

ECE 471/571.

IP security

Application



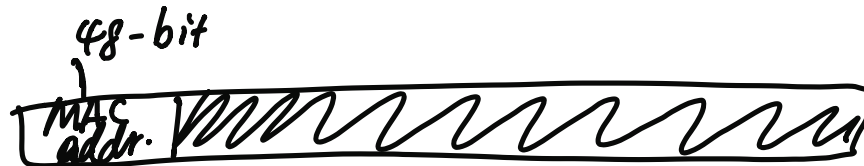
Transport



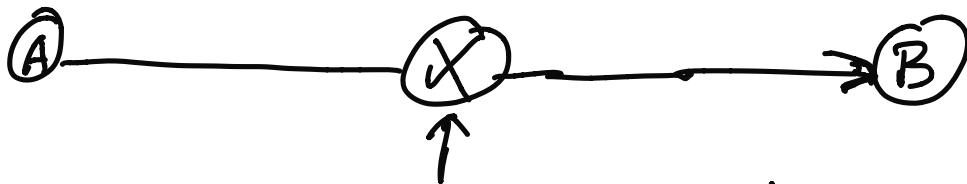
Network (IP)



MAC



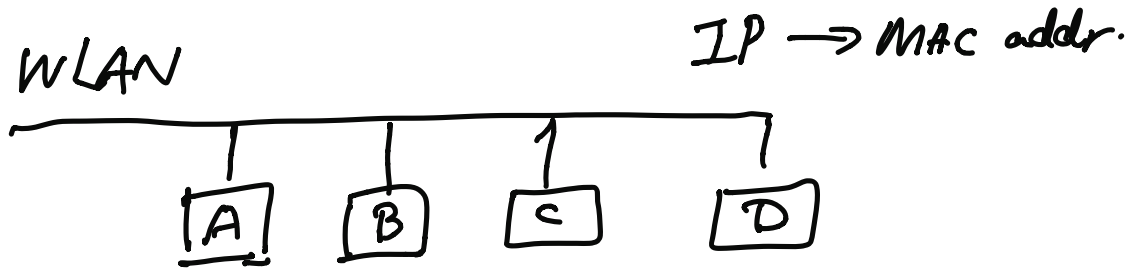
PHY layer



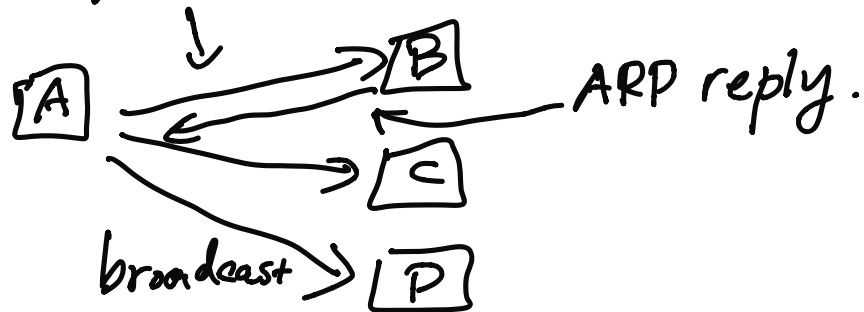
Man in the middle attack

e.g. rogue access point.

ARP (address resolution protocol)

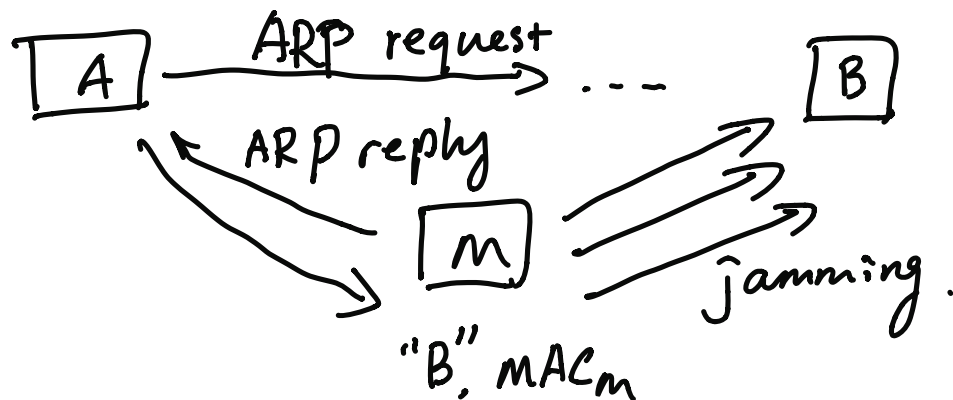


ARP request. "who is B"



B	MAC <sub>B</sub>
C	MAC <sub>C</sub>
⋮	⋮

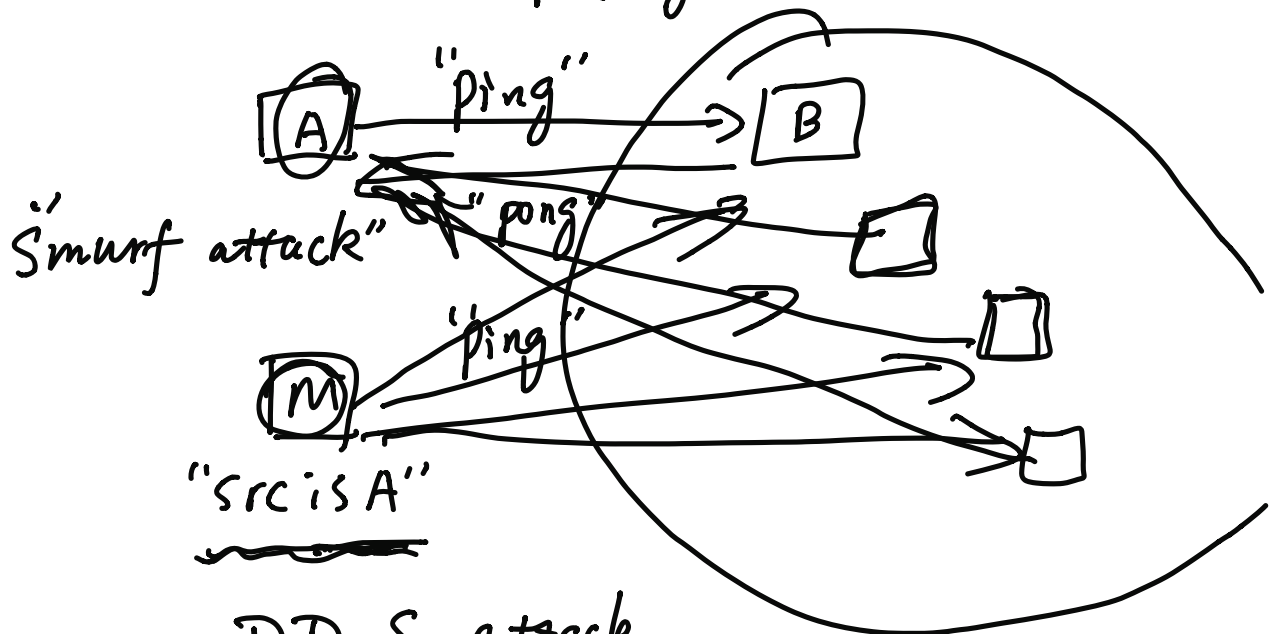
ARP cache poisoning attack



ARP address spoofing attack.

IP address spoofing

IP address spoofing.

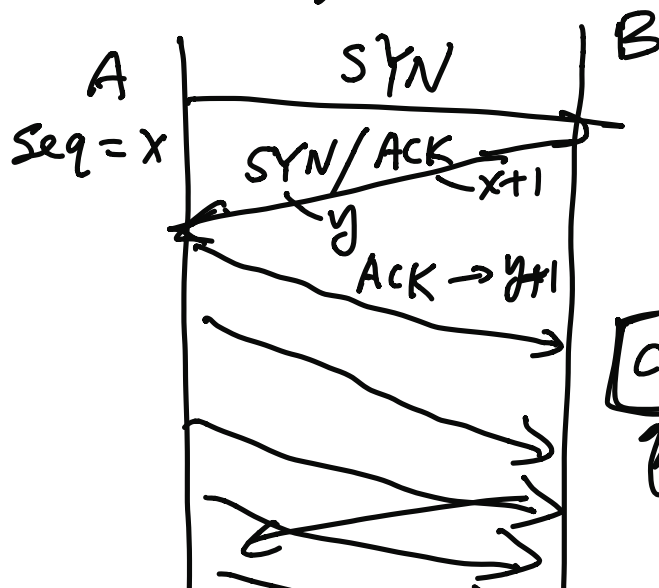


DDoS attack

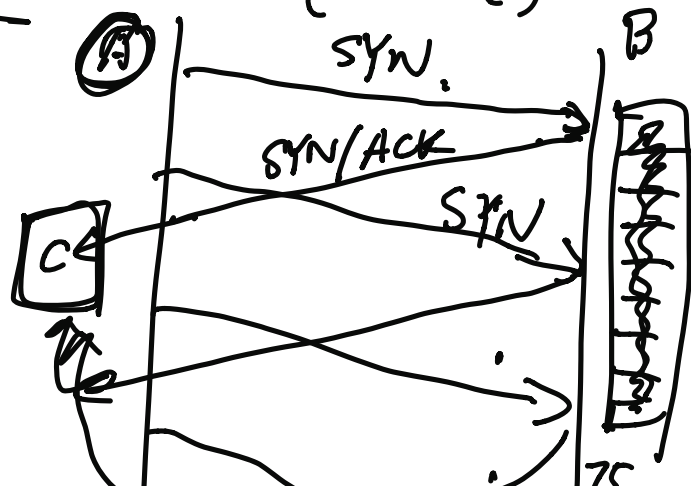
distributed denial of service

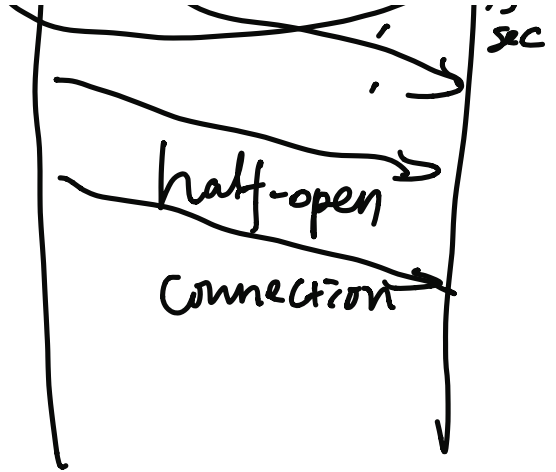
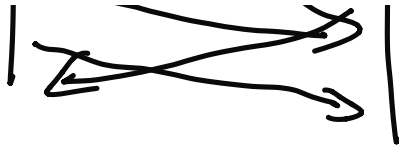
need authentication of IP address

TCP layer



Connection setup  
three-way handshake  
(src = c)





SYN Flooding attack