14주 2강

정보통신과 보안

1. 정보통신 보안의 개요

◆ 정보통신 보안의 필요성

- 해킹 : 정보 시스템이나 정보통신 시스템에 허가받지 않고 침투하는 행위
- 기술이 발전해가는 만큼 해킹 기술도 발전하고 있으며, 이에 따라 보안 기술도 발전할 수밖에 없음

2. 보안 위협과 악성 프로그램

◆ 크래커와 불법 공격

- 크래커 : 다른 사람의 컴퓨터 시스템에 무단으로 침입해 정보를 훔치거나 프로그램을 훼손하는 불법 행위를 하는 사람
  - 방해
    - 송신자의 데이터를 수신자에게 전달하지 못하도록 시스템의 일부를 파괴하거나 사용할 수 없게 하는 것
  - 가로채기
    - 가로채서 데이터를 얻는 행위
  - 변조
    - 허가되지 않은 주체가 시스템에 불법으로 접근하여 데이터를 변경하는 것
  - 위조
    - 허가되지 않은 주체가 시스템에 거짓정보를 삽입하여 수신자가 착각하게 만드는 것

2. 보안 위협과 악성 프로그램

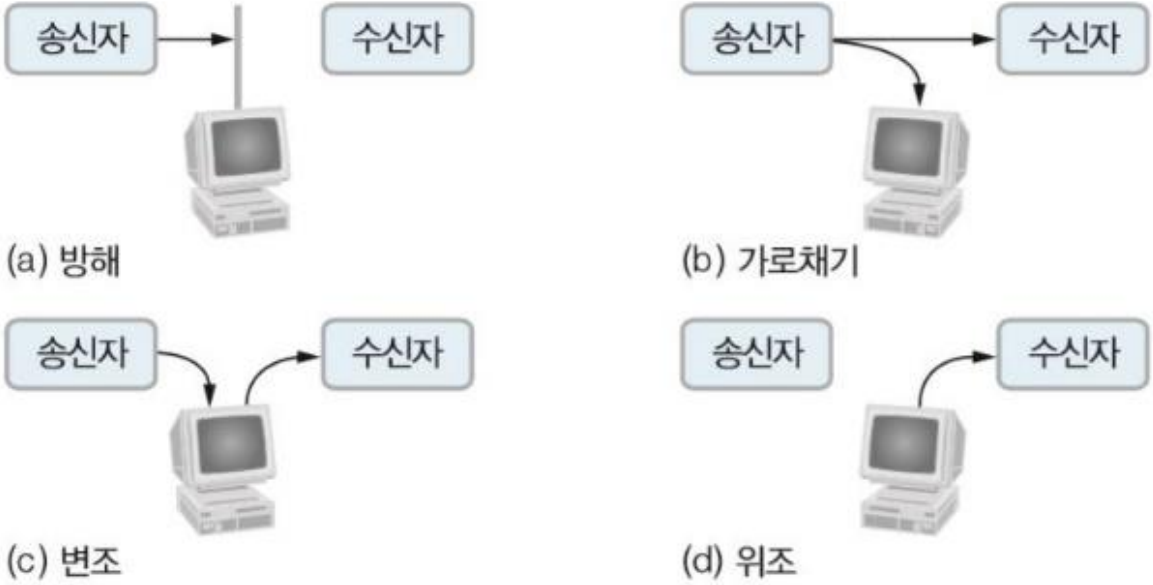

그림 11-3 불법 공격의 유형

2. 보안 위협과 악성 프로그램

◆ 악성 프로그램

▪ 악성 소프트웨어, 또는 악성 코드라고도 함

- 컴퓨터 바이러스
  - MS 워드나 엑셀처럼 컴퓨터에서 실행되는 프로그램의 일종
  - 자기 복제를 하며, 컴퓨터 시스템을 파괴하거나 작업을 지연 및 방해
- 웜
  - 실행 코드 자체로 번식하며, 주로 PC에서 실행
  - 1999년 들어 전자우편을 이용 해 다른 사람에게 전달되는 형태
- 트로이 목마
  - 컴퓨터 사용자의 정보를 빼 가는 악성 프로그램
  - 목마 속에서 나온 그리스 병사가 트로이를 멸망시킨 것에 비유
  - 유틸리티 프로그램에 악의적인 코드를 내장하거나 그 자체를 유틸리티 프로그램으로 위장
  - 컴퓨터 바이러스나 웜과는 달리, 보통 다른 파일에 삽입되거나 스스로 전파되지 않음

2. 보안 위협과 악성 프로그램

◆ 악성 프로그램

- 백도어
  - 시스템 보안이 제거된 비밀 통로
  - 시스템 설계자가 서비스 기술자의 접근 편의를 위해 일부러 만들어 놓은 시스템의 보안 구멍
  - 정상적인 인증 절차를 거치지 않고, 컴퓨터와 암호 시스템 등에 접근할 수 있도록 하는 방법
- 스파이웨어
  - 스파이(spy)와 소프트웨어(software)의 합성어
  - 다른 사람의 컴퓨터에 잠입하여 개인정보를 추적, 모니터 및 소유하며, 제3자에게 유출시키는 프로그램
- 루트킷
  - 불법적인 해킹에 사용되는 기능들을 제공하는 프로그램들의 모음
  - 트로이 목마 설치, 내부사용 흔적 삭제, 관리자 권한 획득, 원격접근, 백도어 등

2. 보안 위협과 악성 프로그램

◆ 불법 공격의 종류

- 스니핑
  - 네트워크상에 돌아다니는 패킷(정보의 작은 조각들)을 중간에서 도청하는 해킹 유형의 하나
  - 원격지로 로그인을 시도하는 사용자들이 입력하는 패스워드를 중간에서 가로채는 해킹용 툴로 많이 사용

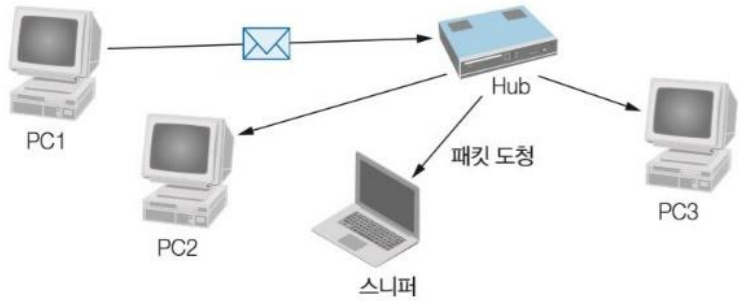

그림 11-5 스니핑 공격

2. 보안 위협과 악성 프로그램

◆ 불법 공격의 종류

- IP 스푸핑
  - 공격자가 다른 사람의 IP를 강탈하여 우회적으로 공격하는 방법(IP를 속이는 것)
  - 현재까지도 TCP/IP 약점을 이용한 여러 가지 공격 기법이 지속적으로 나오고 있음

그림 11-7 IP 스푸핑 공격

2. 보안 위협과 악성 프로그램

◆ 불법 공격의 종류

- APT
  - 일정 기간 잠복하면서 내부 네트워크에 대한 정보를 수집한 후 주요 서버에 침입하여 중요한 자료를 유출시키는 것
  - 2011년 농협 시스템 해킹, 현대 캐피탈 고객 정보 유출
- DoS와 DDoS
  - DoS(서비스 거부) : 관리자 권한 없이도 특정 서버에 처리할 수 없을 정도로 대량의 접속 신호를 한꺼번에 보내 해당 서버가 마비되도록 하는 해킹 기법
  - DDoS(분산 서비스 거부) : 공격자를 분산시켜 여러 PC(좀비 PC)를 이용하여 공격하는 것

2. 보안 위협과 악성 프로그램

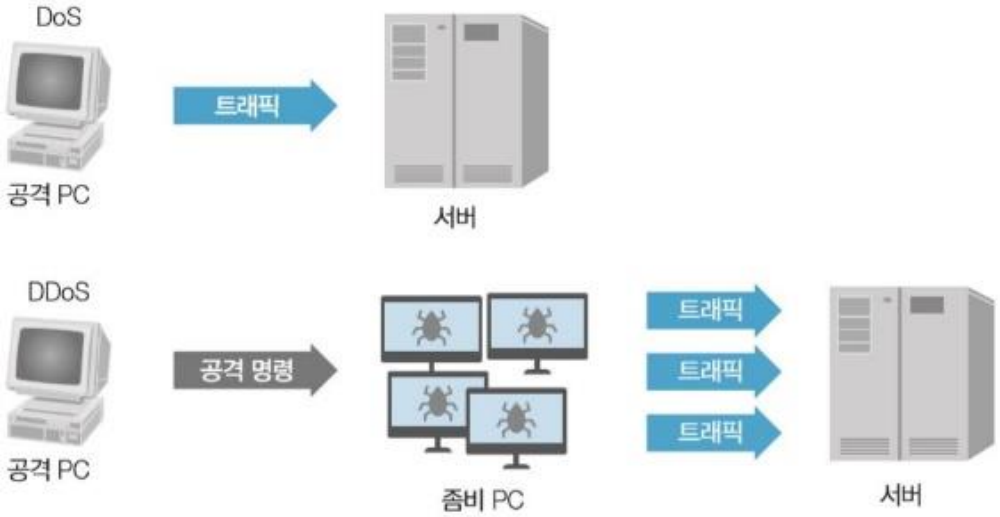

그림 11-10 DoS와 DDos 공격

3. 네트워크 보안

◆ 방화벽

- 내부 네트워크와 외부 네트워크 사이에 있는 하드웨어와 소프트웨어로 구성
- 보통은 라우터나 서버 등에 위치하는 소프트웨어
- 침입차단 시스템이라고도 함

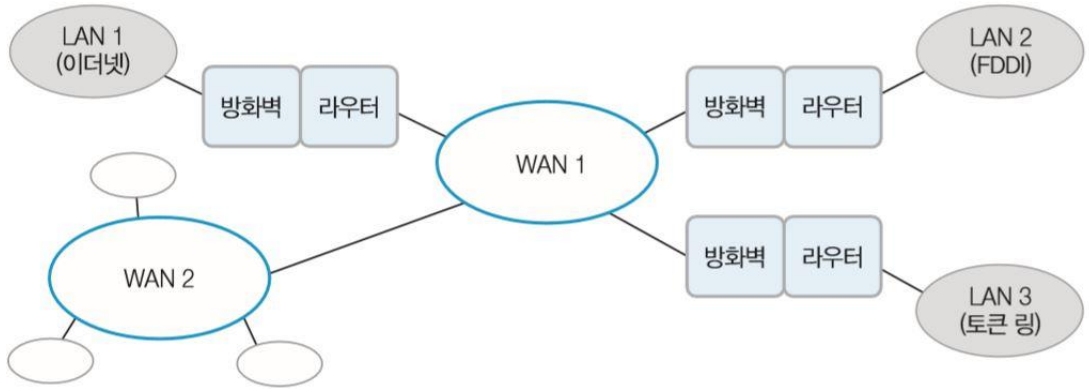

그림 11-11 방화벽의 구성

3. 네트워크 보안

◆ 침입탐지 시스템(IDS)

- 시스템이나 네트워크에 인증 절차를 거치지 않고 불법으로 침입한 사용자를 찾아내는 시스템
- 단순한 접근제어 기능을 넘어 네트워크 시스템을 실시간으로 모니터링하고 비정상적인 침입을 탐지하는 보안 시스템

3. 네트워크 보안

◆ ESM(통합 보안관리)

- 방화벽, 침입탐지 시스템, 가상 사설망 등의 보안 솔루션을 하나로 모은 통합 보안관리 시스템

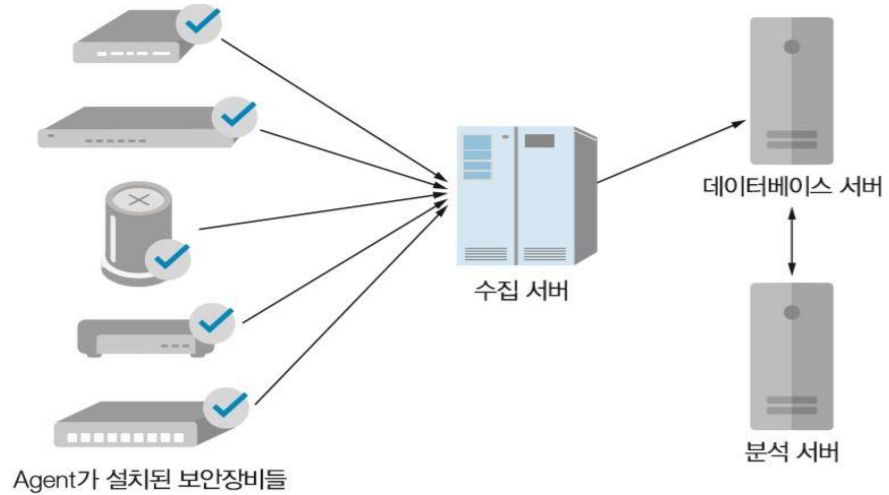

그림 11-14 ESM의 개념

3. 네트워크 보안

◆ IPS(침입방지 시스템)

- 침입탐지 시스템의 탐지와 방화벽의 차단 능력을 결합한 보안 방식
- 비정상적인 트래픽을 능동적으로 차단하고 격리하는 등 방어 조치를 취하는 보안 솔루션

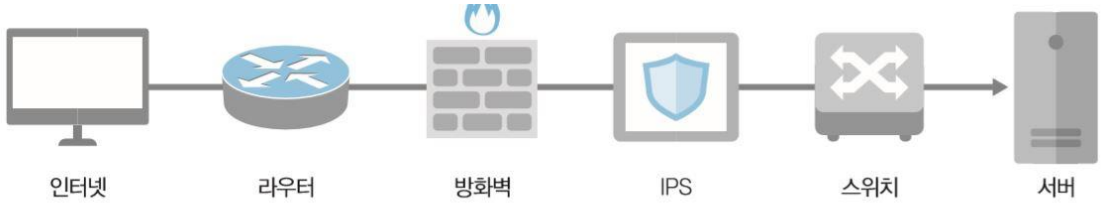

그림 11-15 IPS의 개념

3. 네트워크 보안

◆ NAC(네트워크 접근 제어)

- 허가되지 않거나 악성 코드에 감염된 컴퓨터나 모바일 기기 등을 네트워크에 접속하는 것을 원천적으로 차단하여 시스템 전체를 보호하는 보안 솔루션
- 사전 방어적인 목적

◆ 역추적 시스템

- 공격을 시도하는 공격자의 위치와 네트워크상 실제 위치가 서로 다르다 하더라도 실제 공격자의 근원지를 실시간으로 추적하는 기술

4. 애플리케이션 보안

◆ DRM

- 디지털콘텐츠가 무분별하게 복제될 수 없도록 하는 보안 기술
- 허가된 사용자만 접근할 수 있도록 만드는 제한 기술

◆ 전자서명

- 개인의 고유성을 주장하고 인정받기 위해 디지털 문서에 전자 방식을 이용해 서명하는 것

◆ 전자 인증서

- 전자상거래나 비즈니스를 위한 문서 교환 시 사용자의 신원과 문서의 내용을 보증하는 문서

6. 정보보안 요소기술과 암호학

◆ 암호화와 복호화

- 암호화 : 암호화되지 않은 상태의 평문을 암호문으로 만드는 것
- 복호화 : 암호문을 평문으로 바꾸는 것

◆ 암호화와 복호화

▪ 대치 암호

- 평문의 각 문자를 다른 문자나 기호로 일-대-일 대응시켜 암호문자로 변환하는 방식
  - 시저 암호 : 각 문자를 세 번째 뒤에 있는 문자로 대체

M(평문)	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
E_k(M) (암호문)	d e f g h i j k l m n o p q r s t u v w x y z a b c

  - 단일 알파벳 암호 : 문자를 다른 문자로 일-대-일 매핑

M(평문)	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
E_k(M) (암호문)	o f j g z h r e k t a x d v q i s l u p m y n c b w

◆ 암호화와 복호화

▪ 치환 암호

- 평문에 있는 문자의 위치를 바꾸는 방식
  - 각 단어의 알파벳 순서를 뒤집어 끝부터 적는 방법으로, 간단하게 암호화

M(평문)	data communication
E_k(M)(암호문)	atad noitacinummoc

7. 디지털 포렌식과 인터넷 품질보증(SLA)

- 디지털 포렌식
  - PC나 노트북, 휴대전화 등 각종 저장매체 또는 인터넷 상에 남아 있는 각종 디지털 정보를 분석해 범죄 단서를 찾는 수사기법
- 인터넷 품질 보증(SLA)
  - 주로 호스팅 업체가 사용자와 맺는 계약(기업, 개인)

8. 4차 산업혁명 시대의 정보통신 보안

◆ 블록체인

- 블록에 데이터를 담아 연결한 모음 형태로 연결 하여 수많은 컴퓨터에 동시에 이를 복제해 저장하는 분산형 데이터 저장 기술
- 중앙 집중형 서버에 거래 기록을 보관하지 않고 거래에 참여하는 모든 사용자에게 거래내역을 보냄

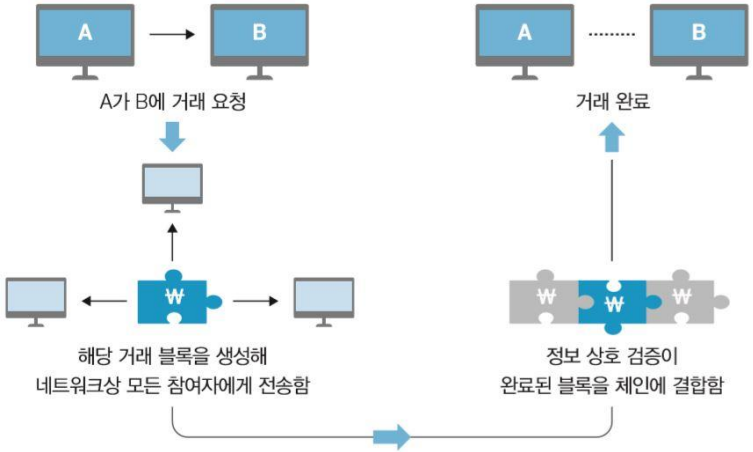

그림 11-35 블록체인의 거래 과정 예

8. 4차 산업혁명 시대의 정보통신 보안

◆ 생체인식

- 각 개인이 갖고 있는 특징을 인식하여 보안을 유지하는 기술
- 신체적 특성으로는 지문, 홍채, 얼굴, 정맥 등이 있으며 행동적 특성으로는 목소리, 서명 등

◆ 양자 암호통신

- 양자의 복제 불가능 특성을 이용하여 완벽한 보안 통신을 구현하는 것

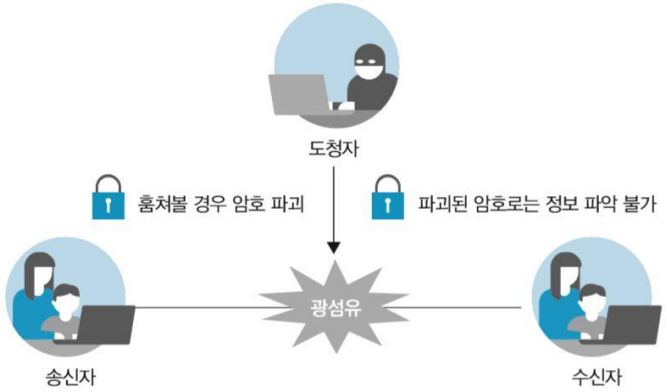

그림 11-37 양자 암호통신의 개념

수고하셨습니다.