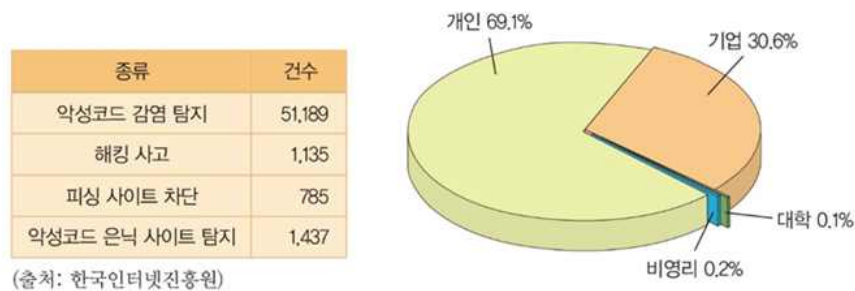


1. 컴퓨터 보안의 개요

1) 컴퓨터보안

- 개인이나 기관이 사용하는 컴퓨터와 관련된 모든 것을 안전하게 보호하는 것으로, 대부분의 경우 컴퓨터 안에 들어있는 중요한 정보를 보호하는 행위를 말함
- 컴퓨터 보안 중 하드웨어를 지키는 가장 간단한 방법은 컴퓨터에 암호를 걸어두는 것
- 우리가 사용하는 컴퓨터를 아무나 사용할 수 없도록 암호를 저장해둔 후 허가된 사람만 사용할 수 있게 하는 것



<인터넷 침해 사고 탐지 건수 및 기관별 피해 비율>

- 인터넷보안: 인터넷의 주요 통신 프로토콜인 TCP/IP를 통해 연결된 수많은 호스트들 사이에서 정보의 유출과 불법적인 서비스 이용을 방지하는 것
- 정보 보안: 정보를 수집하여 가공하고 저장한 후 송수신하는 과정에서 발생하는 정보의 불법 훼손 및 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법

(1) 정보 보안의 목표

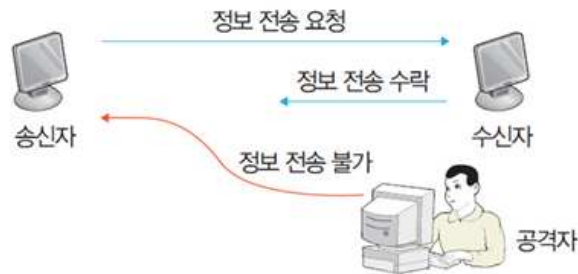
- 기밀성: 허가되지 않은 사용자 또는 객체가 해당 정보의 내용을 알 수 없도록 비밀을 보장하는 것
- 무결성: 허가되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없게 하는 것
- 가용성: 허가된 사용자 또는 객체가 정보에 접근하면 언제든지 사용할 수 있게 하는 것

(2) 정상적인 정보의 통신 과정

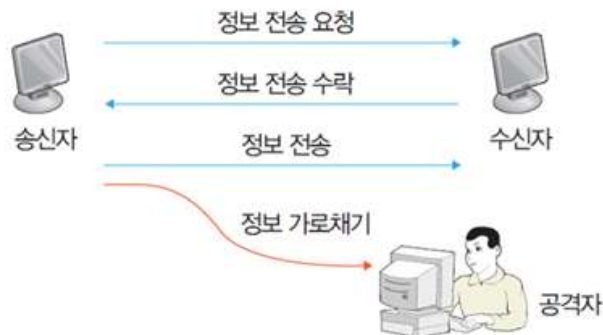


(3) 정보 보안을 위협하는 공격 형태

- ① 정보 가로막기: 송신자가 수신자에게 정보를 전송해도 되는지 묻은 다음 수신자로부터 수락 응답을 기다리는 사이에 일어남, 수신자로 위장한 제3자인 공격자가 송신자에게 전송이 불가능하다는 응답을 보내는 것, 중간에 끼어들어 고의적인 정보의 흐름을 차단하는 행위



② 정보 가로채기: 수신자로부터 수락 응답을 받은 송신자가 정보를 전송할 때 일어남, 허가받지 않은 침입자인 공격자가 전송 중인 정보를 불법으로 도청 또는 유출시키는 행위, 이때 송수신자는 정보가 가로채인 사실을 전혀 모름



③ 정보 수정: 수신자로부터 수락 응답을 받은 송신자가 정보를 전송할 때 일어남, 허가받지 않은 침입자인 공격자가 전송 중인 정보를 가로채 후 정보의 전체 또는 일부를 수정하여 수신자에게 보내는 행위임, 송수신자는 정상적으로 정보가 전송되었다고 판단하지만 수신자는 잘못된 정보를 수신하게 되므로 나중에 송신자가 잘못 보낸 것으로 오해할 수 있음



④ 정보 위조: (a) 과 같이 수신자로부터의 수락 응답이 송신자가 아닌 공격자에게 보내져 공격자가 송신자인 것처럼 위장해 정보를 보내거나, (b)와 같이 송신자가 수신자에게 정보를 보내지 않는 경우에도 공격자가 송신자인 것처럼 위장하여 정보를 보내는 행위임, 두 가지 경우 모두 수신자는 문제가 없다고 판단하지만 결과적으로 잘못된 정보를 수신하게 되므로 송신자가 잘못된 정보를 보낸 것으로 오해할 수 있음



(2) 컴퓨터 보안 대책

- 방화벽: 외부에서 침입을 막음
- 침입탐지 시스템(IDS: Intrusion Detection System): 침투해 오는 징후 포착
- 안티 바이러스: 정보 훼손 바이러스를 예방, 치료함
- 암호인증: 정보를 인증된 사람들에게만 공개
- 가상 시설망(VPN: Virtual Private Network): 인터넷에서 독점적으로 사용할 수 있는 네트워크를 이용함

2) 인터넷 해킹

(1) 국내 주요 해킹 사건

- 시스템공학연구소의 슈퍼컴퓨터센터에 해커들이 침입하여 장애를 일으킴(1992)
- 서울대학교 정보 관리 시스템 해커 침입 워크스테이션 6대에 저장된 정보 삭제함(1993)
- 원자력연구소 영국 해커 소년의 침투, 정보 유출됨(1994)
- 외국 해커가 KAIST시스템 해킹 중 KUS팀에 의해 적발됨 (1994)
- 중국인으로 추정하는 자가 국책 연구소를 해킹함(2004)
- Ddos 공격으로 인한 국내외 수만 대의 컴퓨터가 악성 바이러스를 퍼뜨리는 좀비PC의 역할을 하여 국내 주요 기관 및 포털 사이트들을 다운시킴(2009년 10월)
- SK커뮤니케이션즈 해킹 사고로 3,500만 명에 이르는 네이트와 싸이월드 회원의 개인정보가 털림(2011년 7월)
- 지능형 지속 공격(APT)으로 언론기관과 금융기관의 내부망을 뚫은 사이버 테러가 발생함 (2013년 3월)

(2) 외국의 주요 해킹 사건

- 서독 간첩 사건(1989): 서독의 간첩 해커들이 KGB사주로 전세계 주요 군사 정보를 탈취함
- 인터넷 웜 사건(1988): 네트워크에 뿌린 인터넷 웜은 약 7,000여 대의 호스트를 다운시킴
- NY414S 해커 사건: 뉴욕 암치료 센터의 암치료 정보를 파괴한 사건으로 미국 정부 청문회까지 열림
- NASA WANK(Worm Against Killer) 사건: 미국의 NASA연구소에 침입한 해커들이 연구개발 문서 열람 후 NASA가 군사용 연구 개발에만 치중한다고 비난함
- 오퍼레이션 오로도 사건(2011): APT 공격의 일종인 '오퍼레이션 오로도' 사건으로 구글과 미국 정부기관을 비롯한 70여 곳이 해킹 당해 큰 파장을 일으킨 해킹 공격 사건임

(3) 해커

- 컴퓨터를 광적으로 좋아하고, 이상을 컴퓨터에 건 사람들로 정보공유와 시스템에 대한 학습, 모험심을 기반으로 다른 시스템에 침투하거나 공격함

(4) 크래커

- 일부 해커들이 경제적 이익이나 공격 그 자체를 목적으로 다른 시스템들을 파괴하거나 침투하는 경우로 악의적인 의도로 활동하는 사람들을 말함

<컴퓨터 해킹 분야>

해킹 분야	설명	비고
시스템 해킹	전산망과 시스템의 취약점 해킹	일반 해킹
하드웨어 해킹	상용시스템 하드웨어의 해킹	신용 카드 등
무정부주의 해킹	파괴와 혼란을 노리는 공격	사이버 테러
바이러스 해킹	웜, 바이러스 등의 제작과 배포	자료 파괴, 작동 정지
전화망 해킹	전화망의 과금 조작과 파괴	프리킹(Pheraking)

<해커와 동기에 의한 분류>

해커의 종류	동기	비고
단순 해커	호기심과 영웅심리	대부분의 해커
내부 불순자 해커	특정 개인이나 집단의 이익 추구	내부 직원
범죄적 해커	금전적 이익 추구	금융망 등 대상
테러리스트/그룹	개인과 그룹의 이상 추구	혼란과 파괴 목적
기업체 고용 해커	기업의 이익 추구	기업 정보 유출
국가 고용 해커	국가 이익 추구	경쟁국의 정보 유출

2. 보안 기술

1) 암호의 역사와 배경

- 세계 어느 나라에서나 군사적인 활동은 물론 정치, 경제, 사회적인 활동에 있어서도 암호의 이용은 빈번함
- 냉전 시대가 붕괴되어 군사적 이용이 줄어들 수도 있겠지만 국제화의 촉진으로 무선에 의한 교신이 급격히 늘어남에 따라 암호의 중요성과 이용도는 오히려 비중이 커짐

2) 암호의 개념

- 허가되지 않은 사용자의 접근을 막는 것임
- 현재의 네트워크 환경은 접근을 막는 역할, 자료의 접근 제한, 변경금지, 전자 서명, 사용자 인증 등의 역할을 필요로 하기 때문임

안녕하세요 → 암호화 → dkssudgkipdy

- 암호화: 평문의 메시지를 암호화시켜 특정 키를 가지고 있는 사람만이 그 내용을 알아볼

수 있게 하는 것임

안녕하세요 → 암호화 → dkssudgktpdy → 복호화 → 안녕하세요
(평문) (암호문) (평문)

3) 암호를 만드는 방법

(1) 환자식

- 원문의 글자 순서를 그대로 두고 문자를 다른 문자로 바꾸는 방법

원어	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a

- 예: "I LOVE YOU"라면 암호문은 "r olev blf"로 바뀜
반대로 암호문이 "prhh nv"이면 원문은 "KISS ME"가 되는 방식임

(2) 전치식

- 문자는 그대로 두고 문자의 순서만 바꾸는 방법

키워드 : SUNDAY
원문 : OH MY MAMA HELP ME

"Y MMA MPOMEHAL HE"					
453216					
4	5	3	2	1	6
S	U	N	D	A	Y
O	H		M	Y	
M	A	M	A		H
E	L	P		M	E

<암호표>

4) 암호화 기술

- 평문을 암호문으로 변경하고, 다시 암호문을 평문으로 바꾸는 기술



(1) 비밀키(대칭키) 암호화

- 암호화할 때의 키와 복호화할 때의 키가 같은 경우
- 간단하면서 빠른 속도로 암호화와 복호화를 할 수 있다는 장점으로 널리 사용함

12345 → 각 자리에 10을 더해 붙임 → 1112131415

DES 알고리즘

- 1973년 미국 국방성의 암호 표준화 요구에 대해 IBM이 DES를 제안함
- 기본방식은 '키'를 사용하여 블록 암호라고도 함
- 가능한 조합이 너무 많아 해독이 거의 불가능함
- DES의 평문 처리는 초기순열, 16단계의 반복 처리 과정, 역초기 순열의 3단계의 과정으로 이루어짐



▲DES 알고리즘의 평문 처리 과정

(2) 공개키(비대칭키) 암호화 방식

- 비밀키 암호의 문제점을 해결하고자 하는 시도로부터 발전된 개념임
- 수학적으로 복잡한 과정을 거치는 암호화 방법임
- 매우 큰 두 소수의 곱을 구하면 그 수를 인수분해하기 어려운 점을 이용하여 암호화를 진행한 것임
- 평문을 암호화한 키와 복호화하는 키가 서로 다름
- 두 개 키 중 하나를 공개키(public key)라고 하고 다른 하나를 비밀키(private key)라고 함



<공개키 암호화 기법을 이용하는 방식>

① Diffie-Hellman 키 교환 방식

- 1976년 스탠포드 대학의 Diffie와 Hellman이 발표한 논문에 의해 제안

- 처음에 이 두 사람은 공개키 암호화 방식을 의도했으나 실제로 이 방식은 암호화 방식이라기보다는 키를 안전하게 전달하는 방법이었음

② RSA 알고리즘

- MIT의 R. Rivest 등에 의해 1977년에 개발
- DES 알고리즘과는 달리 암호화할 때의 키와 복호화할 때의 키를 각각 다른 것으로 취하는 원리로서, 공개키 암호를 위한 접근 방법에 응용되었음

(3) 최근의 암호화

- 비밀키 방식: 빠른 속도와 간편한 사용법으로 주로 대량의 자료를 암호화하고 복호화하는데 사용됨
- 공개키 방식: 비밀키에 비해 일반적으로 속도가 느리며 많은 연산을 해야 하므로 비교적 소량 자료의 암호화에 많이 사용됨
- 전자상거래나 전자 결제에 대한 결제 방식으로 공개키 방식을 응용한 DSA 등도 많이 쓰임

3. 컴퓨터 바이러스

1) 컴퓨터 바이러스

- 다른 사람의 컴퓨터나 프로그램에 침입하여 타인의 컴퓨터 파일에 자신을 복제하는 등의 피해를 입히는 행동을 하는 프로그램

2) 컴퓨터 바이러스의 역사

1986년

- 파키스탄의 PC수리공 암샤드 형제가 그들이 생산한 소프트웨어를 불법 복제한 사람들의 컴퓨터를 마비시키고 그들에게 수리를 의뢰하도록 자기 증식 바이러스를 만든 것이 세계 최초의 바이러스임

1988년

- 미국의 코넬대학 전산학과 대학원생인 로버트 모리스가 만든 바이러스에 의해 1시간 만에 미국 전역의 7천여 대의 연구기관과 미국의 주요 대학의 컴퓨터를 감염시킴

▶ CIH 악성 바이러스

- 컴퓨터의 시스템 자체를 못쓰게 하는 기능을 가짐

▶ Love 바이러스

- 스크립트와 e-메일을 이용하여 감염시키는 바이러스임
- 컴퓨터 바이러스에 대한 기초 지식
- 바이러스란 자기 증식을 한다는 이유에서 붙은 이름이지 특별한 프로그램이란 의미는 아님

- 감염되는 부위에 따른 바이러스 구분
- ▶ 부트(Boot) 바이러스
 - MS-DOS에서 디스크의 제일 첫 부분인 부트라는 부분에 바이러스 코드를 넣어 놓는 방식임
 - (c)Brain
- ▶ 부트/파일 바이러스
 - 부트 바이러스와 파일 바이러스의 특징을 모두 가지고 있음
 - 나타스 바이러스, 절반(One_half) 바이러스, 테킬라 바이러스
- ▶ 파일 바이러스
 - 실행 파일이나 그에 준하는 오버레이 파일 등에 감염되는 것으로 알려진 바이러스 중 가장 많은 수를 차지함
 - 예루살렘 바이러스
- ▶ 매크로 바이러스
 - 매크로 기능을 제공하는 엑셀이나 워드 등 Visual Basic 매크로를 사용하여 컴퓨터에 피해를 입힘. 주로 e-메일을 통해 전파됨
 - 멜리사 바이러스
- ▶ e-메일 바이러스
 - 인터넷 상에서 사용할 수 있는 e-메일 검색 프로그램들이 기본적으로 VBScript나 JavaScript 등을 자동적으로 실행한다는 점에서 착안하여 만들어짐
- ▶ 트로이목마(trojan)
 - 악의적인 목적으로 일부러 특정 컴퓨터에 넣어놓았다가 컴퓨터시스템을 파괴하거나 해당 컴퓨터내의 자료를 몰래 훔쳐내는데 쓰임

3) 바이러스 분류

분류	특징	종류
제1세대 원시형 바이러스 (Primitive virus)	<ul style="list-style-type: none"> - 도스나 윈도우 초기 버전에서 출현한 대부분의 바이러스를 칭함 - 구조가 단순해 분석하기 쉬움 	미켈란젤로 바이러스, 브레인 바이러스, 돌 바이러스(stoned virus), LBC 바이러스, 예루살렘 바이러스(Jerusalem virus), CIH 바이러스
제2세대 암호화 바이러스	<ul style="list-style-type: none"> - 백신이 등장하면서부터 출현 - 백신이 바이러스를 진단할 수 없도록 바 	폭포 바이러스(cascade virus), 느림

(encryption virus)	이러스가 암호화되어 저장되어 있음	보 바이러스(slow virus)
제3세대 은폐형 바이러스 (stealth virus)	<ul style="list-style-type: none"> - 컴퓨터를 감염시킨 후에도 메모리 손실이나 파일 크기의 변화가 없는 것처럼 은폐함 - 기억 장소에 기생하면서 감염된 파일의 길이가 늘어나지 않은 것처럼 보이게 함 - 백신 프로그램이 치료하려고 해도 감염되기 전의 내용을 보여줌으로써 바이러스가 없는 것처럼 속임 	브레인 바이러스(brain virus), 조시 바이러스(Joshi virus), 방랑자.1347 바이러스(Wanderer.1347 virus), 프로도 바이러스(Frodo virus)
제4세대 갑옷형 바이러스 (armor virus)	<ul style="list-style-type: none"> - 암호를 푸는 부분을 감염시켜 실행할 때마다 자기 변형을 시도하기 때문에 사용자나 백신 프로그램이 감염 사실을 알지 못하게 함 	고래 바이러스(whale virus), 다형성 바이러스(polymorphic virus)
제5세대 매크로 바이러스 (macro virus)	<ul style="list-style-type: none"> - 아래아한글이나 MS 오피스 같은 응용 프로그램의 매크로 내부에서 기생하여 동작 	엑셀 매크로 바이러스(ExcelMacro virus)
제6세대 차세대 바이러스 (next generation virus)	<ul style="list-style-type: none"> - 개인 정보의 유출 및 도용이나 시스템의 파괴 및 장악 등 사이버 범죄에 사용되어 심각한 피해를 줄 수 있는 바이러스를 모두 말함 	-

4) 바이러스 예방법

- 정품 소프트웨어와 같이 안전한 프로그램만 쓰는 것이 좋음
- 인터넷으로 다운 받은 프로그램을 설치하고 실행할 때에는 반드시 바이러스 검사를 한 후 실행하는 것이 좋음
- 가능한 자주 최신의 백신 프로그램으로 시스템에 바이러스가 있는지 검사해야 함

5) 바이러스 복구법

- 깨끗한 부팅 디스크로 부팅한 후 최신 버전의 백신 프로그램으로 바이러스를 치료해야 함
- 바이러스가 계속 생긴다면 일단 컴퓨터의 모든 자료 파일만 백업을 받고 포맷하는 것도 좋은 방법임