Imperial College
London

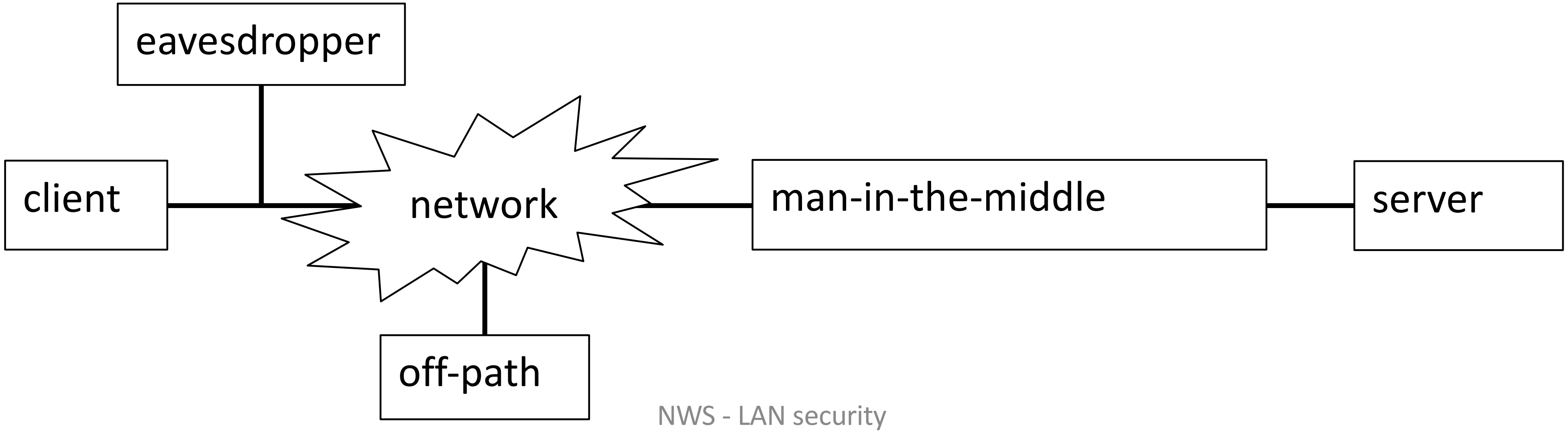
Network and Web Security

LAN Security

Dr Sergio Maffeis
Department of Computing
Course web page: https://331.cybersec.fun

Network capabilities

- Participant
  - Capabilities: send and receive legitimate packets that respect the protocol
  - Examples: web browser, web application
- Eavesdropper
  - Capabilities: read packets sent to others, cannot (or will not) participate
  - Examples: wiretapper, sniffer on a broadcast network (WiFi)
- Off-path
  - Capabilities: participate; create arbitrary packets
  - Examples: machine connected to WiFi, ethernet
- Man in the middle (MITM)
  - Capabilities: participate; read, modify, create or delete packets
  - Example: proxy, ISP, router, WiFi access point

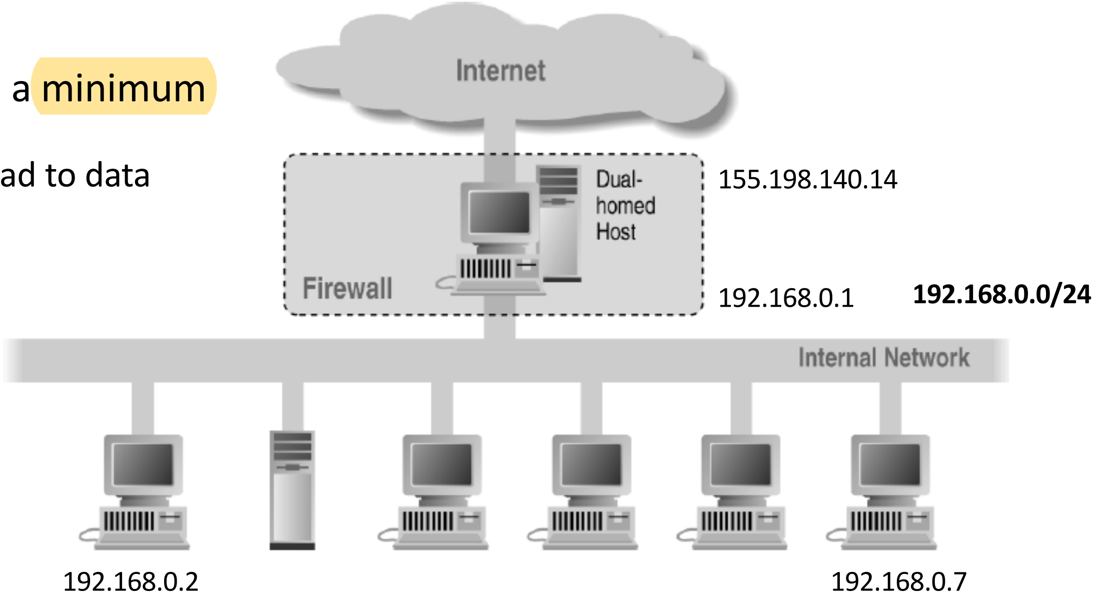


Local Area Networks

Imperial College London

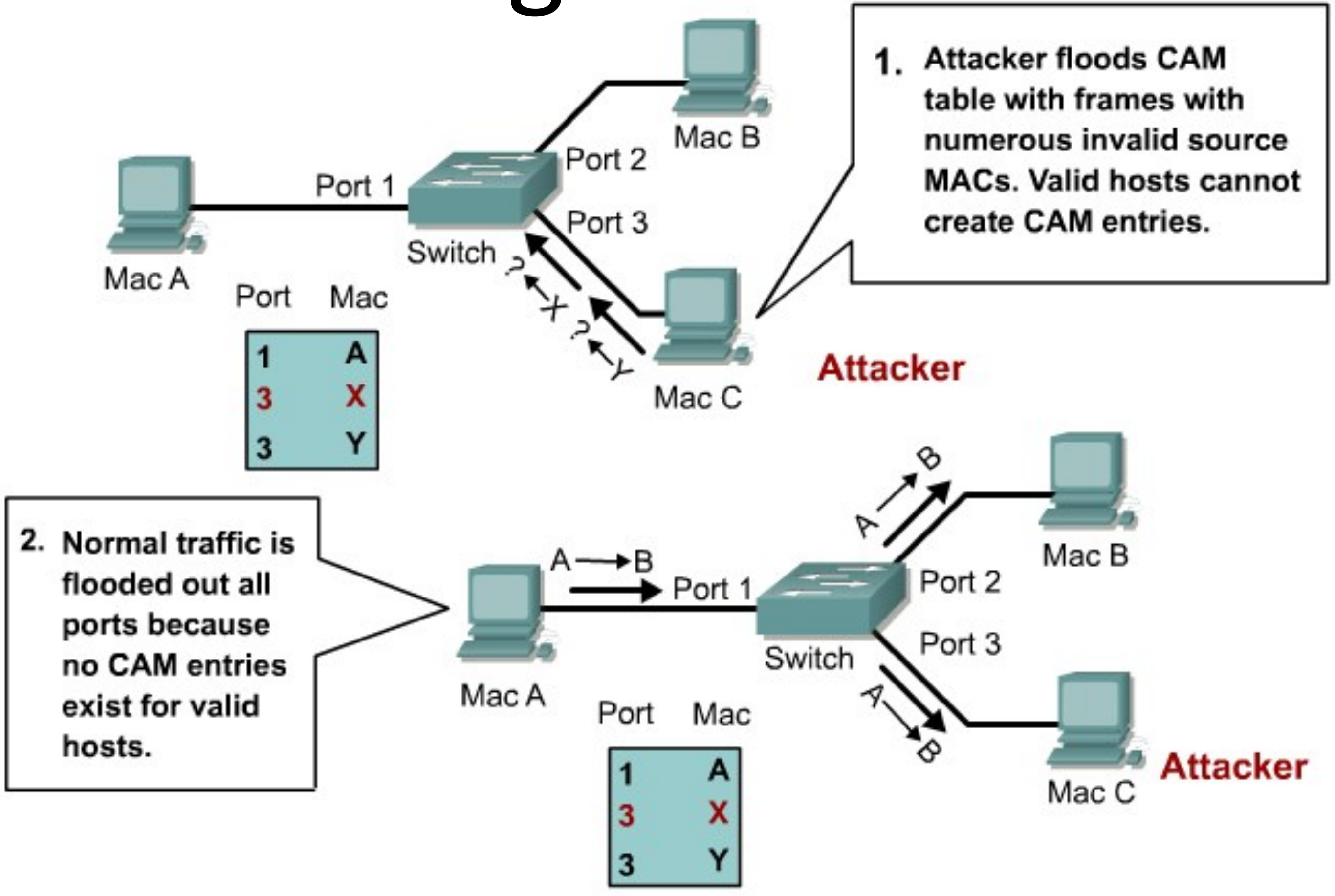
ARP: used to get the MAC address inside the same LAN for sending a message from machine A to B

- Local Area Network (LAN)
  - The network interface of each host has a Media Access Control (MAC) address
  - Messages on the LAN are sent based on MAC addresses
  - The Dynamic Host Configuration Protocol (DHCP) tells new hosts their IP and other configuration information (network mask, DNS server, router IP)
  - The Address Resolution Protocol (ARP) is used to find the MAC of an IP on the same LAN
- Some IP ranges are reserved for private networks
  - 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- LANs typically rely on broadcast medium such as cable (Ethernet) or wireless (WiFi)
  - Conflict resolution requirements prescribe a minimum packet size
    - If padding data is not initialized this may lead to data disclosure
  - Eavesdropper hosts can sniff the network



MAC flooding

For Mac B, it does not have a valid entry in the table, so the switch will broadcast traffic instead



1. Attacker floods CAM table with frames with numerous invalid source MACs. Valid hosts cannot create CAM entries.

Port	Mac
1	A
3	X
3	Y

2. Normal traffic is flooded out all ports because no CAM entries exist for valid hosts.

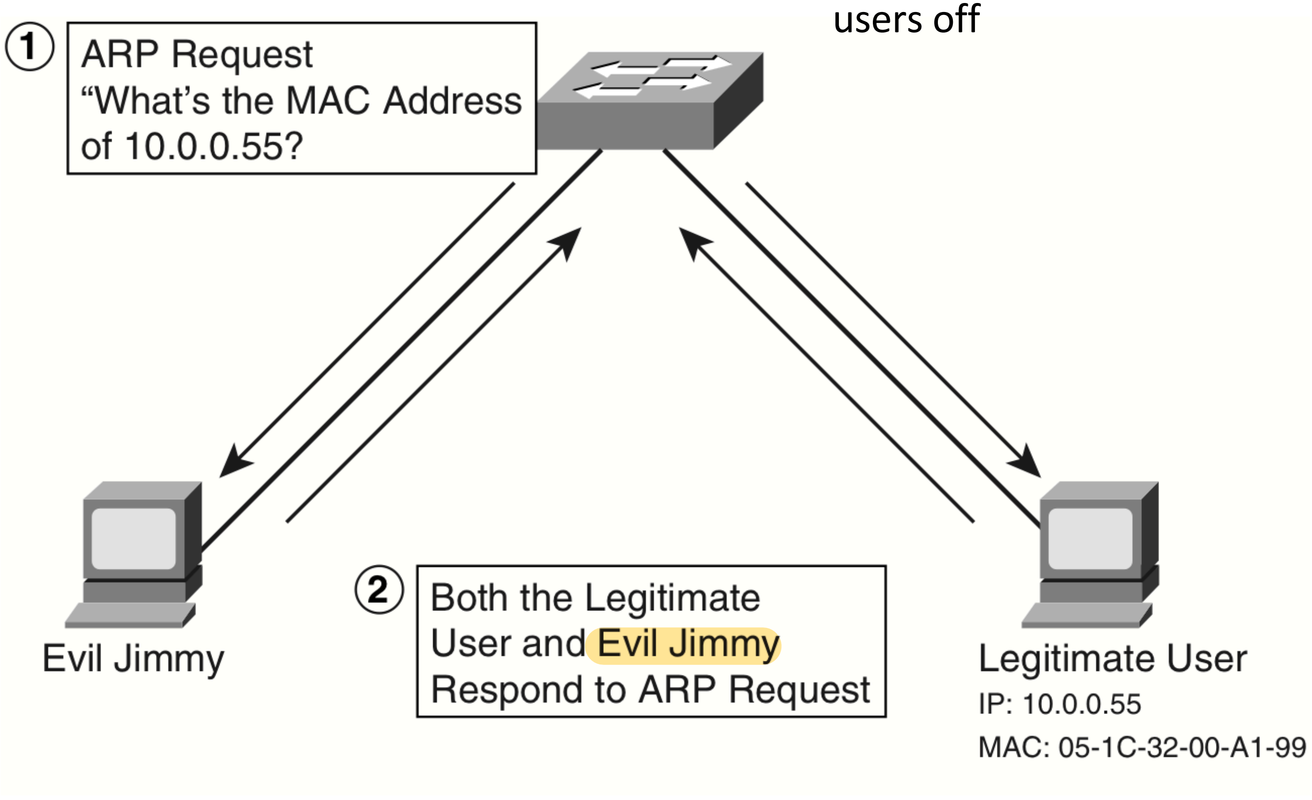
Port	Mac
1	A
3	X
3	Y

- Network switches cache Port-MAC associations
- Attacker forces switch to broadcast traffic, so he can sniff packets
- Typical countermeasures
  - “Port security”: limit ability to flood caches
  - Keep track of authorised MAC addresses in the system

ARP poisoning

- MAC is easy to spoof: feature to deal with conflicting hardware
  - Attacker can evade MAC-based filtering and access control
  - Off-path attacker spoofing router becomes MITM!
- ARP poisoning
  - Switch needs to find MAC corresponding to an IP
  - Attacker spoofs MAC of victim and replies, like victim does
  - Message is forwarded to both ports that replied (including Evil Jimmy's)
  - Typical countermeasure: static ARP rules or spoofed ARP message detection

When concurrent queries are received, kick both users off


1
ARP Request
"What's the MAC Address
of 10.0.0.55?
2
Both the Legitimate
User and Evil Jimmy
Respond to ARP Request
Evil Jimmy
Legitimate User
IP: 10.0.0.55
MAC: 05-1C-32-00-A1-99