특 집

차세대 VoIP 망에 있어서의 Security 기술고찰

조 원 상*, 김 용 건**

● 목 차 ●

1. 서 론
2. VoIP Protocol에 있어서의 Security 특성
3. Security 저해요인
4. 결 론

1. 서 론

기존의 PSTN 사용자들에게 제공되고 있는 양질의 통신 서비스와 통신보안의 수준이 현재 VoIP 기술이 발전함에따라 동등한 수준으로 요구되고 있다. 특히, IP 망에 있어서의 보안 문제는 지금도 많은 논의가 이루어지고 있으며 문제점들이 점차 해결되어 가는 추세에 있다. 이러한 문제점은 우리가 차세대 VoIP 통신망을 설계하는데 있어서도 매우 중요한 관심 사항이 되고 있으며 필수적으로 차세대 VoIP 망이 해결해야할 커다란 문제점중의 하나이다. 따라서 본 고에서는 수년간 발전을 거듭해온 다양한 VoIP Protocol, 즉 H.323, SIP 및 H.248/ MEGACO/ MGCP 등에서 지향하는 Security 기술의 동향을 살펴보고 차세대 VoIP망의 설계시 기술적인 저해요인을 도출하여 극복키 위한 방향을 정립코자 한다.

2. VoIP Protocol에있어서의 Security 특성

VoIP Protocol은 TCP/UDP/IP 상의 세가지 기능적인 측면에서 구분을 할수 있다.

첫째로, Call Signalling Part H.323의 H.225, H.245, H.450이 이에 포함되며, SIP도 마찬가지로 SAP과 SDP로 구성된 부분이 해당된다.

둘째로, Gateway or Device Control Part MGCP/MEGACO/H.248 Protocol이 해당된다.

셋째로, Media Transmission Part Audio나 Video 정보 전송과 관련된 Protocol로써 RTP, RTCP, RTSP등이 해당된다.

Media Transmission 과 관련된 Protocol은 H.323, SIP, MGCP/MEGACO/H.248이 가지고 있는 공통된 부분이며 Security 관련된 기능도 어느 정보의 보호에 관점을 두는가에 따라 VoIP protocol에 포함 되느냐 아니면 Application Layer 혹은 Network Layer에 포함시키는가가 결정 된다고 볼 수 있다.

현재 제안된 VoIP Protocol로써 H.323과 SIP 및 MGCP/MEGACO/H.248로 나누어 이력과 구조를 살펴본후 차세대 VoIP 망에서의 각자가 가지는 Security 기술의 특징과 저해요인을 살펴 보도록 한다.

2.1 VoIP Protocol의 이력요약

2.1.1 H.323

1990년대 초반부터 H.32x series의 표준이 승인되

* 삼성전자 네트웍(사) 개발팀장
** 삼성전자 네트웍(사) 사업팀장

기 시작하여, 1996년 처음으로 H.323 관련된 ITU-T 에서 표준으로 제정하게 되었으며, 1998년 1월 Version 2가 승인이 되었고 1999년 5월 Version 3가 또한 2000년 11월 Version 4가 승인 되었다. 현재는 Version 5가 작업중에 있다.

2.1.2 SIP

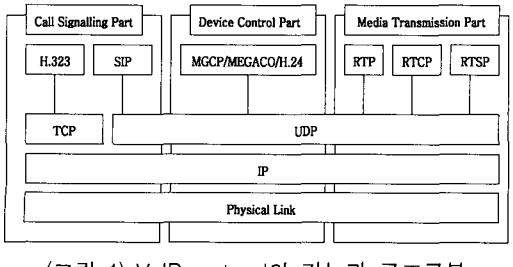
SIP은 IETF의 Multiparty Multimedia Session Control (MMUSIC) working group 안에서 검토가 시작되어 1999년 3월 RFC2543으로 표준을 제안하였고 Call Processing Language (CPL)와 과련있는 iptel working group 및 PSTN and Internet Internetworking (pint) working group과 연계된 작업을 진행중에 있다.

2.1.3 MGCP/MEGACO/H.248

IETF는 1999년 10월 Media Gateway Control (MEGACO) Working Group에서 RFC 2705로 표준을 발표하게 되었고, 보다 개선된 새로운 Version으로 MEGACO를 발표하게 되었으며, 동시에 ITU-T에서도 MEGACO와 유사한 H.248을 제안하여 통합화를 추진중에 있다.

2.2 각종 VoIP Protocol의 구조와 Security

다양하고 복잡한 protocol로 이루어져 있는 H.323과 비교하여 SIP과 MGCP는 단순하면서도 확장성이 있다고 볼수 있으며 Security 기술을 응용하는것도 각 protocol의 성격에따라 다소의 차이가 있다.



(그림 1) VoIP protocol의 기능과 구조구분

VoIP protocol에 Security 기술을 적용하는데는 크게 다음과 같이 두가지의 방법론을 고려해 볼수 있다.

첫째로, H.235와 같이 VoIP protocol의 일부로 포함시켜 Security 기능을 제공하는 방법을 고려해 볼수 있고 둘째로, MGCP와 같이 Network layer protocol에서 IPSec같은것을 고려해 볼구 있다.

H.323 Protocol에 있어는 전송코자 하는 정보의 종류나 특성에따라 세가지 경우의 Channel 개념을 생각해 볼수 있다. 즉, Call Connection Channel, Call Control Channel 과 Media Channel 개념으로 나누어 볼 수 있다.

Version 2에서부터 제안된 H.235에서는 Security 개념을 위와같은 세가지의 구분으로 접근할수 있다. Call Connection Channel은 optional하게 SSL/TLS(TCP port : 1300)이나 IPSec에의해 Security를 보장 받을수 있으며, Connection 이 이루어진 뒤 H.245 Call Control Channel에의해 인증을 거칠수 있으며 RTP와 관련된 security parameter 정보도 교환하게 된다.

인증시 사용되는 방법으로는 대칭형 암호화 기반의 절차와 Subscription 기반의(password, signature) 대칭, 비대칭 암호화 기술이 사용되며 Diffie & Hellman의 Key Exchange 기법이 제안되고 있다. 물론 이외의 IPSec나 TLS를 이용한방법도 가능하다.

마지막으로 RTP 즉 Media Channel에 대해서는 DES나 Triple DES, RC2를 이용하여 Security를 지원하여 주는 방법이 있다.

SIP에 있어서는 RFC 2543에 Security 관련 내용이 언급되어 있으며, Authentication 과 관련되어서는 Basic authentication, Digest authentication, Proxy authentication, PGP authentication 으로 선택적으로 결정할수 있다.특히, IPSec을 이용한 End-to-End 와 Hop-by-Hop Encryption을 제공할수 있다.

MGCP/MEGACO/H.248 에 있어서는 RFC2885에 언급되어 있듯이 IPSec을 이용하여 authentication 과 encryption에 이용하고 있다.

2.3 차세대 VoIP망에 있어서의 Security 필요성

우리가 사용하는 일반적인 Internet 환경에서는 Computer를 이용한 Hacking이 많은 문제점으로 대두되고 있고, VoIP를 이용한 전화서비스를 하는데 있어 간단하게 VoIP Packet Sniffer를 이용하여 원하는 정보를 추출하여 낼 수 있기 때문에 Security의 중요성이 더욱 부각되고 있다.

- 이에 따라 타인의 전화번호를 도용할수 있는 여지가 있고
- 임의의 악의호를 발생시켜 특정인을 attack 할 수도있다.
- 또한 거짓정보를 발생시켜 특정인의 전화 사용을 제한시킬수도 있다.

이러한 각종의 문제를 해결하기 위해 각종의 VoIP protocol들은 Security에 관련된 기능을 갖추게 되어있고 향후 차세대 VoIP 망을설계할 때 고려해야할 중요한 관심사중의 하나로 부각되고 있다.

3. Security 기술보급의 저해 요인

VoIP 통신은 완전한 Multi-media 환경의 통신을 위한 여러 Network 요소를 감안하지 못하여 Security를 보장하는데 있어서도 여러가지 어려움을 초래 하고 있다. 때문에 차세대의 VoIP 망의 설계에도 Security를 고려한다면 기존의 Network element나 protocol을 일부 수정할 필요도 있을 것으로 예상된다.

또한 Security기술을 적용하는데 있어서도 VoIP 망의 효율화를 생각하여 다음과 같은 3 단계의 적용방법을 고려할수 있다.

- 1 단계 : Link Level의 Security
  Security가 link-level 즉, IP 하단의 data link layer에서 모든 packet에 대하여 처리되어일반 사용자는 크게 관여치 않아도 된다.
- 2 단계 : Secured Packet
  VoIP와 관련된 각종 information중에서 중요한 packet에 대하여 security 처리를 한다.
- 3 단계 : Packet내부의 선택적인 Field만 Security 처리
  특정 packet만 처리해도 security 처리에 대한 performance overhead 를 만족 시키지 못할경우 packet의 특정 field만을 security 처리할수도 있다.

또한 VoIP 망에서 바라보았을 때 Authentication과 Encryption 기술을 적용하는 관점으로 다음과 같은 두가지의 구분이 가능하다.

- end to end security
- hop by hop security

end to end security는 모든 end point들이 동등한 security 기능을 가져야 하는 개념인 반면, hop by hop security는 다음과 같은 장단점을 가지고 있다.

- hop by hop security의 장점
  이미 web 기술에서 안정성이 증명되었고 public key 정보를 end point가 가질 필요가 없기 때문에 end point 입장에서는 보다더 간단해 질수 있다.
- hop by hop security의 단점
  hop과 hop 간의 사전에 약속이 되어 있어야 하며 VoIP 망안의 각 hop들간의 security policy에 의한 설계가 되어 있어야 한다.

위와 같은 요소들을 감안하여 security를 차세대 VoIP 망에 구현한다 하더라도 또다른 다음과 같은 저해 요인을 생각해 볼수 있다.

3.1 VoIP QoS와 연관된 delay 요인 발생

VoIP 망에 있어서 QoS는 중요한 고려 대상이며 이러한 QoS에 영향을 줄 수 있는 parameter들로써는 latency, jitter, delay등을 고려해 볼 수 있다.

일반적으로 security 관점에서 볼 때 Public key cryptography 기반의 authentication과 encryption 기능은 Gateway나 Terminal의 많은 computing power를

요구하게 된다.

이는 결국 packet processing delay를 초래하게 되고 나아가 전체적인 VoIP packet의 delay를 초래하게 되어 VoIP 망에 있어서의 QoS를 저해 시키는 결과를 초래하게 된다.

물론 현재 상용화되어 나오는 일부 Chip vendor들은 Security를 H/W적으로 지원 할수 있게도(예: DES, Triple DES 지원) 되어 있으며 이러한 시도는 차세대 VoIP 망의 Security 도입에 견인차 역할을 할수 있으리라 보인다.

3.2 Data Network 장비의 security 기능 부정합

H.323, SIP, MGCP/MEGACO/H.248에서 제안하는 IPSec같은 Security 기술을 Data망에 적용할 때 Encryption 한 정보와 NAT와는 정합되기 어려운점이 있다. 왜냐하면 IP Address 자체도 Encryption 해야하기 때문에 NAT로써는 동작상에 문제점을 야기할 수 있다. 앞으로 계속된 개선이 이루어 지겠지만, 이러한 문제를 피하기 위해 차세대 VoIP Gateway 입장에서는 Hop by Hop Security를 채택하고, Terminal 입장에서는 Secured Packet 이나 Packet 내부의 선택적인 Field만 Security 처리 하는 형태로 망을 진화시켜 나가는 것도 생각해 볼 수 있는 하나의 방안이라 생각한다.

4. 결 론

차세대 VoIP 망을 설계하는데 있어 기존의 PSTN이 가지는 안정성에 맞추기위해 점점더 Security에 대한 요구는 증가하고 있다. 이에 따라 표준화 측면에서는 H.323, SIP, MGCP/MEGACO/H.248등 VoIP 관련된 Protocol안에 Security 관련 내용을 제안되게 되었다. 하지만 구현 측면에서는 아직 IPSec과 같이 대중화 되지 않은 부분도 있고 Public Key Certification을 위한 경제성등도 논란이 될수 있다. 또한 기존의 Firewall이나 NAT와 같은 Network Component와의 부정합성도 문제가 되고 있지만, 많은 Solution이 등장함으로써 곧 실용화 되리라고 생각한다. 특히 차세대 VoIP망이 가지는 Multi Media 통신과 Application은 더욱더 개인 보안 문제를 중요하게 다루게 될 것이며 이러한 요구 사항이 발생됨으로써 아직 미개척 분야인 Security의 문제점들은 앞으로 계속 더 연구하고 발전시켜야 할 분야가 될 것이다.

참고문헌

[1] Mika Marjalaakso, "Security Requirements and Constraints of VoIP," Helsinki University of Technology, 2000.

[2] ITU-T, ITU-T Recommendation H.235 (02/98), Security and encryption for H-Series(H.323 and other H.245-based) multimedia terminals, 1998.

[3] IETF, *RFC 2543*, 1999 [Referenced: 23.11.1999]

[4] Huovinen, L., Niu S., *IP Telephony*, [Referenced: 19.12.1997]

[5] Lawrence, J., *MGCP Update*, Presentation given at VON Europe 2000,[Referenced: 6.7.2000]

[6] IETF, *SIP Working Group*, [Referenced: 26.10.2000]

[7] IETF, *Megaco Protocol version* 0.8, RFC2885, 2000, [Referenced: 31.8.2000]

[8] Rosenberg, J., *SIP Security*, [Referenced: 8.5.2000]

[9] Thernelius, F., *SIP, NAT and Firewalls*, Master s Thesis, Kungl Tekniska,Högskolan, Stockholm, 2000.

[10] Kotha, S., *Deploying H.323 Applications in Cisco Networks*, White Paper,[Referenced: 2.7.2000]

저자약력

김 용 건

1985년 성균관대 전자공학과졸업
2000년 성균관대 대학원(석사과정)
1984년 삼성전자 통신연구소 입사(연구원)
2000년-현재 삼성전자 네트웍(사) iPCX개발그룹 VoIP개발팀장(수석 연구원)
관심분야 : VoIP Protocol, Internet Security, RTOS, NMS

조 원 상

1978년 동국대학교 전자공학과 졸업
1980년 육군중위제대(ROTC 16기)
1982년 동국대학교대학원 졸업 (전자공학 석사)
1982년 삼성전자 통신연구소 입사 (연구원) 삼성전자 네트웍(사) iPCX개발그룹장(수석연구원),
2001년-현재 삼성전자 네트웍(사) iPCX 사업팀장(상무보)
관심분야 : VoIP, CTI, Corporate CDMA, Mobile IP