1 네트워크와 보안

IT CookBook, 정보 보안 개론과 실습 : 네트워크 해킹과 보안(개정판)

한빛미디어 Hanbit Media, Inc.

Contents

❖ 학습목표

- 네트워크의 정의를 이해한다.
- 네트워크의 분류와 특성을 이해한다.
- 네트워크 보안의 요소를 이해한다.

❖ 내용

- 네트워크의 정의
- 네트워크의 분류
- 네트워크 보안의 요소

데이터 전송 방식에 따른 네트워크 분류 (★★)

❖ 네트워크

- 지역적으로 분산된 컴퓨터 간에 통신을 위한 하드웨어 및 소프트웨어들의 시스템.

❖ 회선 교환망(Circuit Switched Network)

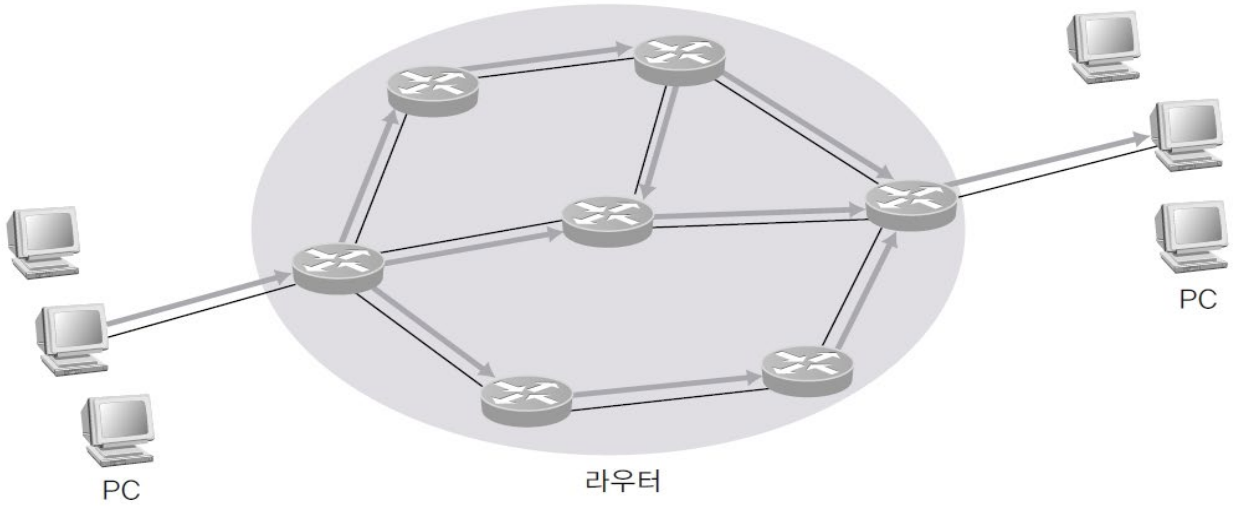
- **통신 전에 물리적인 연결로 전용 통신 선로를 설정**하여 통신이 끝날 때까지 연결을 독점적으로 사용하는 방식. 예) **전화망**
- 연결에 상대적으로 긴 시간이 필요하나, 연결이 이루어지면 **전송 지연이 거의 없음**.

[그림 1-10] 전화 연결 회로

데이터 전송 방식에 따른 네트워크 분류 (★★)

❖ 패킷 교환망(Packet Switched Network)

- 전송하고자 하는 정보를 **패킷**이라는 작은 단위로 나눔.
- 패킷마다 **발신지와 수신지의 주소**를 넣어 전송. **패킷 교환기**가 그 주소를 보고 최종 목적지까지 전달.
- 회선 교환망처럼 통신 경로가 통신 시에 확정되지 않음. 각 패킷은 네트워크 상태에 따라 **여러 경로를 통해 전송**될 수 있음.

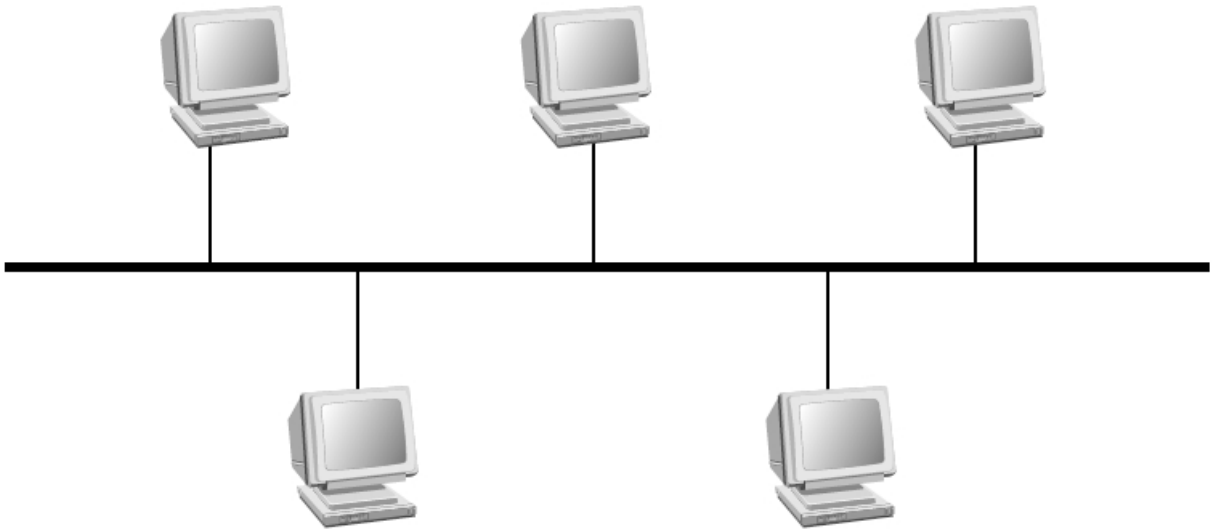


[그림 1-11] 패킷 교환망에서의 패킷 전송

위상에 따른 네트워크의 분류 (★★)

❖ 버스형(bus topology) 네트워크

- 하나의 **통신 회선**을 모든 노드가 **공유**.
- 한 노드에서 전송한 메시지가 **모든 노드에 전달(broadcasting)** 됨.
- 노드가 많아지면 **충돌**로 인해 속도가 급격히 떨어지는 단점이 있음.

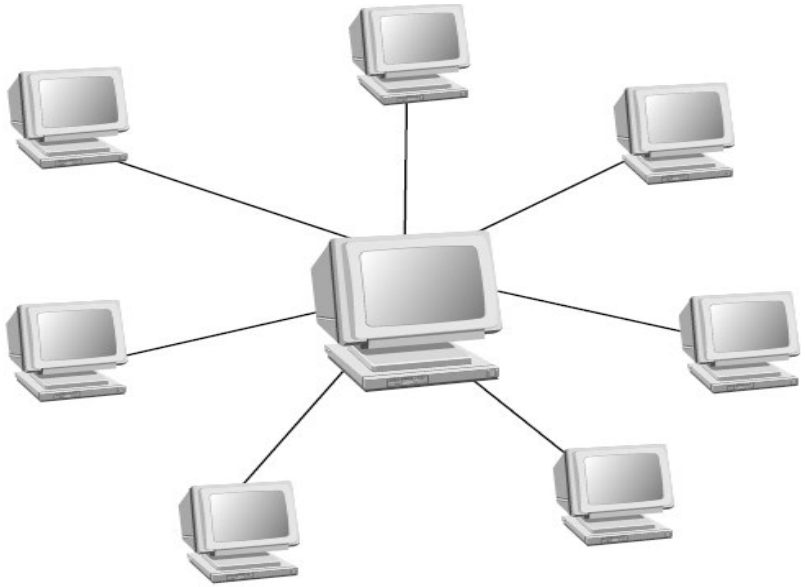


[그림 1-12] 버스형 네트워크

위상에 따른 네트워크의 분류 (★★)

❖ 스타형(star topology) 네트워크

- 중앙 제어 노드가 통신의 모든 제어 관장함. 예) 교환기
- 노드 간의 데이터가 다른 노드에 전달되지 않음. 통신 회선 전용
- 중앙 제어 노드가 작동을 못하면 네트워크가 정지되는 단점.



[그림 1-13] 스타형 네트워크

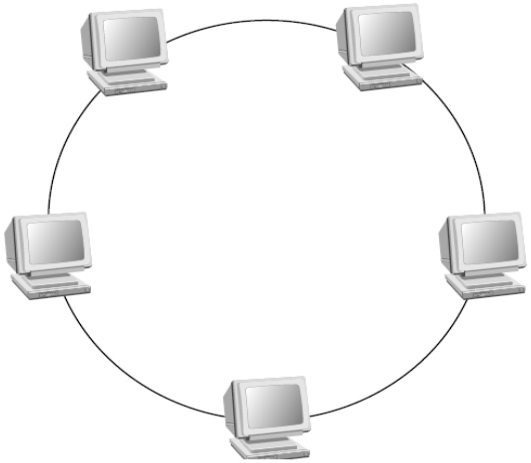
위상에 따른 네트워크의 분류 (★★)

❖ 링형(ring topology) 네트워크

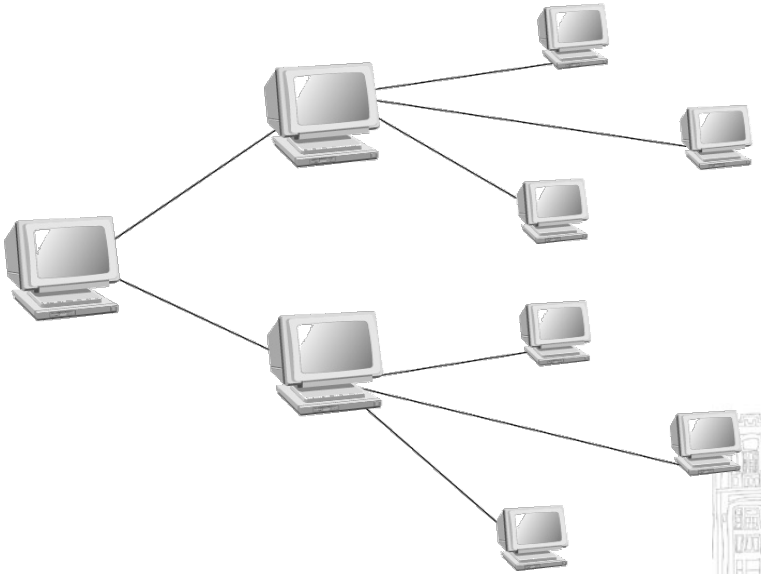
- 토큰을 받아야 데이터를 전송할 수 있는 **토큰 링**형 네트워크.
- 네트워크의 한 노드에라도 이상이 생기면 통신망이 정지됨.

❖ 허브/트리형(hub/tree topology) 네트워크

- **스위치와 허브**를 이용한 네트워크.



[그림 1-14] 링형 네트워크



[그림 1-15] 허브/트리형 네트워크

규모에 따른 네트워크의 분류 (★★)

❖ LAN(Local Area Network)

- 일반적으로 300m 이하의 통신 회선으로 연결된 네트워크. 예) 건물, 대학, 공장
- 컴퓨터 사이의 전류나 전파 신호가 정확히 전달될 수 있는 거리, 즉 한 기관의 건물에 설치된 컴퓨터를 가장 효과적으로 사용할 수 있도록 연결한 고속 통신망.
- 1980년대 초 제록스의 이더넷(Ethernet)이 LAN 실용화의 시초가 됨.

❖ MAN(Metropolitan Area Network)

- LAN을 고속의 백본(backbone)으로 묶은 도심형 네트워크. 예) 시, 도 단위
- 보통 도시나 큰 캠퍼스를 하나의 네트워크로 연결하는 데 적용.
- LAN 수준의 높은 데이터 전송률을 제공.

❖ WAN(Wide Area Network)

- 지리적으로 흩어진 거대 통신망을 의미 예) 국가, 국가간
- 지방-지방, 국가-국가, 대륙-대륙처럼 장거리 지역 사이를 연결하는 네트워크.

2. 네트워크 보안 (★)

■ 네트워크 보안의 5요소

- 기밀성(Confidentiality) - 비밀보장
- 무결성(Integrity) - 변조방지
- 가용성(Availability) - 지속적 서비스
- 서버 인증(Server Authentication) - 정당한 서버
- 클라이언트 인증(Client Authentication) - 정당한 클라이언트

네트워크 보안의 요소 (★)

■ 기밀성

- 허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것.
- **'시스템 간 안전한 데이터 전송'**과 관련됨.
- 스니핑(Sniffing)은 기밀성을 해치는 가장 일반적인 공격 형태.
- 통신의 암호화가 가장 일반적인 보안 대책.

■ 무결성

- 허락되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것.
- **'데이터가 변조되지 않고 전송되는가 '** 와 관련됨.
- 중간에서 다른 연결을 빼앗는 세션 하이재킹, 두 시스템 간의 데이터를 중간에 변조하는 MITM 공격은 무결성을 해치는 대표적인 공격.
- 통신의 암호화가 가장 일반적인 보안 대책.

네트워크 보안의 요소 (★)

■ 가용성

- 허락된 사용자 또는 객체가 정보에 접근하려 할 때 방해받지 않도록 하는 것,
- **'언제든지 필요할 때 정보 접근이 가능한가'** 와 관련됨.
- DoS가 가용성을 해치는 대표적인 공격.

■ 서버 인증

- **'클라이언트가 올바른 서버로 접속하는가 '** 를 의미
- 일반적으로 DNS 스푸핑이나 서버 파밍 등이 있음.
- SSL(HTTPS)을 통해 서버 인증을 함.

■ 클라이언트 인증

- **'올바른 클라이언트가 접속을 시도하는가 '** 를 의미
- 아이디와 패스워드가 대표적인 클라이언트 인증임.

Thank You !

IT CookBook, 정보 보안 개론과 실습 : 네트워크 해킹과 보안(개정판)

한빛미디어 Hanbit Media, Inc.