FMC 환경에서 VoIP 보안위협, 요구사항 및 아키텍처 구조

한경수*, 정현미*,이강수 *
*한남대학교 컴퓨터공학과
e-mail:psksmail@hnu.kr ,mihj@se.hannam.ac.kr,gslee@eve.hannam.ac.kr

VoIP security threats, requirements and architectures in FMC environment

Kyung-su Han*,Hyun-mi Jung *,Gang-Soo Lee *
*Dept of Computer Engineering, Hannam University

요 약

와이파이 기능이 탑재된 모바일 기기 보급이 확산되면서 무선네트워크를 이용한 많은 서비스가 개발되고 있다. 그중 기존 전화망(PSTN)에서 발전하여 인터넷 네트워크를 이용한, 음성과 데이터 네트워크 융합의 대표적인 인터넷 전화(VoIP)서비스 이용률이 증가하고 있는 추세다. VoIP 기술은 FMC(Fixed Mobile Convergence) 서비스의 기반이 되며, 이에 따라 FMC서비스는 기존의 VoIP 보안위협 및 특성을 상속 받게 된다. 본 논문은 유무선 통합에 의한 여러 가지 유무선 단말, 네트워크 및 서비스 특성에 대한 보안 위협을 상속 받게 되는 FMC 환경에서의 VoIP보안 위협을 소개하고 보안 요구사항을 설계한다. 또한 안전한 FMC서비스를 위해 총체적인 보안망 설계 시 VoIP보안 위협 및 보안요구사항에 적합한 보안솔루션의 아키텍처 구조를 제안한다.

1. 서론

무선네트워크 기능이 탑재된 모바일 기기 보급이 확산되면서 무선네트워크를 이용한 많은 서비스가 개발되고 있다. 이에 따른 네트워크 용량에 대한 부담을 줄이는 방법 중, 유무선 융합서비스 FMC(Fixed Mobile Convergence)가 주목 받고 있다. 모바일 단말을 이용하여 기업 및 가정에서는 인터넷 전화 VoIP(Voice over Internet Protocol)로 사용할 수 있고(고정된 지역을 의미) 그 외의 지역(이동성을 가진 지역을 의미)에서는 3G 이동통신네트워크를 통한 휴대전화로 사용할 수 있어, 저비용·고효율 서비스로써 사용자가 증가하고 있다.

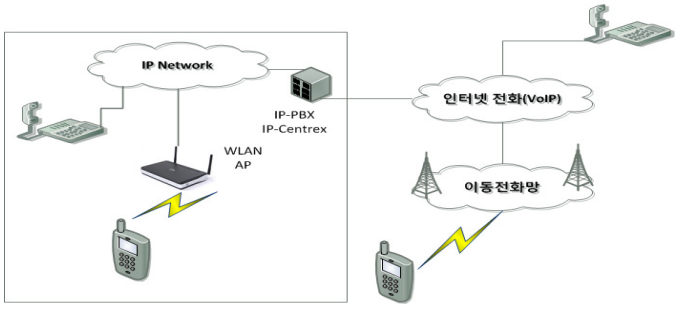
무선네트워크 인프라를 기반으로 한 스마트폰 이용자가 늘어남에 따라 언제 어디서나 자신의 단말을 이용하려는 성향이 강해진다. 이는 곧 4G네트워크의 수요로 이어지기 때문에 FMC시장은 점차 확대되며 이에 따른 보안위협 또한 이슈가 된다.

FMC서비스의 기반인 인터넷 전화 VoIP는 음성과 데이터의 융합뿐만 아니라 동영상까지 하나의 네트워크로 전송하는 TPS(Triple Play Service)로 진화하기 시작했다. 따라서 FMC환경에서 안전한 VoIP서비스 제공을 위한 VoIP 프로토콜의 보안 특성과 IP 기반 환경에서 현재 알려진 취약점 및 잠재적인 보안 위협 유형을 이해하는 것이 중요하며, VoIP 서비스가 FMC 서비스와 결합한 m-VoIP(Mobile-VoIP) 서비스로 확장되기 때문에 이와 관련 보안대책을 수립·이행하는 것이 필요하다.

본 논문은 2장에서 네트워크 융합 기반인 FMC 환경과 이에 따르는 보안이슈를 알아보고, 3장과 4장에서 FMC 서비스의 중심기술인 VoIP 구성과 보안위협 및 보안요구사항에 대하여 중점적으로 분석한다. 5장에서는 안전한 FMC 서비스를 위한 네트워크 설계 시 VoIP 보안 위협 및 보안요구사항에 적합한 보안 솔루션 아키텍처 구조를 제안 하며 결론을 맺는다.

2. FMC구성과 보안 이슈

FMC 구성망은 (그림 1)과 같이, 무선인터넷을 기반으로 저렴한 음성·데이터 통신환경을 제공한다. 무선네트워크 내에서 AP를 통한 IP-PBX와 연동하므로 구내전화와 외부전화통화가 가능하다. 무선 네트워크 구축 및 스마트폰 연동을 통해 기업 내부에서는 무선네트워크와 연결된 유선망을, 외부에서는 이동전화망을 이용한 통화 및 사내 업무를 볼 수 있는 유무선 통합서비스를 구성하여 업무를 수행함에 있어, 기업은 통신비의 절감 효과를 기대할 수 있으며, 구성원은 외부에서도 스마트 오피스를 실현 한다.



(그림 1) FMC망 구성도

위와 같은 FMC서비스는 <표 1>과 같이 Single Mode FMC와 Dual Mode FMC로 나눌 수 있으며, 보통 VoIP와 3G(이동통신)가 가능한 듀얼 모드 휴대폰을 사용한다**[1]**.

<표 1 > Single Mode FMC 와 Dual Mode FMC 비교.

	Single Mode FMC	Dual Mode FMC
비 교	• WPBX를 사용하여, 핸드폰이 위치한 곳에 따라 이동통신망의 접속과 내선 접속으로 구분. • 실내에서 휴대폰 가입자나 유선가입자 사이의 무료통화를 제공. • 외부에서는 이동통신망을 이용한 휴대폰으로 사용. • 내부와 외부 망과의 구별을 위해 접속하는 중계기간 상호 연동이 필요.	• 접속 구분은 single Mode 방식과 동일. • 외부에서도 PBX의 내선으로 접속이 가능하며, Wi-Fi를 통한 Wireless LAN으로 접속. • 무선네트워크만 제공된다면 어느 지역에서도 PBX의 내선으로 접속이 가능.

2.1 FMC 보안 이슈

FMC서비스는 통신환경의 변화에 따라 PSTN(음성, 회선교환 방식)에서 VoIP(인터넷 이용한 음성전달)로 발전하며 모든 통신 수단이 IP화되는 IPT(IP Telephony)로 성장했기 때문에 가능한 기술이다. 이와 같이 단말과 접속망, 서비스가 모바일화 및 융합화 되면서 각각의 많은 보안위협이 상속된다. 아래 <표2>는 FMC 환경에서 발생할 수 있는 대표적인 위협을 나타낸다.

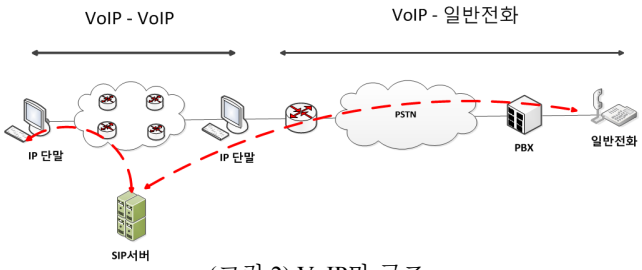
<표 2> FMC서비스 보안 위협**[2]**.

구 분	FMC 위협 유형
단 말	단말기 분실/ 도난
	개인정보 유출
	악성코드/바이러스 감염
접속망	스니핑
	자원 무단 사용
	Man in the meddle Attack (가짜 웹 사이트를 통해 소비자와 조직 간의 통신을 빼내는 컴퓨터 공격)
	Femtocell jamming (가정용 소형 기지국 전파방해)
서비스	DDOS
	VoIP도청, 스팸
	Vishing (Voice Phishing 줄임말)
	Caller Spoofing (발신자번호 속임)
	Cross-Service Attack (복합단말내의 과금이나 배터리 소모 공격등)

FMC환경의 보안 위협 중, 특히 최근 국내 주요 m-VoIP 서비스 테스트 결과 국내 기술로 개발된 m-VoIP는 모두 수·발신 내용이 도청된 것으로 확인됐다. 국내 m-VoIP기술은 국제 표준 프로토콜을 사용하지만 패킷을 암호화하지 않아 양쪽의 통화내용을 도청할 수 있었다. VoIP서비스의 품질보다 가입자 경쟁에만 치중하다보니 무선 통화의 보안 취약성에 대한 기본적인 안내나 경고가 없으며, FMC서비스의 주요기술인 VoIP에 대한 보안피해는 개인 및 기업의 몫이 되기 때문에 안전한 FMC 환경위한 VoIP의 보안문제가 선행되어야 한다**[3]**.

3. FMC환경에서 VoIP구성 네트워크

VoIP구성네트워크는 (그림 2)와 같이 기존 PSTN(회선 교환 방식)과 달리 양단에 각각의 단말 IP폰이 설치되어있다.



(그림 2) VoIP망 구조

VoIP 대 VoIP통신은 PSTN망을 경유하지 않고SIP서버를 통해 단말간 네트워크 주소를 할당하거나, 해당 네트워크로 라우팅 해주며, IP를 갖고 있는 단말은 음성을 패킷으로 변환 처리하여 인터넷을 통해 전달되고, 기존의 인터넷네트워크에서 데이터 패킷을 전달하여 음성을 변환한 패킷 역시 전달이 가능해진다**[4]**. 기존 IP네트워크를 활용해 전화서비스를 통합 구현함으로써 전화 사용자들은 인터넷 환경에서 기존 PSTN망에서 실현 할 수 없었던 유무선 통합 커뮤니케이션(UC, Unified Communication)을 가능하게 한다.

3.1 안전한 FMC서비스를 위한 VoIP 보안 위협 분석

FMC 서비스는 인터넷뿐만 아니라 사설 IP기반망(VPN), 공중전화망(PSTN)등 여러 복합 망에서 연동 되어야 하는 서비스다. 다음은 VoIP의 보안 위협 및 요구사항을 중점적으로 분석한다.

3.1.1 VoIP 보안위협요소 및 대응책

VoIP 기술은 기존 인터넷 프로토콜 기술을 이용하여 음성통신 서비스를 제공하기 때문에 IP기반의 위협을 그대로 상속하며, 그중 FMC환경에서의 공격가능성 및 피해 규모 등을 고려할 때, VoIP SPAM, 서비스오용공격도청, ARP Spoofing 공격(도청), SIP Flooding DOS공격 등은 치명적인 보안상의 위협이다.

<표 3> VoIP 대표적인 보안위협 요소**[5].**

구 분	보안 위협
VoIP SPAM	VoIP 환경에서 광고성 전화나 메시지를 지속적으로 유발시키는 공격.
서비스 오용공격	사용자 정보 변조, 과금 우회, 회피를 통해 정상적인 서비스 이용을 방해하는 공격.
ARP Spoofing 공격(도청)	개인 정보 침해 . 사용자가 점점 증가 하고 있는 IP 전화기간 통화내용을 불법적으로 녹취 하는 침해.
SIP Flooding DOS공격	SIP기반 요청메시지를 보내 DOS공격을 유발할 수 있음.

(1) VoIP SPAM: 사용자 이름이나 도메인 이름 등 스팸 발송자 목록으로 관리하여 스팸 필터링에 사용하는 방식인 블랙리스트와 반대 개념인 화이트 리스트를 고려할 수 있다. 인증을 가진 송신자의 호 와 메시지만 걸러서 수신하는 방식으로써

IM(Instant Message) 스팸에 효과적이다. 하지만 잘 알려진 파밍 공격에 취약성을 들어내고 있어 사용자의 상대 주소정보가 송신자로 인증 받을 수 있는 방법이 문제가 된다. 스팸 예방을 위한 완벽한 솔루션은 현재 존재 하지 않으며 여러 기술의 접목이 필요하다**[6]**.

(2) 서비스 오용공격: 취약한 비밀번호, 적절한 권한제어 없이 국제전화 허용 등으로 인한 과금 우회 공격에 노출되어있다.
대응방안으로 서버의 네트워크 토폴로지 Hiding 기능으로 SIP헤더에 포함된 시그널의 경로 정보를 삭제하여 서비스네트워크에 대한 정보를 은폐한 사용자의 호 메시지만 처리할 수 있어 인가된 단말만 접근 허용 할 수 있도록 개선되어야 한다.

(3) ARP Spoofing 공격: ARP(Address Resolution Protocol)는 IP 주소를 통하여 MAC address로 변환하는 프로토콜로서, 이점을 이용하여 공격자는 MAC주소를 위장하여 프레임을 보내고, 사용자의 단말 MAC테이블에는 IP 와 MAC주소가 다르게 저장되어 사용자의 정보를 도청 할 수 있다.
대응책으로 인터넷 전화망과 데이터네트워크를 분리하여 운영한다면, 데이터네트워크의 공격이 인터넷네트워크로 전이되는 것을 예방할 수 있다.

(4) SIP Flooding DOS공격: VoIP 단말, SIP 서버, 소프트 스위치등 통화를 설정하는 프로토콜(SIP)을 이용하여 통화가 맺어진 후 음성데이터를 전달하는 프로토콜(RTP)을 사용하여 통화가 이루어진다. 통화를 설정하는 데이터가 노출될 경우, SIP 기반 요청메시지를 보내 DOS공격을 유발할 수 있다. 서비스 거부 공격 대응 예방을 위해서 방화벽, IDS등 보안 솔루션은 VoIP트래픽, 응용 계층 프로토콜 분석이 가능한 시스템으로 설치하여야 하며 주요 VoIP서버는 방화벽 등 보안 솔루션으로 보호해야한다**[7]**.

4. FMC 서비스에서의 VoIP 보안요구사항

FMC 서비스 구현을 위해서는 가능한 위협에 대비한 사용자 중심(개인 및 기업)의 보안요구사항이 필요하므로 사용자 단말 및 IP, 서비스, 개인정보, 인증 등 네트워크 인프라 기반 VoIP 보안요구사항을 분석한다.

4.1 FMC 교환 장비 IP-PBX보안

FMC 서비스는 교환 장비 IP-PBX를 통하여 내·외부의 통화가 가능하기 때문에 IP-PBX를 대상으로 하는 공격에 대한 표준 암호화 알고리즘(sRTP,TLS,AES,SDES)적용으로 도청 및 해킹을 방지해야한다**[8].**

4.2 TTA의 IPv6 인증 보안솔루션 필요

VoIP, FMC기기 등 인터넷 기반의 다양한 서비스가 늘어남에 따라 IPv4의 32비트체계 IP가 고갈되고 있으며 IPv6 128비트 체계로 변화 되고 있다. IP주소체계가 변화에 대비하여 TTA(Telecommunications Technology Association)는 검증 기준에 적합한 IPv6기능에 대한 인증을 하고 있으며 IPv4 체계에 맞춰 개발된 보안장비도 IPv6으로 전환이 필요한 시점이다.

4.3 VoIP개인정보의 관리적, 기술적 조치 기준

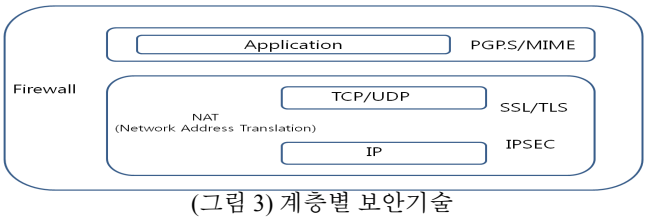
이용자의 개인정보를 기록, 수집하는 때에는 개인정보가 분실, 도난, 누출, 변조, 또는 훼손되지 않도록 방송통신위원회 고시 제 2009-21호에 따를 조치를 취해야 한다.

4.4 X.509 인증

VoIP단말기는 무선네트워크가 설치된 곳이라면 통신이 가능하므로 시스템 설정 정보를 자동적으로 다운로드 할 수 있다. 따라서 권한이 없는 사용자가 단말을 지니고 있더라도 사용가능해 지므로 이용권한이 없는 사용자의 인증이 요구 된다. X.509 시스템에서의 인증서는 X.500 규약에 따라 서로 구별되는 공개키를 가진 인증서를 발행한다. RSA 나 EAP기반의 암호화 방법을 적용하며, RSA는 PKI기반이고 본인만 알고 있는 개인키와 누구나 알고 있는 공개키로 구성되어 있다. 본인의 개인키로 암호화된 데이터는 공개되어 있는 공개키를 통해 해독이 가능하여 데이터 무결성을 보장할 수 있다.
802.1x표준에서 제공하는 EAP프로토콜은 무선네트워크 사용자와 AP, 인증 서버간의 인증을 수행하며 단순히 접근을 승인하거나 거부하는 기능을 한다**[9]**.

4.5 계층별 VoIP 보안 기술 적용

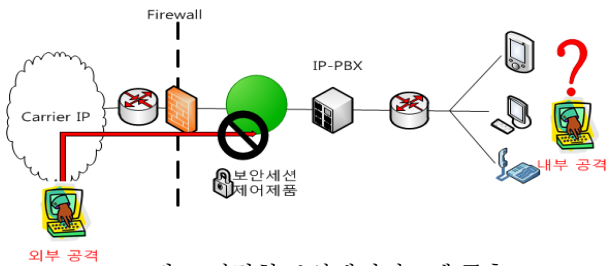
DoS/DDoS Attack, ICMP/DHCP Attack, UDP/MAC/TCP Sync Flooding, 바이러스 감염에 의한 트래픽 발생 등 네트워크의 과부하 발생, 서버의 정상적인 서비스 장애 발생 원인이 된다. 따라서 이러한 공격은 Data 영역만의 문제로 생각할 수 없으며. 네트워크 인프라를 통해 제공되는 VoIP 서비스에 치명적인 영향을 미칠 수 있기 때문에 (그림 3)과 같이 VoIP 시스템에 적용 가능한 보안 기술을 TCP/IP 계층, Application, Transport, Internet Layer 에서 구분하여 적용 할 수 있다**[10][11]**.



(그림 3) 계층별 보안기술

5. 내/외부 보안 아키텍처의 제안

안전한 FMC환경을 위한 VoIP 위협 및 보안요구사항을 만족하는 보안제어시스템을 설계, 개발이 필요하며, 보안 솔루션을 기업에서는 비용절감을 위해 보통 IP-PBX상단에 한 대를 위치시킨다.

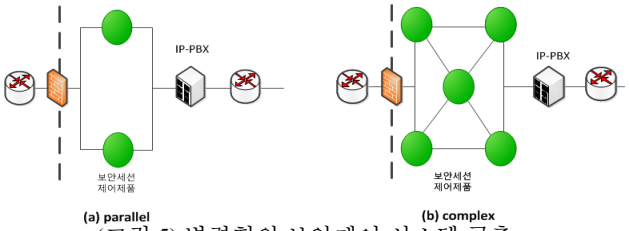


(그림 4) 직렬형 보안제어시스템 구축

(그림 4)와 같이 직렬구조의 보안제어 시스템설계는 외부 공격에대한 방어는 고려되지만 내부 공격에 대한 방어와 암호화(TLS/SRTP)적용이 불가능하며, 내부 사용자에 대한 인증이 어렵다.

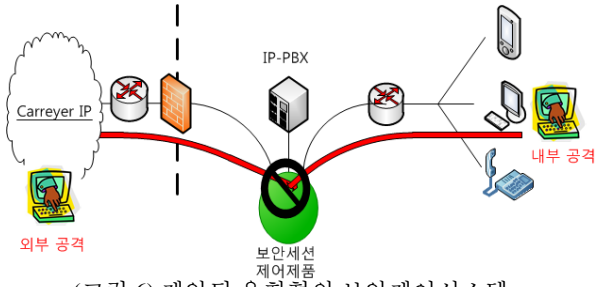
FMC서비스의 핵심은 VoIP 게이트웨이를 사용함으로써 기존 전화선을 IP- PBX에 연결하여 PSTN 선을 통해 전화를 걸고 받을 수 있다. 기존 PBX는 단순 음성통화만 이용이 가능하고, 대용량 설비와 복잡한 구내 선로 배선으로 불편했다. 이와 달리 IP-PBX는 사내 LAN과 통합하여 유지보수가 간단하고, 구성 장비가 간단하여 설치 공간이 절약되며, IP기반으로 기존 기업의 다양한 어플리케이션 통합이 유리하다.

IP-PBX 자체 소프트웨어에서의 보안기능으로 허용되지 않은 IP주소에서 수신되는 SIP, Option 메시지는 무시· 차단하는 기능과, SSH, ICMP, 웹 접속에 대하여 차단하는 기능(허용목록에 추가시 접속가능),차단 목록 삭제 가능을 가지고 있다. 하지만, FMC서비스에서 유무선 융합으로 인한 수많은 보안위협을 IP-PBX의 자체 보안 기능만으로 신뢰하기 힘들며, 국내 IP-PBX제조사별로 보안기능은 천차만별이다.



(그림 5) 병렬형의 보안제어 시스템 구축

IP-PBX를 보안하기 위한 방법으로 (그림 5)와 같이 (a)형과 (b)형구조의 보안솔루션을 기존 방화벽을 앞에 두고 설치한다면, IP기기사이의 통신에서는 양방향에서 공격이 가능하기 때문에 결과적으로 외부공격에 대한 보안의 단계를 높일 뿐만 아니라 비용에 대한 부담도 커지게 된다. FMC서비스는 IP-PBX자체를 보안할 수 있는 솔루션 설치가 필요하다.



(그림 6) 제안된 우회형의 보안제어시스템

대부분 기업에서는 모든 구성을 IP-PBX 및 IP폰으로 구성하여 업무를 극대화 시키려한다. 내·외부 IP기기간의 통신은 IP-PBX서버에 등록되며 전화를 걸고자 할 때 IP-PBX에게 연결을 확립하도록 요청한다. IP-PBX는 모든 전화 사용자의 SIP주소 디렉토리를 가지고 있기 때문에 FMC구성 망 설계 시 (그림 6) 과 같은 인증된 보안제어시스템을 IP-PBX에 우회 설치를 제안 한다. 이동통신망(외선망)과 IP전화에 의한 내선망 사이에서 중계역할을 하는 IP-PBX에 대한 보안 공격은 내외부적으로 모든 통신이 보안솔루션을 거쳐 IP-PBX로 연결되어 안전한 통신을 할 수 있게 구성해야 한다. 내·외부 보안 위협 공격에 대한 보안제어 시스템은 VoIP 트래픽 차단기능이 제공되어야하고, 내부의 Worm, Fuzzing등을 방어할 수 있으며, 암호화를 적용할 수 있어야 한다. 우회 설치는 내부로부터 DoS/DDoS방어가 가능하며 내부 사용자 인증이 강력해 질수 있고 외부 공격에 대한 방어 또한 강화 될 수 있다.

<표 4> 분석 및 평가표

아키텍처 / 기준	직렬형 보안제어시스템	병렬형 보안제어시스템	제안된 시스템
보안성	외부보안 강화	외부보안 등급상승	내·외부보안 강화
경제성	저비용	고비용	저비용
설계 편의성	단순	복잡	단순
사용 환경	PSTN (회선교환)	PSTN (회선교환)	FMC, VoIP (네트워크를 통 한패킷교환방식)

6. 결론

FMC (유무선 융합)기술에서 보안은 기존 무선인터넷 인프라에 비하여 수많은 보안위협과 더불어 인터넷전화망의 보안위협 또한 고려해야한다. 이에 아직까지 완전한 보안은 불가능하다고 볼 수 있으며 저비용-고효율적인 보안방안을 구축해야 한다.

본 논문은 FMC 서비스에서 VoIP관점의 보안을 중점적으로 고려하였다. 나아가 서비스를 위한 convergence 관점에서의 보안 통신망의 구축인 데이터와 음성데이터를 암호화 하는 방안이 IETF국제 표준으로 제정되었고 더불어 FMC 환경에서 VoIP의 원활한 서비스를 위한 보안 기술, Data, 애플리케이션 환경을 고려한 보안 솔루션 도입이필요하다.

제안된 시스템은 내/외부 보안솔루션의 설치와 Data 네트워크부터 고객이 직접 사용하는 단말기에 이르는 총체적인 망 설계가 안전한 FMC서비스를 위한 보안의 단계를 높여 준다.

앞으로 IP-PBX의 보안 소프트웨어와 서브 보안솔루션의 개발은 향후과제로 남긴다.

참고문헌

[1] 이중협, “Fixed Mobile convergence” LG-Ericsson Info radar, 2009.6, pp. 08~11.

[2] 김환국, “WiFi and FMC Service Security”, 한국인터넷진흥원 기술세미나, 2010.6, pp. 07.

[3] www.seoul.co.kr, http://www.seoul.co.kr//news/newsView.php?code=seoul&id=20110323001012&keyword=mvoip,서울 신문 보도 자료, 2011.3.23.

[4] 조혜인 외, “Tunneling 기법을 적용한 VoIP 보안 대응 방안 연구”, 전북대학교 정보 통신 공학, 2010 .6.28, pp. 33～37.

[5] 김지연 외, “정보 보호를 고려한 행정기관 FMC도입 및 활성화 방안연구”. Internet and Inform Security, 제1권 제1호, 2010.5, pp. 126～145.

[6] 정재훈, "인터넷 전화(VoIP)보안위협 및 대책"방송통신위원회, Biz+Comm Winter 2009, pp. 22.

[7] 이재일, “VoIP 위협과 대응방안”, 한국정보보호 진흥원, KISA 발표자료, 2007.5. pp. 18~25

[8] 김환국 외, “안전한 F 환경구축을 위한 보안요구사항 연구”, 한국인터넷진흥원, 2010.6.20. PP. 793~796.

[9] 이윤경,한종욱, "X.509 PKI인증서 프로파일 분석",한국해양 정보 통신학회 춘계학술대회, 2006. pp.757~760.

[10]KISA, “VoIP보안권고 해설서”, 한국인터넷진흥원, 2010.6.

[11] 송주석 외, “모바일환경 에서 경량화 된 VoIP인증 및 암호기술 연구”, 한국인터넷 진흥원 연구개발 결과보고서, 2010.10, pp.757~760.