고하는 단말을 구현하여 실험하였으며 H.235에서 사용하는 보안 알고리즘을 구현, 실험하였다. 결과적으로 단말의 인증, 보안 능력(capability) 교환, 키 분배 및 음성 데이터의 암호화를 구현하였다.

1. 시스템 구현환경

본 논문에서는 VoIP 보안 시스템을 구현하기 위하여 Windows 2000을 운영체제로 하는 Pentium II 시스템을 이용하여 MS Visual C++ 6.0으로 컴파일하여 구현하였으며 네트워크는 일반적인 IP 네트워크를 이용하였고, VoIP의 소스는 openh323.org[10]의 openh323 프로젝트의 공개 소스를 이용하였다. openh323은 리눅스와 윈도우 운영체제를 지원하는 프로그램이다. OpenH323 프로젝트는 ITU의 H.323 프로토콜을 기반으로 구현하였고 음성전화, 화상회의 등을 구현하는 프로젝트로 ohphone은 음성 통신을 IP 네트워크에 적용하도록 구성한 프로그램이다. 본 프로그램은 TCP 1720번 포트로 대기하며 연결 요청이 들어오면 UD와 RTP를 이용하여 쌍방향(Full Duplex)으로 통신하는 구조이며 GSM, G.711, G.729 등의 음성 코덱을 지원한다.

2. 구현 내용 및 동작 시험

1) H.225.0 호 설정 메시지 인증 및 Diffie- Hellman 키 교환

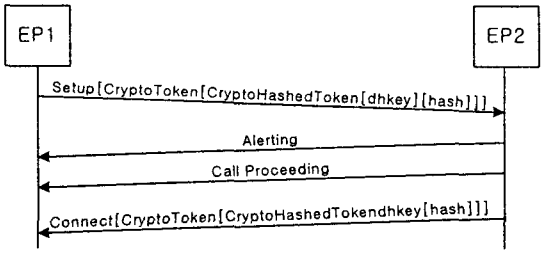

그림 1: H.225.0에서의 보안 메시지

그림 1과 같이 H.225.0에서는 호 설정과 함께 해당 메시지의 인증과 H.245 세션 키 교환을 위한 Diffie-Hellman[7] 키 교환을 수행한다. Caller 측에서 Setup 메시지의 hash 필드에 인증 메시지를 삽입하고 dhkey에 Diffie-Hellman 정보를 삽입하여 전송하면 callee는 전송 받은 메시지에서 hash 필드를 이용하여 인증 여부를 확인하고 dhkey 값을 이용하여 키를 생성한 후 Connect 메시지에 자신의 인증값과 Diffie-Hellman 정보를 삽입하여 전송한다.

H.225.0 메시지 인증 알고리즘은 패스워드 기반의 HMAC-SHA1-96[10]을 이용한다. HMAC-SHA1-96은 패스워드를 키로 이용하는 해쉬 함수로 역함수가 존재하지 않으며 비교적 간단한 알고리즘이므로 고속으로 처리가 가능할 뿐 아니라 보안성 또한 높은 편으로 일반적인 인증 알고리즘으로 널리 사용된다. HMAC-SHA1은 160 비트의 출력이 나오는데 이 중 왼쪽 96비트를 사용하게 된다. H.235에서는 패스워드를 SHA1을 수행하여 나온 값을 64byte로 패딩하여 HMAC의 키로 사용한다.

H.235 annex D에서는 메시지 인코딩 전 인증 코드 부분의 96비트를 임의의 비트 패턴을 삽입하여 인코딩한 후 인코딩된 메시지에서 96비트를 찾아서 해당 부분을 0으로 대체하고 HMAC을 이용하여 인증 메시지를 만들어 0으로 대체한 부분에 생성된 데이터를 대체하도록 하고 있으며 임의의 96비트 패턴은 한 메시지에 두 번 이상 나오지 않도록 적합하게 설정해야 한다. 그러나 96비트의 임의의 패턴이 메시지의 특정 96비트와 일치할 확률은 거의 없기 때문에 구현상 문제로 발생되기는 힘들다.

메시지를 받은 수신단에서는 디코딩 전 인코딩된 메시지를 복사한 후 디코딩한 메시지에서 hash 필드를 해석한 후 hash 필드의 내용과 일치하는 부분을 인코딩된 메시지에서 찾아 그 부분을 0으로 대체한 후 HMAC을 수행시켜 값을 비교한다. 만약 인증 데이터의 비트 패턴과 같은 데이터가 2개 이상 발견되면 위와 같은 방법을 여러 번 반복하여 인증 여부를 검사한다.

H.235에서는 음성 데이터 암호화 키 교환에 사용하기 위하여 그림 1에서의 dhkey를 이용하여 Diffie-Hellman 키 교환을 수행한다. 이 과정에서 생성되는 키로 음성 데이터의 암호화에 필요한 키를 암호화하여 전송하며 이 과정은 H.245에서 이루어진다. 이 때 H.225.0 메시지는 HMAC에 의하여 인증이 이루어지기 때문에 Diffie-Hellman의 약점인 man-in-the-midle 공격을 방지할 수 있다. H.235에서는 Diffie-Hellman에 사용될 512bit의 p(prime number)는 임의의 수를 선택하도록 되어 있으며 g(generator)는 2로 고정시켜 놓았고 3DES 키를 위한 키 생성 시에는 1024bit는 표준안으로 정해진 p를 쓰도록 하고 있다.

2) H.245 Security Capability Exchange

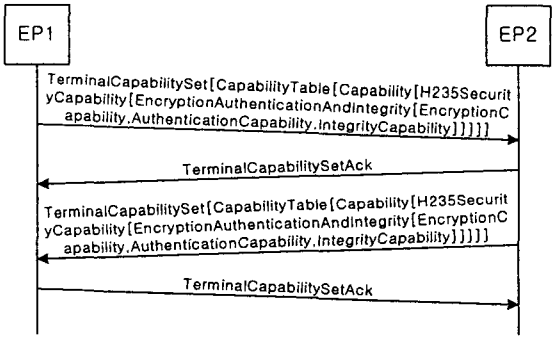

그림 2: H.245 보안 capability 교환 메시지

H.245에서는 음성 데이터의 암호화에 사용될 암호화 알고리즘의 단말 지원 여부(capability)를 그림 2와 같이 교환한다. H.235 security capability는 H.323에서 교환하는 audio, video capability 등과 같은 방법으로 전송되고 같은 방법으로 처리된다.

본 논문에서는 H.235 annex D에서 권장하고 있는 DES, 3DES 외에 다른 암호화 알고리즘의 추가가 용이하도록 구현하였으며 한국형 암호화 알

고리즘인 SEED[11]와 DES를 이을 차기 암호화 알고리즘인 AES[12]를 추가하였다. 이들 알고리즘은 모두 H.235 표준안에 정의되어 있지 않기 때문에 nonStandard로 정의하였다.

3) 암호화 키 생성

Capability 교환 후 H.245 에서는 master slave determination 과정을 거치게 된다. 이 과정을 거치고 나면 마스터로 결정된 단말이 음성 데이터 암호화에 쓰일 키를 생성하게 된다. 이 때 생성되는 random bit 키의 크기는 DES 64bit, 3DES 192bit, SEED 128bit, AES 128bit이다.

4) 보안 알고리즘 설정 및 암호화 키 교환

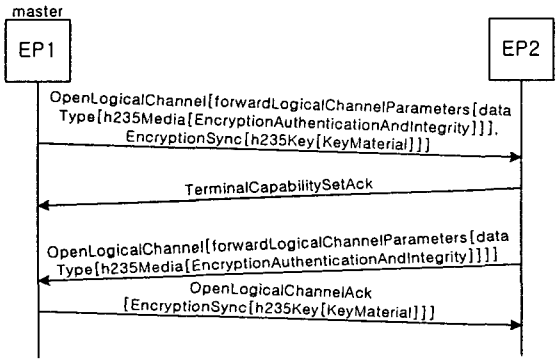

그림 3: OpenLogicalChannel 보안 메시지

일반적으로 H.323에서는 송수신의 음성 코덱을 다르게 사용할 수 있도록 정의되어 있다. 이것은 양 단말이 사용하는 음성 코덱이 다를 경우를 대비한 것인데 암호화라는 점에서는 이에 대한 분석이 필요하다. H.235에서는 마스터가 암호화에 사용될 키를 슬레이브에게 전달하도록 되어 있는데 이는 두 단말이 같은 암호화 알고리즘을 사용한다는 것을 의미할 수 있고, 일반적인 보안 프로토콜의 암호화 시 양단간 같은 알고리즘을 사용한다. 이러한 특성에 따라 본 구현에서는 보안 capability를 교환한 후 마스터의 우선 순위를 적용한 암호화 알고리즘을 선택하도록 하였다. 이러한 구현상 고려는 표준안에는 명시되어 있지 않기 때문에 다른 H.235 기반 VoIP 보안 시스템과의 상호 연동시 문제가 발생할 수 있다.

이와 동시에 EncryptionSync를 통하여 음성 데이터 암호화에 이용될 키를 Diffie-Hellman 키를 이용하여 암호화하여 전송하게 되는데 이 때 사용하는 알고리즘은 모두 CBC(Cipher Block Chaining)모드를 사용하며 이를 위해 IV(Initiation Vector)를 함께 전송해야 하며 이 때 전송된 IV는 음성 데이터의 암호화에도 사용된다.

5) 음성 데이터 암호화

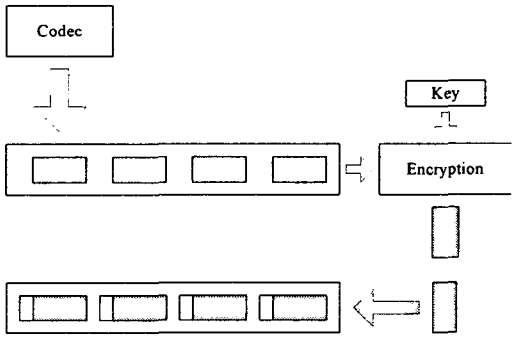

그림 4: 음성 암호화 동작 원리

음성 암호화는 그림 4와 같이 RTP 패킷의 헤더는 제외하고 RTP payload만을 암호화하게 된다. payload만을 암호화하게 되면 헤더까지 암호화하지 않으므로 암호화 지연을 줄일 수 있으며 수신이 잘못되거나 시간이 지난 RTP 패킷을 헤더 정보만을 해석함으로써 복호화하지 않고 바로 삭제할 수 있기 때문에 CPU 자원의 낭비를 막을 수 있는 장점을 갖고 있다.

암호화는 음성 코덱을 거쳐 인코딩된 음성 데이터 프레임을 RTP 패킷에 삽입할 때 이루어지기 때문에 RTP 패킷 생성단에 암호화 모듈을 삽입하는 작업으로 구현할 수 있기 때문에 음성 코덱의 종류에 무관하게 구현할 수 있고 이 때 블록 단위의 암호화로 인한 패딩을 실시한 후 RTP 패킷에 실어서 전송하도록 해야 한다. 수신단에서는 수신한 RTP 패킷의 payload를 복호화하여 패딩 데이터를 제거한 후 음성 코덱의 디코딩 과정을 수행시킨다.

6) 동작 시험 및 고려 사항

실험 결과 구현된 모든 기능은 정상 동작하였으며 표준안에서 원하는 동작을 모두 수행하였다. 본 논문에서는 DES, 3DES, SEED, AES의 암호화 알고리즘과 GSM 음성 코덱을 이용하여 실험

하였고, 암호화는 CBC 모드를 이용하였다.

실험 결과 보안을 적용하지 않은 H.323 시스템과 비교하였을 때 투명하게 동작하였으며 구현상의 문제점은 발생하지 않았다.

암 복호화 연산 지연에 대한 분석을 통하여 본 논문에서 구현한 VoIP 보안 시스템의 성능을 측정한 결과 Pentium III 이상의 PC에서의 성능 저하는 거의 발견되지 않았으며 통화 품질 또한 저하되는 현상을 발견할 수 없었다. 그러나 H.245 메시지 교환 시 Security Capability의 삽입에 의하여 크기가 커진 것을 확인할 수 있었으나 해당 메시지 패킷의 크기가 500바이트보다 작기 때문에 패킷의 조각화(fragmentation) 염려는 없었다.

본 구현의 결과에서 고려할 사항은 상호 동작성(Interoperability)이다. 즉, 표준에는 명시되어 있지 않는 사항에 대한 접근을 주관적으로 하였기 때문에 발생할 수 있는 문제점에 대한 고려가 필요하다.

예를 들어 보안 capability 교환 시 보안 알고리즘의 nonStandard 교환은 상호 운영에서의 걸림돌로 작용할 수 있다. 표준에서는 DES, RC2, 3DES를 지원하도록 권고하고 있지만 해당 알고리즘에 대한 메시지는 정의하고 있지 않기 때문에 nonStandard로 정의해서 사용하였다. 이는 여타 H.235 기반 VoIP 보안 시스템과 상호 운용이 불가능할 수도 있음을 보여주고 있으며 이에 대한 표준화 동향 및 개발자 동향을 파악할 필요가 있다.

IV 결론

본 논문에서는 ITU에서 제안하는 VoIP인 H.323 시스템의 보안 프로토콜인 H.235를 구현하고 실험하여 문제점을 분석하는 연구를 진행하였다. H.235 보안 프로토콜 및 알고리즘을 분석하고 H.235 annex D에서 제안하는 보안 기능들에 대한 동작 실험을 완료하였으며 동작 결과를 도출하고 문제점을 분석하였다.

표준안에서 정의하고 있는 보안 기능들에 대한 구현은 openh323.org의 공개 프로젝트에 구현할 수 있었으며 정상적인 기능 수행을 확인할 수 있었고 HMAC을 이용한 H.225.0 메시지 인증, Diffie-Hellman 키 교환 알고리즘에 의한 키 생성, 보안 capability 교환, 음성 암호화키 생성 및 교환에 대한 구현단계까지의 자세한 사항을 분석하고 구현하였으며 구현 후 성능과 데이터 전송량에 대한 분석을 실시하였다.

본 논문에서 구현한 VoIP 보안 시스템은 상호 동작성(Interoperability)에 대한 테스트가 이루어지지 않아 계속적인 개발자 및 표준화 동향 분석이 이루어져야 할 것이다. 또한 H.235에서 선택적으로 지원할 수 있도록 정의한 media anti spamming에 대한 연구 및 구현이 선행되어야 한다. 이와 함께 H.235의 프로토콜 측면에서의 보안 취약점 및 단점 등에 대한 연구 또한 수행되어야 할 것이다.

참고문헌

[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 Multimedia Communication," ITU-T, 2000

[5] H.235 v2 Annex.D, "Baseline Security Profile," ITU-T, 2000

[6] H.235 v2 Annex.E, "Signature Security Profile," ITU-T, 2000

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

[8] H.323 Annex.J, "Security for H.323 Annex.F(SASET)," ITU-T, 2000

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

[10] http://www.openh323.org "OpenH323 Project"

[11] TTAS.KO-12.0004 , "128비트 블록암호알고리즘 표준(SEED)," 한국정보통신기술협회, 1999

[12] Joan Daemen, Vincent Rijmen, "AES Proposal: Rijndeal," NIST, 1999