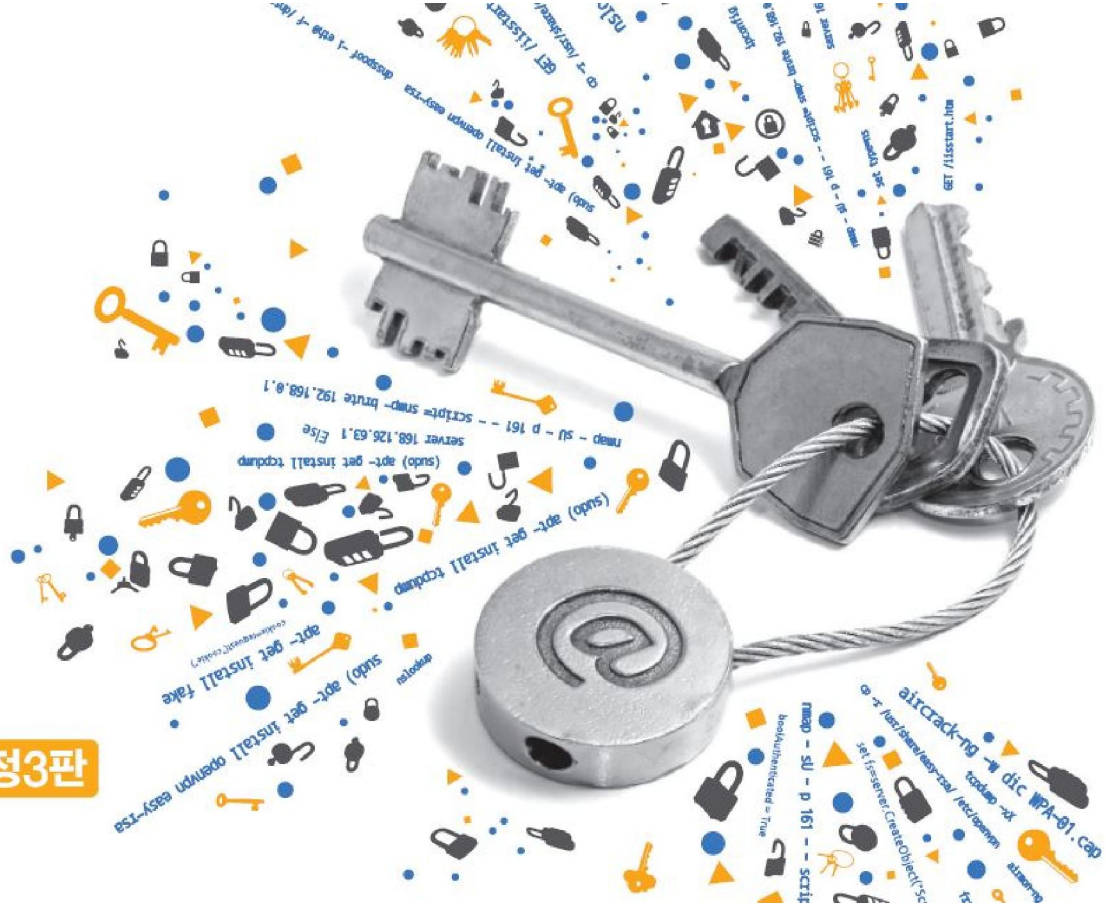
원리를 IT 가르쳐 맛보다

네트워크 해킹과 보안

개정3판

정보 보안 개론과 실습



Chapter 01 네트워크와 보안

IT COOKBOOK

목차

01 네트워크의 역사

02 네트워크 보안

학습목표

- 통신과 네트워크의 역사를 이해한다.
- 네트워크 보안의 요소를 이해한다.

■ 네트워크의 정의

- 지역적으로 분산된 위치에서 컴퓨터 시스템 간에 데이터 통신을 하기 위한 하드웨어 및 소프트웨어의 집합

■ 모스와 전신기

- 1800년경 볼타가 최초로 전지를 발명
- 이후 전선을 통해 신호를 보내는 방법을 연구하기 시작했고, 모스가 처음 실질적인 성과를 냄.
- 1832년 알파벳 문자에 점과 대시를 사용하여 모스 부호를 발명
- 1843년 워싱턴에서 볼티모어까지 전신기 선을 가설
- 1844년 첫 번째 공식 메시지는 '하나임이 행하신 일이 어찌 그리 크뇨(민수기 23:23)'

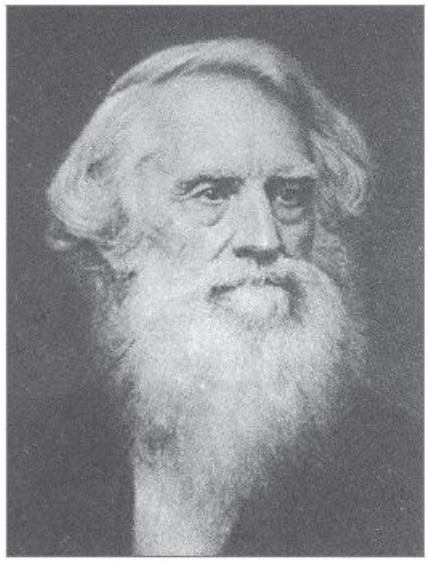


그림 1-1 사무엘 모스

■ 벨의 전화기

- 1876년 알렉산더 그레이엄 벨이 전화기를 개발
- 1876년 3월 미국 특허청에 전화를 특허로 등록
- 1877년 1월 30일 상자 모양의 첫 전화기가 등장(일대일 통신만 가능)
- 1878년 1월 28일 코네티컷의 뉴헤이븐에서 처음으로 교환기가 설치되어 사용자의 전화가 중앙의 교환수를 거쳐 연결됨.
- 우리나라는 1896년 궁내부 전화가 전화기의 효시
- 1902년에는 서울과 인천 사이에 전화가 개설

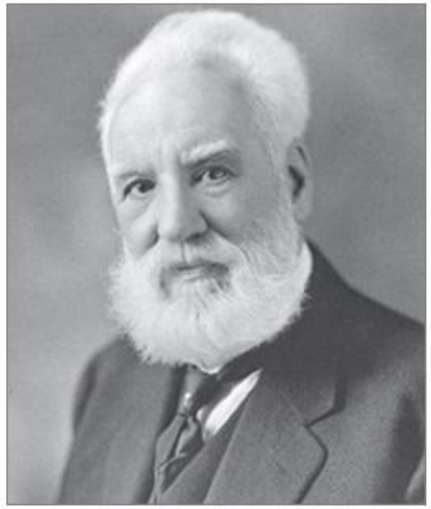


그림 1-3 알렉산더 그레이엄 벨

■ 전자기파의 발견

- 1864년 제임스 클럭 맥스웰이 전자기파가 대기중으로 전파된다고 처음 예측
- 전자기장의 기초 방정식인 맥스웰방정식(전자기방정식)을 도출하여 전자기파의 존재를 증명
- 전자기파의 전파 속도가 광속도와 같고, 횡파라는 사실을 밝힘으로써 빛의 전자기파설에 대한 기초를 세움.

그림 1-4 제임스 클럭 맥스웰

■ 전파 이용의 시작

- 1888년 하인리히 루돌프 헤르츠가 실험을 통해 라디오파를 주고받음으로써 전파의 존재가 실제로 입증됨.
- 굴리엘모 마르코니는 전자기파를 실제 통신에 이용할 수 있는 형태로 만듦
- 마르코니는 무선 전신을 발전시킨 공로로 1909년 노벨 물리학상을 수상
- 1922년 영국방송공사(BBC)가 세계 최초로 음성 뉴스를 무선 방송으로 전송

그림 1-5 하인리히 루돌프 헤르츠

그림 1-6 굴리엘모 마르코니

■ 모뎀의 개발과 네트워크의 시작

- 벨 텔레폰 연구소의 조지 스티비츠가 전화 교환 회로를 '산술 기기 ' 로 발전시킨 '모델-K' 기기를 개발했고, 후에 CNC로 발전
- 스티비치는 1940년 뉴욕의 CNC와 전화선으로 연결해 데이터를 입력하는 과정을 시연했는데, 이는 네트워크 컴퓨팅의 효시로 기록됨.
- 1958년 벨 연구소에서 최초의 상업용 모뎀인 데이터폰을 개발
- 미국 국방부는 군사 작전 수행을 위한 고성능 컴퓨터를 개발하려는 목적으로 1965년 세계 최초의 컴퓨터 네트워크 개발에 착수
- 이때 개발을 시작한 네트워크는 1969년 오늘날 인터넷의 모태가 된 사상 최초의 대단위 컴퓨터 네트워크인 ARPANET의 탄생으로 이어짐.

■ 장거리 컴퓨터 통신과 인터넷의 시작

- 1965년 ARPA는 MIT 링컨 연구소의 TX-2와 캘리포니아 산타모니카 SDC의 Q-32 컴퓨터와 전화선으로 직접 통신하는 장거리 데이터 통신을 최초로 시도
- 프로토콜 : 컴퓨터와 컴퓨터 사이에서 메시지를 전달하는 과정(톰 마릴)
- 1967년 ARPA는 ACM에서 각 호스트를 IMP라는 특정 컴퓨터에 연결하고, IMP를 서로 연결하는 ARPANET을 제안(현재의 라우터와 개념이 유사)
- 1969년 네 개의 노드(UCLA, USCB, SRI, UU)를 네트워크로 구성하고 NCP라는 프로토콜을 호스트 간 통신에 사용
- 1971년 레이 톰린슨이 전자 메일 프로그램을 발명

■ 장거리 컴퓨터 통신과 인터넷의 시작

- 1972년 빈트 서프와 로버트 칸이 게이트웨이를 개발
- 1973년 빈트 서프는 로버트 칸과 함께 TCP/IP 프로토콜과 인터넷 구조를 설계

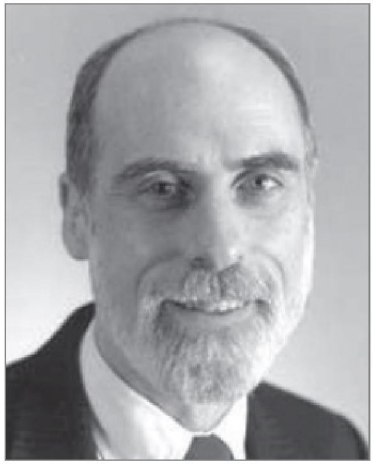


그림 1-7 빈트 서프

그림 1-8 로버트 칸

- 호스트 컴퓨터와 터미널로 구성된 네트워크는 IBM의 SNA 망이 최초
- 1974년 제록스가 이더넷을 개발(오늘날의 클라이언트-서버 구조로 전환)

■ 장거리 컴퓨터 통신과 인터넷의 시작

- 1979년 유즈넷 탄생
- 1981년 유닉스 운영체제에 TCP/IP가 포함되어 배포되었고, TCP/IP가 ARPANET의 공식 프로토콜이 됨.
- 1983년 군사용 MILNET과 군사용이 아닌 ARPANET으로 분리
- 1983년 존 포스텔이 도메인이름 시스템 개발
- 1984년 DNS가 구성되어 네트워크가 폭발적으로 확장됨.
- 1990년 ARPANET이 해체되고 NSFNET이 만들어짐.

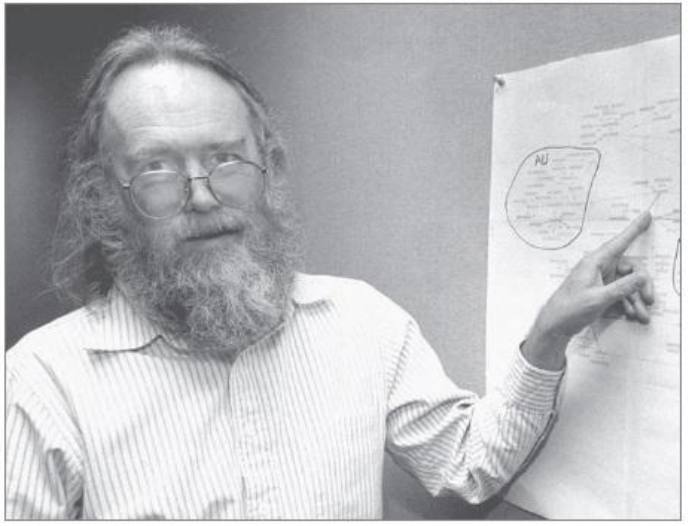


그림 1-9 존 포스텔

■ 장거리 컴퓨터 통신과 인터넷의 시작

- 1989년 3월 버너스-리가 웹 개념을 제안
- 1990년 동료 로버트 카이유와 개정된 개념을 소개

→ 서로 다른 컴퓨터끼리 정보를 공유하고 서로 링크하여 찾기 쉬운 하이퍼텍스트 형태의 서비스를 도입하자는 것

■ 국내 인터넷의 역사

- 1982년 서울대학교와 KIET(전자통신연구소의 전신)가 TCP/IP로 SDN 시작
- 1983년 미국으로 UUCP 다이얼 업(Dial-Up) 연결
- 1984년 유럽으로 X.25를 이용한 UUCP 연결
- 1987년 교육 연구 전산망 추진 위원회 구성
- 1988년 연구 전산망 기본 계획 확정, 교육망을 BITNET과 연결
- 1990년 HANA/SDN이 56Kbps로 인터넷에 연결
- 1991년 연구 전산망이 56Kbps로 인터넷에 연결
- 1993년 HANA/SDN이 56Kbps에서 256Kbps로 확충
- 1994년 한국통신, 데이콤에서 인터넷 상용 서비스 시작
- 1995년 INET, 나우콤에서 인터넷 상용 서비스 시작

■ 국내 인터넷의 역사

- 1995년 초고속 정보통신망 구축 사업 시작
- 1996년 7천 대 이상의 호스트 컴퓨터가 연결됨
- 1997년 한국인터넷협회 설립
- 1998년 초고속 정보통신망 구축 사업 1단계 완료
- 2000년 초고속망 구축 기술로 각종 서비스가 이루어짐(하나로, 두루넷, 드림라인, 신비로 등)
- 2001년 초고속 광전송망 구축(155Mbps~40Gbps)
- 2002년 서울대, 한국전자통신연구원ETRI 등이 참여한 IPv6 활성화를 위한 프로젝트 시작
- 2004년 한국 인터넷 이용자 수 3천만 명 돌파
- 2005년 한국 IPv6 주소 보유율 세계 3위로 평가
- 2012년 한국 인터넷 속도 세계 1위로 평가

■ 정보 보안의 3요소와 추가 요소

- 기밀성(Confidentiality)
- 무결성(Integrity)
- 가용성(Availability)
- 서버 인증(Server Authentication)
- 클라이언트 인증(Client Authentication)

■ 기밀성

- 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것
- 프라이버시 보호와도 밀접한 관계가 있음.
- 네트워크 보안 측면에서 기밀성은 '시스템 간 안전한 데이터 전송'과 관련이 있음.
- 스니핑(Sniffing)은 기밀성을 해치는 가장 일반적인 공격 형태
- 통신의 암호화가 가장 일반적인 보안 대책

■ 무결성

- 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것
- 네트워크에서의 무결성은 '클라이언트와 서버 간의 데이터가 변조되지 않고 전송되는가 ' 와 관련이 있음.
- 중간에 유효한 다른 연결을 빼앗는 세션 하이재킹, 두 시스템 간의 데이터를 중간에 변조하는 MITM 공격은 무결성을 해치는 대표적인 공격
- 통신의 암호화가 가장 일반적인 보안 대책(PKI와 밀접한 관련이 있음)

■ 가용성

- 허락된 사용자 또는 객체가 정보에 접근하려고 할 때 방해받지 않도록 하는 것
- DoS가 가용성을 해치는 대표적인 공격

■ 서버 인증

- '클라이언트가 올바른 서버로 접속하는가 ' 를 의미
- 서버 인증으로 생기는 문제는 무척 다양하며, 일반적으로 DNS 스푸핑이나 서버 파밍 등이 있음.
- SSL(HTTPS)을 통해 서버 인증을 하지만, 경고를 보여주고 사용자에게 선택을 하게 하는 것이 일반적이며 강제적인 서버 인증은 흔치 않음.

■ 클라이언트 인증

- '올바른 클라이언트가 접속을 시도하는가 ' 를 의미
- 웹 사이트에 접근할 때 사용하는 아이디와 패스워드가 대표적인 클라이언트 인증
- 클라이언트 인증과 관련된 해킹은 스푸핑, 세션 하이재킹, 피싱 등이 있음.

감사합니다.

네트워크 해킹과 보안 개정3판

정보 보안 개론과 실습