정보보호 개론

04. Threats & Vulnerability (3)

1. 공격 형태 분류 (1)

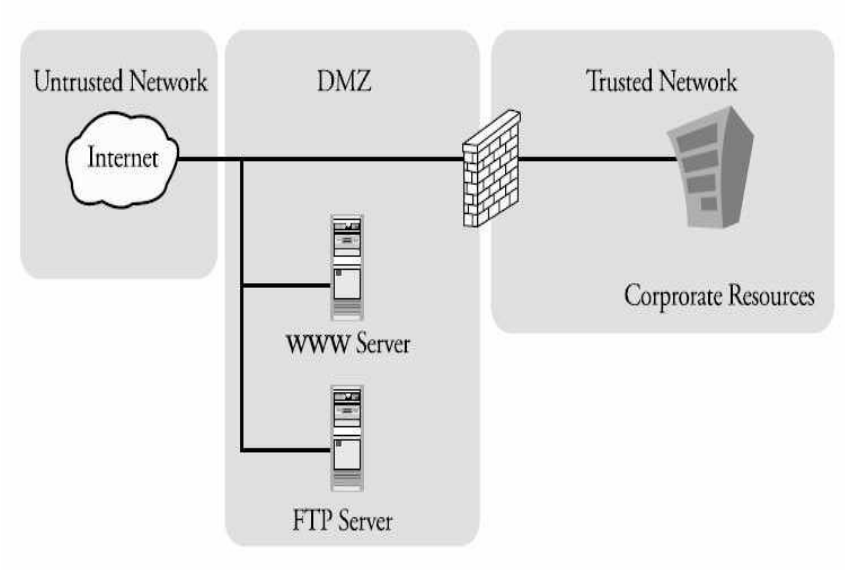
- 의지에 의한 분류
  - 소극적(passive) 공격
    - 특정 공격 목표가 없고, 적극적인 데이터 파괴 및 변조의 목적을 갖지 않는다.
    - 트래픽 상의 정보를 훔쳐보는 정도
    - 유형
      - Folder shared
      - Sniffing
      - Scanning (port, agent)

1. 공격 형태 분류 (2)

- 의지에 의한 분류 (계속)
  - 적극적(active) 공격
    - 목표에 대한 특정 목적을 가지고 데이터 파괴 및 변조를 취하는 공격 형태
    - 전문적인 네트워크 지식이나 공격 관련 지식이 있는 악의적인 해커에 의해 주로 수행
    - 유형
      - Masquerade
      - Eavesdropping
      - Replay
      - Modification of message
      - Denial of Service
      - Spoofing (IP, MAC)
      - Sniffing

1. 공격 형태 분류 (3)

- 공격 위치에 의한 분류
  - 외부(external) 공격
    - Trusted 영역을 기준으로 내부와 외부 구별
    - DMZ(demilitarized zone)
  - 내부(internal) 공격
    - 내부 공격에 의한 성공률이 더 높음



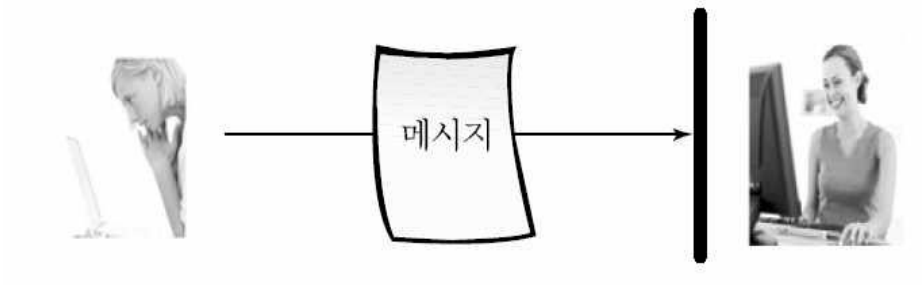
1. 공격 형태 분류 (4)

- 조직적(structured) 공격
  - 공격에 대한 충분한 지식과 경험을 가진 자가 침해방법, 결정, 관련지식, 자금, 시간, 장비 등의 치밀한 준비와 수행을 계획하여 수행하는 공격
- 비조직적(unstructured) 공격
  - 미성년자나 단순 호기심을 가진 자들이 인터넷 검색 등을 통해 얻어진 해킹 툴이나 유틸리티를 사용하여 공격하는 행태

전형적인 공격 유형 (1)

- 정상적

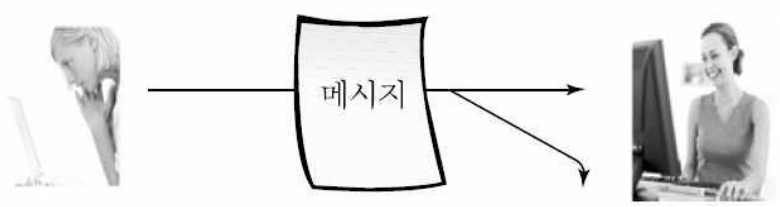
- 방해(interruption)



  - 대표적 예
    - DoS(Denial of Service)
  - 대응책
    - 장애 감지 시 연결 단절 후 다른 통신 수단으로 대체
    - 침입차단시스템을 통한 1차 방어
    - 2차적으로 고가용성 기능을 이용하여 서비스 지속 및 연결 유지

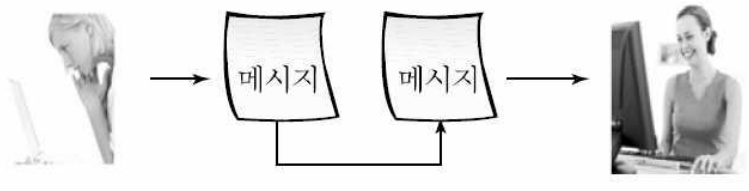
전형적인 공격 유형 (2)

- 가로채기(interception)

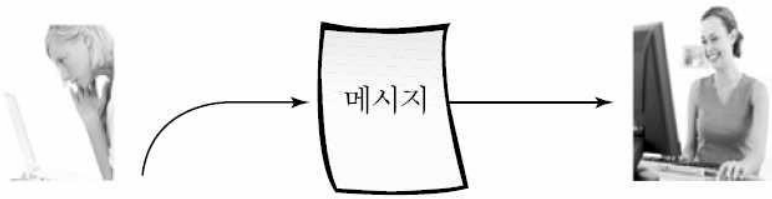


  - 통신의 일부를 엿듣는 행태
  - 대표적인 예
    - Sniffing
  - 대응 방안
    - 기밀성을 패킷에 부여 (암호화)

- 변조(modification)



- 위조(fabrication)



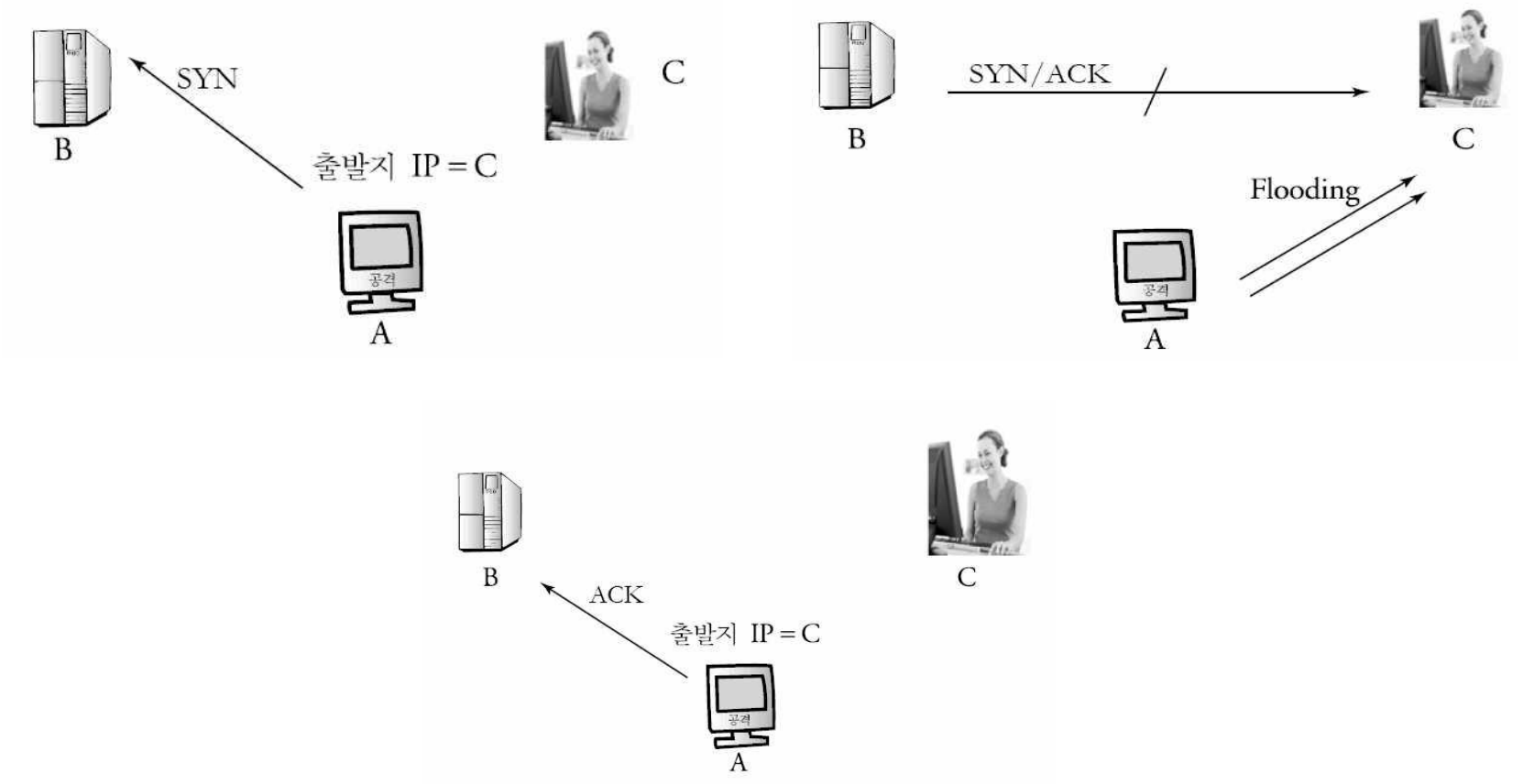
  - 대응 방안
    - 암호 및 서명을 통한 기밀성과 무결성

네트워크 공격 기술 (1)

- SYN Flooding
  - TCP 연결 설정 요청 패킷인 SYN을 다량으로 전송
  - 연결 요청을 처리하기 위한 자원(시스템 큐, 메모리) 소진

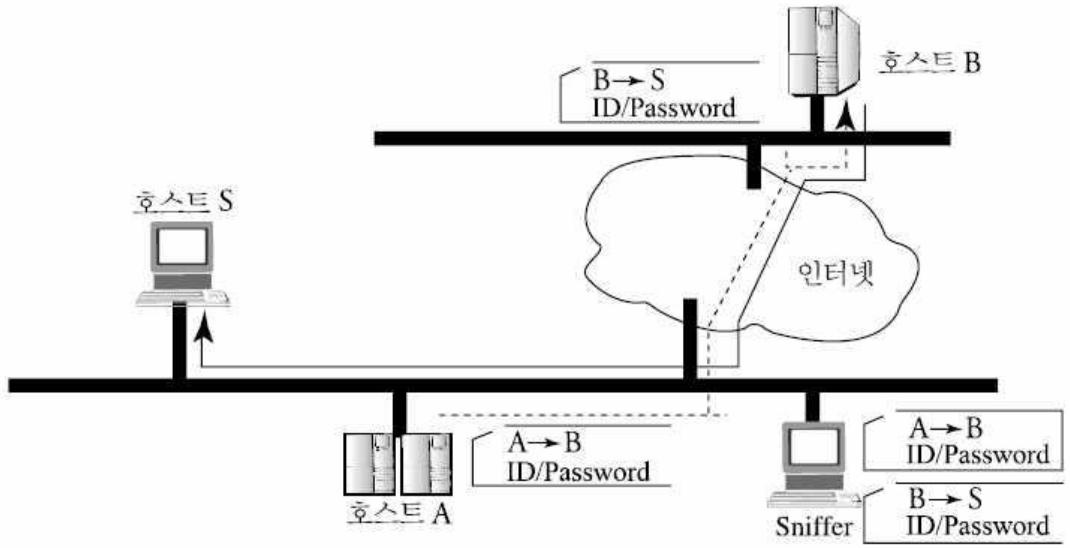
네트워크 공격 기술 (2)

- IP Spoofing



네트워크 공격 기술 (3)

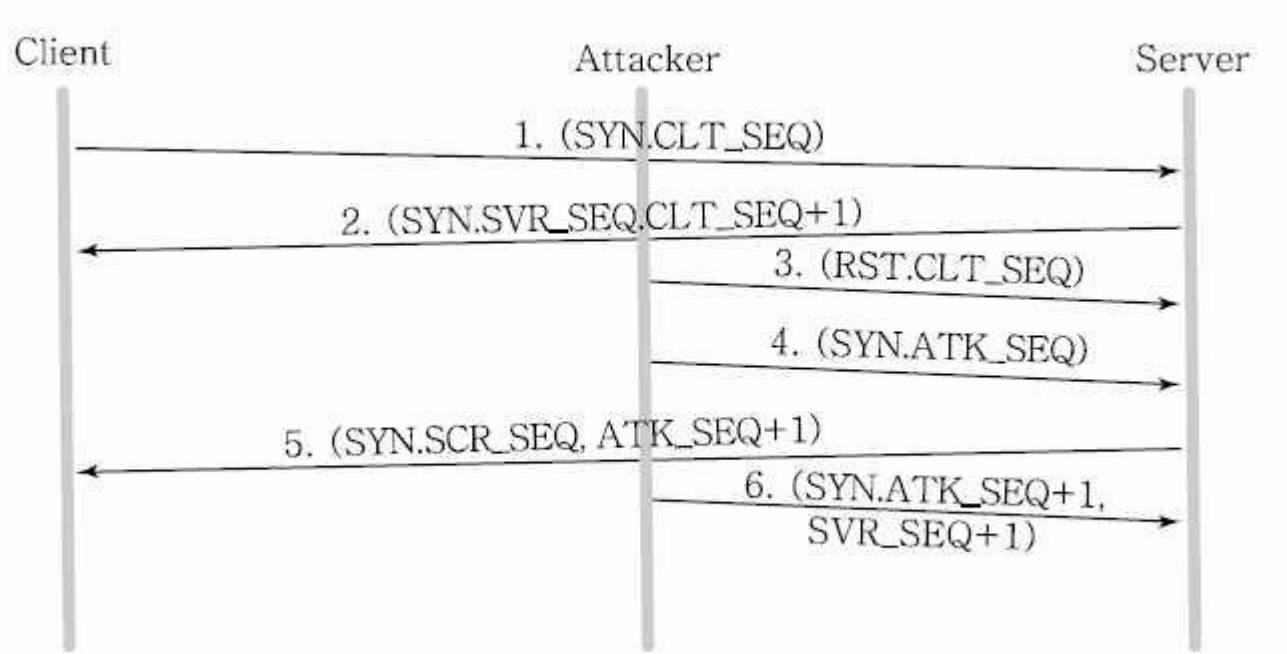
- Sniffing
  - Ethernet의 Promiscuous 모드 설정



  - Broadcast 망들은 모두 취약

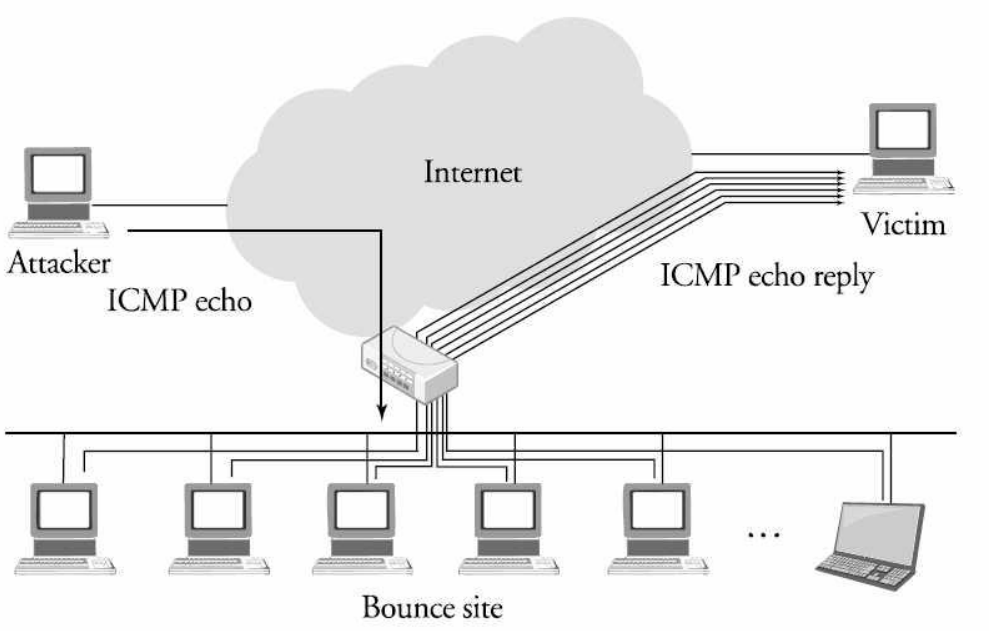
네트워크 공격 기술 (4)

- Session Hijacking
  - 스니핑을 통해 필요한 정보 획득, 적절한 시기에 중간에 끼어들어감



네트워크 공격 기술 (5)

- Smurf Attack
  - ICMP Echo/Reply 취약성 이용
  - 제3자의 Broadcast 주소를 수신자로, 목표의 주소를 송신자로 하여 전송

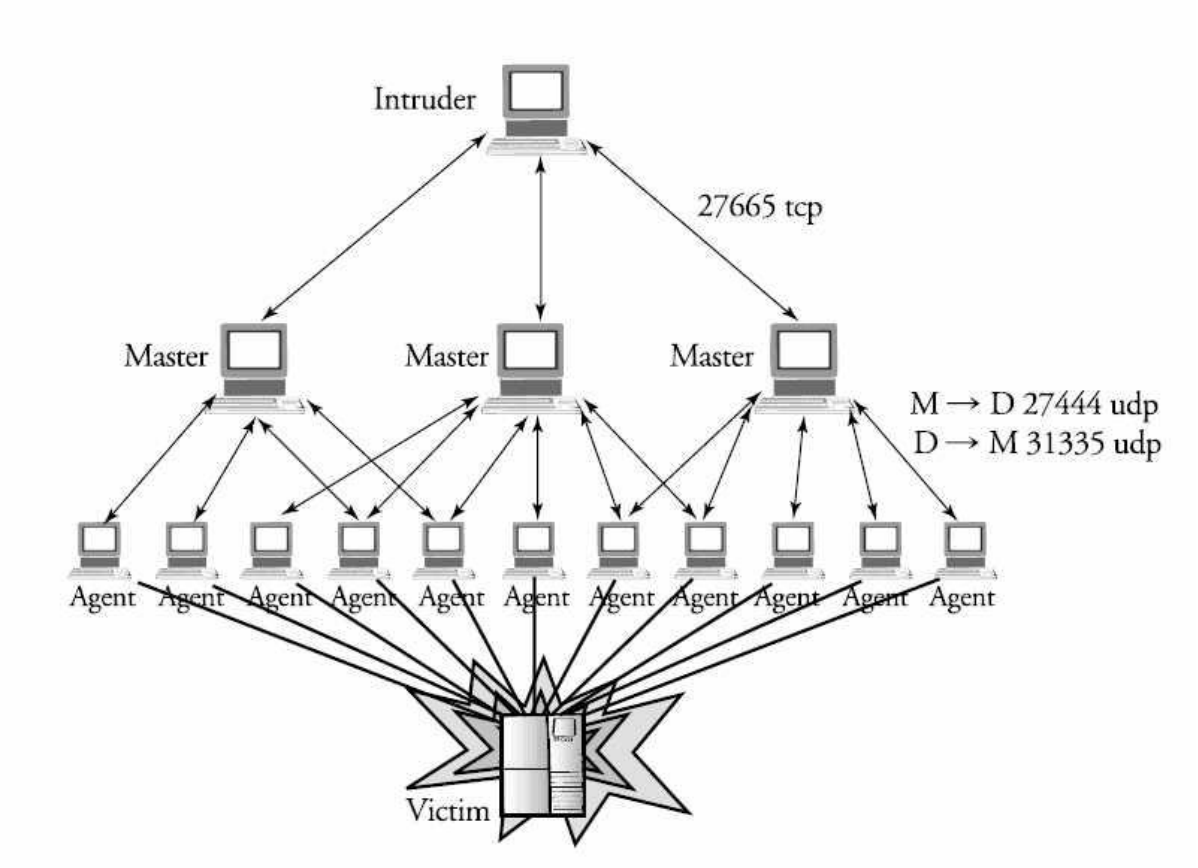


네트워크 공격 기술 (6)

- Land Attack
  - 출발지 주소를 공격 대상자의 IP주소 및 Port 번호로 변조하여 공격 대상자에게 전송
  - 루프 상태에 빠지게 되어 장애 유발
  - 대응 : 라우터에서 출발지 주소가 내부인 외부 패킷 차단

네트워크 공격 기술 (7)

- DoS와 DDoS



네트워크 공격 기술 (8)

- 버퍼 오버플로우(Buffer Overflow)
- 컴퓨터 바이러스
  - 컴퓨터의 부트 영역, 메모리 영역, 파일 영역 등에 기생하면서 자기 증식 및 복제가 가능하고 특종 공격 목표를 가지고 있으면서 인위적인 파괴성을 갖는 컴퓨터 프로그램
- 웜
  - 감염 대상을 갖지 않으며, 복제 기능이 없음
  - 점차 악의적인 기능을 갖는 웜이 등장
    - 슬래머 웜, 코드레드 웜, 님다 웜, 블래스터 웜 등
- 스팸 메일

네트워크 공격 기술 (9)

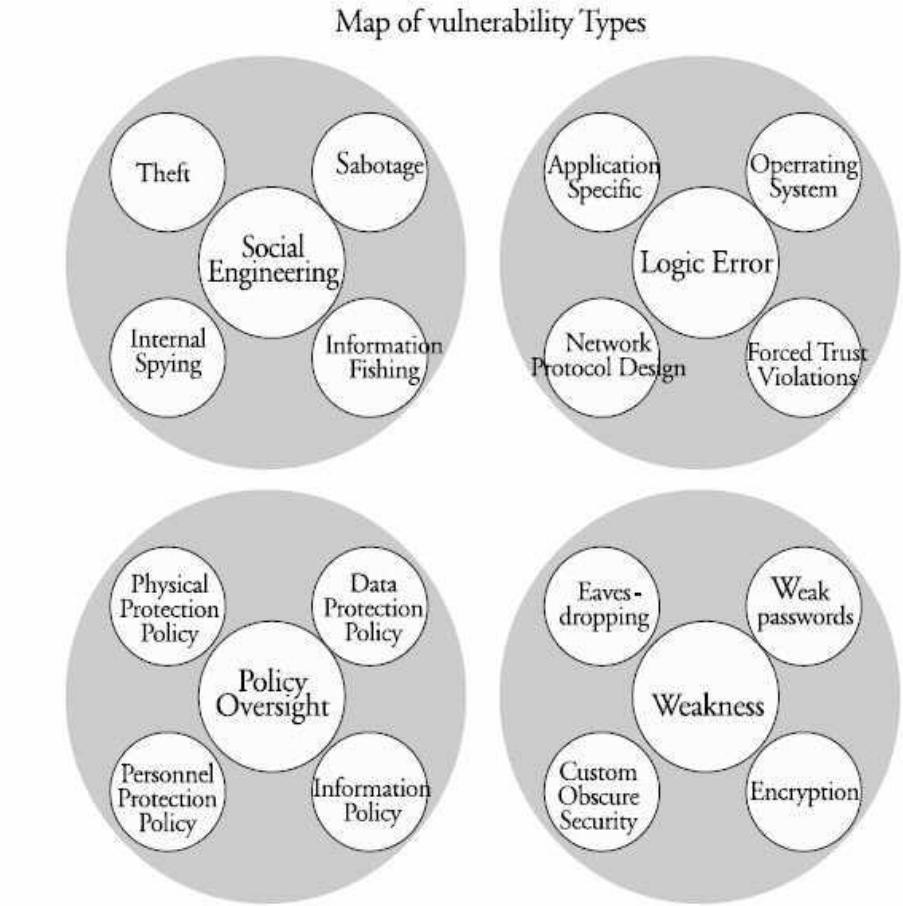
- 논리 폭탄(Logic Bomb)
  - 삽입된 코드의 형태를 가지며, 트로이 목마의 일종으로서 바이러스나 웜 등을 전파하기 위하여 사용
- 치핑(Chipping)
  - 특정 조건을 만족하면 동작하는 기능이나 회로를 칩 일부분에 하드웨어적으로 삽입
- 나노 머신(Nano Machine)
  - 컴퓨터 하드웨어를 파괴하는 작은 크기의 로봇으로, 컴퓨터의 슬롯 등의 틈을 통해 잠입한 뒤, 기관이나 회로 등을 파괴
- 재밍(Jamming)
  - 정상적인 동작을 방해하는 교란 신호를 통해 기능 마비

네트워크 공격 기술 (9)

- HERF(High Energy Radio Frequency) gun
  - 라디오 주파수대의 고출력 전파를 발생시켜 전자장비들을 마비
  - 수백만 와트의 전파를 한 곳에 집중시켜 동시에 발사하는 것과 동일한 출력을 발생
- EMP(Electro Magnetic Pulse) Bomb
  - 핵폭발과 같은 정도의 전자기파를 발생시킴으로써 전자파에 노출된 컴퓨터나 통신 시스템의 모든 전자회로들이 파괴
- AMCW(Autonomous Mobile Cyber Weapon)
  - 자신이 네트워크를 따라 목표를 찾아 바이러스 기술 등을 이용하여 적의 컴퓨터나 네트워크 시스템을 파괴하거나 정보를 조작하는 도구
- 봇넷(BotNet)
  - 악성코드에 감염된 PC들의 네트워크로 연결된 집합으로 공격자의 명령에 따라 목표를 공격하게 됨

2. 취약성

- 취약성(Vulnerability)
  - 위협으로부터 정보자산을 보호하기 위한 물리적, 정책적, 사회적 보호 체계 상의 미약한 부분이나 관리 상의 허점, 실수 오류로 인한 취약 부분



사회공학적

- 사회적 관계를 기반으로 하는 취약성
- 개인이나 회사의 인간 관계를 악용하거나 인위적인, 의도적인 공격으로 패스워드 또는 중요 정보를 얻어내거나 피해를 주는 행위

Social Engineering	Theft	정보의 절도 및 탈취
	Sabotage	불법적인 공작 행위
	Internal Spying	내부 스파이를 이용
	Information Fishing	정보를 인간 관계 등을 통해 획득

논리적 오류

- 프로그램 제작 시 인지하지 못한 버그 또는 오류, 허점 등을 이용해 정보의 획득, 시스템 또는 네트워크로 침입

Logic Error	Operating system	Buffer overflow와 같은 공격
	Application specific	응용 프로그램의 실행 조건을 이용
	Network Protocol design	프로토콜의 통신 방식을 이용한 IP spoofing 공격
	Forced trust violation	침입자가 신뢰할 만한 사용자로 믿게 만드는 것

정책 관리(Policy Oversight)

- 시스템 운영 및 보안 정책 기반에서의 취약성
- 백업 미비, 적절치 못한 권한 부여, 보안 장비 미설치, 침입자에 대한 추적 및 대응 미비

Policy Oversight	Data protection policy	데이터 백업이나 데이터 보호 소홀
	Physical Protection policy	UPS 미비나 돌변 상황에 대한 대응 조치 미비
	Personnel Protection policy	사용자들의 보안 미흡
	Information policy	침입자 보고 미비

약점(weakness)

- 보안이 설정되었다고 하더라도 관찰에 의한 지속적인 취약성 탐색 또는 컴퓨팅 파워의 증가에 따른 기술적 환경의 변화에 따라 생겨날 수 있는 취약성

Weakness Error	Weak password	Password의 지정 패턴을 이용 ex) password attack
	Encryption	보안 알고리즘의 해독
	Eavesdropping	평문(Plain text)를 해독 ex) Sniffing
	Custom obscure security	사용자의 S/W, H/W의 변화

웹 서비스

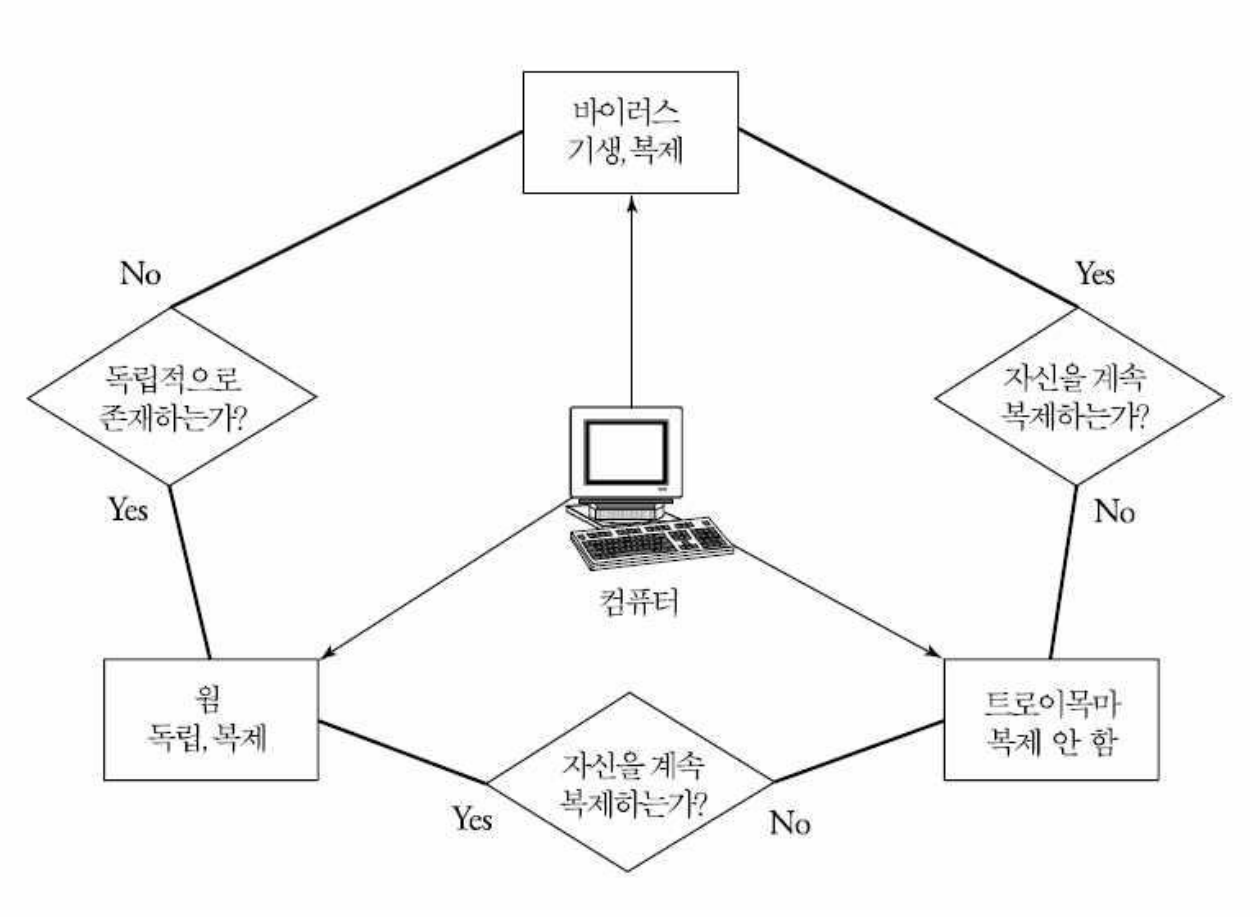
- 주요 요소
  - 웹서버
  - 데이터베이스(DBMS)와 SQL
  - 스크립트 언어(서버/클라이언트)
  - 프록시 서버
- 웹 응용 프로그램 취약점
  - Unvalidated Input
  - Broken Access Point
  - Broken Authentication and Session Management
  - Cross Site Scripting(XSS) Flows
  - Buffer Overflow
  - Injection Flaws
  - Improper Error Handling
  - Insecure Storage
  - Denial of Service
  - Insecure Configuration Management

운영체제 취약성

- 운용상의 취약점
  - 업그레이드의 취약성
  - 설치상의 취약성 (default 설정)
  - 프로그램으로 인한 포트 개방
    - Live update
    - 서버용 포트 개방
  - 웹서비스로 인한 웜의 침해
  - E-mail로 인한 침해
  - P2P 서비스로 인한 침해

악성 프로그램에 따른 취약성

- 바이러스, 웜, 트로이목마



컴퓨터 바이러스 (1)

- 특징
  - 기생
  - 자기 복제
  - 은폐
  - 파괴
  - 전파경로
- 발전단계
  - 1세대 – 원시형
    - 예 : Stoned, Jerusalem, Lbc, Mini, Pingpong
  - 2세대 – 암호형
    - 백신 개발자에게 분석 및 발견이 어렵도록 암호화
    - 메모리에서는 쉽게 탐색됨
    - 예 : Slow, Cascade, Wanderer, Burglar
  - 3세대 – 메모리 상주형
    - 감염 여부를 숨기기 위해 원래 정보를 조작하여 화면에 출력
    - 예 : Hide-and-Seek
  - 4세대 – 다형성
    - 복잡한 형태로 진단 및 백신 개발에 시간이 걸림
    - 예 : Natas, ½, Coffee-shop
  - 5세대 – 매크로
    - 매크로 언어를 이용한 바이러스
    - 운영체제와 독립적으로 감염 가능하고, 문서를 통한 전파 가능
    - 예 : WM_CAP, Excel_Larox, CIH, HPS
  - 현재

컴퓨터 바이러스 (2)

- 감염 위치에 따른 분류
  - 부트 바이러스
  - 파일 바이러스
  - 부트 • 파일 바이러스
  - 매크로 바이러스
  - 메모리 상주 • 비상주 바이러스
- 감염 방법에 따른 분류
  - 기생형
  - 겹쳐쓰기형
  - 산란형
  - 연결형
  - 매크로

악성 프로그램

- 백도어(backdoor)/트랩 도어
- 트로이 목마(Trojan Horse)
- 웜(Worm)
- 스파이웨어(spyware)
- 조크(joke), 혹스(Hoax)
- 악성 스크립트
- 에이전트 프로그램
- 기타