네트워크 보안

네트워크 보안 공격 - 스니핑

네트워크 보안

- 스니퍼를 이용한 스니핑

- 스니핑 방지 대책

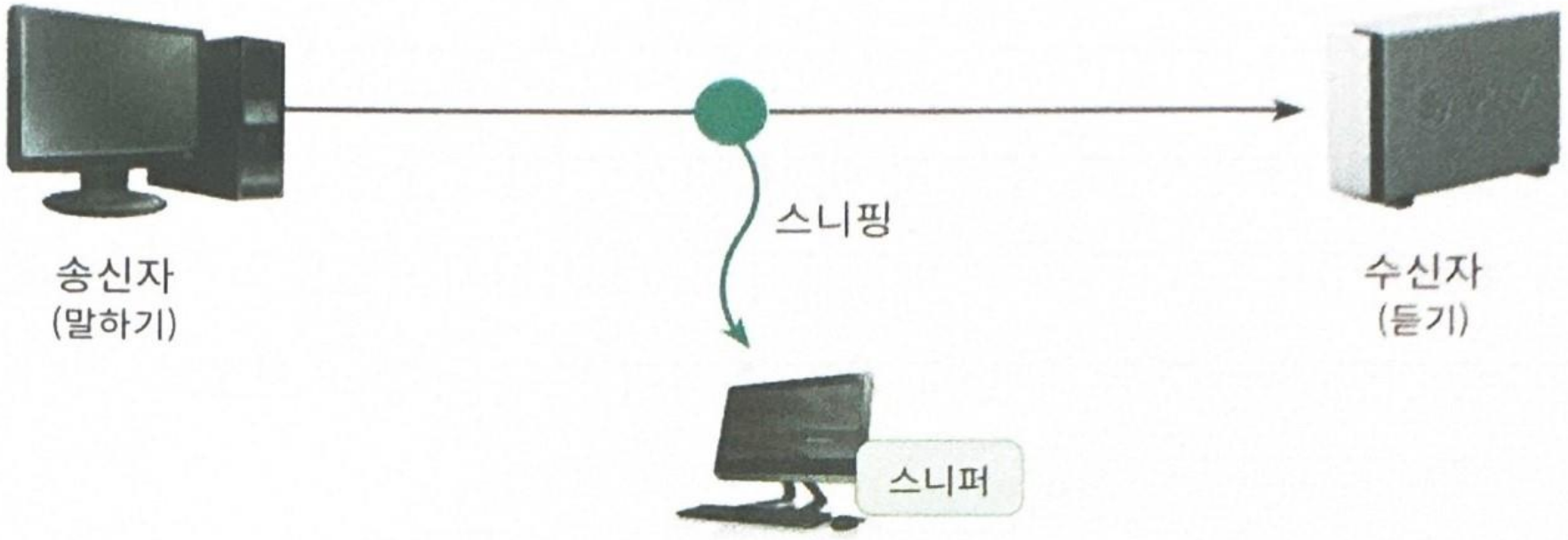
스니핑

- **스니핑(Sniffing)**
  - 도청 대신 네트워크 보안 분야에서 사용
  - 스니프(sniff)
    - 송신자와 수신자가 주고 받는 데이터를 도청 하는 것

스니퍼를 이용한 스니핑

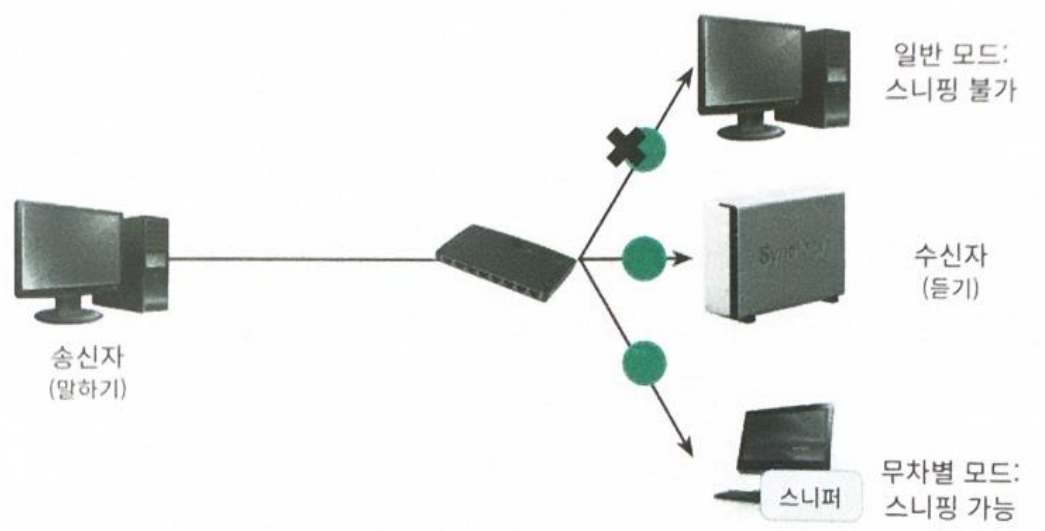
스니퍼를 이용한 스니핑

- 스니퍼(Sniffer)
  - 스니핑을 하기 위한 프로그램
    - 스니퍼를 통한 스니핑은 보통 네트워크의 환경을 공유



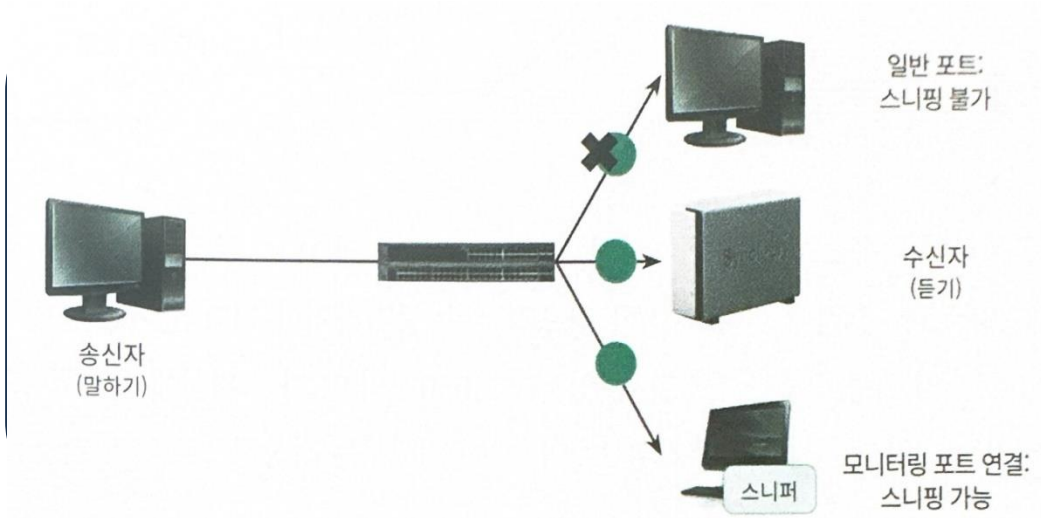
스니퍼를 이용한 스니핑

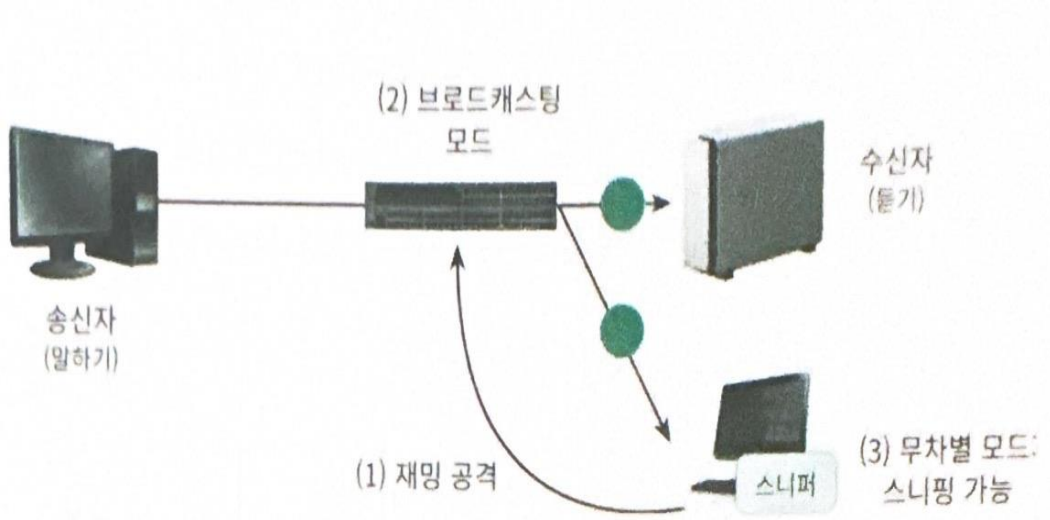
- 허브 환경
  - 더미/ 수동 허브
    - 모든 포트 단순 전달 역할
    - 특정 포트 전달 기능 X
    - 다른 PC 패킷 확인 X
  - 무차별 모드(Promiscuous Mode)
    - 자신의 주소가 아닌 패킷 전달 O
    - 수신 받은 모든 패킷 스니핑 O



스니퍼를 이용한 스니핑

- 스위치 환경
  - 모니터링 포트
    - 포트 연결 시 포트로 스니핑 O
    - 네트워크 사용량, 응답 시간 관리 O
  - 스위치 재밍
    - 특정 주소로 받는 패킷 전달 기능 방해
    - 매핑 테이블(Mapping Table) 사용
    - 최대 저장 개수 초과 시 정상 매핑 O
  - 스푸핑 공격 기법
    - 스푸핑(Spoofing)
      - 공격자가 수진자로 위장하는 기법

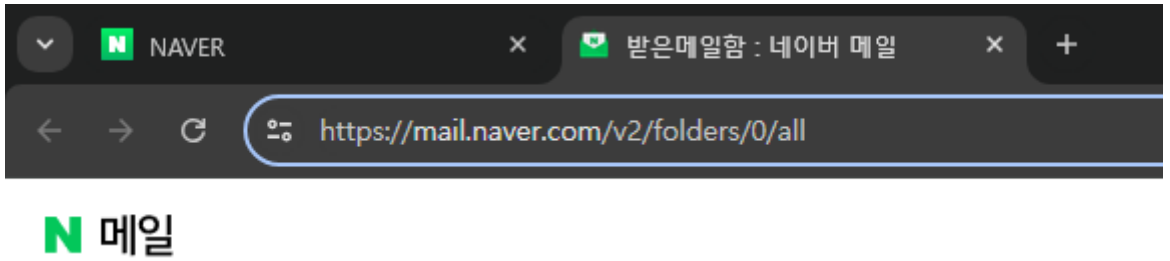




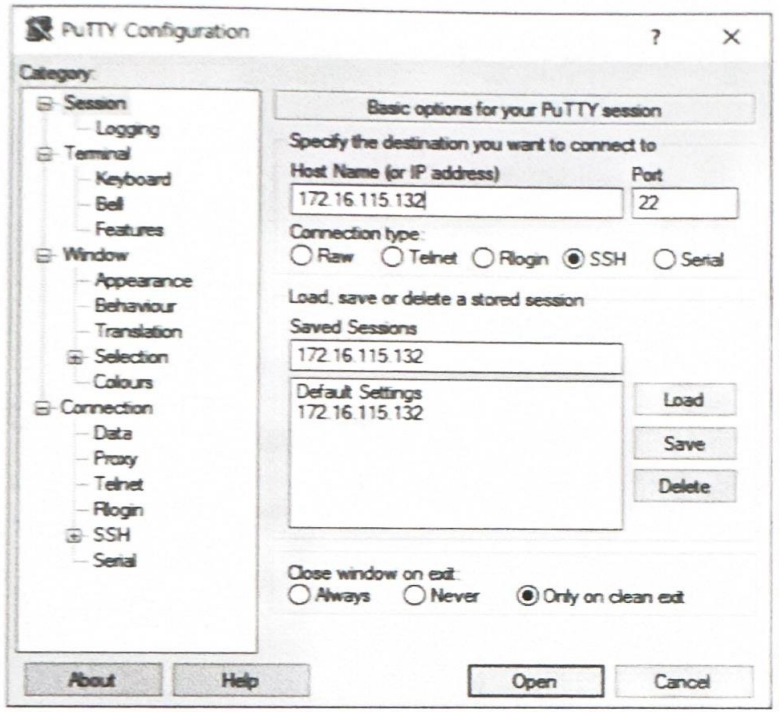
스니핑 방지 대책

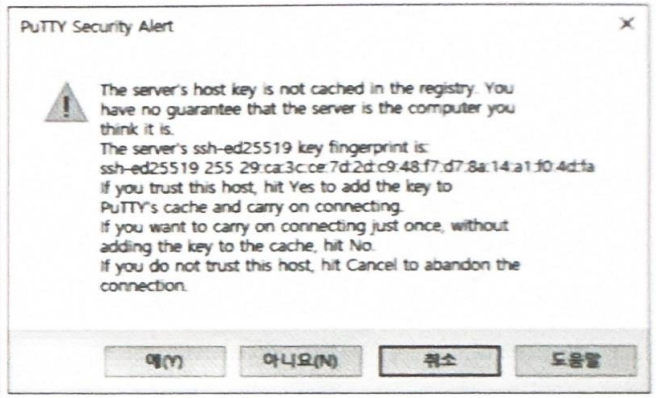
스니핑 방지 대책

- HTTPS 사용
  - HTTP 사용 시 ID와 암호의 노출 위험
  - HTTP의 암호화 기능을 추가
  - SSL/TLS 통신 프로토콜을 사용함



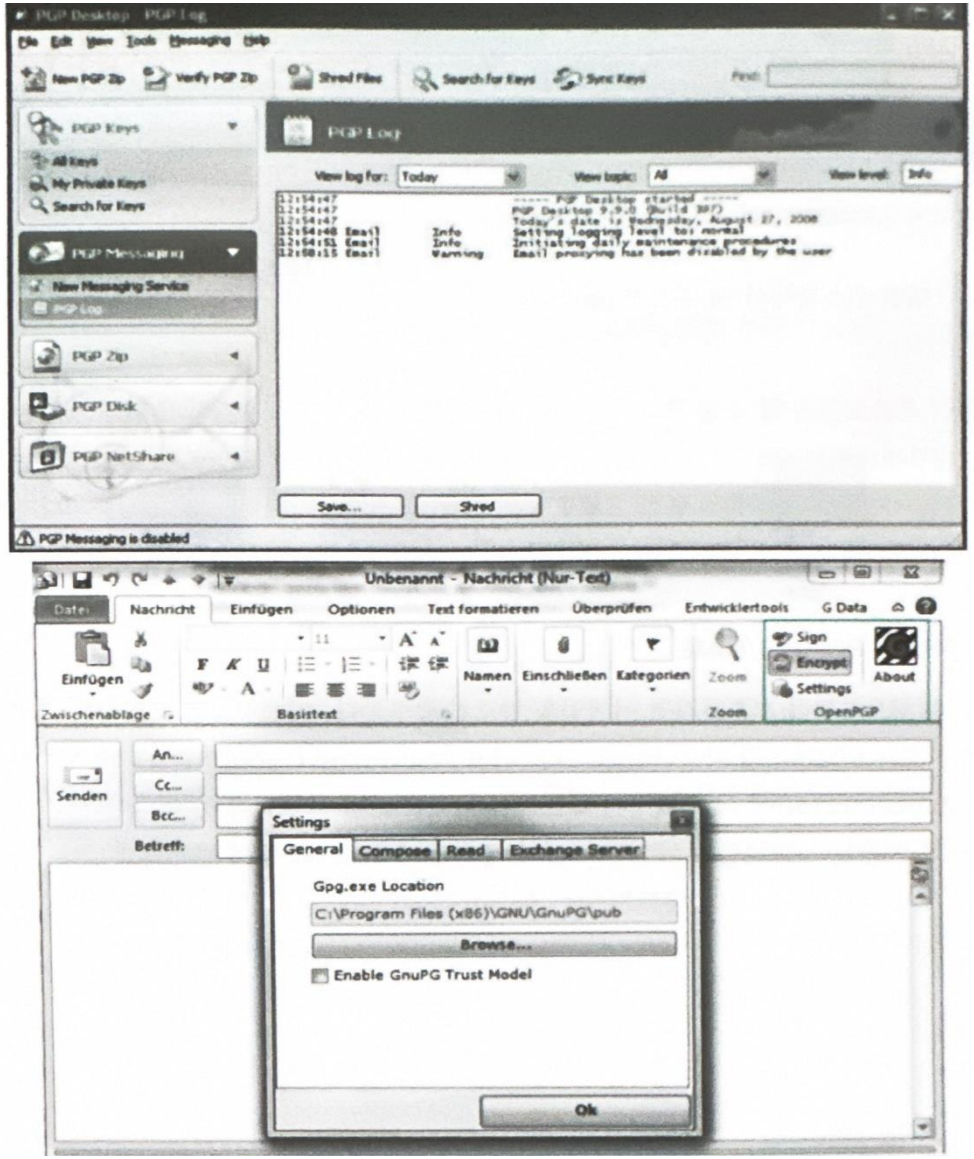
- 원격접속 SSH
  - SSH(Secure Shell)
    - 암호화 원격 접근 방식
    - 스니핑이 어려움
  - PuTTy
    - SSH 사용
    - 가상 단말기 프로그램





스니핑 방지 대책

- PGP와 S/MIME
  - PGP
    - 이메일 보안 프로그램
    - 안전성이 높아 대중적임
  - S/MIME
    - MIME에 암호화 기법을 추가함
    - MIME(Multipurpose Internet Mail Extension)
      - 이메일의 내용을 저장



스니핑 방지 대책

- VPN(Virtual Private Networks)
  - 사설망/사설 가상망
  - 통신 화사에 임대 회선 신청의 경우
  - 공개망을 이용 하는 경우
    - VPN 장비로 인증과 암호화
    - 터널링(Tunneling)