1주차 1차시 보안의 개념과 역사

【학습목표】

1. 보안의 개념을 설명할 수 있다.
2. 보안의 역사를 시대별로 나열할 수 있다.

학습내용1 : 해킹과 보안의 개념

1. 해킹이란

- 국어사전 : '남의 컴퓨터 시스템에 침입하여 장난이나 범죄를 저지르는 일'
- 영어사전 : '컴퓨터 조작을 즐기기, 무엇이나 숙고하지 않고 실행하기'
- 영영사전 : '디자이너가 의도하지 않았던 방법으로 시스템의 특성이나 규칙을 이용한 창조적인 사용법을 찾는 것

2. 보안이란

1) 국어사전
- 안전을 유지함
- 사회의 안녕과 질서를 유지함

2) 영어사전
- Security
- Protection

3. 정보보호란 무엇인가

1) 국어사전 : 없음
- 보안의 개념과 유사하게 사용됨
- 정보통신망 및 정보통신 기기를 해킹으로부터 보호하려는 조직이나 체계를 통틀어 일컬음.

4. 정보보호의 학습방법

- 해킹과 보안에 관련한 기술 및 사례를 폭넓게 학습함
- 학습한 개념을 S/W분야, H/W분야, N/W분야에 적극 반영함

학습내용2 : 해킹과 보안의 역사

1. 1950년대 이전

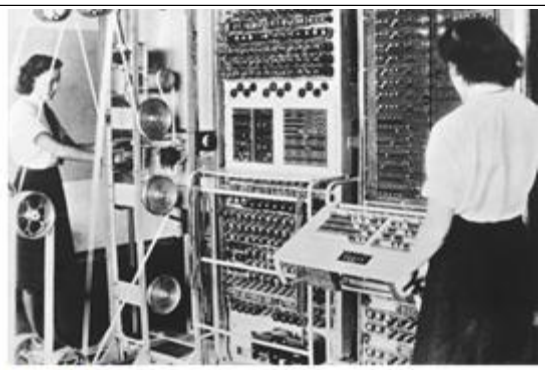
1) 1918년에 폴란드의 암호 보안 전문가들이 에니그마(Enigma)를 개발

2) 에니그마는 평문 메시지를 암호화된 메시지로 변환하는 전기/기계 장치

3) 처음에는 은행에서 통신 보안 강화를 위해 개발되었지만, 제2차 세계대전에서 독일군에 의해 군사통신 보안용으로 사용

4) 알파벳이 새겨진 원판 3개와 문자판으로 구성되어 있는데, 문자판 위에 하나의 키를 누르면 나란히 놓인 3개의 원판이 회전하면서 복잡한 체계로 암호가 만들어짐

5) 알란 튜링이 최초의 컴퓨터 콜로서스를 개발



[그림 1-3] 콜로서스

- 콜로서스는 2400개의 진공관을 이용해 만들어짐
- 높이 3m
- 초당 5천 자의 암호문이 종이 테이프를 타고 들어가면서 에니그마의 암호와 일치할 때까지 비교하는 방식
- 수를 세거나 비교, 간단한 산술 연산을 하는 전자 부속들을 갖추고 있음.

- 계산 결과는 전기타자기를 경유하도록 설계되었으며, 프로그램은 플러그판의 스위치를 조작함으로써 가능. 각 세트는 한 차례에 1만 7,576개의 조합을 점검

2. Hack 의미

1) 'Hack'이라는 말은 1948년도에 설립된 메사추세츠 공과대학(MIT)의 모형 기차 제작 동아리인TMRC(Tech Model Railroad Club)에서 '전기 기차, 트랙, 스위치를 보다 빠르게 조작하다'라는 의미로 처음 사용됨.

2) TMRC의 해킹의 정의
- " We at TMRC use the term 'hacker' only in its original meaning, someone who applies ingenuity to create a clever result, called a ' hack ' "
(우리 TMRC는 '해커'라는 용어를 똑똑한 결과를 만들기 위한 '창조성(hack)'을 적용하는 사람이라는 원래의 의미로만 사용한다.)

3. 1960년대

1) 최초의 미니 컴퓨터 PDP-1
- 1964년에 DEC라는 회사는 TMRC에 조그마한 컴퓨터를 기증하는데, 이것이 VAX 컴퓨터의 전신인 PDP-1
- TMRC의 해커들은 PDP-1을 광적으로 좋아하게 됨

2) 최초의 컴퓨터 연동망 ARPA
- 1967년에 미 국방부(DoD)는 연구 기관과 국방 관련 사업체 등 관련 기관 사이의 정보 공유를 지원하기 위한 ARPA(The Advanced Research Project Agency) 프로젝트를 통해 컴퓨터 연동망 개발

3) 운영체제 유닉스의 개발
- 1969년에는 켄 톰프슨 (Ken Thompson)와 데니스리치 (Dennis MacAlistair Ritchi)가 유닉스 (UNIX)운영체제를 개발

[그림 1-6] 켄 톰프슨(좌)와 데니스 리치(우)

4) 전화망 침입을 통한 무료 전화 해킹
- 1969년에 프리킹의 아버지로 불리는 조 앙그레시아(Joe Engressia, 공식 이름은 조이버블스)는 2,600Hz의 휘파람을 불면 장거리 전화를 무료로 쓸 수 있다는 사실을 알아냄
- 존 드래퍼는 월남전 참전 중에 군용 식량으로 지급되는 '캡앤 크런치' 라는 시리얼 박스 안에 포장되어 있던 장난감 호루라기를 불면 무료 통화가 가능하다는 사실을 발견

5) 전화망 침입을 통한 무료 전화 해킹

6. 1970년대

1) 최초의 이메일 전송
- 1971년에 레이 토밀슨(Raymond Samuel Tomlinson)은 최초의 이메일 프로그램을 개발
- 64 노드의 ARPANet에서 @를 사용하여 최초의 이메일을 발송

[그림 1-9] DEC의 KA10(PDP-10)

2) 마이크로소프트 설립

[그림 1-10] 빌 게이츠

- 빌 게이츠 (William H. Gates)는 1973년에 폴 앨런 (Paul G. Allen)과 마이크로소프트를 함께 설립

3) 최초의 데스크톱 컴퓨터 솔
- 1975년 : 리 펠젠스파인이 인류 최초의 데스크톱 컴퓨터인 '솔' 을 개발

4) 애플 컴퓨터의 탄생
- 1979년 : 스티브 워즈니악과 스티브 잡스에 의해 애플 컴퓨터가 탄생

5. 1980년대

1) 초기의 PC
- 1980년 : 마이크로소프트는 베이직(Basic)과 도스(DOS)를 개발
- 1981년 : IBM은 인텔 8086 마이크로프로세서를 기초로 한 비교적 저렴한 가격의 PC를 판매

2) 네트워크 해킹의 시작
1980년 : 네트워크 해커라는 개념이 처음 생겨남
* 네트워크 해킹의 대표적인 사건 '414 Gang'

① 414 Gang은 미국 밀워키의 로날드 마크 오스틴 등 6명이 운영했던 '414 Private'이라는 BBS의 일원들이 만든 해커 그룹임
② 암센터와 로스알라모스 국립연구소를 포함해 60개의 컴퓨터 시스템에 침입함
③ 중요 파일을 실수로 지워 몇 년 간의 연구 결과를 날려버림

- 1981년 : 이안 머피(Ian Arthur Murph)가 AT&T의컴퓨터 시스템에 침입해 전화 요금과 관련된 시계를바꾸어 낮은 가격의 심야 요금이 대낮에 적용되도록 조작

3) 카오스 컴퓨터 클럽
- 1981년에는 독일의 전설적인 해커 그룹인 카오스 컴퓨터 클럽(Chaos Computer Club, CCC)이 결성되었는데, 소식지 창간호를 통해 다음과 같은 설립 목표를 규정함
- 정보 사회로 발전하기 위해서는 전 세계와 자유로운 커뮤니케이션을 가능케 하는 새로운 인권이 필요하다. 인간 사회 및 개인에게 기술적 영향을 미치는 정보 교류에서 국경은 사라져야 한다. 우리들은 지식과 정보의 창조에 기여할 것이다.

[그림 1-11] 독일의 카오스 컴퓨터 클럽

4) 1983년 리처드 스톨만에 의해 GNU(Gnu's Not Unix) 계획이 세상에 알려짐


[그림 1-12] 리처드 스톨만

① GNU는 유닉스와 완벽하게 호환하는 소프트웨어 시스템으로 모든 사람이 무료로 사용하도록 작성됨
② 소프트웨어의 저작권 개념에 처음부터 함정이 있었으며, Copyright가 아니라 Copyleft가 되어야 한다고 주장함

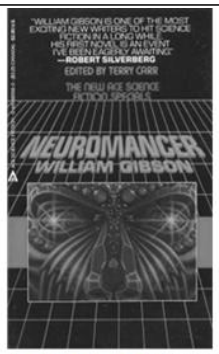
③ 1985년에는 FSF(Free Software Foundation)를 만들고, 그곳에서 리눅스 탄생의 배경이 된 GNU 프로젝트가 시작됨
5) GNU 사이트를 보면
- 자유 소프트웨어(Free Software)에 대한 4가지 자유를 확인할 수 있음

① 자유 0 : 프로그램을 어떠한 목적을 위해서도 실행할 수 있는 자유
② 자유 1 : 프로그램의 작동 원리를 연구하고 이를 자신의 필요에 맞게 변경시킬 수 있는 자유(이를 위해 소스코드에 대한 접근이 선행되어야 한다.)
③ 자유 2 : 이웃을 돕기 위해서 프로그램을 복제하고 배포할 수 있는 자유
④ 자유 3 : 프로그램을 향상시키고 공동체 전체의 이익을 위해서 다시 환원시킬 수 있는 자유(이를 위해 소스코드에 대한 접근이 선행되어야 한다.)

6) 해킹과 관련된 문화의 등장
- 1983년에 상영된 워게임즈(WarGames)라는 영화는 해커를 소재로 한 최초의 영화
- 1984년에는 윌리엄 깁슨(William Gibbson)의 공상과학소설『뉴로맨서(Neuromancer)』이 발간됨

① 사이버스페이스라는 용어를 최초로 사용
② 인공지능(AI, Artificial Intelligence), 가상세계, 유전자 공학, 다국적기업 등에 대한 개념이 등장

[그림 1-13] 워게임즈



[그림 1-14] 윌리엄 깁슨의 뉴로맨서

- 1985년은 유명한 해킹 잡지인 프랙(Phrack)이 나이트 라이트닝(본명: 크레이그 나이도프)과 타란 킹(본명: 랜디 티슐러)에 의해 창간
- 1년 후 온라인 잡지 프랙에 이어 해커 잡지인 2600이 정기 출판됨
- 1985년에 7명의 미국 소년이 뉴저지 소재 미 국방부 컴퓨터에 침입해, 통신위성 위치를 변경하는 코드를 포함한 극비 군사통신 데이터를 빼낸 사건이 발생

7) 케빈 미트닉(Kevin Mitnick) : 1987년 산타 크루즈 오퍼레이션 시스템에 침입

8) 로버트 타판 모리스

① 미 전역의 컴퓨터가 정체불명의 바이러스에 감염되어 멎고 겁먹은 사용자들이 인터넷 연결을 끊는 사건이 발생함
② 22세의 로버트 타판 모리스가 만든 웜(Worm)에 의한 인터넷의 마비로 밝혀짐
③ 네트워크로 연결된 6,000여 대의 컴퓨터를 감염시켜 정부 및 대학의 시스템을 마비시킴
④ 미 국방부가 1988년 11월 카네기 멜론 대학에 컴퓨터 비상 대응팀(CERT) 설립함

[그림 1-16] 케빈 미트닉

[그림 1-17] 로버트 타판 모리스

- 1986년 8월에는 캘리포니아에 있는 로렌스 버클리 연구소의 컴퓨터 계좌에서 컴퓨터 사용 요금에 75센트의 오차가 생기는 일이 발생. 클리프 스톨(Cliff Stoll)이 1년 반 정도 추적을 하여, 서독 해커들이 전 세계 3백여 기관에 불법적인 접근을 시도하고 군사 기밀 정보를 탈취한다는 사실을 알게 됨

9) 1989년에는
- '해커 선언문 (The Conscience of a Hacker)' 의 저자로 유명한, 로이드 블렌켄쉽(Loyd Blankenship)이 체포됨

6. 1990년대

1) 해킹 대회 데프콘
- 1990년에는 최초의 해킹 대회인 데프콘이 라스베가스에서 개최됨

[그림 1-18] 데프콘 홈페이지

2) 리눅스 0.01
- 리누스 토발즈(Linus Benedict Torvalds)는 PC에서 돌릴 수 있는 유닉스 운영체제를 만들기 시작해 1991년에 리눅스 0.01 버전을 공개함

[그림 1-19] 리누스 토발즈

3) 윈도우 NT 3.1
- 1993년 7월 27일에 마이크로소프트는 윈도우 NT 3.1을 발표

4) 해킹 도구의 개발
- 1994년에는 인터넷 브라우저 넷스케이프가 개발되고 웹 정보 접근이 가능해짐.

5) 아메리칸온라인 해킹
- 1997년에는 아메리카온라인(AOL) 침입만을 목적으로 고안된 무료 해킹 툴인 AOHell이 공개됨
- 이후 며칠 동안 초보 해커들에 의해 악용되어 수백 만의 미국 온라인 사용자의 메일함이 대용량 메일 폭탄으로부터 공격 받음

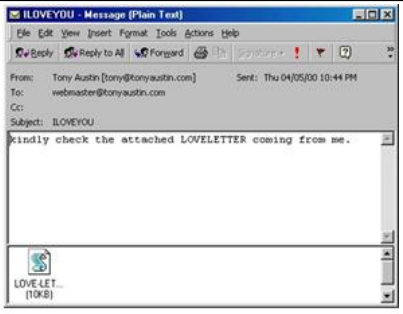
6) 트로이 목마, 백 오리피스
- 1998년에는 Cult of the Dead Cow라는 해킹 그룹이 데프콘 회의에서 강력한 해킹 툴로 사용할 수 있는 트로이 목마 프로그램인 백 오리피스(Back Orifice)를 발표

7. 2000년대

1) 분산 서비스 거부 공격
- 2000년 2월에는 인터넷에서 가장 소통량이 많은 몇 개의 사이트에 분산 서비스 거부 공격(DDoS, Distributed Denial of Service)이 가해짐
- 이로 인해 야후, CNN, 아마존 등의 사이트가 ICMP 패킷을 이용한 스머프(Smurf) 공격으로 몇 시간 동안 마비됨

2) 웜과 바이러스
2000년에는 러브 버그(Love Bug) 바이러스가 등장해서 87억 5천만 달러의 경제적 손실을 발생시킴
- 2003년 1월 25일 오후 2시 30분부터 약 2일 동안 마이크로소프트의 MS-SQL 2000서버를 공격하는 슬래머(Slammer)라는 웜이 전국의 네트워크를 마비시킴
- 2004년에는 베이글 웜, 마이둠 웜, 넷스카이 웜 이라는 웜 삼총사가 등장

3) 개인정보 유출과 도용
- 2005년 10월부터 2006년 2월 사이에는 주민등록번호 수십만 개가 유출돼, 인터넷 게임사이트 가입에 사용되는 등



[그림 1-20] 이메일에 첨부된 러브 바이러스

개인정보가 무단 도용됨

- 2005년 11월에는 국내 모 은행의 피싱 사이트를 만들어놓고 인터넷 카페 등에 대출 광고를 한 다음, 연락해온 피해자들을 피싱 사이트에 접속하도록 유도함
- 이들이 입력한 금융정보를 이용해서 총 12명으로부터 1억 2천만 원 상당을 가로채는 사건이 발생

4) 해킹 기술을 이용한 전자상거래 교란

- 2006년 7월에는 안심클릭의 허점을 이용한 해킹 사기 사건 발생
- 2006년 3월에는 클릭 수를 자동 증가시키는 방법으로, 국내 대형 포털 사이트의 정보 검색 순위를 조작한 인터넷 광고 대행업체 대표 이 씨가 업무 방해 등의 혐의로 불구속 입건
- 2007년 2월 8일에는 공인인증서 유출로 인한 시중 은행 불법 인출 사건이 발생
- 2007년 2월 11일에는 한국 시티은행 해킹 사건이 발생하는 등 금전적 이익을 노린 해킹이 급증

8. 2010년대

1) 농협 사이버테러

- 2011년 4월에 농협의 전산 시스템이 대규모 데이터 삭제로 인해 중단되는 사건 발생

[그림 1-21] 농협 사이버테러

2) APT 공격

- 개인정보 유출 등을 목적으로 특정한 사이트를 장기간에 걸쳐 공격하는 것을 APT(지능적 지속 위협, Advanced Persistent Threat) 공격이라고 함

3) 해킹 도구이자 해킹 대상이 되는 스마트폰

- 스마트폰은 공격 대상이 되기도 하지만 공격 도구로도 활용도가 매우 높아 스마트폰을 이용한 보안 사건은 점차 그 범위가 확대될 것으로 예상됨

【학습정리】

1. 정보보호란 보안의 개념과 유사하게 사용됨

2. 정보보호란 정보통신망 및 정보통신 기기를 해킹으로부터 보호하려는 조직이나 체계를 통틀어 일컬음

3. 1980년대 해킹과 관련된 문화가 등장함