VoIP 보안 위협과 보안요구사항 분석 및 보호프로파일 개발

홍원순*, 최용준**, 성윤기*, 심원태*
*한국정보보호진흥원 평가기획팀
**한국시스템보증
e-mail:wshong@kisa.or.kr

Security Threats and Security Requirements Analysis of VoIP and Protection Profile Development

Won-Soon Hong*, Yong-Joon Choi**, Yune Gie Sung*, Won-Tae Sim*
*Korea Information Security Agency
**KOSYAS

요 약

인터넷망을 이용하여 음성 및 영상통화를 제공하는 VoIP(인터넷전화)서비스가 확대되고, VoIP 서비스가 인터넷망을 이용함에 따라 기존의 인터넷망에서 제기된 보안위협이 증가하고 사이버 공격에 노출되고 있다. 이에 따라 본 고에서는 국제 표준인 공통평가기준(ISO 15408)에서 규정된 방법에 따라 VoIP 서비스를 제공하는 IP Phone 및 IP PBX시스템이 노출되는 사이버 상의 보안위협사항을 도출하고, 보안목적과 VoIP 및 IP PBX 시스템 보안위협에 대응할 수 있는 보안요구사항을 정의하였다.

1. 서론

최근 급속히 보편화된 VoIP(인터넷 전화:Voice Over Internet Protocol)는 번호이동성 제도시행, 통화품질의 지속적 향상, 요금경쟁력 등으로 향후 VoIP 서비스 가입자 수가 급격하게 증가할 것으로 전망되고 있다. 한편, VoIP는 기존의 일반전화와 달리 인터넷망을 이용하여 음성 및 영상통화를 제공하는 서비스이다. 따라서 악성 트래픽 공격으로 서비스가 중단되거나 데이터가 변조될 수 있어서 최근 많은 이슈가 되고 있다.

본 논문에서는 IP Phone 및 IP PBX시스템의 보안위협, 가정사항 등 보안문제를 정의하고, 위협에 대응하기 위한 보안목적 도출을 통해 IP Phone 및 IP PBX시스템이 갖춰야 하는 보안요구사항 등을 분석한다.

2. VoIP 보안 위협 및 취약성

VoIP 서비스에 대한 보안 위협은 IP 네트워크 상에서 음성/영상 등을 데이터화하여 전송하는 IP 기반 방식으로 하기 때문에 IP 기술에서 나타났던 위협들을 그대로 상속하며, 새로이 사용되는 VoIP 기술을 사용함으로 인하여 나타나는 새로운 위협들이 존재한다. VoIP에 가해질 수 있는 보안 위협을 정리하면 <표 1>과 같다. 통화내용 도청은 기존 유선전화에서의 물리적 접근에 의한 도청과 비교해볼 때, VoIP의 경우 해외에서 해킹을 통한 원격도청이 가능하다는 차이가 있으며, VoIP 스팸은 기존의 스팸과 비교하여 저렴한 비용 및 대량 발송의 편의성으로 인해 커다란 사회문제로 대두될 것이 예상된다. 도청 행위자체는 서비스의 질에 직접적인 위협을 가하지는 못하지만, 서비스거부 공격, 서비스오용, VoIP 스팸은 VoIP 서비스의 질에 직접적인 타격을 주어 서비스 사용자에게 큰 피해를 야기 시킬 수 있다.

<표 1> VoIP 보안 위협

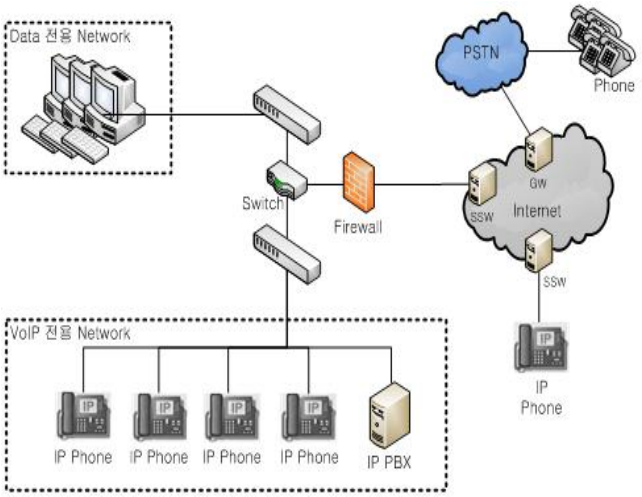
분류	내 용
통화내용 도청	o 사용자의 통화내용을 공격자가 청취
서비스거부 공격	o 다수 공격자에 의한 인터넷전화 시스템 마비 시도 o 특정 단말에 대한 인터넷전화 통화 방해
서비스 오용	o 정상적인 사용자의 등록정보 등을 위조, 불법 무료통화
호 가로채기	o 등록정보를 가로채거나 내용을 수정하여 신원을 속임으로써 통화가 불가능하게 만들거나 통화 내용을 가로챔
VoIP 스팸	o 자동화된 도구를 이용하여 불특정 다수에게 스팸발송

3. 운영환경

TOE(Target of Evaluation, 평가대상)는 IP Phone간 안전한 통신을 위해 암호화된 호 설정 데이터 및 미디어 데이터를 송·수신하며, IP Phone간 통신시 호 처리 및 제

어, 불법 Phone에 대한 접근통제, IP Phone에 대한 인증 및 관리 기능, 감사데이터 생성 및 조회 등의 보안감사 기능을 수행한다.

VoIP 서비스를 안전하게 이용하기 위해서 TOE 운영환경 내 외부망과의 연결지점에 침입차단시스템을 설치하여 논리적 또는 물리적으로 VoIP 서비스 망과 데이터 망을 분리하고, 스위칭 환경의 네트워크를 구성하며, DHCP 서버 등을 이용하여 IP Phone에 사설 IP를 할당하여 운영함으로써 운영환경에 대한 보안을 향상시킬 수 있다. 그리고 논리적 또는 물리적으로 분리된 VoIP 서비스 망에 IP Phone과 IP PBX를 설치함으로써 사용자는 안전한 VoIP 서비스를 이용할 수 있는 환경이 된다. TOE가 설치되어 운영되는 환경은 아래 (그림 1)과 같다.



(그림 1) 운영환경

4. 보안문제정의 및 보안목적

4.1 보안문제정의

보안문제는 TOE 및 운영환경에 의해 대응되어야 하는 위협, 수행되어야 하는 조직의 보안정책, 지원되어야 하는 가정사항을 서술하고 있으며, 다음 <표 2>는 IP Phone 및 IP PBX시스템의 보안문제정의에 해당된다.

TOE 및 운영환경에 의해 대응되어야 하는 위협은 위협원, 자산, 공격 행동의 관점에서 서술되어야 한다. VoIP 스팸 대응기술 관련 연구가 진행 중이지만 IP Phone에 현재 구현된 사례가 많지 않음을 고려하여 본 보호프로파일에서는 VoIP 스팸 위협에 대한 부분은 다루지 않았다.

가정사항은 TOE가 사용될 환경에 대한 보안성을 설명하고, 조직의 보안정책은 TOE가 따라야 하는 조직의 보안정책 또는 규칙을 식별해서 서술한다.

<표 2> 보안문제정의

위협	조직의보안정책	가정사항
T.가장	P.감사	A.물리적보안
T.기록실패	P.비밀성	A.사용자단말
T.도청	P.안전한관리	A.상호호환성
T.비정상정인패킷발송	P.접근통제	A.신뢰된관리자
T.암호해독	P.평문전송	A.운영체제보강
T.연속인증시도		A.운영환경분리
T.저장용량소진		A.표준프로토콜
T.저장데이터훼손		
T.전송데이터무결송훼손		
T.재사용공격		
T.통신방해공격		

4.2 보안목적

보안목적은 보안문제정의에서 서술된 문제에 대한 해결책을 표현한다. 즉, 보안목적은 식별된 모든 위협을 대응하는데 적합해야 하며, TOE 보안목적 및 운영환경에 대한 보안목적으로 분류해서 정의한다. TOE 보안목적은 TOE에 의해서 직접적으로 다루어지는 보안목적이고, 운영환경에 대한 보안목적은 TOE가 보안기능성을 정확히 제공할 수 있도록 운영환경에서 지원하는 비기술적/절차적 수단에 의해 다루어지는 보안목적이다. <표 3>은 TOE 및 운영환경에 대한 보안목적을 보여준다. IP PBX에만 해당되는 TOE 보안목적은 O.감사, O.비정상적인패킷차단, O.저장데이터보호, O.정보흐름통제, O.접근통제이고, IP PBX에만 해당되는 운영환경에 대한 보안목적은 OE.물리적보안, OE.운영체제보강, OE.타임스탬프이다.

VoIP서비스에 대한 가장 큰 보안위협 중 하나인 T.도청은 송수신 데이터에 대해 비밀성 및 무결성을 보장하고, 사용자의 선택에 따라 보안통신을 가능하게 하므로 O.전송데이터보호에 대응된다. O.전송데이터보호는 T.전송데이터무결성훼손, T.통신방해공격, T.재사용공격에도 대응하며, 조직의 보안정책 P.비밀성, P.평문전송을 수행하는데 필요하다.

<표 3> 보안목적

TOE 보안목적	운영환경에 대한 보안목적
O.감사	OE.물리적보안
O.비정상적인패킷차단	OE.신뢰된관리자
O.식별및인증	OE.운영체제보강
O.안전한관리	OE.운영환경분리
O.저장데이터보호	OE.타임스탬프
O.전송데이터보호	OE.표준프로토콜
O.정보흐름통제	
O.접근통제	
O.키보안	

5. 보안기능요구사항

보안기능요구사항은 기능 컴포넌트에 따라 TOE에 대한 기능요구사항을 정의하며, TOE 보안목적을 변환한 것이다. 다음의 <표 4>에서는 TOE의 보안기능요구사항을 보여준다. 보안감사, 암호 지원, 사용자 데이터 보호, 식별 및 인증, 보안관리, TSF 보호 등 총 6개의 보안기능클래스와 총 34개의 보안기능 컴포넌트로 구성되어 있다. 보안기능클래스 중 IP PBX시스템에만 요구되는 보안기능으로는 보안감사, 사용자 데이터 보호, TSF 보호 클래스가 해당된다.

<표 4> 보안기능요굿사항

보안기능 클래스	보안기능 컴포넌트	
보안감사	FAU_ARP.1	보안 경보
	FAU_GEN.1	감사 데이터 생성
	FAU_SAA.1	잠재적인 위반 분석
	FAU_SAR.1	감사 검토
	FAU_STG.1	감사 증적 저장소 보호
	FAU_STG.3	감사 데이터 손실 예측시 대응행동
	FAU_STG.4	감사 데이터의 손실 방지
암호 지원	FCS_CKM.1	암호키 생성
	FCS_CKM.2	암호키 분배
	FCS_CKM.4	암호키 파기
	FCS_COP.1	암호 연산
사용자 데이터 보호	FDP_ACC.1	부분적인 접근통제
	FDP_ACF.1	보안속성에 기반한 접근통제
	FDP_IFC.1(1)	부분적인 정보흐름 통제(1)
	FDP_IFC.1(2)	부분적인 정보흐름 통제(2)
	FDP_IFF.1	단일 계층 보안 속성
식별 및 인증	FIA_AFL.1(1)	인증 실패 처리(1)
	FIA_AFL.1(2)	인증 실패 처리(2)
	FIA_ATD.1	사용자 속성 정의
	FIA_UAU.2(1)	모든 행동 이전에 사용자 인증(1)
	FIA_UAU.2(2)	모든 행동 이전에 사용자 인증(2)
	FIA_UAU.7	인증 피드백 보호
	FIA_UID.2(1)	모든 행동 이전에 사용자 식별(1)
	FIA_UID.2(2)	모든 행동 이전에 사용자 식별(2)
보안 관리	FMT_MOF.1	보안기능 관리
	FMT_MSA.1	보안속성 관리
	FMT_MSA.3	정적 속성 초기화
	FMT_MTD.1(1)	TSF 데이터 관리(1)
	FMT_MTD.1(2)	TSF 데이터 관리(2)
	FMT_MTD.1(3)	TSF 데이터 관리(3)
	FMT_SMF.1	관리기능 명세
	FMT_SMR.1	보안 역할
TSF 보호	FPT_RPL.1	재사용 공격 탐지 및 대응행동
	FPT_TST.1	TSF 자체 시험

IP Phone 및 IP PBX시스템에 각각 요구되는 보안기능요구사항은 <표 5>와 같다. IP Phone의 보안기능은 도청, 서비스거부 및 서비스 오용 위협에 대한 대응방안으로 암호화 기능 등이 요구된다. 즉, 암호화, 사용자 식별·인증, 암호키 속성. 식별·인증 데이터 관리, 관리기능 명세, 보안역할 등이 해당된다.

<표 5 > TOE 구성요소별 보안기능요구사항

보안기능요구사항	IP Phone	IP PBX
FAU_ARP.1	X	O
FAU_GEN.1	X	O
FAU_SAA.1	X	O
FAU_SAR.1	X	O
FAU_STG.1	X	O
FAU_STG.3	X	O
FAU_STG.4	X	O
FCS_CKM.1	O	O
FCS_CKM.2	O	O
FCS_CKM.4	O	O
FCS_COP.1	O	O
FDP_ACC.1	X	O
FDP_ACF.1	X	O
FDP_IFC.1(1)	X	O
FDP_IFC.1(2)	X	O
FDP_IFF.1	X	O
FIA_AFL.1(1)	O	O
FIA_AFL.1(2)	X	O
FIA_ATD.1	X	O
FIA_UAU.2(1)	O	O
FIA_UAU.2(2)	X	O
FIA_UAU.7	O	O
FIA_UID.2(1)	O	O
FIA_UID.2(2)	X	O
FMT_MOF.1	X	O
FMT_MSA.1	X	O
FMT_MSA.3	X	O
FMT_MTD.1(1)	O	O
FMT_MTD.1(2)	O	O
FMT_MTD.1(3)	X	O
FMT_SMF.1	O	O
FMT_SMR.1	O	O
FPT_RPL.1	X	O
FPT_TST.1	X	O

6. 결론

본 연구에서는 국가·공공기관, 기업 등에서 사용되는 VoIP의 IP Phone 및 IP PBX가 갖추어야 하는 위협, 보안목적 및 보안기능요구사항 등을 정의하였다. IP Phone 및 IP PBX 개발업체에서 VoIP 보호프로파일을 수용하여 제품을 개발하였을 경우, VoIP의 기본적인 보안요구사항을 만족함을 의미한다. 또한, VoIP의 보안관리에 있어서 IP Phone 및 IP PBX를 안전하게 운영하기 위한 요구사항을 정의할 때 VoIP 보호프로파일을 참고자료로 활용할 수 있다. 또한 IP Phone 및 IP PBX 개발자는 보호프로파일에서 정의된 내용을 참고하여 보안목표명세서를 작성할 수 있다.

참고문헌

[1] 정보보호시스템 공통평가기준, 행정안전부, 한국정보보호진흥원, 2008. 7. 16

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, CCMB, 2006. 9

[3] Common Methodology for Information Technology Security Evaluation Part 2, Version 3.1, CCMB, 2006. 9

[4] BCN/VoIP 정보보호 대책에 관한 연구, 한국정보사회진흥원, 2006. 12. 22

[5] 인터넷전화 보안기술 세미나 자료집, 방송통신위원회, 한국정보보호진흥원, 2008. 12. 9