# MITM Attack

Youtube : https://youtu.be/COyV9uZcMnw

IT융합공학부 이준희

# MITM(Man In The Middle) 공격

- MITM(Man In The Middle) 공격
  - 글자 그대로 누군가의 사이에 끼어드는 것
  - 클라이언트와 서버의 통신에 암호화된 채널을 이용하면서 ARP 리다이렉트와 ICMP 리다이렉트, ARP 스푸핑이 무용지물이 되자 이를 극복하기 위해 탄생
  - MITM은 패킷 내용을 바꾸기 시도

# MITM 공격 유형

- 이메일 탈취
- 세션 탈취
- Wi-Fi 도청
- IP 스푸핑
- DNS 스푸핑
- HTTPS 스푸핑
- SSL 탈취
- **ARP 스푸핑**
- mDNS 스푸핑

**… 등**

# ARP 스푸핑

- **MAC 주소를 속이는 것 (2계층**에서 작동해 공격 대상이 **같은 랜에 있어야 함)**

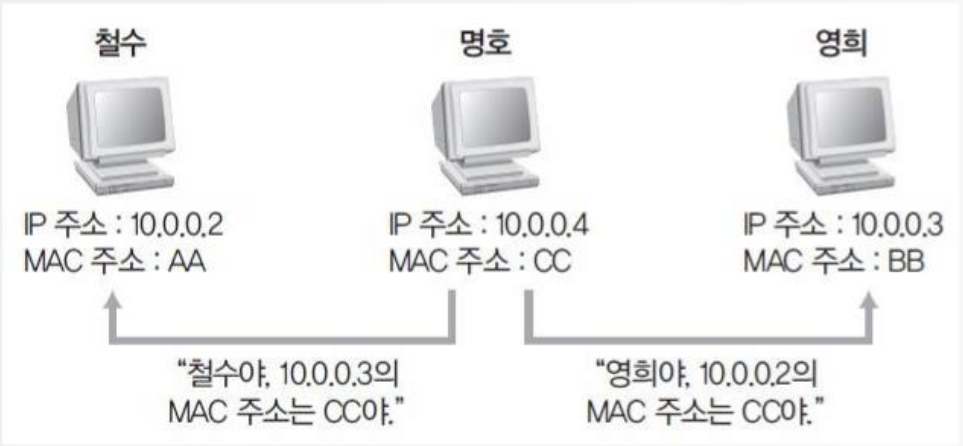


그림 7-3
ARP 스푸핑 예

| 호스트 이름 | IP 주소 | MAC 주소 |
|---|---|---|
| 철수 | 10.0.0.2 | AA |
| 영희 | 10.0.0.3 | BB |
| 명호 | 10.0.0.4 | CC |

# ARP 스푸핑

- 스니핑의 또 다른 기법

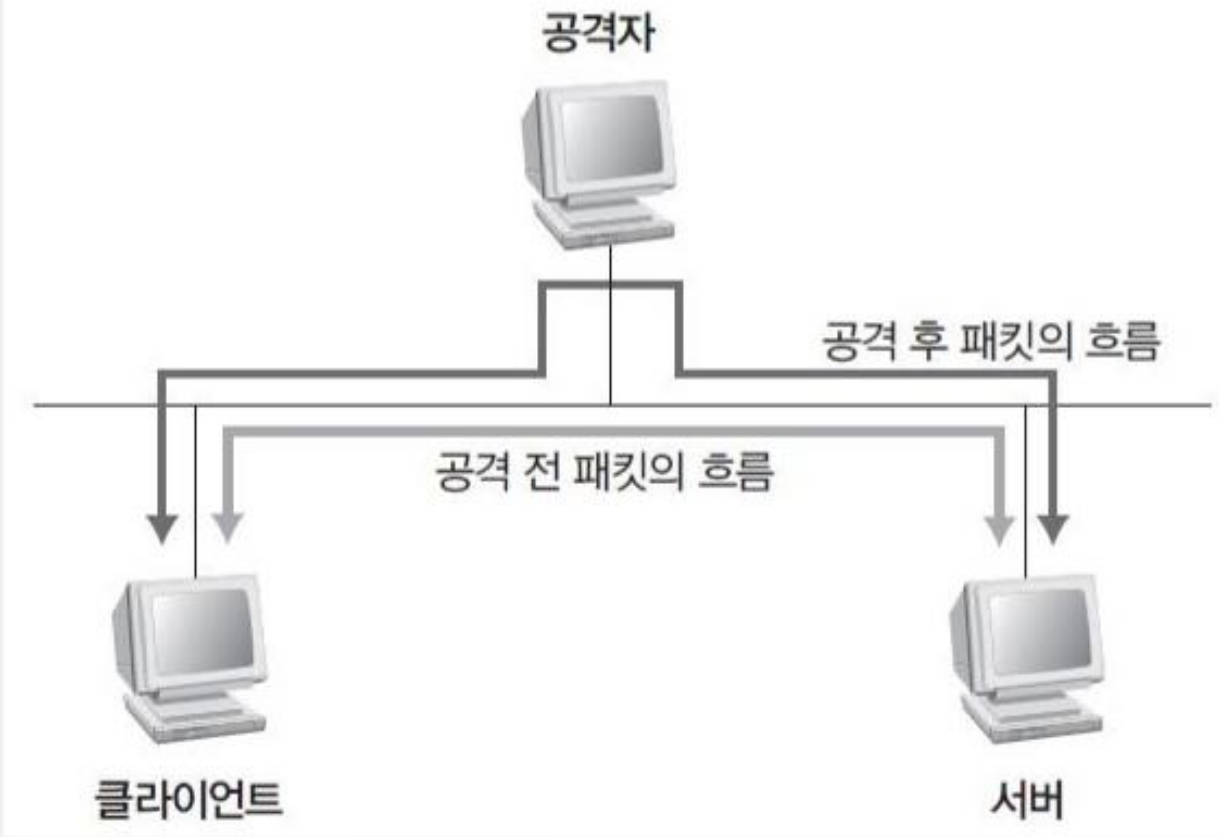


그림 7-4 ARP 스푸핑 공격의 개념도

# ARP 스푸핑

- MITM 공격 중에 **ARP 스푸핑**으로 웹페이지 타이틀을 변조하는 시연 영상

- [시연 내용]

  - Kali Linux의 기본 프로그램인 ettercap을 활용하여 타켓 사이트가 **SSL이 적용되지 않은 사이트에 접속했을 때, 타이틀을 변조** 시킨다

시연 영상 링크 : https://youtu.be/COyV9uZcMnw

# Q & A