컴퓨터 네트워크

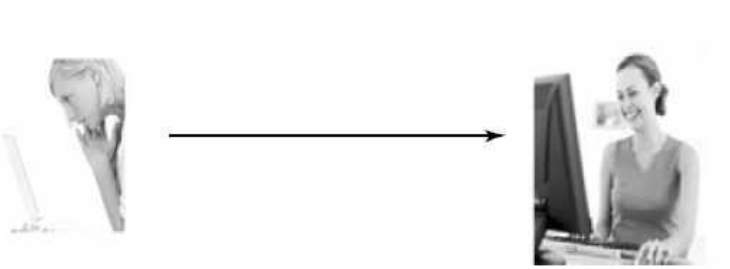
13장. 네트워크 보안 (3)
- 보안 프로토콜

이번 시간의 학습 목표

- 네트워크 보안의 개념과 관련 이슈 이해
- 라우터와 프록시로 구현한 방화벽의 원리 이해

전형적인 공격 유형 (1)

- 정상적

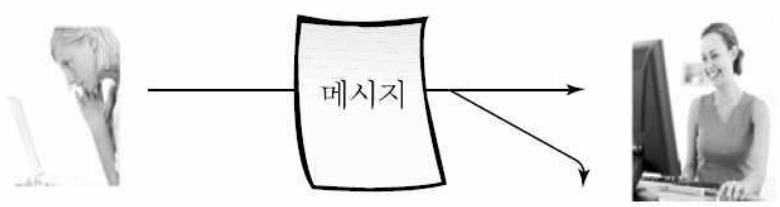


- 방해(interruption)

  - 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

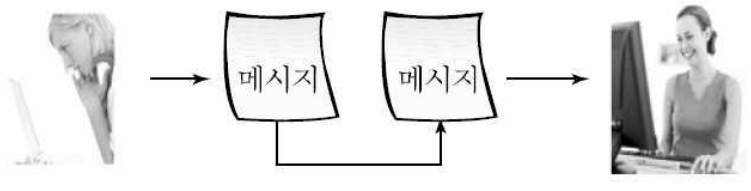
전형적인 공격 유형 (2)

- 가로채기(interception)

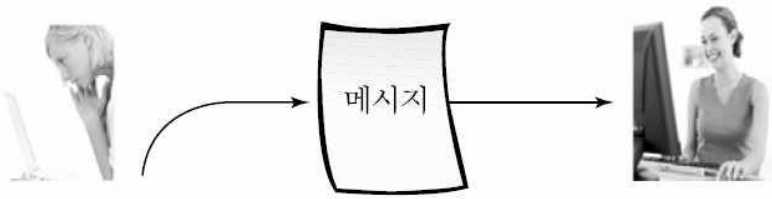


  - 통신의 일부를 엿듣는 행태
  - 대표적인 예
    - Sniffing
  - 대응 방안
    - 기밀성을 패킷에 부여 (암호화)

- 변조(modification)



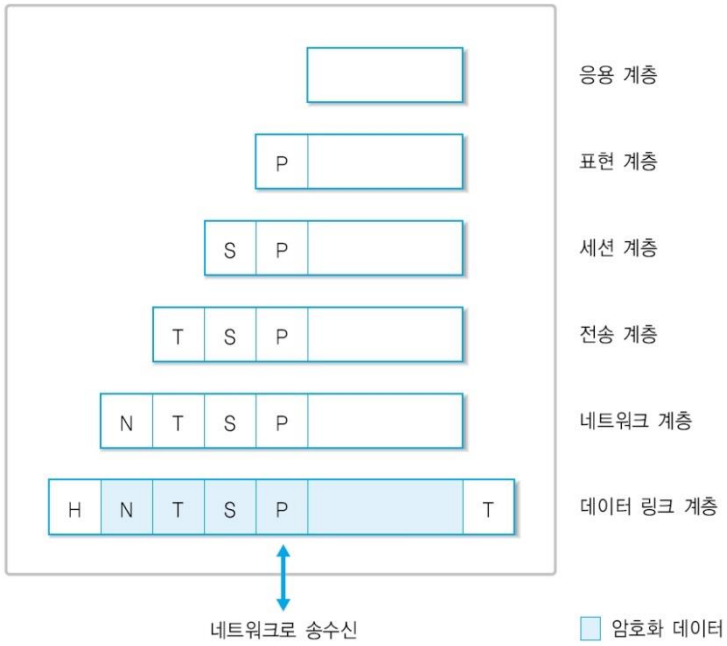
- 위조(fabrication)



  - 대응 방안
    - 암호 및 서명을 통한 기밀성과 무결성

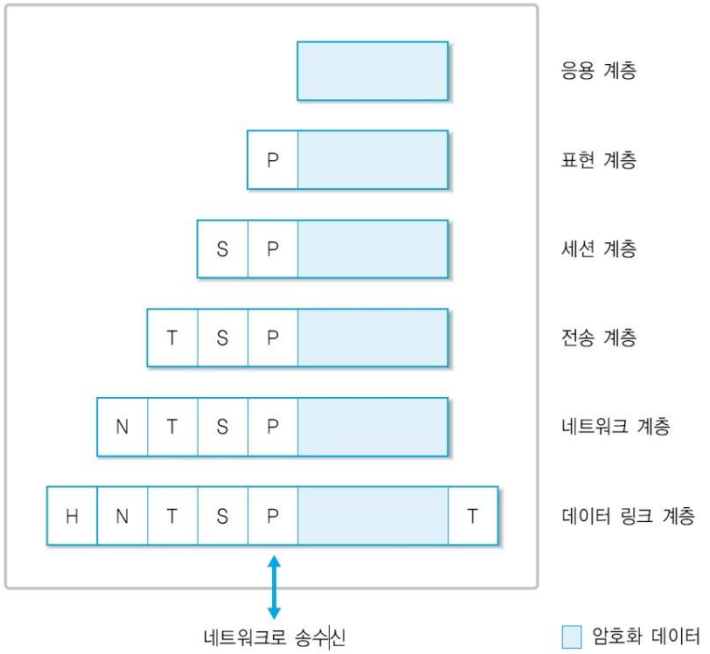
암호화

- 데이터링크 계층 암호화
  - 전송 선로상의 감청으로부터 보호
  - 단점: 라우터 등 호스트 내부에서는 보호가 안됨



[그림 13-9] 데이터 링크 계층 암호화

- 응용 계층 암호화
  - 호스트 내부에서 보안을 지원



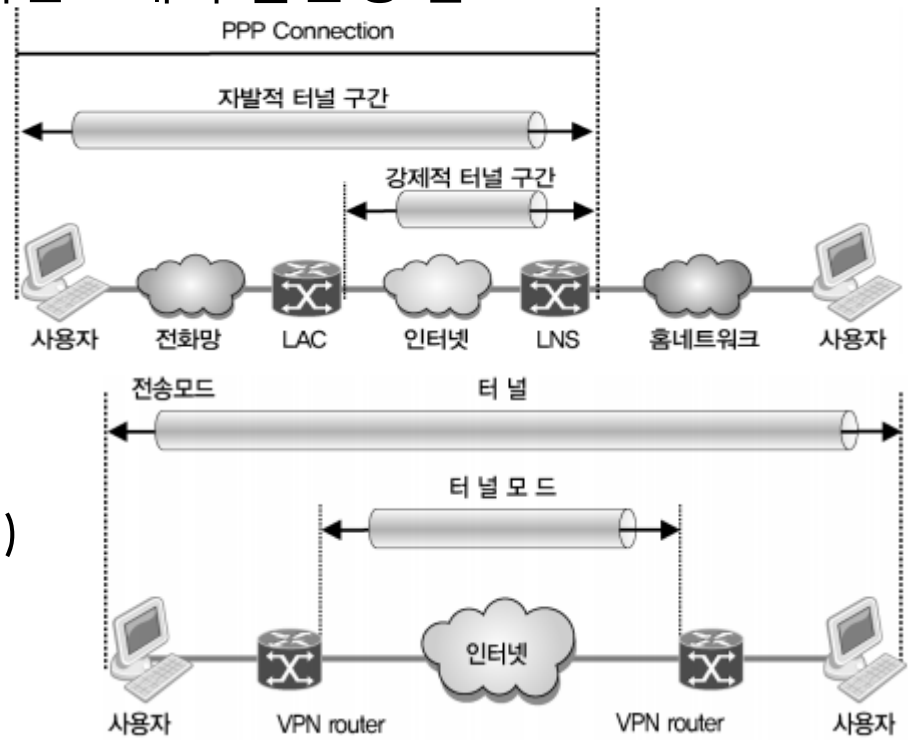
[그림 13-10] 응용 계층 암호화

VPN (1)

- 가상사설망(Virtual Private Network)
  - 공중망을 사설망처럼 이용할 수 있도록 사이트 양단 간 암호화통신을 지원하는 장치
  - 원격사용자가 공중망 및 인터넷을 통해 내부망의 시스템 사용 시, 공중망 구간에서의 도청으로 인한 정보유출을 방지하기 위해 사용자와 내부망간 암호화 통신을 지원
- 가상 사설망의 장점
  - 저비용으로 광범위한 사설 네트워크의 구성이 가능
  - 기업 네트워크 관리 및 운영비용이 절감 됨
  - 재택근무자 등 개별 사용자 지원 및 무선 이동 환경의 사용자 지원, 기업
  - 네트워크의 유동성 지원이 가능

VPN (2)

- 가상 사설망의 단점
  - 인터넷 상황에 따라 네트워크 성능이 종속적
  - 전용선보다는 신뢰성 및 보안성 수준이 낮음
  - 서비스에 문제가 발생하면 책임소재가 불분명 함
- 가상 사설망의 기능
  - 암호화 기능
  - 사용자 인증 기능
  - 무결성 기능
  - 터널링 기능
- 관련 프로토콜
  - L2TP(Layer 2 Tunneling Protocol)
  - IPSec(IP Security Protocol)



트래픽 제어

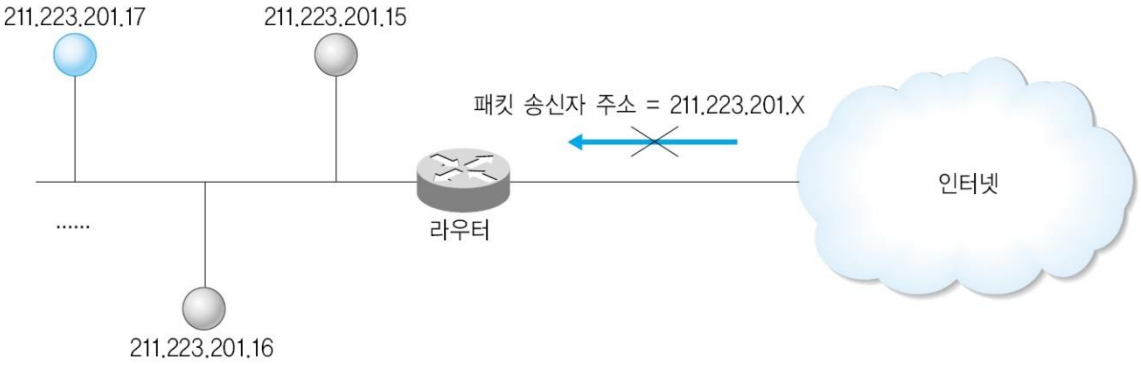
- 특정 호스트의 트래픽 량 자체가 중요한 정보가 될 수 있음
- 예: 특정 군부대의 통화량이 많으면 모종의 군사 작전의 가능성
- 무의미한 가공 데이터를 추가적으로 발생시켜 통계 자료에 혼란을 줄 필요가 있음
  - 자료의 통신량, 송신자, 수신자 랜덤하게 생성

방화벽

- 방화벽(Firewall)
  - 개방적인 공중 인터넷망과 제한된 그룹의 사설망 사이에서 보안 기능 제공
    - 패킷 필터링
      - 패킷의 헤더 또는 내용을 검색하여 차단 여부 결정
      - 일반적으로 라우터에서 제공
    - 트래픽 관찰을 통한 의심스러운 사용자 감시

라우터를 이용한 방화벽 구현

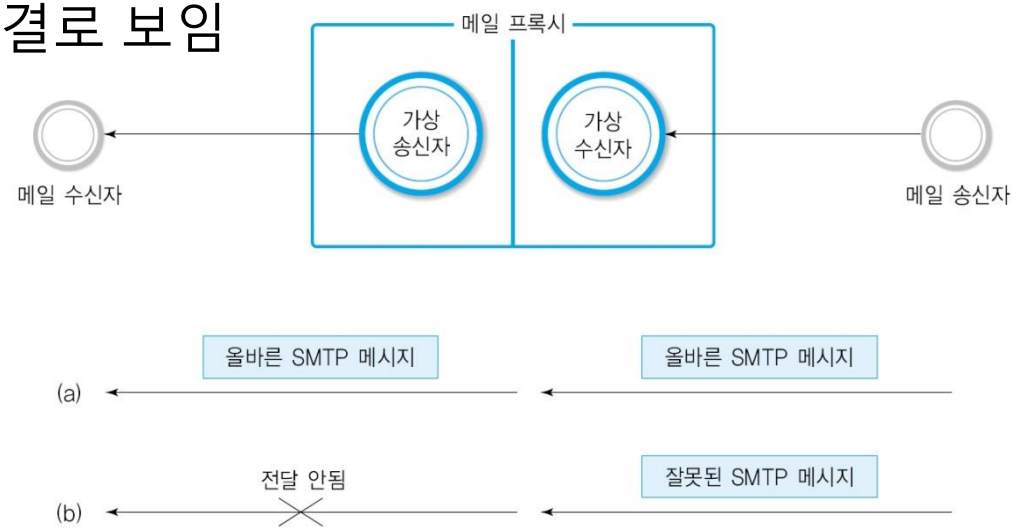
- 외부망과의 중개 기능을 수행하므로 간단하면서도 매우 효과적
  - IP 주소 기반
    - 위장 IP 주소의 차단
      - 인터넷으로부터 211.223.201.X를 발신자로 하는 패킷은 입력될 수 없음
    - 스팸 메일을 발송하는 외부 호스트 차단
    - 내부 사용자가 유해 사이트로 접속하는 것 차단
  - 포트 번호 기반: 특정 서비스 이용을 차단
    - Web, FTP 등 서비스별로 허용/차단 설정



[그림 13-12] 위장 IP 주소의 차단

프록시를 이용한 방화벽 구현

- 라우터 기반
  - 네트워크 계층과 전송 계층의 헤더에 기초하여 방화벽 기능 수행
- 프록시 기반
  - 응용 환경에서 적절하게 처리할 수 있는 정보만 수신하도록 가상의 응용 프로그램을 시뮬레이션하는 방화벽
  - 내부에서는 외부 연결로 보이고, 외부 네트워크에서는 내부의 응용 연결로 보임



[그림 13-13] 메일 프록시

질의 / 응답