발언대

정보침해 이렇게 준비하자

**정보화를 통해 인류의 생활은 완전한 변혁을 맞고 있다.
생활속에 깊이 스며든 정보화를 통한 편의성이 극대화되는 만큼 새로운 문제에 봉착하게 된다.
수많은 정보들을 어떻게 보호할 것인가하는 문제이다.
최근 인터넷의 폭발적인 발흥으로 대두된 정보침해 사고들은 더 이상 남의 얘기가 아니다.
바로 지금 우리에게 닥친 반드시 풀어야 할 과제인 것이다.**

임휘성/한국정보보호센터 선임연구원

정보사회

오늘날 우리들의 삶은 우리가 인지하지 못하는 사이에 중요한 많은 부분을 컴퓨터와 같은 정보시스템에 의존하게 되었다. 이른 새벽에 전해지는 신문도 컴퓨터를 통해 기사가 접수되고 수집된 기사는 온라인으로 편집된 후 컴퓨터를 이용하여 조판되고 인쇄된다. 직장에 출근하여 업무에 필요한 정보를 수집하기위해 정보의 바다라 일컫는 인터넷을 컴퓨터를 이용하여 검색하고 항해한다.

점심시간 짬을 내어 은행에 입금된 특별보너스를 찾기위해 신용카드를 ATM 기계에 넣고 예금 인출을 요구하면 ATM 기계는 은행의 컴퓨터에 잔고를 조회하고 금융결재원의 컴퓨터를 통해 결재되어 현금을 내준다. 새로 태어난 딸을 의료보험에 추가하기 위해 필요한 서류를 발급받으려 서둘러 직장 근처의 동사무소를 방문하여 증명서를 신청하면 행정전산망을 통해 온라인으로 즉석에서 발급받을 수 있다. 퇴근시간, 백화점에 들러 아이들의 선물을 사기 위해 백화점 카드를 이용하여 완구를 구입할때도 컴퓨터를 통해 카드를 확인하고 매출을 등록한 뒤에야 상품을 건네받을 수 있다. 이같은 일상 생활로부터 컴퓨터가 갑자기 모든 것을 거부한다고 생각해 보라. 이처럼 정보시스템은 우리의 삶을 좌우할 만큼 중요한 역할을 담당하고 있다.

기업의 업무에 있어서도 정보시스템은 핵심적인 위치를 차지한다. 기업의 활동에 필요한 정보의 수집에 있어 인터넷은 가장 효과적인 정보의 원천이다. 대외적인 대화는 대부분 인터넷을 통한 전자우편을 이용하며, 기업의 홍보와 함께 직접적인 영업활동이 최근 폭발적인 성장을 보이고 있는 월드와이드웹을 이용하여 이루어진다. 컴퓨터를 이용한 인터넷상의 통신판매가 이미 활발하게 이루어지고 있으며 나아가 전자적인 정보만으로 만들어진 전자화폐를 이용한 전자상거래의 실용화가 활발히 추진되고 있다. 기업의 성공에는 국경과 시간의 제한이 없는 사이버스페이스의 활용이 필수적이며 따라서 모든 기업들이 인터넷에 그들의 정보시스템들을 연

〈표1〉 정보시스템 취약요소

분류	예	설명
시스템	관리자 및 사용자 부주의	추측이 쉬운 패스워드 사용, 부주의한 시스템 신뢰관계 설정, 사용자 미확인, 퇴직자 계정 미처리 등
	응용프로그램 버그	응용프로그램의 보안관련 버그들
	구성 오류	응용프로그램 구성상의 보안관련 오류들
네트워크	구조적 취약점	프로토콜의 설계상 보안 취약점
	응용 프로그램 버그	네크워크 서비스 프로그램의 보안관련 버그들
	구성 오류	네트워크 서비스 구성상의 보안관련 오류들

결하고 있다. 정부와 행정기관들도 필요한 정보를 얻고 대민업무를 수행하고 정책과 활동등을 홍보하기 위해 인터넷에 정보시스템을 연결하고 있다. 그외에도 원격강의, 원격진료, 개인으로부터 정부에 이르기까지 누구나가 경쟁적으로 인터넷에 그들의 정보시스템을 연결하고 있다.

정보시스템에 대한 위협

우리는 소설이나 영화들을 통해 중요한 군사정보시스템에 장난삼아 침입한 소년에 의해 제3차 세계대전이 발발한다거나, 금융기관의 컴퓨터시스템에 침입하여 고액의 금전을 빼돌리거나, 고의적으로 대형 컴퓨터 사고를 유발시켜 자신들의 요구를 보호 프로그램을 사용하게 한 뒤 숨겨진 백도어를 이용하여 마음대로 정보를 빼돌리기 위한 음모, 심지어 이같은 자신들의 비밀을 알아낸 사람의 모든 신상 정보를 컴퓨터상에서 범죄자의 정보로 바꿔치기해서 경찰에 쫓기게한다는 흥미진진한 이야기들을 접해왔다.

물론 가상현실을 이용하여 컴퓨터 속에 들어가 손에 부착된 특수장치를 이용하여 화면들을 상하좌우로 옮기면서 필요한 정보를 찾는 등의 아직은 실용화되지 않은 기술들을 이용하는 장면들이 흥미를 위해 가미되기는 하였지만 근본적으로 컴퓨터시스템에 침입하여 대혼란을 일으키거나 정보를 조작한다거나 기밀을 빼돌리는 일들은 얼마든지 가능하다. 해외에서는 물론이거니와 최근에는 국내에서도 금융기관의 컴퓨터시스템에 불법적인 프로그램을 수행시켜 개인의 계좌번호와 비밀번호를 빼돌려 고액의 금전을 갈취하다 적발되거나, 수많은 사람들이 이용하는 정보통신망 시스템에 불법적으로 침입한 뒤 증거를 없애기 위해 시스템의 모든 데이터를 삭제하여 수만명의 개인자료를 일순간에 지워버리는 등, 많은 정보시스템 침해사고 사례들이 보도되고 있다.

기업의 업무에 있어서도 정보시스템은 핵심적인 위치를 차지한다. 기업의 활동에 필요한 정보의 수집에 있어 인터넷은 가장 효과적인 정보의 원천이다. 대외적인 대화는 대부분 인터넷을 통한 전자우편을 이용하며, 기업의 홍보와 함께 직접적인 영업활동이 최근 폭발적인 성장을 보이고 있는 월드와이드웹을 이용하여 이루어진다.

그간 거의 대부분의 기업이나 기관들이 각자 독립적으로 운영되던 정보시스템을 서로 연결하여 네트워크화하였으며, 오늘에 이르러는 심지어 가정용 컴퓨터까지도 전화선을 이용하여 인터넷에 접속할 정도로 대부분의 정보시스템들이 인터넷이라는 거대한 네트워크로 연

〈표2〉 정보시스템 해킹수법 사례

수법 분류	예	설명
사회공학	신분위장	정당한 사용자로 속여 관리자에게 권한 요구
역사회공학	지원 위장	장애를 발생시켜 지원을 요청하게 한 뒤 백도어(Backdoor)등을 설치
계정도용	패스워드 추측	패스워드를 추측하여 로그인 시도
	패스워드 크랙(Password Crack)	패스워드 파일의 사용자 패스워드를 알아냄
	패스워드 스니프(Password Sniff)	네트워크 도청으로 ID와 패스워드 알아냄
호스트위장	신뢰하는 호스트로 위장	.rhost, /etc/hosts.equiv 등에 불법 호스트 삽입
취약점 및 구조적문제 이용	전자우편 취약점 이용	Sendmail 프로그램의 문제점을 이용한 경우로서, 패스워드파일 전송, root접근, 명령수행 등
	NFS 취약점	잘못 구성된 NFS 디스크를 불법으로 마운트
	Wu-ftpd, Gopher 문제	버그가 삽입된 버전이나 Shell Escape 허용
	rlogin 문제	root 계정으로 패스워드 묻지않고 로그인
	lpr, ELM, autoreply 문제	root 프로세스 작업을 수행하게 한다
	/usr/bin/pass wd 문제	임의의 파일 생성(/ .rhosts)
	NCSA http 문제	임의의 외부 작업 수행, cgi-bin 예제의 취약
	tftp 문제	패스워드 파일 전송 가능
	NIS 문제	YP클라이어트의 rpc.ypupdate의 수행시 문제
	IP Spoofing	원격지 시스템이 내부의 신뢰하는 호스트로 위장하여 불법 접속
서비스 방해	Mail Storm	불필요한 메일을 반복전송, 디스크 용량 초과
	ICMP 공격	라우팅을 교란하여 네크워크 전상운영 방해
	TCP Flooding	불완전한 접속을 반복적으로 시도하여 정상적인 TCP 접속을 방해

결되어 있다. 누구나가 인터넷을 통해 중요한 정보시스템에 보다 저렴한 방법으로 쉽게 접근할 수 있게 되었으며 이에따라 정보시스템에 대한 위협도 비례적으로 증가하고 있다. 그러나 여전히 많은 정보시스템 사용자들, 심지어는 비교적 규모가 크고 중요한 컴퓨터 시스템이나 네트워크를 관리하는 전문적인 관리자들 조차도 정보시스템에 대한 보호를 소홀히 하고 있는 실정이다.

정보시스템의 취약요소들

물론 정보시스템의 완벽한 보호는 정보시스템에 대한 철저한 이해가 바탕이 되어야만 가능하다. 여기에서는 인터넷 등에 연결되어 있는 정보시스템의 취약 요소들, 정보시스템에 대한 외부로부터의 위협, 그리고 정보시스템의 보호방법에 대해 개략적인 설명을 통해 조금이나마 이해를 돕고자 한다.

먼저 인터넷에 연결된 정보시스템들에 대해 매우 다양한 보안상 취약점들이 존재하지만 이들을 다음과 같이 분류하여 볼 수 있다.

이같은 보안 취약점들과 관련하여, 정보시스템에 대해 매우 다양한 형태와 수법들을 이용한 위협들이 존재하지만 이들 역시 다음과 같이 분류하여 볼 수 있을 것이다.

시회공학수법

사회공학적인 수법은 가장 전통적인 수법중의 하나이며 인간관계의 감정적인 측면을 이용한다는 점에서 관리적인 대책이 필요하다. 예를들어

정보의 보호는 정보가 원래 가지는 가치를 지키는 데 목적이 있으며 이를 위해서는 반드시 필요한 사람에게만 공개되어야 한다는 기밀성, 정보의 내용이 조작되지 않아야 한다는 무결성, 언제나 필요할 때 접근할 수 있어야 한다는 가용성의 요구가 만족되어야 한다. 여기에 추가적으로 일관성, 접근제어 감사, 부인방지등의 요구사항들이 추가되기도 한다.

시스템관리자에게 전화하여 조직의 관리자로 신분을 속인 뒤, 패스워드를 잊었으므로 패스워드를 xxxyyz로 변경하여줄 것을 요청한다.

역사회공학적 수법

역사회공학적인 수법은 보다 지능적이고 실제적인 기술이 필요한 수법이다. 우선 자신이 특정 문제를 해결할 능력이 있음을 인지시키고 목표 시스템에 그같은 장애를 발생시킨다. 시스템의 관리자가 스스로 그같은 문제를 해결할 수 없을 경우, 해결 능력을 가진 공격자에게 연락할 것이며 공격자는 해당 문제는 깨끗하게 처리하면서 이후 자신이 무단으로 시스템에 출입하는 데 사용할 수 있는 백도어 프로그램 등을 설치해 둔다.

실제로 지난 96년 9월 이와 유사한 사건이 보도된 적이 있다. 피해를 당한 시스템은 가입자에 대해 시스템 계정 및 인터넷 접속 서비스를 제공하는 시스템으로서 해당 시스템의 관리자가 평소에 알던 가해자에게 보안점검 서비스를 요청하였으며 이때 가해자는 시스템 보안을 점검하는 외에 가입자의 통신내용을 유출시키는 Telnet 변형 프로그램을 설치해 두었다가 추후 홈뱅킹 서비스 이용자의 사용자 계정, 비밀번호, 거래정보 등을 빼내어 실제로 계좌이체등의 방법으로 현금을 갈취하다 적발되었다.

계정도용 수법

계정 도용 수법의 경우, 단순한 패스워드를 추측하여 로그인을 시도하거나, 암호화된 패스워드가 저장된 파일을 입수하여 패스워드를 알아내는 프로그램을 이용하거나, 네트워크상의 통신내용을 도청하여 사용자 id와 패스워드를 알아내는 수법까지 다양한 방법들이 있다. 실제로 telnet 등과 같은 많은 유닉스 네트워크 서비스들이 사용자 ID와 패스워드를 암호화하지 않은 채 네트워크상에 전달하기 때문에 아무나 스니퍼 프로그램을 이용하여 타인의 사용자 ID와 비밀번호 등을 매우 쉽게 알아낼 수 있다.

97년 5월, PC 통신 사용자로부터 자신의 ID가 도용당하였다는 신고를 접수한 적이 있었다. 자신의 계정을 수시로 누군가가 사용하는 것 같아 패스워드를 변경하였으나 최근 패스워드가 다른 사람에 의해 무단 변경되어 로그인할 수 없다는 것이었다. 추후 배우자의 직장동료가 이전에 업무를 위해 잠시 빌려쓰기 위해 알았던 패스워드를 변형하

여 새로운 패스워드를 추측하여 사용하다가 실수로 패스워드를 변경하였다는 사실을 알게 되었다. 패스워드는 변경하였으나, 패스워드 작성 규칙을 그대로 사용하였기 때문에 쉽게 추측이 가능하였던 것이다. 97년 5월 보도된 사건의 경우에도 암호화된 패스워드 파일인 shadow 파일을 빼내어 암호를 알아내고, 스니퍼 프로그램을 이용하여 하이텔이나 천리안등을 이용하는 사람들의 ID를 도용하여 무단으로 사용한 사실이 있다.

서비스방해 수법

응용 프로그램이나 네트워크 서비스 프로그램들의 보안관련 버그들이나 구성상의 문제점, 그리고 네트워크 프로토콜의 구조적인 보안, 보안 취약점들은 끊임없이 발표되고 있다. 이들과 관련된 해킹 수법에 대한 설명들이나 해킹용 툴들이 인터넷의 여러 경로를 통해 널리 유포되고 있기 때문에 누구나가 쉽게 구하여 사용할 수 있다. 97년 5월 보도된 사건의 경우, 인터넷의 해킹 동호회를 통해 입수한 해킹프로그램들을 이용하여 인터넷 서비스제공사의 시스템의 루트권한을 획득하여 마음대로 조작하였다.

96년 말부터 97년 전반기를 통해 서비스방해 공격 수법이 널리 퍼지면서 서비스방해 공격이 관심의 대상이 되었다. 이것은 주로 제한된 시스템의 자원을 강제적으로 낭비시키는 방법으로 정상적인 서비스를 방해하는 공격이다. 쉬운 예로, 공유디렉토리에 불필요한 파일을 대량으로 작성하여 다른 사용자가 해당 디렉토리를 사용할 수 없게 만든다거나, 불필요한 메일을 대량으로 특정 시스템에 전송시켜 메일 서비스를 중단시킨다거나 하는 간단한 방법으로부터 TCP 접속 절차상의 취약점을 이용하여 존재하지 않는 호스트로 위장한 공격자 시스템으로부터 공격대상 시스템에 비정상적인 TCP 접속을 반복적으로 시도하여 더 이상의 정상적인 TCP 접속을 할 수 없도록 방해하는 방법(SYNC Flooding)에 이르기까지 매우 다양한 방법이 존재한다.

실제로 지난 96년 12월 외신 보도에 따르면 미국의 대형 웹서비스 제공업체인 WebCom사가 SYNC Flooding 공격에 피해를 당해 이에 가입된 3000여 웹사이트의 서비스가 40여 시간동안 중단된 사태가 발생하였다.

정보의 보호

정보의 보호는 정보가 원래 가지는 가치를 지키는 데 목적이 있으며 이를 위해서는 반드시 필요한 사람에게만 공개되어야 한다는 기밀성(confidentiality), 정보의 내용이 조작되지 않아야 한다는 무결성(integrity), 언제나 필요할 때 접근할 수 있어야 한다는 가용성(availability)의 요구가 만족되어야 한다. 여기에 추가적으로 일관성(consistency), 접근제어(access control), 감사(audit), 부인방지(nonrepudiation)등의 요구사항들이 추가되기도 한다.

〈표 3〉 정보시스템 보호모델

단계	단 계 명	설 명	비 고
1	물리적 보안	모뎀/회선 보호	Call-Back 모뎀 등
	외부와 연결되는 통신선로, 모뎀 등에 시건장치의 설치나 콜백모뎀 활용		
2	패킷 필터링	패킷 접근제어	라우터 Access List 적용
	기본적인 방화벽(Firewall) 기능으로서 출입패킷의 ①출발지/목적지 주소, ②응용프로그램종류에 따라 출입 제한 가능		
3	보안게이트웨이	응용프락시, 인증	방화벽
	방화벽을 설치하여 출입트래픽이 항상 이를 거쳐 가도록 구성, 전자우편, 가상터미널, WWW 등의 응용 프락시 기능이 제공되어야 한다.		
4	서브넷 보안	서브넷간 격리	라우터 이상의 LAN 연결
	내부서브넷간 상호 접속시 라우터, 게이트웨이 등으로 적절하게 서로 격리 가능		
5	호스트 보안	시스템 보안대책	보안관리(Administration)기술
	호스트 차원의 불법접근방지, 계정/패스워드 보안, 파일시스템 보안, 네트워크 보안, 보안 점검, 암호 저장 등의 관리가 요구됨		
6	응용 보안	응용프로그램 보안	전자우편, WWW 보안 등
	응용사용자들간의 보안서비스로서, 비밀보장(암호), 무결성(변조방지), 신분확인(디지탈서명) 등의 서비스 제공하는 보안응용(PEM, PGP, SSL, SSH 등)		
7	보안 방침	전산망 보안 방침	관리자 사용자 지침 등
	기관의 전산망 운영 상의 보안 내규, 보안 구현 상의 방침 등으로서 http://www.certcc.or.kr/Paper/policy.html 에서 사례들을 찾아볼 수 있음.		

〈표 4〉 해킹수법별 방지대책

수법 분류	예	설 명
사회공학	신분 위장	철저한 관리적인 보안, 보안 내규 및 절차등을 마련하고 예외없이 운영
역사회공학	지원 위장	정보시스템의 보안을 외부인에게 완전히 맡기지 않도록 할것
계정도용	패스워드 추측	Shadow 패스워드 파일 사용,
	패스워드 크랙 (Password Crack)	추측하기 힘든 안전한 패스워드 사용,
		일회용 패스워드 사용,
	패스워드 스니프 (Password Sniff)	압축/암호 기능이 있는 Telnet, rlogin 등 이용
		내부/외부 접근 통제
		sniffing 탐지 도구 이용
호스트위장	신뢰하는 호스트로 위장	개인별 .rhost 허용하지 않을 것, 개인의 홈디렉토리 찾아 이를 지울 것
취약점 및 구조적문제 이용	전자우편 취약점 이용	수시로 점검하여 최신 버전 설치,가능한 프락시를 사용
	NFS 취약점	외부 공개 디스크의 올바른 정의 모든 사용자 쓰기 모드 허용 금지
	Wu-ftpd, Gopher 문제	최신 버전 설치
	rlogin 문제	최신 버전 설치
	lpr, ELM, autoreply 문제	autoreply 사용 금지 모드를 666으로 변경
	/usr/bin/passwd 문제	최신 버전 설치 또는 옵션 제거
	NCSA http 문제	최신 버전 설치
	tftp 문제	tftp 사용 금지 -s 보안 옵션 사용
	NIS 문제	사용하지 않거나 최신 버전 설치
	IP Spoofing	내부 주소를 가진 외부 패킷 차단
서비스 방해	Mail Storm	전자우편 모니터링
	ICMP 공격	내부에서는 동적 라우팅 사용 않음
	TCP SYN Flooding	시스템 파라메터 수정

이같은 요구사항들을 모두 만족하기 위해서는 다양한 기술들을 체계적으로 적용하여 대책을 세워야 한다. 상세한 대책에 대해서는 후일 기회가 있을 때 다시 다루기로 하고, 우선은 전반적인 정보보호의 방법에 대해 살펴본 후, 각각의 해킹 수법에 대한 추가적인 대책에 대해 살펴보기로 한다.

정보보호 대책

먼저 인터넷에 연결된 정보시스템들에 대한 전반적인 단계별 정보보호 방법은 다음과 같이 분류할 수 있을 것이다.

다음으로 해킹 수법별 방지 대책에는 다음과 같은 방법들이 있다.

정보의 절대적인 가치가 높아가고 사회 모든 면에 걸친 정보시스템의 역할이 증대됨에 따라 정보시스템에 대한 직접적인 침해의 위협도 날로 증가하고 있다. 지면의 제약으로 이같은 위협들이나 이에 대한 대책들에 대해 세세하게 살펴보지는 못하였으나 전반적인 윤곽은 그려졌으리라 여겨진다. 정보시스템에 대한 완벽한 보안 대책은 아직까지는 없다. 또 해커들은 프로그램 개발자나 시스템 보안 관리자들보다 앞서 시스템에 대한 새로운 취약점들을 발견하기 위해 끊임없이 노력하고 있기 때문에 보안 위협의 종류와 기술 수준은 날로 증가하고 있다. 시스템 보안에 대한 이해가 부족한 일반 사용자들은 보안 관리자의 보안 지침에 충실히 따라야 한다. 또한 시스템에 대한 세부적인 이해와 보안 문제점의 분석에 많은 시간을 투자할 수 없는 보안 관리자들로서는, 그들을 대신하여 보안 위협에 관한 정보와 그에 대한 대책을 개발하여 제공하고 있는 CERT(Computer Emergency Response Team), 또는 CIRT (Computer Incident Response Team) 등의 여러 가지 이름으로 불리우는 침해사고대응팀들의 홈페이지를 방문하거나 보안관련 메일링리스트 및 뉴스그룹등에 가입하여 끊임없이 새로운 보안문제점과 대책 정보를 입수하여 부지런히 따르는 것이 중요하다.

마지막으로 국가적인 정보보호를 위해 설립된 한국정보보호센터에서 운영중인 침해사고대응지원센터의 홈페이지(http://www.certcc.or.kr)을 방문하여 보다 상세하고 다양한 정보를 접하기 바란다. DC