H.323 VoIP보안을 위한 H.235 보안기술 현황 및 구현☆

황 선 철*

◈ 목 차 ◈

1. 서 론

1세기 이상 지켜오던 아날로그 전화의 자리를 패킷 데이터를 이용한 인터넷 전화에게 넘겨주는 단계에 이르렀다. 편리함에도 불구하고 음성의 연속성이 보장되지 못하였던 패킷망의 특성적 한계점을 극복할 수 있게 해준 RTP (Real-time Transport Protocol)기술의 발전과 초고속 통신망의 등장으로 이제는 인터넷에서 음성 통화가 가능하게 되었다. 국제통신협회(ITU: International Telecommunication Union) 에서는 인터넷 전화를 위해 지난 90년대 초부터 종합정보통신망(ISDN)을 통한 디지털 음성 및 동영상 전송 규약인 H.320 표준을 제정하기 시작하면서 일반 전화망(PSTN)을 통한 H.324 표준과 인터넷을 통한 전송 표준인 H.323을 잇따라 내놓았다. 이로써 우리는 저렴하고 편리하게 전 세계를 연결할 수 있는 인터넷 음성 전화를 사용할 수 있게 되었다.

그러나 현재의 인터넷에서는 패킷 데이터에 대한 보안 기능이 제공되지 않으므로 인터넷 전화에 대한 보안은 미비한 상태이다. 향후 IP 버전 6 즉 IPv6가 상용화되면 IPSEC이라고 하는 보안 기능이 탑재될 수 있다. 그러나 IP보안 기능이 없는 IPv4를 사용하고 있는 현재의 상황에서는 네트워크 보안기능이 없이 인터넷 전화를 사용할 수밖에 없다. 이런 문제는 인터넷 전화에 치명적인 문제를 불러올 수 있다. 인터넷 보안 문제는 인터넷 폰만의 문제가 아닌 인터넷 전반에 대한 문제다. 현재 인터넷 보안의 주요 문제는 1) 상대방에 대한 인증이 어렵기 때문에 불순한 개체가 중간에서 전송자인 것처럼 가장할 수 있다는 점 2) 데이터를 중간에서 가로채 없앨 수 있다는 점, 3) 중간에서 데이터를 가로채서 변경하여 다시 보낼 수 있다는 점, 4) 중간에서 데이터를 복사할 수 있기 때문에 도청 등이 용이하다는 점, 5) 수신자에게 의도적으로 다수의 데이터를 집중적으로 전송해서 수신자의 기능을 마비시킬 수 있다는 점 등이다.

이러한 문제를 해결하기 위해 ITU에서는 H.323 인터넷 폰에 보안 기능을 첨가하기 위한 H.235 표준을 발표하게 되었다. 이 표준의 특징은 기존의 H.323 프로토콜을 그대로 유지하면서 사용하고 있던 데이터 구조 중 일부 데이터에 보안 기능을 첨가시키거나 암호화하는 방식으로 보안 기능을 부여하는 것이다. H.235의 보안 범위는 1) 상대방 및 사용자의 인증, 2) 호 설정 채널에 대한 보안, 3) 호 제어 및 H.245에 대한 보안, 4) 음성 데이터에 대한 암호화, 5) 각 단계의 보안 및 암호화 알고리즘의 규정 등에 대한 것이다. H.235의 기본 개념은 앞에서도 언급한바와 마찬가지

☆ 본 논문은 산업자원부에서 시행한 산업기반기술 개발 사업에 의한 기술개발 연구의 일부임

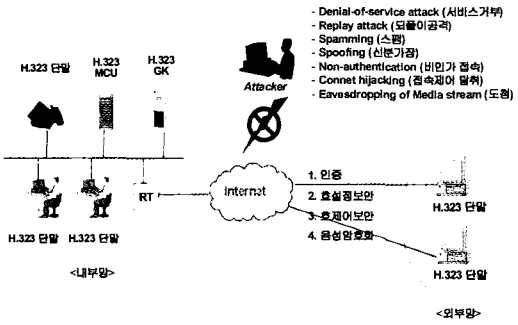
* 인덕대학 인터넷·TV방송과 교수

로 H.323의 프로토콜에 유연하게 보안할 수 있는 방법을 제시하는 것이다. 그러므로 H.323에 부담을 주지 않기 때문에 H.323의 성능을 저해하지 않고 H.323에 탑재할 때 유연성을 주고 있다.

본 논문에서는 H.235 표준의 보안기능 및 동향에 대해서 살펴보고 필자 등이 산업자원부 산업기반기술 개발사업의 지원을 받아 개발하여 H.323에 탑재한 사례를 중심으로 H.235의 개발에 대해 예시해보고자 한다.

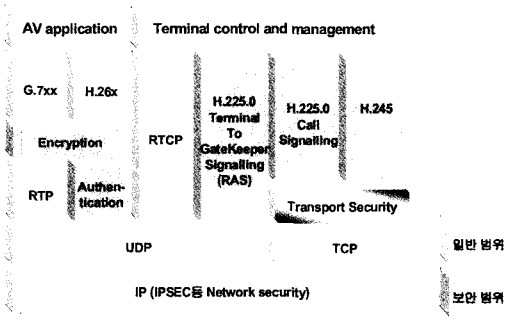
2. H.323에 대한 H.235의 보안 범위

H.323은 일반적으로 단말과 Gatekeeper, MCU (Multipoint Control Unit) 등으로 다양한 기능을 제공한다. 단말은 사용자가 인터넷 전화를 걸거나 받기 위한 터미널이며 Gatekeeper는 단말의 등록, 호의 허가 및 상태를 제어해주는 역할 (RAS: Registration, Admission and Status)과 H.245 호제어를 수행하는 일종의 서버이다. MCU는 두 명 이상의 사용자가 동시에 전화할 수 있도록 해주는 다중 제어 장치이다. 이들 H.323 엔티티들은 그림 1과 같이 여러 가지 공격에 무방비 상태에 있게 된다. 이러한 공격들을 효과적으로 차단해 주기 위해 H.235는 H.323을 이루고 있는 각 부분에 알맞은 보안 기능을 제공한다.



(그림 1) 인터넷 폰에 대한 공격유형

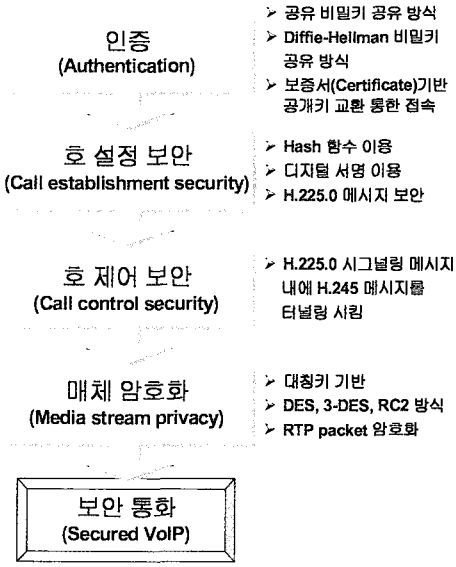
ITU-T에서는 H.323의 구조를 변형하지 않은 상태에서 유연한 방식으로 H.323 스택을 보안하는 H.235를 권고안으로 제안하고 있다. H.323의 스택 중 H.235로 보안되는 부분은 다음 그림 2에 나타낸 바와 같다. H.235는 호 설정 절차에 들어가기에 앞서 상호 인증을 위해 인증 절차를 두고 있다. 또한 호 설정(Call Establishment)을 위한 호 시그널링 및 게이트키퍼 등록 제어부분인 H.225.0을 보안하고 호 설정 이후 호 제어(Call Control)를 위해 H.245 부분을 제어해 준다. 호가 완전히 시작 된 이후에는 필요에 따라 음성데이터의 암호화 기능을 제공하고 있다.



(그림 2) H.323에 대한 H.235의 보안 범위

3. H.235의 보안 개요

H.323으로 통화를 위해서는 크게 두 가지 방식을 이용한다. 하나는 단말 대 단말 간 직접 통화방식이고 두 번째는 게이트키퍼에 등록한 후 단말에 전화하는 방식이다. 두 가지 방식 모두 처음 전화를 걸기 위해서는 상호 인증 또는 게이트키퍼에 대한 사용자 인증 절차를 마련하여 자신이 올바른 사용자임을 입증한다. 다음 단계로는 호 시그널링 절차에 대한 보안 기능으로 호 시그널링에 사용하는 PDU(Packet Data Unit)를 암호화하거나 디지털 서명을 첨부하여 인증 및 무결성을 제공하는 방식으로 호 시그널링을 보안한다. 호 시그널링 보안을 토대로 호 제어 채널을 보안하여 각종 데이터의 흐름을 보호한 후 호 연결이 시작되면 음성 암호화를 선택적으로 수행하게 된다. 이러한 일련의 보안 개요를 그림으로 나타내면 다음과 같다.



(그림 3) H.235의 보안 절차 개요

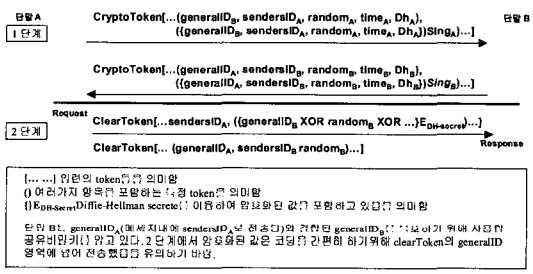
3.1 인증(Authentication)

인증이란 응답자가 자신을 입증하는 것으로서 보증서(Certificate) 기반의 공개키 교환을 통해 접속함으로써 이루어진다. 또 다른 인증방식으로는 단말 간에 공유된 비밀(패스워드 혹은 비밀정보)을 교환함으로써 이루어질 수도 있다.

일반적으로 보증서란 디지털 보증서 (Digital certificate)를 사용하여, 인증 프로토콜은 응답자가 보증서에 담겨있는 공개키에 대응하는 개인키(private key)를 갖고 있음을 증명한다. 이러한 인증은 man-in-the-middle attacks을 막아낼 수는 있지만 응답자가 누구인지 자동으로 증명하지는 않는다. H.235 권고안의 인증 구조는 인증 프로토콜에 의해 요구되는 것 이상의 인증서 내용을 규정하지는 않지만 대개 X.509 방식에 입각하여 개발하는 경우가 많다. 디지털 인증서를 사용하지 않는 인증에 대해서, H.235에서는 다양한 도전/응답(challenge/response) 시나리오를 완성하기 위한 시그널링을 구성한다. 이러한 인증 방식은 공유된 비밀을 얻기 위해 통신 단말들에 의해 사전 조정이 필요한데 이 방법의 한 예가 등록 기반의 서비스 사용이다. H.235에서 사용하는 인증 방식은 구체적으로 다음과 같다.

(1) Diffie-Hellman with optional authentication
(2) Subscription-based authentication
① password-based with symmetric encryption
② password-based with hashing
③ password-based with signatures

3.1.1 Diffie-Hellman with optional authentication



(그림 4) Diffie-Hellman with optional authentication

이 방식은 완벽한 사용자 레벨의 인증을 제공하는 것이 아니라 두 단말들 사이에서 기밀 통신을 위한 키 성분을 전달하기 위해 공유 비밀을 생성하기 위한 시그널링을 제공하는 절차이다. 이 교환절차가 끝나면 두 단말은 공유된 비밀키를 갖게 되고 이와 함께 이 키를 사용하게 될 알고리즘이 선택된다. 이 공유 비밀키는 이어서 발생하는 request/reponse 교환에서 사용된다. 그림 4의 첫단계는 Diffie-Hallman이 이루어지는 동안 교환되는 데이터를 보여준다. 두 번째 단계에서 응답자는 응용프로그램- 또는 프로토콜 특화된 메시지를 인증할 수 있다. 새로운 랜덤 값이 각 응답과 함께 되돌려질 수 있다.

3.1.2 Subscription-based authentication

H.235에서 차용하고 있는 인증 절차는 ISO 알고리즘 등에서 도출되어 나온 방식 등을 사용하고 있는데 이들 절차는 원래 양방향성이지만 단방향에서만 필요하다면 한쪽 방향으로만 사용될 수 있다. two-pass와

three-pass 절차가 모두 사용될 수 있으며 역방향에서 발생한 메시지가 인증될 필요가 없을 때 단방향으로만 상호 two-pass authentication이 이루어진다. 각 단말은 이렇게 교환된 유일하게 신분을 증명해주는 잘 알려진 신분증명자(텍스트 ID: text identifier)를 갖고 있다고 간주하게 된다. two-pass 절차에 있어서 상호간에 받아들일 수 있는 시간(timestamp로부터 파생된)에 대한 참조사항이 존재한다고 가정한다. three-pass 절차에서는 무작위로 발생된, 예측 불가능한 challenge number를 인증자로부터 나온 도전(challenge)으로 사용한다. 이 난수(random number)를 이용하여 재생공격(replay attack)으로부터 방어한다. two-pass 절차와는 다르게, three-pass 절차는 시작한 측의 도전을 지니고 있는 첫 시작 메시지를 인증하지는 않는다.

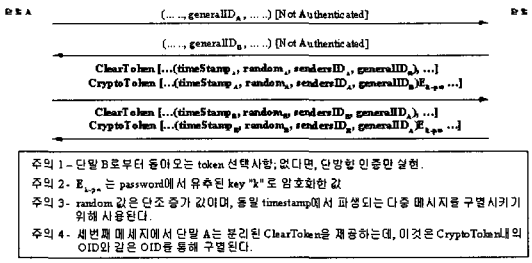
등록기반의 인증 방식에는 요구사항에 따라 다음과 같은 세 가지 방식이 있다.

① password-based with symmetric encryption;
② password-based with hashing;
③ certificate-based with signatures;

대부분의 경우, 여러 가지 선택에 따라 다음절에서 설명되어지는 것처럼 token이 정보를 담게된다. 대개의 경우에서, generalID는 온라인 방식으로 교환되기보다는 배열이나 디렉토리 참조표를 통해 알려진다는 것을 유념해야한다. 수신단에서의 절차를 단순화시키기 위해, 송신단은 자신의 신원을 sendersID에 포함시켜야하며, generalID로 수신자의 신원 증명을 하도록 해야한다.

(가) Password with symmetric encryption

이 방법에는 각각 two pass 와 three pass가 있을 수 있는데 본 논문에서는 지면제한에 의해 two pass만 나타내었다. 다음 그림 5는 대칭 암호화 형식의 인증을 수행하는데 필요한 토큰 형식과 메시지 교환방법을 보여준다. 이 프로토콜은 ISO/IEC 9798-2의 5.2.1절(two-pass)와 5.2.2절(three-pass)를 바탕으로 하고 있다. 신원 확인자(ID)와 패스워드가 등록 도중에 교환된다고 가정한다. 암호화 키는 길이 N octet (AlgorithmID에 의해 표시됨)이고, 다음과 같은 형식으로 이루어진다.

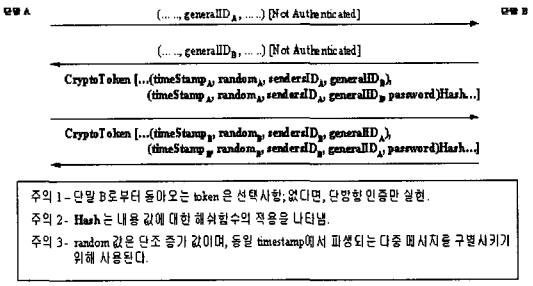


(그림 5) Password with symmetric encryption, two pass

- *패스워드 길이 = N이면, Key = password*
- *패스워드 길이 < N이면, Key 는 0으로 채워진다*
- *패스워드 길이 > N이면, 첫 N octet는 Key로 할당되고, 그런 후 패스워드의 N+M번째 octet 는 Mmod(N)번째 octet(N을 넘는 모든 octet에 대해)에 대해 XOR를 한다(즉, 모든 "초과" 패스워드 octet는 XORing에 의해 반복적으로 키 위로 접어 넣는다)*

(나) Password with hashing

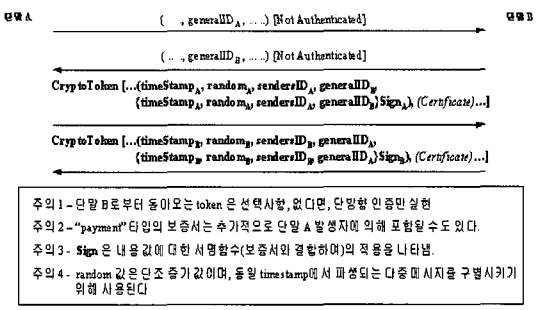
다음 그림 6은 각각 two pass에 대해 해쉬 형식의 인증을 수행하는데 필요한 토큰 형식과 메시지 교환 방법을 보여준다. 이 프로토콜은 ISO/IEC 9798-4의 5.2.1절(two-pass)와 5.2.2절(three-pass)를 바탕으로 한다. 신원 확인자(ID)와 이에 결합된 패스워드가 등록 도중에 교환된다고 가정한다. 본 연구에서 개발한 등록 기반의 해쉬함수를 이용한 보안방식이 바로 이 항목에서 설명하고 있는 방식 중 two-pass hashing 절차를 사용하고 있는 것으로서 H.235 권고안 Annex D 에 자세한 설명을 제공하고 있다.



(그림 6) Password with hashing, two pass

(다) Certificate-based with signature

다음 그림 7은 서명 형식의 인증을 수행하는데 필요한 토큰 형식과 메시지 교환을 보여준다. 이 프로토콜은 ISO/IEC 9798-3의 5.2.1절을 바탕으로 한다. 신원 확인자(ID)와 이에 결합된 인증서가 등록 도중에 할당/교환된다고 가정한다. 본 연구에서는 이 방식을 바탕으로 H.235의 Annex E에 있는 two-pass 서명 절차를 이용하여 보증서 기반의 시스템을 개발하였다.



(그림 7) Certificate-based with signature, two pass

3.2 호 설정 보안 (Call establishment security)

Q.931을 사용하는 H.323 시스템에서 호 설정 채널을 보호하도록 하는데는 두 가지 이유가 있는데 하나는 호를 수락하기 전에 단순한 인증을 위한 것이고 두 번째는 호 자체를 인증하기 위한 것이다. H-시리즈 터미널에서 이런 기능이 필요하다면 호 연결 메시지가 교환되기 전에 TLS/IPSEC과 같은 보안 통신 모드가 반드시 사용되어야 한다. 그렇지 않다면 대안으로 서비스 특화된 인증을 바탕으로 한 인증이 제공될 수도 있는데 이것은 시스템을 설계하는 사람에 따른 것으로 H.235 권고안의 범위를 벗어난다.

▶ 연결 설정 절차

호 연결 채널은 가장 먼저 연결되므로 최초로 보안되는 채널이다. H.323에서는 Q.931을 통해 호가 연결되는데 이를 위해 TLS(Transport level security)로 보안된 TSAP(port 1300)을 사용해야한다. H-시리즈 터미널에서는 최초의 연결 셋업 프로토콜에서 교환되는 정보에 의해 호 제어 채널에 대한 보안 모드가 결정된다. 만약 부합되는 보안 능력이 없다면 피호출단에서는 연결을 거부한다. 이때 되돌아온 에러에는 보안이 맞지 않다는 정보를 전혀 포함하지 않기 때문에 호출단에서는 다른 방법으로 장애를 알아내야 한다. 호출단에서 충분한 보안 능력 내용이 실리지 않은 'CONNECT ACKNOW- LEDGE' 메시지를 받을 경우 연결을 종료해야한다.

호출단이나 피호출단에서 부합되는 보안 능력을 갖게되면 양단에서는 H.245채널을 협상된 보안모드로 동작해야한다. 하지만 H.245 채널을 보안 모드로 설정하는데 실패했다면 프로토콜 에러가 발생했다고 가정하고 반드시 연결을 종료해야한다.

3.3 호 제어(H.245) 보안 (Call control security)

호 제어 채널은 이어서 연결되는 미디어 채널의 보안을 제공하기 위해 보안되어야 하는데 H.245 채널은 양단간에 협상된 기밀 메카니즘을 사용하여 보안되어야한다. H.245 메시지를 이용하여 공유된 기밀 미디어 채널에서 사용될 암호화 알고리즘과 암호 키를 전송한다. 논리 채널을 기반으로 하는 채널 상에서 이런 능력으로 인해 서로 다른 미디어 채널이 서로 다른 메카니즘으로 암호화될 수 있게되는 것이다. 예컨대 중앙 집중화된 다중 회의에서는 각 단말에 대해 서로 다른 키가 사용된다. 이렇게 되면 회의에 참가한 각 단말들이 미디어 스트림을 각각 암호화할 수 있게 된다. 보안 방식으로 H.245 메시지를 사용하기 위해서는 H.245 채널(논리 채널 0)전체가 서로 협상된 보안 방식으로 열려야만 한다.

H.245를 보안하는 메카니즘은 자신이 속한 H-시리즈 터미널에 달려있다. 다만 이러한 보안 구조를 사용하는 모든 시스템들은 실제적으로 초기화되기 전에 H.245 채널이 작동되게 될 구체적인 보안 방식을 협상하거나 알려주는 수단을 반드시 갖고 있어야 한다는 것이 유일한 요구사항이다. 예컨대 H.323은 H.225.0 연결 시그널링 메시지를 사용하여 이런 기능을 수행한다.

▶ H.245 시그널링과 절차

일반적으로 미디어 채널의 암호화 양상은 기타 다른 압축 파라미터와 같은 방법으로 제어되는데 즉, 각 터미널은 자신의 능력치를 알려주고, 데이터를 보내는 측에서는 사용할 포맷을 선택하고 수신 측에서는 모드에 대해 ACK를 보내거나 거부하는 것과 같은 양상이다. 알고리즘 선택과 같은 전송과 독립적인 메카니즘은 일반 논리채널 성분 안에 나타내고 키/암호화 알고리즘 동기화와 같은 전송에 특화된 기능은 전송 특화된 구조에 실어 보낸다.

(1) 보안 H.245 채널 운용

연결 설정 절차가 완결되어 연결이 보안 모드로 이루어졌다고 추정되면 기타 H.245 메시지가 교환되기 전에 H.245 논리 채널에 대해 협상된 핸드세이크와 인증이 이루어진다. 양단간에 협상이 되면, H-시리즈 터미널에 적합한 메카니즘을 이용하여 인증서 교환이 이루어진다. H.245 채널에 대한 보안이 완료되면 터미널은 일반 모드에서 사용되는 방법과 같은 방식으로 H.245 프로토콜을 사용하면 된다.

(2) 비보안 H.245 채널 운용

보안 채널과는 다르게 H.245 채널은 비보안 방식으로 운용될 수도 있는데 두 엔티티는 인증과 공유 비밀을 얻기 위해서 보안 논리채널을 열게 된다. 예컨대 H.235Control 값을 갖는 dataType을 채워보냄으로써 (H.245 ASN.1의 OpenLogicalChannel 참조) 논리 채널을 열 때 TLS나 IPSEC등을 사용하게 된다. 그러면 미디어 세션 키를 보호하는 공유 비밀을 얻거나 EncryptionSync를 보내기 위해 이 채널이 사용될 수 있게 된다.

(3) 능력 교환

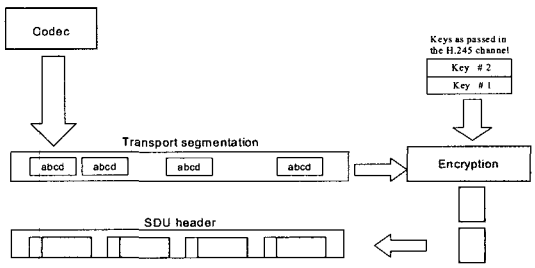
H.245 절차에 이어 단말은 H.245 메시지를 이용하여 능력치를 교환한다. 이 능력치에는 보안과 암호화 파라미터를 표시하는 정의를 담고 있다. 예컨대 단말은 H.261 비디오 송수신 능력치를 제공할 수 있는데 암호화된 H.261 비디오의 송수신 능력치도 보낼 수 있게 된다.

특정 미디어 코덱과 연결되어 사용되는 각 암호화 알고리즘은 새로운 능력치 정의를 포함하고 있다. 기타 다른 능력치와 마찬가지로 단말은 그들이 능력치 교환을 할 때 독립적이거나 의존적인 암호화된 코덱을 제공한다. 이것은 오버헤드나 리소스 능력에 근거하여 단말들이 그들의 보안 능력치를 조절할 수 있도록할 것이다. 능력교환이 이루어진 후 단말들은 일반적인 방식에서 수행하듯 미디어 논리채널을 보안상태로 개방할 수 있게된다.

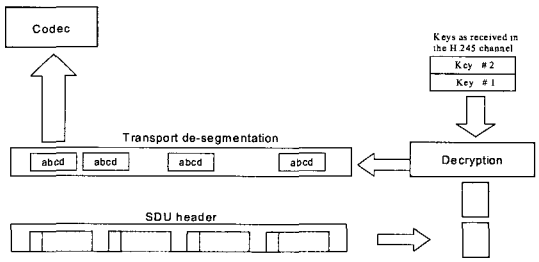
3.4 음성 암호화 절차 (Media stream encryption procedures)

음성데이터는 RTP 단에서 패킷 형태로 전송된다. 그러므로 RTP의 UDP 전송 직전에 암호화 단계를 삽입하면 된다. 이때 사용되는 암호화 알고리즘으로는 대칭키를 사용하는 DES, triple-DES, RC2 호환 방식 등이 있다.

미디어 스트림은 H.245 채널에서 능력교환 때 소개된 알고리즘과 키를 사용하여 암호화된다. 다음 그림은 일반적인 데이터의 흐름을 보여준다. 트랜스포트 헤더는 SDU(Service Data Unit)가 암호화된 후 transport SDU에 덧붙여진다. 음영 부분이 암호화된 부분을 나타내고 있다. 새로운 키가 송신자로부터 수신되어 암호화에 사용되면, SDU 헤더는 수신자에게 새로운 키가 현재 사용되고 있다는 사실을 알려야만 한다. 예컨대, H.323에서 RTP 헤더(SDU)는 자신의 payload type을 변경하여 새로운 키에 대한 변경을 알려준다.



(그림 8) 미디어의 암호화 과정



(그림 9) 미디어의 복호화 과정

4. 시스템 적용 사례

H.235 버전 2에서는 시스템 개발을 위한 적용 사례를 세 가지로 제시하고 있다. 하나는 기본 방식으로 패스워드를 이용하여 Hash 값을 산출하여 사용하는 방식이며 다른 방식은 서명방식이다. 서명방식에는 다시 두 가지 방식으로 나뉘는데 하나는 Authentication-only (인증전용)방식이고 나머지는 Authentication and integrity (인증 및 무결성) 방식이다. 인증전용방식은 메시지가 목적지에 갈 때까지 인증만 수행하는 방식이고 인증 및 무결성 방식은 메시지에 대해 인증과 무결성 검사를 동시에 수행하는 방식이다. 이들 서명방식은 다시 Procedure II와 Procedure III로 나뉘어 구성하고 있다.

4.1 기본 방식 (Baseline security profile : Procedure I)

이 방식은 H.235의 ANNEX D에서 권고하는 내용이다. 이 방식은 가장 기본이 되면서 간단한 방식으로 password 기반의 보안 방식을 사용하며 다음과 같은 공격을 막아준다.

- Denial-of-service attacks : 암호 hash 값의 빠른 검사로 막을 수 있음
- Man-in-the-middle attacks : 응용 레벨의 hop-by-hop 메시지 인증 & 무결성을 이용하여 man-in-the-middle이 응용 레벨의 hop 즉, 적대적 라우터 사이에 있을 때 이 공격을 방지함
- Replay attacks : timestamp와 일련번호를 사용하여 예방
- Spoofing : 사용자 인증을 사용하여 예방
- Connection hijacking : 각각의 시그널링 메시지의 인증/무결성을 사용하여 예방
- Eavesdropping of media stream : 암호화와 비밀키의 사용으로 방지

이 방식은 다음과 같은 장점도 지닌다.

- IMTC/ ETSI/ IETF 자료를 근거로 하는 강력하고, 잘 알려졌으며, 넓게 적용되었던 알고리즘의 사용
- 비지니스 모델의 보안 요구에 의거하는 상황에서 적용성
- 다자간 회의, 신축성 있는 환경, 닫힌 그룹 등과 같이 다양하게 적용 가능함

이 방식의 적용 범위는 다음 표와 같다. 일반적으로 RAS는 게이트키퍼와의 등록, 수락, 상태표시 등을 위한 데이터의 교환 단계이고, H.225.0은 호 제어, H.245는 능력 교환 등의 데이터가 전송되며 RTP는 미디어 데이터를 관장하는 부분이다.

(표 1) Annex D Security Profiles 개요표

보안 서비스	호 기능					
	RAS	H.225.0		H.245	RTP	
인증	Password HMAC-SHA-96	Password HMAC-SHA-96		Password HMAC-SHA-96		
부인방지						
무결성	Password HMAC-SHA-96	Password HMAC-SHA-96		Password HMAC-SHA-96		
암호화					56-bit DES	56-bit RC2-호환 / 168-bit 3-Des
접근제어						
키관리	등록기반 패스워드 할당	등록 기반 패스워드 할당	인증 기반 DH 키 교환	종합 H.235 세션키 관리 (56 bit DES, RC2, 168 bit 3-DES)		

(1) Baseline security profile

위의 표에서 푸른색(왼쪽 부분) 부분이baseline security profile이다. 이 방식은 상호간에 동의된 password/대칭키가 안전한 H.323 시스템과 네트워크 요소(GK, Proxy 등)에 할당 될 수 있는 환경에 적용할 수 있다. 이 방식은 password에 기반한 HMAC-SHA1-96 해쉬를 사용하여 RAS와 H.225.0, 터널링된 H.245에 대한 인증과 무결성을 제공한다. GK대GK 또는 단대단 FastStart를 사용하는 H.225.0 호 설정은 Diffie-Hellman의 키관리를 포함하고 있다. Baseline security profile에서는 통합된 키 관리 요소와 빠른 연결 절차를 필수로 하고 있다. 시그널링 방식은 또한 tunneled H.245 key- update와 동기화에 제공된다. 긴 통화를 위해 이 메시지들은 H.225.0 메시지 내에 H.245의 터널링을 필요로 한다.

(2) Voice encryption security profile

이 절차에서는 음성데이터를 암호화하기 위해 음성 암호화 security profile이 제공된다. 음성의 암호화는 선택사항이다. 이 방식은 호 시그널링과 연결 setup 절차와 같은 부분에서 Diffie-Hellman key agreement와 그 밖의 키 관리 기능에 의해 이루어진다.
H.323 시스템은 음성의 비밀성을 얻기 위하여 음성 암호화 profile을 구성할 수도 있다. 본 연구에서는 국제 표준을 따르기 위해 앞 절에서 설명한 RC2-compatible, DES 또는 Triple- DES 암호화 알고리즘을 개발하였다. 그런데 어느 정도의 비밀성이 제공되는 환경에서는 이들 음성 암호화가 필요하지 않을 수도 있는데, 이 경우 Diffie-Hellman key agreement와 다른 키관리 절차는 필요 없을 수도 있다.

H.323 시스템에서 필수항목으로 지정하고 있는 음성암호화는 56bit DES 방식이다. 또한 부수적으로 168bit Triple-DES를 사용할 수 있고 수출 등 상업적인 목적이라면 56bit RC2- compatible을 이용하여 개발할 수도 있다.

(3) 실제 적용 사례

필자는 산업자원부 공통핵심 개발사업의 일환으로 H.235를 바탕으로 하는 인터넷 폰의 사용자 인증과 데이터 암호화 관련 기술 개발을 수행하였다. 이때 H.235 버전 2에서 권고하는 기본 방식 보안 (Procedure I)과 서명방식 보안 (Procedure II/III)을 개발하였다.

H.235에서는 별도 시스템의 개발 없이 기존의 H.323 프로토콜에서 PDU(Packet Data Unit)의 파라미터에 보안 요소를 첨부함으로써 인터넷 폰의 보안을 이룰 수 있는 프로토콜의 제시 및 권고하고 있다. 이때 보안 기능을 부여하는 데이터 구조를 'H.235 ANNEX A-H.235 ASN.1'에 마련하였으며 이를 이용하여 본 연구에서는 다음 그림과 같이 Baseline Security Profile (Procedure I)에서 사용하는 데이터 구조를 구성하여 개발하였다.

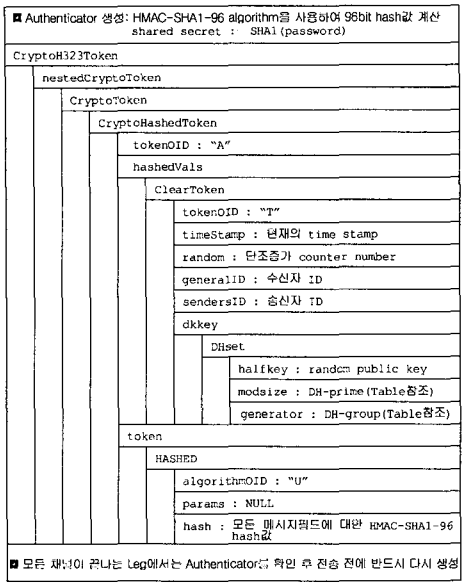
H.323을 이용한 인터넷 전화 방식은 최초에 RAS나 호 설정을 위한 호 시그널링이 수행되고 다음은 H.245 프로토콜이 수행된다. 그 후에는 선택사항에 따라 음성 데이터의 암호화가 수행된다.

가장 먼저 호 설정을 위한 각종 시그널링을 보안하는 방법을 개발하였다.

이를 위해 H.323 시스템은
① Fast connect
② GK-routed model
을 지원해야 한다.

보안 정책에 따라서 인증은 역방향에서의 인증/무결성이 적용되기 때문에 단방향 혹은 양방향성인데 그 때문에 더 높은 수준의 인증이 가능하다. 게이트키퍼는 역방향에서 인증/무결성을 적용해야 하는지를 정한다.

보안된 단말이나 상대 게이트키퍼로부터 받은 RAS나 호 시그널링 메시지에 인증 실패, 무결성 검증 실패를 감지한 게이트키퍼는 응답 reject message에 securityDenial 이라고 거절 이유를 세팅하여 보안 실패를 알리는 응답을 한다.



(그림 10) Procedure I의 주요 데이터

이 방식은 H.235 ICV 필드를 사용하지 않는다. 암호의 무결성 검사 값은 암호의 해쉬로 취급되고 CryptoToken의 해쉬 필드에 넣어진다. 다음 그림에 H.323 및 H.235의 ASN structure에 해당되는 각 항목에 들어가야하는 데이터를 상세히 설명하였다. 이를 바탕으로 ASN 구조체에 Procedure I에 해당하는 데이터를 넣으면 인터넷 폰의 보안 및 인증이 이루어진다.

4.2 서명 방식 (Signature profile)

본 연구에서는 대칭키 방식의 Procedure I과 더불어 디지털 서명을 이용하는 보안방식을 개발하였다. 이 보안 방식은 매우 향상된 보안 기능을 H.323 시스템에 제공하게 된다. 서명 보안방식은 H.245 Tunneling 기술에 기반하며 GK- routed Model을 쓰도록 되어있다.

서명 보안방식은 단말의 숫자가 매우 많은 광역적 인터넷 폰에 적절하다. 이 보안방식은 Procedure I의 단순한 기본 보안방식의 한계를 극복할 수 있게 해준다. 예컨대, 서명 보안방식은 서로 다른 도메인간에 상호 공유비밀 관리에 의존하지 않다. 이 방식은 H.245 메시지의 무결성을 위해 H.245 메시지 Tunneling을 제공하고 메시지의 부인방지 기능을 제공하고 있다. 본 연구에서 개발한 서명 보안방식은 H.235 proxy나 중간 게이트키퍼를 동시에 사용하는 진정한 단대단 인증뿐만 아니라 hop-by-hop 보안까지 지원하고 있다. 서명 보안방식에서 제공하는 기능은 다음과 같다.

RAS, H.225.0, H.245 메시지에 대해,
- 메시지가 지나가는 응용레벨 Hop의 개수에 관계없이 원하는 엔티티에 대해 인증 사용
- 메시지가 지나가는 응용레벨 Hop의 개수에 관계없이 임의의 엔티티에 도착한 메시지에 대해 전부 혹은 주요 부분에 대한 무결성. 강력하게 생성된 난수를 이용하는 메시지 무결성이 또한 선택사항.
- 전체 메시지에 대해 응용레벨 Hop-by-hop 인증, 무결성, 부인방지가 제공됨
- 중간에 지나가는 응용레벨의 Hop 개수에 관계없이 두 엔티티 간에 전달되는 메시지에 대한 부인방지가 제공됨. 특히 부인방지는 메시지의 주요 부분에 대해 제공됨.

이러한 기능은 다음과 같은 공격을 효과적으로 차단해 준다.
- Denial-of-service attacks : 전자서명 값의 빠른 검사로 막을 수 있음
- Man-in-the-middle attacks : 응용 레벨의 hop-by-hop 메시지 인증 & 무결성을 이용하여 man-in-the-middle이 응용 계층의 hop, say, 적대 라우터 사이에 있을 때 이 공격을 방지함
- Replay attacks : timestamp와 일련번호를 사용하여 예방
- Spoofing : 사용자 인증을 사용하여 예방
- Connection hijacking : 각각의 시그널링 메시지의 인증/무결성을 사용하여 예방

(표 2) Signature security profile 개요표

보안 서비스	호 기능			
	RAS	H.225.0	H.245	RTP
인증	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	디지털서명	디지털서명	디지털서명	
부인 방지	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	디지털서명	디지털서명	디지털서명	
무결성	SHA1/ MD5	SHA1/ MD5	SHA1/ MD5	
	디지털서명	디지털서명	디지털서명	
암호화				
접근 제어				
키 관리	인증서에 위치	인증서에 위치		

서명 보안방식 즉 Procedure II/III에서 보안 기능을 제공해주는 부분은 다음 표에 나타나 있는 RAS, H.225.0 호제어 절차 및 H.245 등이 있다. 여기에 사용하는 암호화 방식은 RSA- SHA1 알고리즘과 RSA-MD5 알고리즘을 사용한 디지털 전자서명이며 인증 전용(Authen- tication-only) 방식과 인증/부인방지/무결성을 제공하는 방식으로 나뉠 수 있다. 음성 암호화는 Procedure I의 방식을 사용할 수 있으며 음성 암호화의 사용은 선택사항이다.

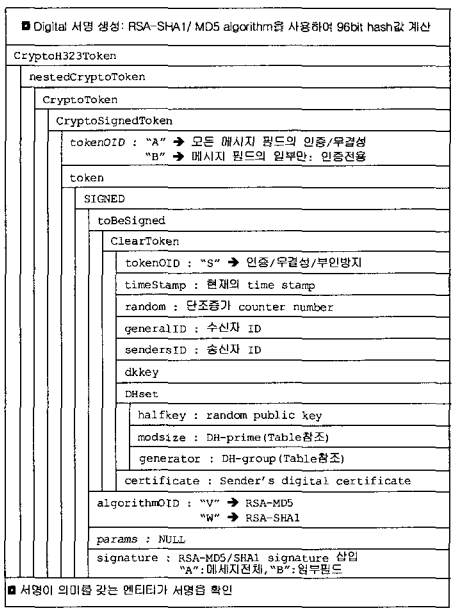
서명 보안방식에서는 두 가지의 보안 서비스를 제공한다. 하나는 인증전용 서비스이고 다른 하나는 인증 및 무결성 보안 서비스이다.

① Authentication-only : 이 보안 서비스는 개인키에 의해 올바르게 디지털 서명되었을 때, 사용자 인증을 제공한다. 이 서비스는 중간 삭제나 첨부, 메시지조작 또는 부정한 공격에 대한 대응책이 없음을 유의해야한다. 인증전용방식은 메시지를 다른 목적지(이를테면 GK)로 forwarding할 때 메시지의 인증을 확인하는 보안 proxy들에 대해 유용하다. 그럼에도 불구하고, 인증전용방식은 hop-by-hop 기반에서도 잘 적용될 수 있다. 즉 Procedure III은 이 보안 서비스를 단대단 시나리오에 대해서 설명하고 있고, Procedure II는 hop-by-hop 경우에 대해 설명하고 있다.

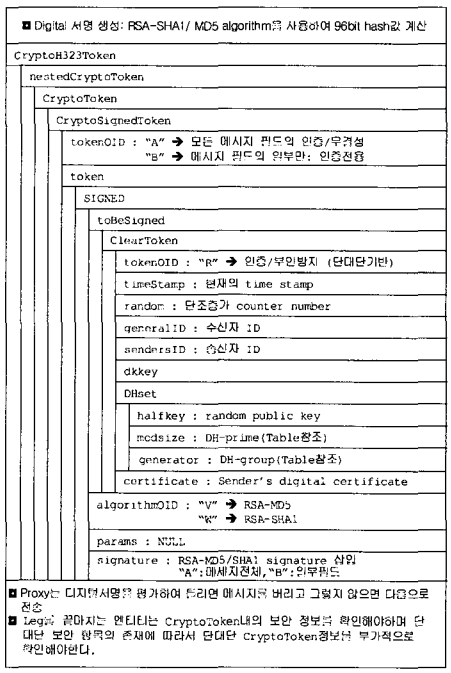
② Authentication and integrity : 이 보안 서비스는 메시지 무결성을 사용자 인증과 함께 제공하도록 결합시켜 놓았다. 사용자는 개인키에 의한 디지털 서명된 데이터들에 의해서 인증된다. 이 기능에 더해서 메시지는 부정한 공격에 대해 보호받는 기능도 있다. 두 가지 보안 서비스는 같은 보안 방식에 의해서 제공된다. 인증과 무결성의 결합은 오직 hop-by-hop 기반에서만 가능하다. Procedure II는 이 보안 서비스에 대해 다루고 있다.

(1) Procedure II

Procedure II를 위한 파라미터들은 다음 그림과 같다. 특히 Procedure II는 hop-by-hop 보안을 지원하는데 이 방식은 중간에 거쳐가는 모든 엔티티들이 인증과 무결성을 체크하게 된다.



(그림 11) Procedure II의 주요 데이터



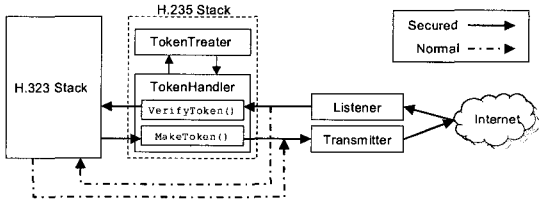
(그림 12) Procedure III의 주요 데이터

(2) Procedure III

Procedure III을 위한 파라미터들은 다음 그림과 같다. Procedure III은 Procedure II와는 달리 end-to-end 보안 모드에 대해서 적용되는데 이 경우는 중간에 경유하는 엔티티에서는 보안 정보를 재연산하지 않고 통과시키고 최종단에 가서 처리되도록 설계되어있다.

4.3 H.235 Stack 개발 내용

필자가 수행한 연구에서는 H.235 표준의 보안 stack을 개발하여 H.323에 탑재하여 기존 인터넷 폰에 보안 기능을 부여할 수 있게 계층화된 구조로 H.235 stack을 개발하였다. H.235에 정의된 절차는 필연적으로 H.323 절차와 맞물려 진행된다. 그러므로 H.323의 각 단계에서 H.235의 보안 기능이 필요한 경우 적절하게 H.235 기능을 그때마다 불러서 사용하는 형식(DLL: Dynamic Link Library)으로 개발하였다. 본 연구에서는 이를 위하여 보안 절차를 관장하는 TokenHandler Class와 각종 보안에 필요한 연산을 수행하는 TokenTreater Class로 크게 구별하여 개발하여 구조적인 편의성을 제공하였다. 전체적인 구조는 다음 그림과 같다.



(그림 13) 개발된 H.235 Stack의 구조도

이 구조는 H.323에서 주고받는 PDU(Protocol Data Unit)를 작성할 때 보안 여부에 따라서 TokenHandler를 사용할지 여부를 결정하게 되고 TokenHandler에서도 Procedure I, Procedure II, Procedure III에 따라서 알맞은 루틴을 수행하게 된다.

6. 결 론

본 논문에서는 H.235에 대한 기본적인 개념과 구조, 절차 및 권고안에 따른 시스템 응용에 이르기까지 전반적인 내용을 살펴보았다. H.323이 방대하듯이 H.235도 간단한 내용은 아니지만 인터넷 폰에 대한 보안 방법과 절차에 대한 개괄적인 고찰을 시도하였다. H.235의 특징은 ITU-T에서 제창하였듯이 기존의 H.323 시스템 개발자들에게 개발에 따르는 부담을 줄여주고 보안을 수행할 때 H.323의 성능 저하를 최소화 또는 제거하는데 목적이 있다. 그러므로 H.235는 기존의 H.323 PDU 내부에 존재하는 파라미터들에 보안 항목을 첨가하여 인터넷 폰을 보안하는 방식을 사용하고 있다. 이 경우 호 설정 및 호 제어에 오버헤드가 걸리지 않을 뿐만 아니라 음성을 암호화하는데 소요되는 시간이 통신 지연 시간 이내에서 가능하게 되므로 보안에 따르는 시스템 적인 부담 또한 경미하게 된다.

인터넷 폰 보안을 위한 본 연구에서는 인터넷을 통한 데이터 전송에서 발생하는 여러 가지 경우의 보안 공격에 대해 효율적으로 공격을 차단할 수 있는 알고리즘을 개발하여 인터넷 폰에 적용하였다. 또한 통신

시스템에서 가장 중요한 국제 표준을 철저히 준수함으로써 국제적인 호환성을 유지할 수 있었다. 본 연구에서 개발된 기술은 향후 안전한 통신의 필요성이 크게 대두되고 있는 인터넷 환경에서 효율적으로 상대방을 확인하고 데이터를 보호함으로써 지식과 재산에 대한 완벽한 보호장치를 마련할 수 있게 되었다.

현재 ITU-T에서 지속적으로 H.235에 대한 보강 작업이 진행되고 있으며 H.235 버전 3이 나오고 있다. 앞으로의 과제는 지속적인 보안기능의 향상과 함께 다양한 기능을 탑재한 보안 VoIP의 개발이 시급하다고 판단된다.

참 고 문 헌

[1] ITU-T Recommendation H.235 : Security and encryption for H-series (H.323 and other H.245-based) multimdeia terminals, Nov. 2000

[2] ITU-T Recommendation H.323 : Packet- based multimedia communications systems , Nov. 2000

[3] ITU-T Recommendation H.225.0 : Call signalling protocols and media stream packetization for packet-based multimedia communication systems, Nov. 2000

[4] ITU-T Recommendation H.245 : Control protocol for multimedia communication, Nov. 2000

[5] D. Minoli and E. Minoli, Dilivering Voice over IP Networks, Wiley Computer Publishing, 1998

[6] Bill Douskalis, IP Telephony, Prentice Hall PRT, 2000

[7] Jeremy Goldstein, Video Conferencing, Picturephone Direct, Inc., 1995

[8] P. K. Andleigh and K. Thakrar, Multimedia Systems Design, Prentice Hall PRT, 1996

[9] J. D. Spragins, J. L. Hammond and K. Pawlikowski, Telecommunications Pro- tocols and Design, Addison-Wesley, 1994

[10] (사)개방형컴퓨터통신연구회, 정보보호기술 개론서, 한국전자통신연구원, 1999

[11] 박창섭, 암호이론과 보안, 대영사, 1999

[12] 김철, 암호학의 이해, 홍릉문고, 1996

◐ 저 자 소 개 ◑

황 선 철

1982년～1986년 연세대학교 전기공학과(공학사)
1986년～1988년 연세대학교 전기공학과(공학석사)
1989년～1999년 연세대학교 전기공학과(공학박사)
1991년～1998년 LG 전자 선임연구원
1999년～현재 : 인덕대학 인터넷·TV방송과 교수
관심분야 : H.323 VoIP, H.235 보안프로토콜, 영상통신, 영상압축