SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience
Advanced Security

TCP/IP Threats

Lecture five

Outline of Lecture

- Network layer attacks
  - Packet sniffers and password attacks
  - IP spoofing
  - Sequence number prediction
  - TCP hijacking
- Distributed denial of service attacks
  - Operating system attacks
  - Network based DOS attacks

Learning objectives

- You should be able to
  - Explain the following terms
    - packet sniffing, IP spoofing, TCP sequence number prediction, TCP hijacking, Distributed Denial of Service
  - Identify TCP hijacking and TCP sequence number attacks from sequence diagrams
  - Explain how SYN flooding is used in Denial of Service attacks

Network layer attacks

- Packet sniffing
- IP spoofing
- TCP session hijacking
- TCP sequence number attack

Packet sniffers

- Basic tool of the trade
- Attached to a part of the network that sees all traffic of interest
  - hub, SPAN from a router
- Displays packets and frames as they are transmitted
- Need to be able to interpret specific protocols
  - eg Ethernet, IP, TCP, WLAN
- Sniffers are useful (and legal) tools
  - Wireshark
    - use to diagnose network problems
    - measure traffic loads
- However can be used for illegal purposes
  - passwords transmitted in the clear

Port scanners

- Like packet sniffers can be used for good as well as evil
  - Send probes to all the ports on a host
  - Probes made up of ICMP ECHO REQUESTs, UDP messages, TCP SYN/ACK messages
- Can be used to determine
  - What hosts available on the network
  - What ports are available on each host
  - What state the ports are in
  - What operating system is used
  - What packet filters and firewalls are in use

Threats to TCP

- Threats
  - IP Spoofing
  - TCP sequence number hijacking
  - TCP session hijacking
- All exploit TCP weaknesses
- Source code of TCP stacks freely available on the Internet
- IP Spoofing and TCP sequence number hijacking are components of TCP session hijacking

IP spoofing

- Internet Protocol spoofing (IP spoofing) is the creation of IP packets with a forged (spoofed) source IP address
  - The header of every IP packet contains its source address.
- An attacker can make it appear that the packet was sent by a different machine.
  - can be used attackers where authentication based on IP addresses.
  - most effective where trust relationships exist between machines.
- Example
  - on some corporate networks internal systems trust each other
  - a user can log in without a username or password provided they are connecting from another machine on the internal network
  - By spoofing a connection from a trusted machine, an attacker may be able to access the target machine without authentication

Defense against IP spoofing

- Limit use of trusted machines
  - Not always possible
    - DNS, DHCP, file shares in windows
- Ingress packet filtering in the firewall
  - Any external packets with an internal source address should be dropped
- Egress filtering a good idea as well
  - Any internal packets transmitted outside your network with a source address outside your network should be dropped
  - Stops anyone inside your network mounting an IP spoofing attack

Question

- Suppose a user at a terminal at IP address 137.186.223.10 wishes to spoof packets from a DNS server located at IP address 137.186.30.4 to a user located on IP address 137.186.1.15
  - What will be the source address of the spoofed datagrams?
  - What will be the destination address of the spoofed datagrams?
  - What will be the source port number of the spoofed datagrams?
  - What will be the destination port number of the spoofed datagrams?

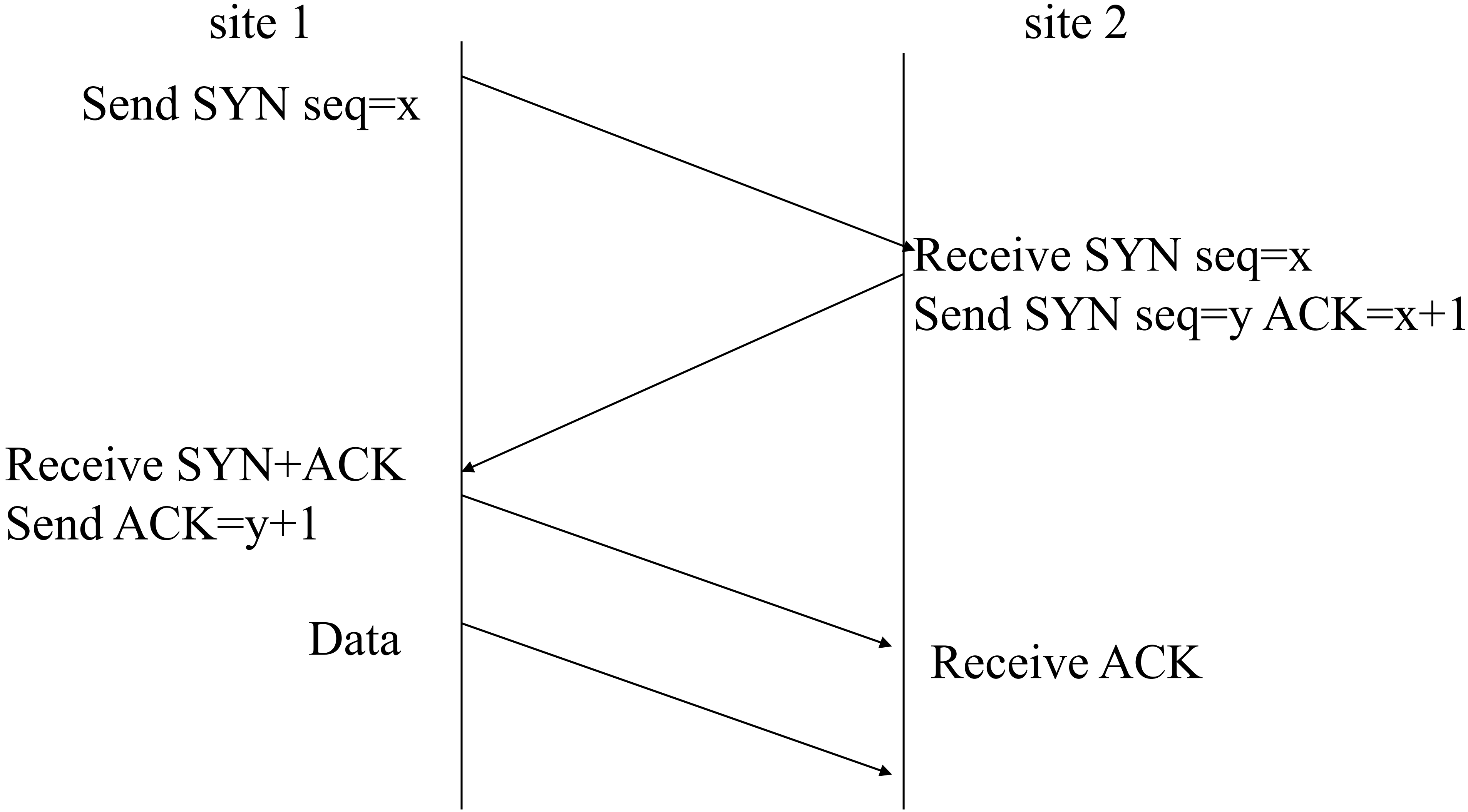
TCP sequence number attack

- An important attack
- Usually well defended against
  - Firewalls, software implementations etc usually incorporate defences to it
- However, important to understand the attack so as to understand the defences
- Enables us to answer questions such as
  - Why are ISNs random in tcp connections?
  - Why is source routing a very bad idea?
  - Why should firewalls drop packets that originate externally but have an internal IP address?
  - Shy should all servers (DHCP, DNS, etc) authenticate themselves?
  - Why should a host respond with a RST when it receives a packet from a connection it hasn't set up?

TCP sequence number attack

- Usually used with IP spoofing
- TCP sequence number used for assembly of TCP segments
- Each TCP segment is numbered
- If attacker determines correct sequence then they can transmit their own TCP segments
  - Perhaps to terminate the connection
  - Perhaps to open a root shell
  - Race against time to get receiver to accept spoofed packet
- Take over TCP handshake using IP spoofing
  - Most useful when spoofing a trusted machine
- Ref Bellovin RFC 6528 “Defending against Sequence Number Attacks” February 2012

TCP three way handshake



site 1

site 2

Send SYN seq=x

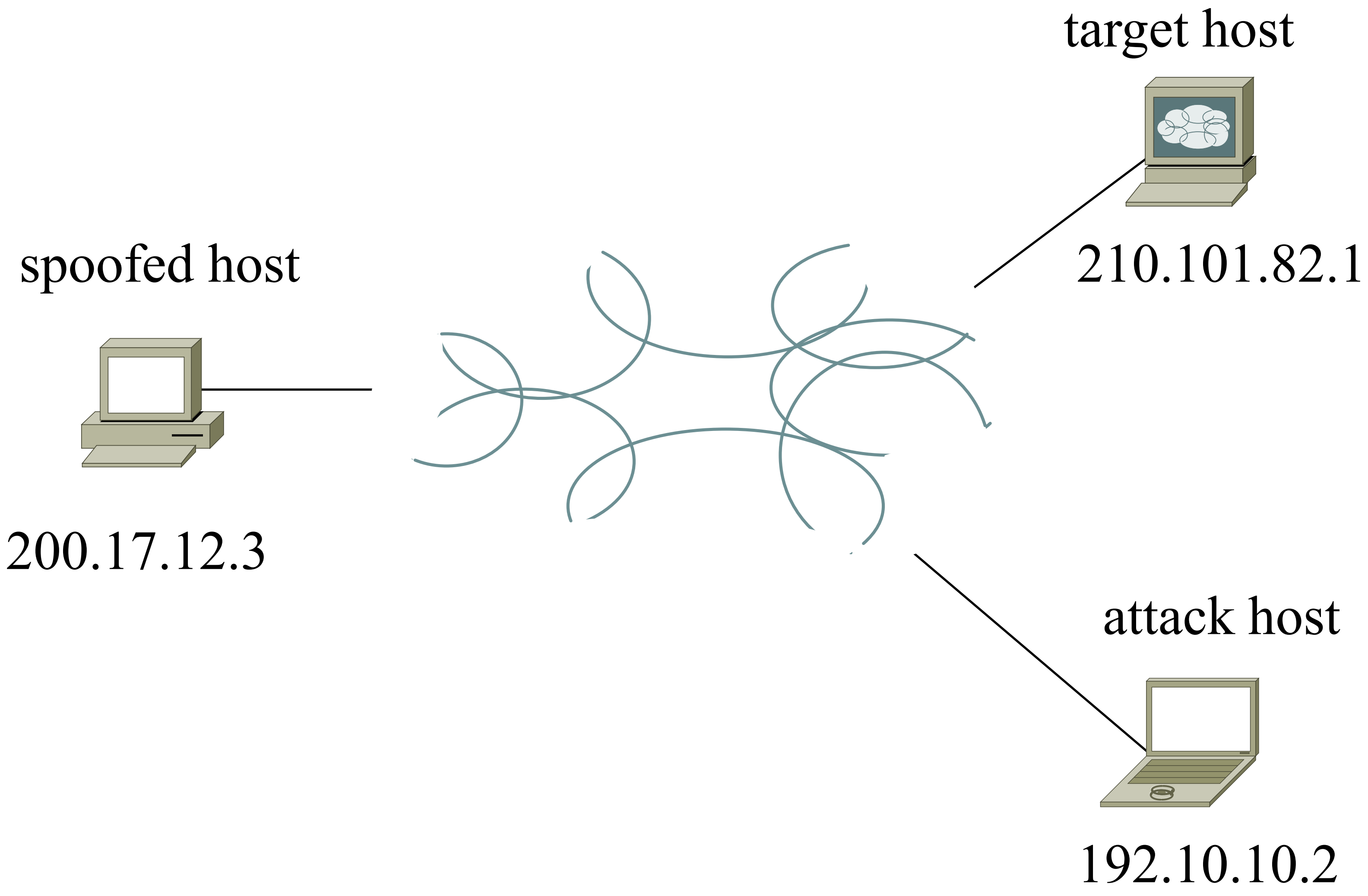
Receive SYN seq=x
Send SYN seq=y ACK=x+1

Receive SYN+ACK
Send ACK=y+1

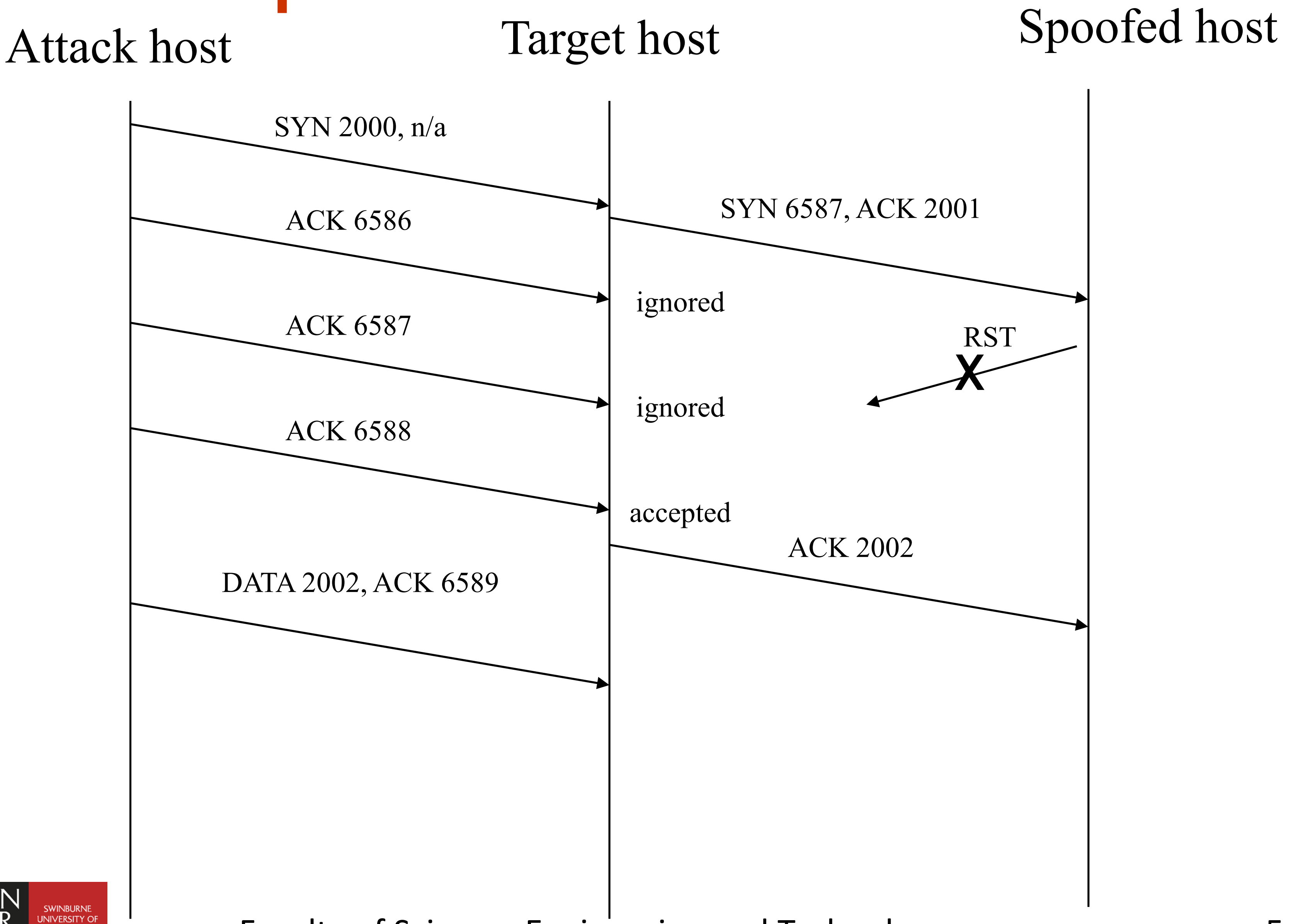
Data

Receive ACK

TCP sequence number attack



TCP sequence number attack



TCP sequence number attack

- Need to take spoofed host offline
  - Maybe through a DOS attack
  - Otherwise it will transmit a Reset (RST) message
- Attacker needs to be able to obtain the initial sequence number (ISN) or have a reasonable guess as to its value
  - If on the same LAN segment or a WLAN then possible or using source routing then reasonably simple
    - Non-blind spoofing
  - If on a different LAN segment then much harder
    - In some operating systems the initial sequence number can be predicted
    - ISN should be a random number

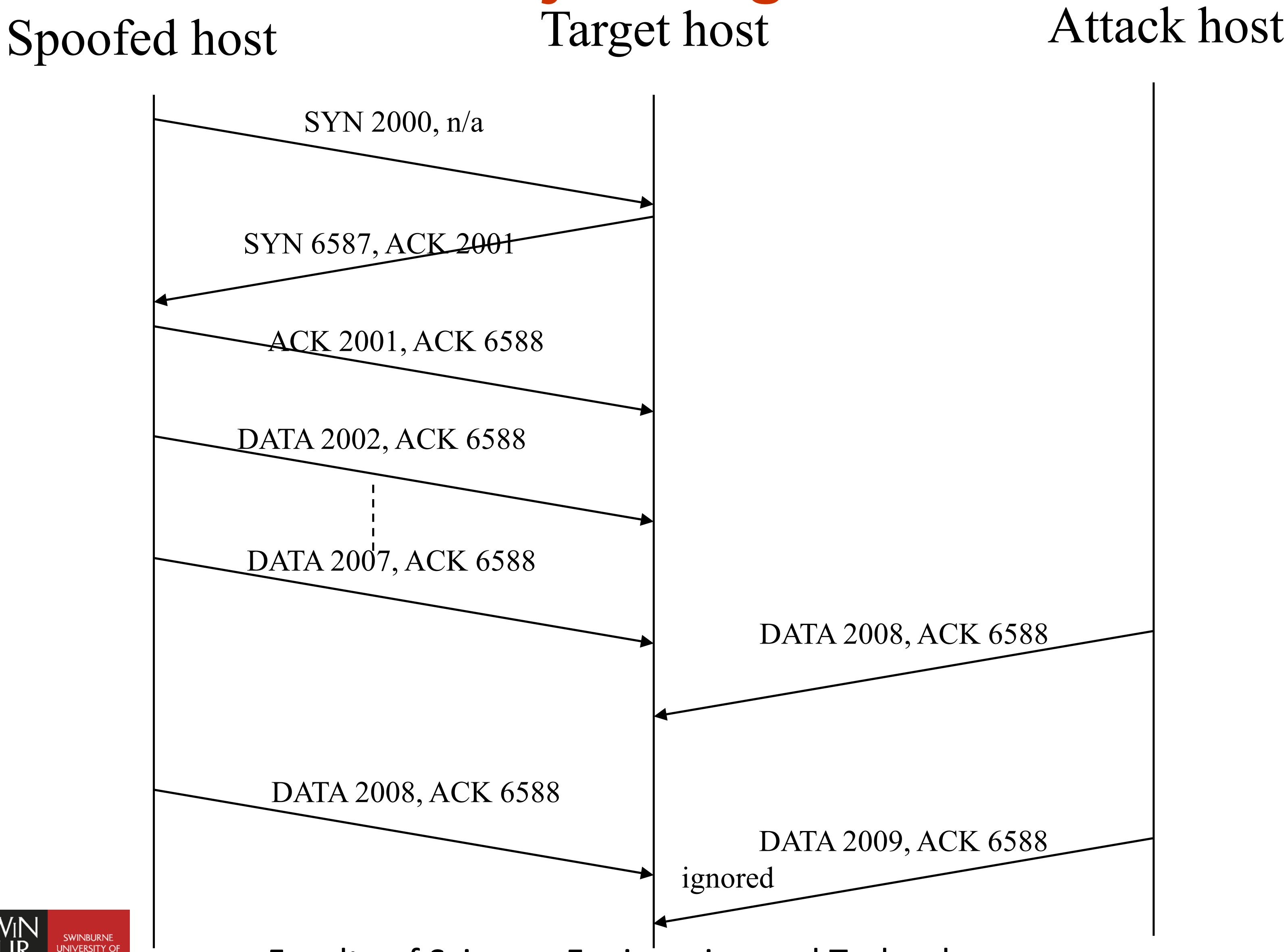
TCP sequence number attack

- Blind spoofing can be made non-blind spoofing by using source routed IP packets
  - Source routed IP packets allow return route to be specified in the IP packet header
    - Can be spoofed by attacker
  - Very important for firewall to drop source routed packets
- Can also make non-blind by ARP poisoning and masquerading as the default gateway
  - Need to defend against ARP poisoning

TCP session hijacking

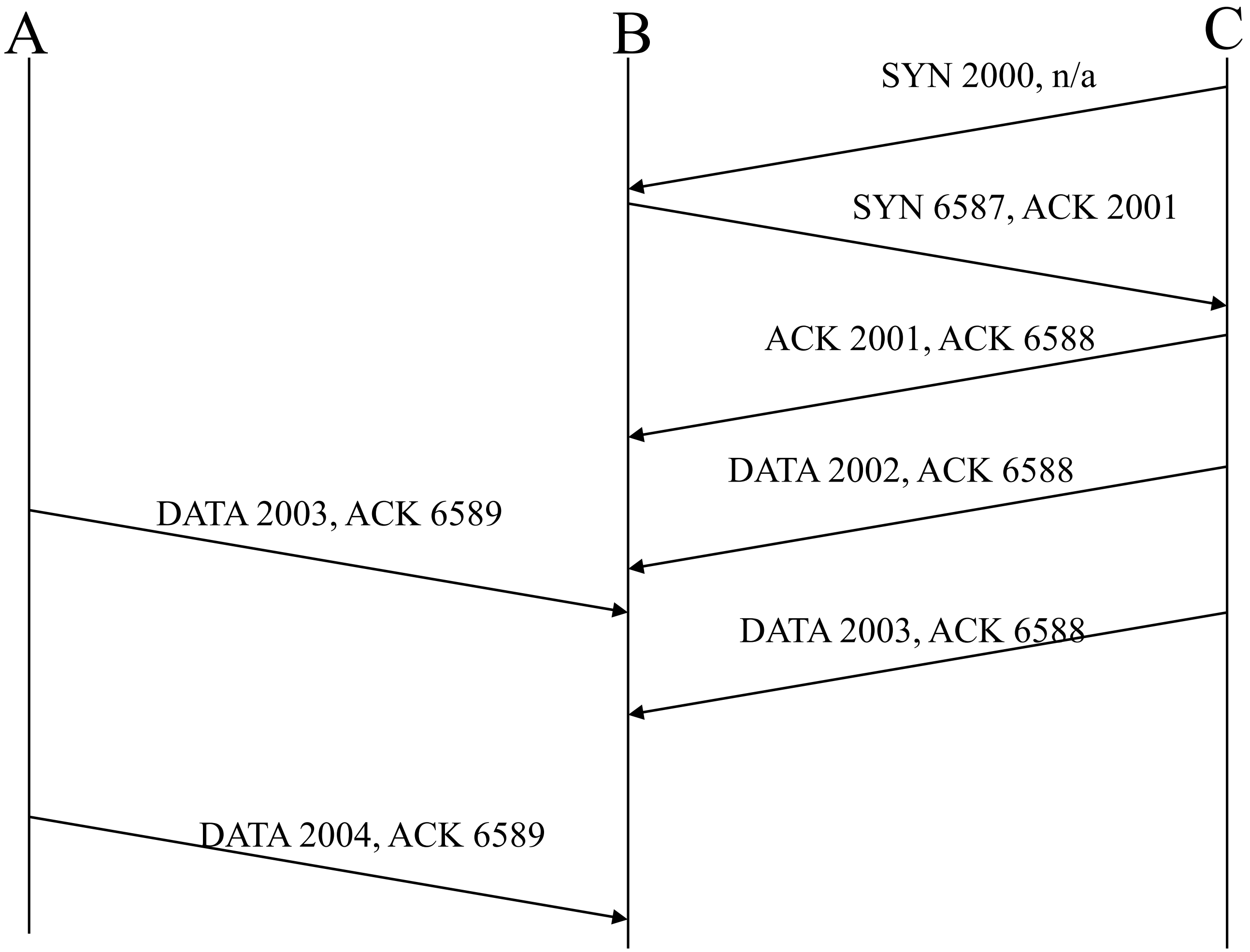
- A ‘man in the middle’ attack
- Another attack that explains why encryption is important
- TCP session hijacking used to take over TCP applications such as remote logins, http connections etc
- Attacker determines next TCP segment sequence numbers and then takes over connection
- Subsequent packets sent by spoofed host will be ignored
  - Sequence numbers will be incorrect
- Usually needs non-blind spoofing

TCP session hijacking



Question

- What sort of attack is happening here?
- Which is the attacking host, the spoofed host and the target host?



Dealing with TCP session hijacking

- Usually used to take over a session once the user has been authenticated
  - Typically telnet
    - User on spoofed host assumes a network problem and opens up a new telnet session
  - Can make authentication with one-time passwords ineffective
- Can be prevented by care with trusted hosts
  - use encryption and authentication wherever possible
- Can be minimized by prohibiting telnet sessions and only using ssh

Denial of Service attacks

- Aim of denial of service (DOS) attacks is to make a network server or service unavailable
- Based on some kind of flooding of messages which overwhelm the server
- Prevention, detection and recovery difficult
  - More later in semester

Denial of Service attacks

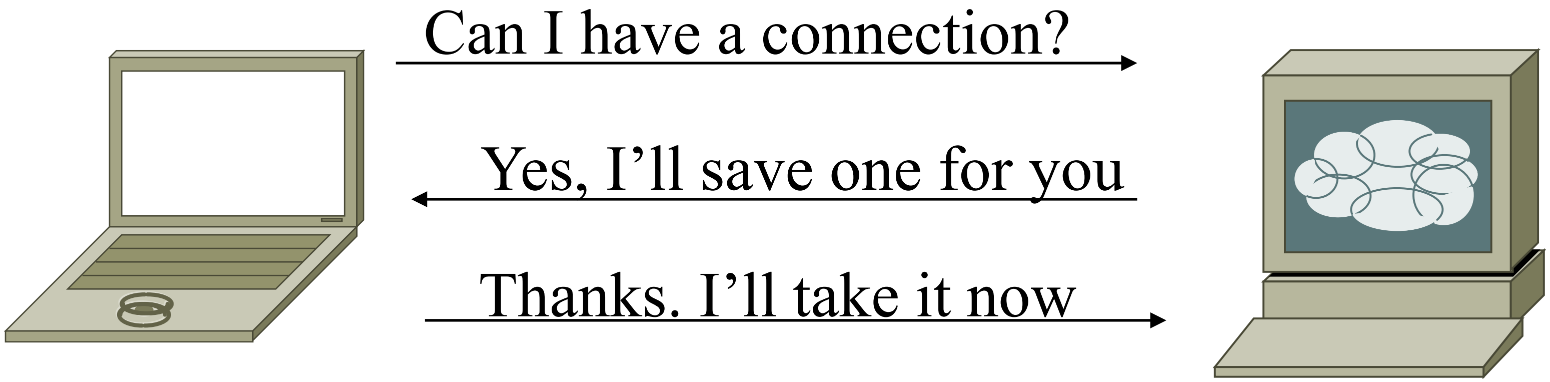
- Denial of service attacks are most effective when many attackers are involved
  - Distributed Denial of Service attack (DDoS)
- Most successful attacks have been through the use of hijacked intermediate sites
- Typically, attackers are machines taken over through the use of trojans
  - Zombies or bots
  - ‘botnets’

SYN flooding

- An important DOS attack
- Server receives more connection requests than it has resources to deal with
- The number of half-open connections that a server will allow is limited
- Once limit is reached, new requests are rejected until existing request time out
    - Denial of service
- Usually implemented by spoofing a routable but unreachable source address

SYN flooding

- Normal TCP connection set up



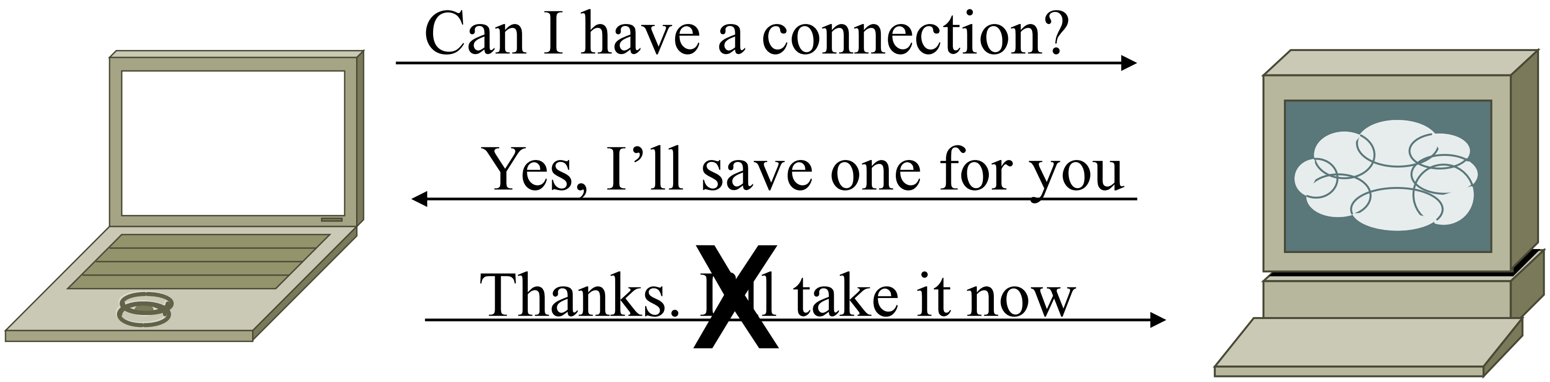
Can I have a connection?

Yes, I’ll save one for you

Thanks. I’ll take it now

SYN flooding

- Abnormal TCP connection set up



Can I have a connection?

Yes, I’ll save one for you

Thanks. I’ll take it now

- Resources allocated in attacked server for TCP connection but setup is not complete
- A DOS attack is successful when all resources available for connection are allocated to incomplete connections

Dealing with SYN flooding

- ISP’s firewall configuration should block IP packets with invalid source addresses
- SYN Cookies
  - Cryptographic techniques that enable state information to be stored in the SYN value
  - More after we’ve done some cryptography
- Intrusion detection systems
  - More later in the semester
- The TCP protocol stack can be made more robust
  - increase the number of half-open connections allowed
  - randomly drop half-open connections
    - implemented in most firewalls

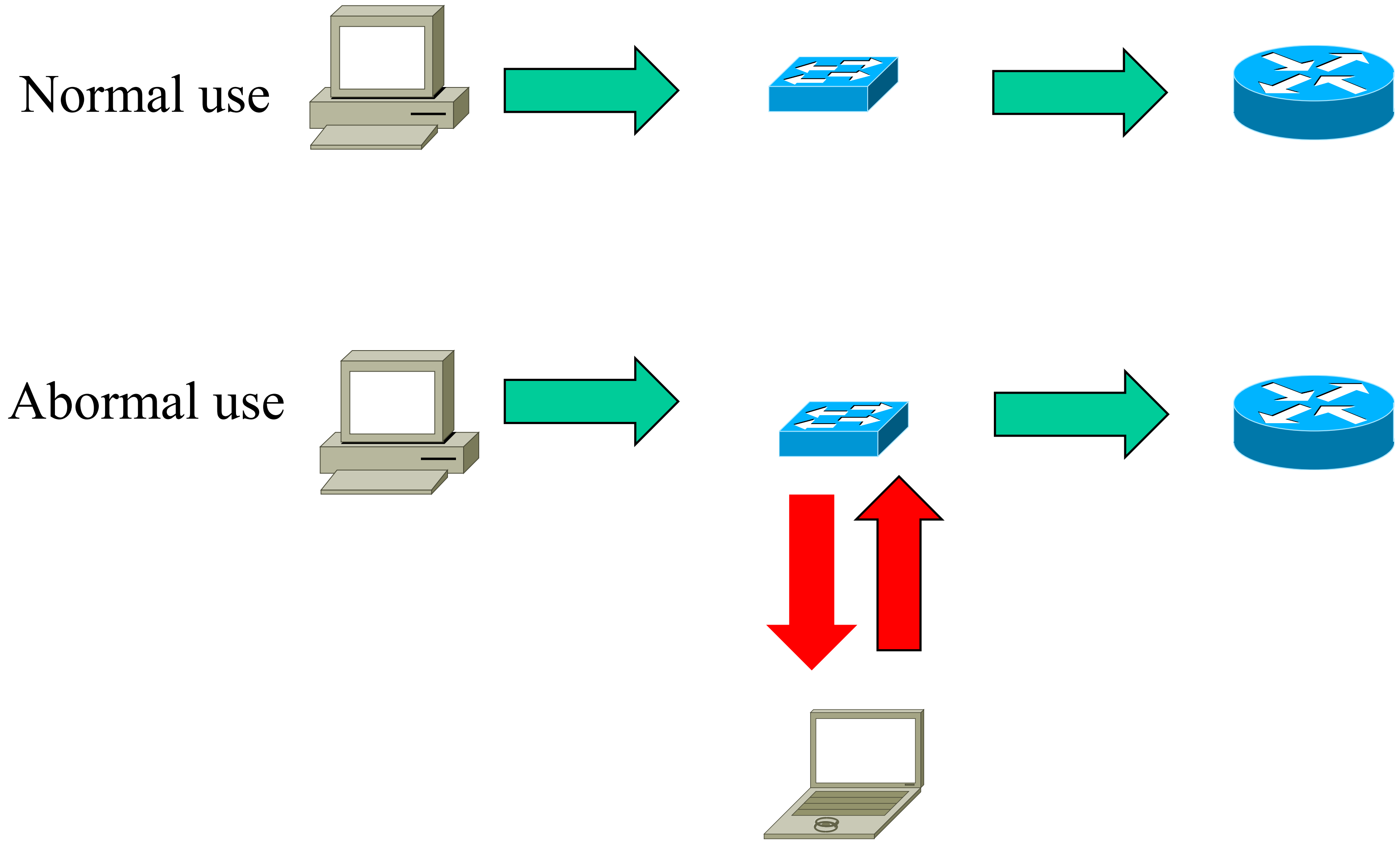
TCP RST and FIN DoS attacks

- TCP has a number of flags specifying segment status
  - Already seen SYN and ACK
  - Also has RST for reset connection and FIN for finish of data
- These can be used for DOS attacks
  - If RST or FIN contain correct sequence number then attacked host will accept them
  - Connection will be closed
- For DOS attack, TCP sequence numbers need to be obtained in the same way as described earlier
- RST or FIN is accepted and connection closed

ARP poisoning

- Used to attack an Ethernet or WLAN network
- Goal is to associate attacker's MAC address with IP address of another node
  - Often the default gateway
- Attacker then sees all the traffic destined for the spoofed node
  - Attacker can forward traffic onto spoofed node
    - Passive sniffing
  - Attacker can modify the traffic
    - Man in the middle attack
- ARP poisoning can also be used for denial of service
  - By associating a spurious MAC address with default gateway for example

ARP poisoning



Normal use

Abormal use

Defenses against ARP poisoning

- DHCP snooping
  - DHCP is usually used to associate IP addresses with a MAC address
  - Frequent checking of ARP table to make sure association has not been corrupted
- Can monitor important entries in ARP table
  - Gateway MAC usually changes infrequently
  - IDS might monitor ARP table and act if unexpected change occurs
- Can attempt to make it difficult for an attacker to inject spurious ARP traffic
  - Attacker needs access to Ethernet segment
  - Prevent physical access by unauthorised hosts
    - (but can be difficult with wireless network)

HTTP

- Web protocol
- Lots of threats…
  - Usually an open port
  - Temptation to overload has been very strong
    - Eg. SOAP allows remote procedure calls via HTTP
    - Perhaps not a good idea
  - Social engineering based attacks
    - Phishing
  - Attacks where the server is the victim
    - Buffer overflow, denial of service
  - Attacks where the client is the victim
    - Eg Cross site request forgery

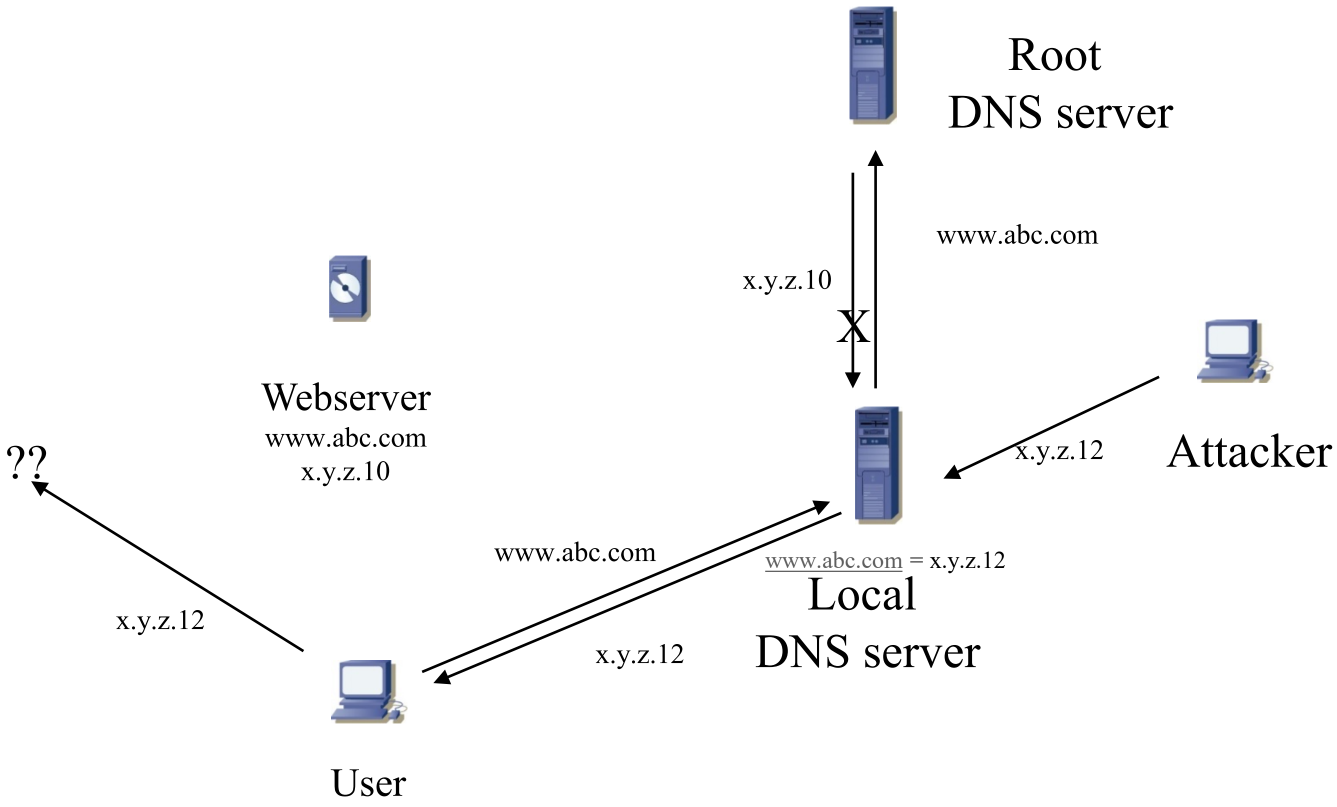
HTTP

- Cross-site request forgery using webmail as an example
  - User is authenticated in webmail
  - Browser visits a malicious website
  - Website contains some code (perhaps hidden in an IMG element) that accesses webmail and that the visitor unwittlingly executes
    - Eg deletes all mails, copies all mail, emails contacts with SPAM
  - Works because browser is currently authenticated to webmail
- Defense
  - Log off sites explicitly when leaving them (user)
  - Be careful about sites you visit
    - Emailed links are particularly susceptible
  - Include one off values in authentication (nonce)

DNS

- Domain Name Server
  - Translates domain names to IP addresses
- Can be used in denial of service attacks
  - DNS system is hierarchical
  - DNS server asks a root server to resolve an unknown domain name
  - Attacker transmits bogus response to request
  - DNS server caches bogus response
  - Domain name resolutions to that server return an invalid IP address resulting in a denial of service
- Secure extension to DNS (DNSSEC)
  - Secondary DNS servers authenticate messages from other DNS servers

DNS Denial of service



Smurf attack

- Attacker sends ping (ICMP ECHO REQUEST) to broadcast address
- Source address is spoofed to be that of the victim
- Every host in the broadcast domain might reply
  - The ‘amplifying network’
- For n hosts and m broadcasts then the victim may receive nxm responses
- ‘Fraggle’ a related attack that uses UDP instead of ICMP

Conclusion

- This lecture introduces some important basic attacks on TCP and IP. There are many different types of TCP and IP attacks and many variations of what we've seen here
  - Not all of them covered here
- It also showed sequence diagrams of TCP sequence number prediction and TCP hijacking attacks