□특집□

정보보호 기술 분류

고 승 철† 성 맹 희††

◈ 목 차 ◈

요 약 문

본 기술문서는 정보보호 기술 중장기 개발 계획을 수립하기 위한 사전단계로 정보보호 기술분류에 관한 내용을 기술한다. 먼저 정보화 추진에 의하여 부수적으로 발생 가능한 문제점 및 그 문제점을 유발하는 정보통신망 안전 위협 요소와 문제점과 위협요소간의 상관관계를 기술한다. 위협요소를 방지하는 기술적 대책을 고찰하며 대책별로 필요한 상세 기술을 정의하고 이를 분류한다. 우리는 추후 기술별로 국내 현황 및 외국 동향을 분석하며, 이를 근거로 정보보호 중장기 기술개발 계획을 수립하고자 한다.

1. 서 론

미국의 엘 고어 부통령이 국가 정보화(National Information Infrastructure)와 정보화 사회(National Information Society)를 주장한 이래, 우리 나라를 포함한 세계 각국은 국가별 정보화를 추진하고 있으며, 현재 국제 사회는 세계 정보화(Global Information Infrastructure) 및 정보화 사회(Global Information Society)를 추진하고 있다. 또한 국내 및 국제 사회에서는 정보화 추진에 의하여 부수적으로 발생 가능한 문제점 최소화, 즉 국가 중요 정보보호, 국민 개개인의 프라이버시 보호, 마약 등의 국제 범죄 예방, 인터넷을 통한 전자 상거래시의 세금 부과 문제 등을 해결하기 위하여 국가별로 정보 보호와 관련된 제도 및 기술 개발을 추진하고 있으며, OECD를 통하여 국제 협력을 도모하고 있다.

이러한 국제 추세에 비추어 볼 때, 세계 최고 수준의 정보보호 기술 확보 및 관련 중장기 계획 수립이 시급하며, 이를 위하여 먼저 정부 및 한국정보보호센터를 중심으로 산업계, 연구계, 학계의 협동 연구가 필수적이라고 할 수 있다.

본 기술문서는 정보보호 기술 중장기 개발 계획을 수립하기 위한 사전단계로 정보보호 기술 분류에 관한 내용을 고찰한다. 먼저 정보화 추진에 의하여 부수적으로 발생 가능한 문제점 및 그 문제점을 유발하는 정보통신망 안전 위협 요소와

† 정회원 : 한국정보보호센터 수석연구원
†† 정회원 : 한국정보보호센터 연구원

문제점과 위협요소간의 상관관계를 기술한다. 위협요소를 방지하는 기술적 대책을 고찰하며 대책별로 필요한 상세 기술을 정의하고 이를 분류한다. 우리는 추후 기술별로 국내 현황 및 외국 동향을 분석하며, 이를 근거로 정보보호 중장기 기술개발 계획을 수립하고자 한다.

2. 정보통신망 위협요소와 문제점

가. 정보보호 관련 문제점

정보화 추진에 따른 부수적 문제점중의 핵심은 바로 정보 자산에 직접적으로 악영향을 미치는 사건이라고 정의되며, 구체적으로 정보 자산과 관련된 정보의 노출사건, 데이터가 중도에서 위, 변조되는 사건, 고의적으로 정보통신 시스템의 장애를 유발하는 사건 및 부정한 방법으로 정보 자산을 사용하는 사건을 들 수 있다

- ㅇ 정보 누출(Information leakage)

통신망 도청에 의하여 전송되는 정보가 누출되는 사건을 의미하며, 주요 기법은 통신로 태핑, 통신 단말기에서 방출되는 전자파 수집 및 트래픽을 분석에 의한 정보 추측 등을 들 수 있다.

- ㅇ 데이터 위변조(Integrity violation)

데이터를 부정한 방법으로 위조, 변조, 또는 파괴하는 사건

- ㅇ 시스템 장애 유발(Denial of service)

시스템이 정상적으로 동작하는 경우에도, 정당한 권한을 가진 자가 정보 자산을 사용할 수 없도록 악의적으로 정보 통신 시스템 장애를 유발하는 사건

- ㅇ 정보자산 부정사용(Illegitimatc use)

비인가자가 부정적인 방법에 의하여 정보 자원(컴퓨터, 통신 기기 등)을 사용하며 데이터를 열람하는 사건

나. 정보통신망 안전 위협요소

- ㅇ 도청

송수신 양단간의 통신 선로 또는 통신기기의 전자파를 수집하여 정보를 유출하는 방식으로 Wiretapping, 전자파 수집, 무선주파수 가로채기 등

- ㅇ 신분 위장

자신의 신분을 정당한 사용자(타인)의 명의로 위장하여 시스템에 침투, 비인가된 정보를 열람, 위변조 하거나 또는 송신, 수신중인 통신 선로를 조작한 후, 정당한 송, 수신자에 허위 정보를 전송하여 통신 내용을 가로채는 행위

- ㅇ 전송 메시지의 내용 부인

정당한 방법으로 메시지를 송신 또는 수신한 후, 고의적으로 메시지의 내용을 부정하는 행위 (예: TV 100대를 컴퓨터 통신에 의하여 1,000만원에 구매 계약을 맺은 후, 고의적으로 구매자 또는 판매자가 계약 사실 또는 내용을 부인하는 행위)

- ㅇ 부당 목적 S/W 은닉

정보통신망의 안전성을 저해할 목적으로, 통신 서버 등의 중요한 컴퓨터에 트로이 목마, 트랩 도어, 악성 바이러스 등을 은닉하는 행위

- ㅇ 시스템 보안 관리 미비

시스템의 보안관리 대책이 미비하거나 또는 관리자 또는 사용자가 관리 대책을 준수하지 않아서 정보통신망 또는 컴퓨터 시스템의 안전을 저해하는 사건

(관리자 또는 사용자 비밀번호 분실, 절도, 플라피 디스크 등의 정보 매체 관리 미비)

3. 안전 위협요소에 대한 기술적 대책

전장에서 언급한 안전 위협요소에 대하여 일반적으로 관리적 측면과 기술적 측면으로 대책을 수립하여 문제점을 해결한다. 본 기술문서에서는

<표 1> 안전 위협요소와 문제점

위협요소 \ 문제점		정보누출	데이터 위변조	시스템 장애유발	정보자산 부정사용	비 고
도 청	통신로 태핑	○				수 동 적 위협요소
	전자파 수집	○				
	RF 가로채기	○				
	트래픽 분석	○				
위 장	신분 위장	○	○	○	○	능 동 적 위협요소
	권한 위배	○	○	○	○	
	서비스 사기		○	○	○	
내용 부인	송신 내용 부인		○			전자상거래, 전자결재 위협요소
	수신 내용 부인		○			
부당목적 S/W 은닉	트로이 목마	○	○	○	○	
	트랩 도어	○	○	○	○	
	바이러스			○		
시스템 보 안 관리 미비	비밀정보 발설	○				
	패스워드 분실/절도	○	○	○	○	
	물리적 침투	○	○	○	○	
	부정 자원 소모			○		

기술적 대책을 기술한다.

○ 인증 기술(Authentication)
송,수신자가 상대방의 신원을 확인, 식별하는 기술.

○ 접근통제 기술(Access Control)
비인가자가 정보통신망 자산(컴퓨터, 통신 기기, 데이터 베이스, 응용 소프트웨어 등)을 부정한 방법으로 사용하는 것을 방지하는 기술

○ 정보 내용 보호 기술(기밀성, Confidentiality))
비인가자가 부당한 방법으로 정보를 입수한 경

우에도 정보의 내용을 알 수 없도록 하는 기술. 암호 기술이 정보 내용을 보호할 수 있는 가장 효과적인 기술임.

ㅇ 데이터 위변조 방지 기술(Integrity)

데이터가 전송 도중 또는 데이터 베이스에 저장되어 있는 동안 악의의 목적으로 위조 또는 변조되는 것을 방지하는 기술

ㅇ 데이터 내용 부인 방지 기술(Non-Repudiation)

송수신 당사자가 각각 전송된 데이터의 내용을 추후 고의적으로 부인하는 것을 방지하는 기술

<표 2> 안전 위협요소와 문제점

위협요소 \ 기술		인증	접근통제	데이터 내용보호 (암호화)	위·변조 방 지 (무결성)	데이터 내 용 부인방지	바 고
도 청	통신로 태핑			○			TEMPEST
	전자파 수집			○			
	RF 가로채기						
위 장	신분 위장	○					
	권한 위배		○				
	서비스 사기	○					
내용 부인	송신 내용 부인					○	
	수신 내용 부인					○	
부당목적 S/W 은닉	트로이 목마		○		○		
	트랩 도어		○		○		
	바이러스		○		○		

4. 정보보호 기술별 분류

전장에서 기술한 정보보호 기술별로 세부 방식 및 주요 내용을 <표 3>에서 기술한다.

<표 3> 정보보호 기술분류

기 술	구 분	세 부 방 식	비 고
인증 기술	일반적 기술	비밀번호	패스워드
		도전/응전 프로토콜	일회용 패스워드
		주소 기반 방식	Firewall
	암호적 기술	비밀키 방식	Kerberos
		공개키 방식	RSA,D-H, OSS, ESIGN,
		ID 기반 방식	FFS, GQ, Schnorr
접근통제 기 술	접근통제정책	접근통제 정책	개인기반정책, 그룹기반정책, 기능기반정책, 보안등급기반정책, 범주기반정책,
	접근요구여과	접근통제 장치	접근제어리스트, 보안꼬리표, 패스워드 기반 장치, FTAM control
		망 접근통제	입력통제, 출력통제, 통신노드통제, 포워딩 접근통제
		접근제어 정보관리	정보생성, 분배, 저장, 파기, 재생
	접근요구금지	정보흐름 모델	
		라우팅 제어	망 데이터 접근통제, 망 연결통제
데 이 터 내 용 보호기술 (암호기술)	암호 설계	비밀키 알고리즘	블록 알고리즘, 스트림 알고리즘
		공개키 알고리즘	인수분해 기반, 이산대수 기반
		키 관리	키 생성, 분배, 저장, 파기, 재생
	암호 분석	분석 기법 개발	암호문공격, 기지평문공격, 선택평문공격, 선택암호문공격, 인수분해, 이산대수
		분석 Tool 개발	고속연산시스템에 의한 분석 S/W 개발, 분석 H/W 개발
	암호 구현	S/W에 의한 구현	
		H/W에 의한 구현 방식	고속 연산용 집적회로 구현 (RSA 768/RSA 1024/ECC 250)
위·변조 방지기술 (무결성)	일방향 함수	해쉬, 에러탐지코드	CRC, SHA, MD5
	암호적 기술	블록 암호 이용	DES-CBC-MAC
데 이 터 내 용 부인방지 기 술	송신 부인 봉 쇄	송신자 디지탈 서명	서명 생성, 서명 확인, 공개키 방식
		TTP의 전자서명	서명 생성, 서명 확인, 공개키 방식
		TTP의 서명토큰	비밀키 방식
		Time Stamp	
	수신 부인 봉 쇄	수신자 디지탈 서명	서명 생성, 서명 확인,공개키 방식
		수신상황 보고	e-mail, EDI
	TTP	TTP 역할	키 보증, 송수신 ID 보증, 현황기록, Time-stamping, 수신 대리, 중재
		TTP 제도	법적 효과

5. 정보보호 업무

정보보호와 관련되고 있는 주요한 정보보호 업무를 <표 4>에서 기술한다.

<표 4> 정보보호 업무

구 분		주 요 내 용	비 고
정보보호 응용 서비스	전자우편	PGP, PEM/RIPEM, TMail, S/MIME	
	전자상거래	전자화폐, 전자자금이체, 홈뱅킹, 홈쇼핑, 인터넷상거래	
	전자투표	익명통신	
	EDI/MHS	정보보호 프로토콜, 정보보호 서비스	X.400
	행정문서	전자결재, 데이터보호, 키관리	SC18
	Directory Service	디렉토리 인증 프레임워크, 디렉토리 접근통제, 디렉토리 프로토콜	X.500, X.509
정보보호 기술	NetSec	Firewall, 원격 로긴, Kerberos, OSI 저계위/고계위 정보보호 프로토콜	일회용패스워드, 식별프로토콜
	ComSec	음성/비음성 서비스보호, 무선망보호,사설망,공중망, ISDN, 중·저속통신, 고속통신, 초고속통신	
	CompuSec	DB 보호, 해킹방지,바이러스방지, 침입탐지,CERT	
	전자파 차폐	TEMPEST, EMI/EMC	
	정보보호서비스	Authentication, Integrity, Confidentiality, Non-repudation, Availability	
	암호기술	암호화기술, 키관리기술,	
	인증·식별기술	정보보호 프로토콜, 전자서명,해쉬함수	
	안전성평가기술	Cryptanalysis, Life-cycle Eng.	
	Chip 개발	공개키 암호 칩, 칩 물리적 보호, 스마트 카드 장착	
정보보호 정책	관리적 대책	Security 경보, 보안감사추적, 자원접근통제, 재난복구, 물리적보안, Risk Analysis	
	법·제도	OECD Security/암호정책, TTP Service, 암호키 위탁방식,	
	평가·인증	평가·인증 제도, 안전성평가기술	
	표준화	ISO/IEC/JTC1(SC6, 14, 17, 18, 21, 22, 27), EWOS, ECMA, ETSI	
차세대 정보보호	Info Warfare		

6. 결 론

본 기술문서는 정보보호 기술 중장기 개발 계획을 수립하기 위한 사전단계로 정보보호 기술 분류에 관한 내용을 고찰하였다. 먼저 정보통신망 안전 위협 요소를 기술하였으며, 또한 위협요소를 방지하는 기술적 대책을 고찰하였다. 대책별로 필요한 정보보호 상세 기술 및 업무를 정의하고 분류하였다. 우리는 추후 기술별로 국내 현황 및 외국 동향을 분석하며, 이를 근거로 정보보호 중장기 기술개발 계획을 수립하고자 한다.

<표 5> 약어표

ID	Identity
RSA	Rivest-Shamir-Adleman Algorithm
D-H	Diffie-Hellman Algorithm
OSS	Ong-Shamir-Schnorr Algorithm
FFS	Feige-Fiat-Shamir Protocol
GQ	Guillou-Quisquater Protocol
FTAM	File Transfer Access and Management standards
ECC	Elliptic Curve Cryptosystem
CRC	Check Redundancy Code
SHA	Secure Hash Algorithm
MD5	Message Digest 5 Algorithm
DES	Data Encryption Standard
CBC	Cipher Block Chaining Mode
MAC	Message Authentication Code
EDI	Electronic Data Interchange
TTP	Trusted Third Party
PGP	Pretty Good Privacy
PEM	Privacy Enhanced mail
ISO	International Organzation for Standardization
IEC	Internation Electrotechnical Commission
JTC	Joint Technical Committee
S/MIME	Secure/Multipurpose Internet Mail Extensions
EMI/EMC	ElectroMagnatic Interference/ ElectroMagnatic Compatibility
OSI	Open System Interconnection
SC	SubCommittee
ETSI	European Telecommunications Standards Institute
EWOS	European Open System Workshop
ECMA	European Computer Manufacturers Association

참고문헌

[1] Warwick Ford, "Computer Communications Security", PTR Prentice Hall, Englewood Cliffs, New Jersey 07632, 1994.

[2] William Stallings. "Network and internetwork security principles and practice", PTR Prentice Hall, Englewood Cliffs, New Jersey 07632, 1995.

[3] Patrick Horster, "Communications and Multimedia Security II", Chapman & Hall, International Federation for Information Processing(IFIP), 1996.

[4] "Guideline For The Use of Advanced Authentication Technology Alternatives", Federal Information Processing Standards Publication 190, 1994.

[5] Bruce Schneier, "Applied Cryptography : Protocols, Aogorithms, and Source Code in C", John Wiley & Sons, Inc., 1996.

고 승 철

1981년 연세대학교 이과대학 수학과 졸업
1983년 연세대학교 대학원 수학과 졸업(이학석사)
1992년 포항공대 대학원 수학과 졸업(이학박사)

1984년-1996년 한국전자통신연구원 책임연구원
1996년-현재 한국정보보호센터 수석연구원

성 맹 희

1990년 이화여자대학교 이과대학 수학과 졸업
1987년 이화여자대학교 대학원 수학과 졸업(이학석사)

1996년-현재 한국정보보호센터 연구원