SWINBURNE UNIVERSITY OF TECHNOLOGY

Network Security and Resilience / Advanced Security

# TCP/IP Protocol Review

Lecture three

# Outline of Lecture

- Review of TCP/IP Protocol
- Overview of vulnerabilities
- IPv6 approach to security

# Learning objectives

- You should be able to
  - Describe (briefly) the TCP/IP protocol suite
  - Describe (in general terms) its vulnerabilities
  - Describe (briefly) the IPv6 approach to security

# TCP/IP Protocol

- A suite of protocols
- Defines how to form a network of networks
- Main protocols
  - Internet Protocol (IP)
  - Transmission Control Protocol (TCP)
  - Many others
- Important to understand TCP
  - is the basis of other protocols (HTTP, ssh etc)
  - a common vehicle for attacks

# TCP/IP security issues

- TCP/IP was developed in the 60s and 70s for an entirely different environment to the one it now occupies
  - trusted networks
    - assumed no-one on the network was (especially) vindictive
  - small networks with small numbers of users
    - if they were, they could be identified
  - limited computing power and limited bandwidth
  - Knowledge as to how to carry out security exploits very limited (and jealously guarded)
  - limited access to computers
  - absence of sophisticated encryption techniques
  - enterprises much less reliant on networks (and computers) than they are now

# TCP/IP security issues

- Current environment entirely different
  - Everyone depends on networks and computers to a huge extent in most aspects of their lives
  - Much more threatening environment
    - Dangerous to trust anyone on the Internet
    - Many hundreds of millions of users
    - Huge network
    - Millions of cheap powerful computers
    - Can download hacking tools from website
    - Much higher bandwidths
  - But we do have some techniques and tools for fighting back
    - Powerful (unbreakable) encryption
    - Authentication technologies
    - Firewalls, IDS, IPS, PKI… etc

# TCP/IP security issues

- Version 4 of TCP/IP has very limited security features
  - It has been necessary to graft security features onto it
- Much room for error
  - relies a great deal on good practice of system administrators, network designers, protocol designers, software developers and users
  - many mistakes can and have been made
    - Early Windows implementations riddled with security flaws
    - WLAN (IEEE 802.11) security a fiasco
    - Naïve users swindled in ‘phishing’, Nigerian bank account and other frauds

# TCP/IP security issues

- Version 6 of IP (IPv6)
  - Scoped addresses, enabling restriction of specific addresses for file and print servers
  - IPSec integrated into IPv6 enabling authentication and encryption by default
    - Still needs to be configured
  - Removes the need for NAT and helps restore the end-to-end principle of IP that was compromised by NAT
  - Privacy extensions through generation of random host identifiers
  - Autoconfiguration built in through Stateless Address AutoConfiguration (SLAAC)
- Removes many of the issues of IPv4 but introduces new ones
  - Privacy
  - Still requires configuration of IPSec

# Internet Protocol: Connectionless Datagram Delivery

- Connectionless
  - No predetermined path for transfer of packets
  - Each datagram contains a hierarchical destination address
  - At each hop, the router decides where the packet is to go
- Datagram
  - Data packaged in chunks referred to as datagrams

# Internet Protocol: Routing IP Datagrams

- Two forms of delivery
  - Direct
    - destination is on this network
  - Indirect
    - destination is on another network
    - packet is routed to a default gateway
- Depends on routing and ARP tables
- Security implications
  - ARP tables can be corrupted
  - Routing updates can be forged
    - (Cisco routers now provide authentication for routing updates)

# Security implications

- Connectionless datagrams are a flexible and resilient communications mechanism but have a number of security weaknesses
  - if a network node is compromised it can be used to
    - route packets to an unexpected destination
    - copy packets
  - the destination and source addresses can be modified in-transit for malign purposes
    - hide source of attack
    - send a response to someone who did not send the packet

# IP Multicast

- Each subnet has a number of multicast addresses and a broadcast address
- Multicast allows all hosts in the multicast group to be communicated with through a single IP address
- The broadcast address is used to transmit a message to all members of the subnet
- Security implications
  - Can be used for a denial of service attack
    - smurf

# Internet Protocol: Error and Control Messages

- ICMP : Internet control message protocol
- reports on errors, requests information, instructs some sources to reduce their transmission rate
- most important messages are
  - echo and echo reply (ping)
  - destination unreachable
  - source quench
  - router advertisement and solicitation
  - subnet mask request and reply

# Security implications

- Can be used to find out a great deal of information about a network
  - ping and router solicitation can provide useful information to would-be attackers
- Can be used to generate a great deal of activity by nodes leading to denial of service
  - basis of the “smurf” attack
- Source quench can be used in a malign way to cause denial of service

# User Datagram Protocol (UDP)

- Largely a framing mechanism for IP packets
- Has a source and destination port number to specify which source process generated it and which destination process should receive it
- Security implications
  - No mechanism for reducing packet rate
  - Can force out TCP connections

# Reliable Stream Transport (TCP)

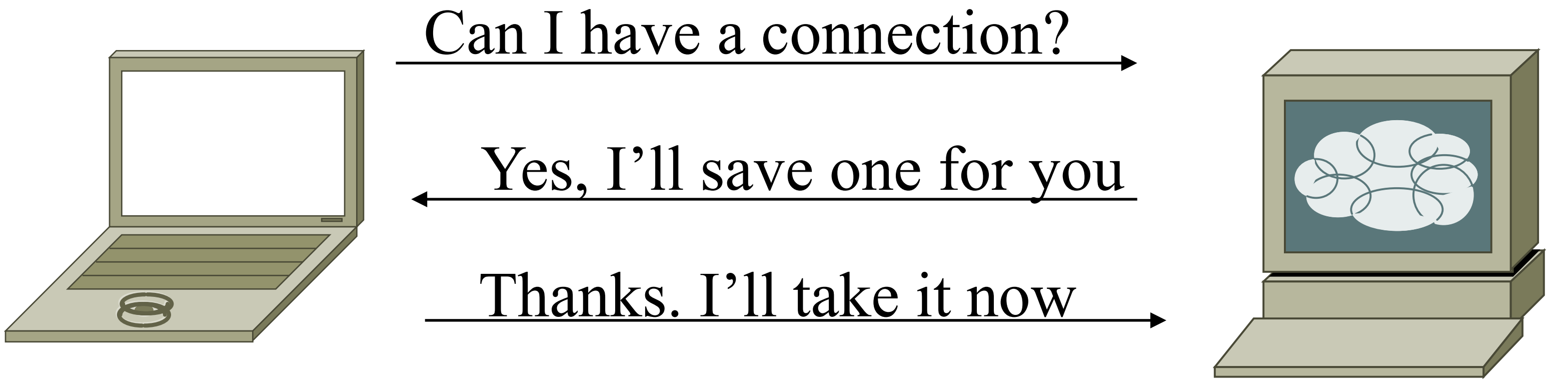
- Transmission Control Protocol
  - A reliable transport mechanism
  - Stream orientation
    - bit sequence is preserved
    - Data segments at source do not necessarily match those at destination
  - Virtual Circuit Connection
    - An initial signalling process setting up the connection
  - Buffered transfer
    - Datagrams are received at the destination and their contents reconstructed in a buffer
    - Allows for reliable transfer
    - missing data can be requested to be resent
  - Full duplex

# TCP

- Connection set up through a ‘three-way handshake’ with positive acknowledgement
- Timeouts to identify when a packet is lost
  - interpreted as congestion within the network
  - source will retransmit and cause the rate to slow by reducing the “sliding window” size
- Sliding windows
  - Transmit packets without acknowledgment up to the window size
  - don’t wait to acknowledge every packet
    - Waiting wastes transmission bandwidth
- Has a source and destination port number to specify which source process generated it and which destination process should receive it

# TCP three-way handshake

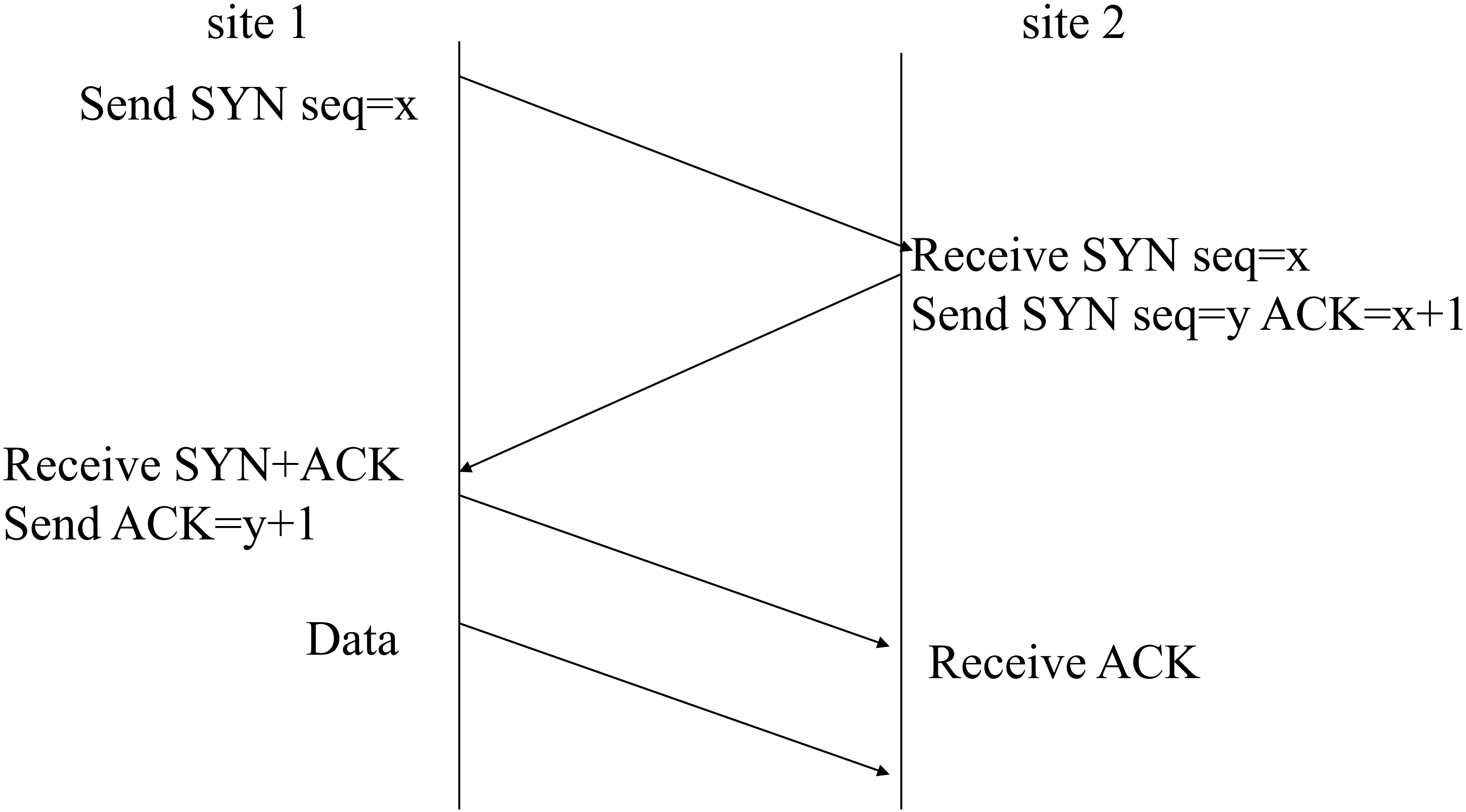
- A source of many security weaknesses
- TCP connection set up



# TCP three-way handshake

- A number of sequence numbers are exchanged during the three-way handshake
- These are then incremented as communication progresses
- Each TCP header has a number of single bit flags that are either set or unset
  - URG urgent
  - ACK acknowledgement field is valid
  - PSH push this segment
  - RST reset the connection
  - SYN synchronise sequence numbers
  - FIN finish communication
- SYN, ACK, RST, FIN of most interest to us

# 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

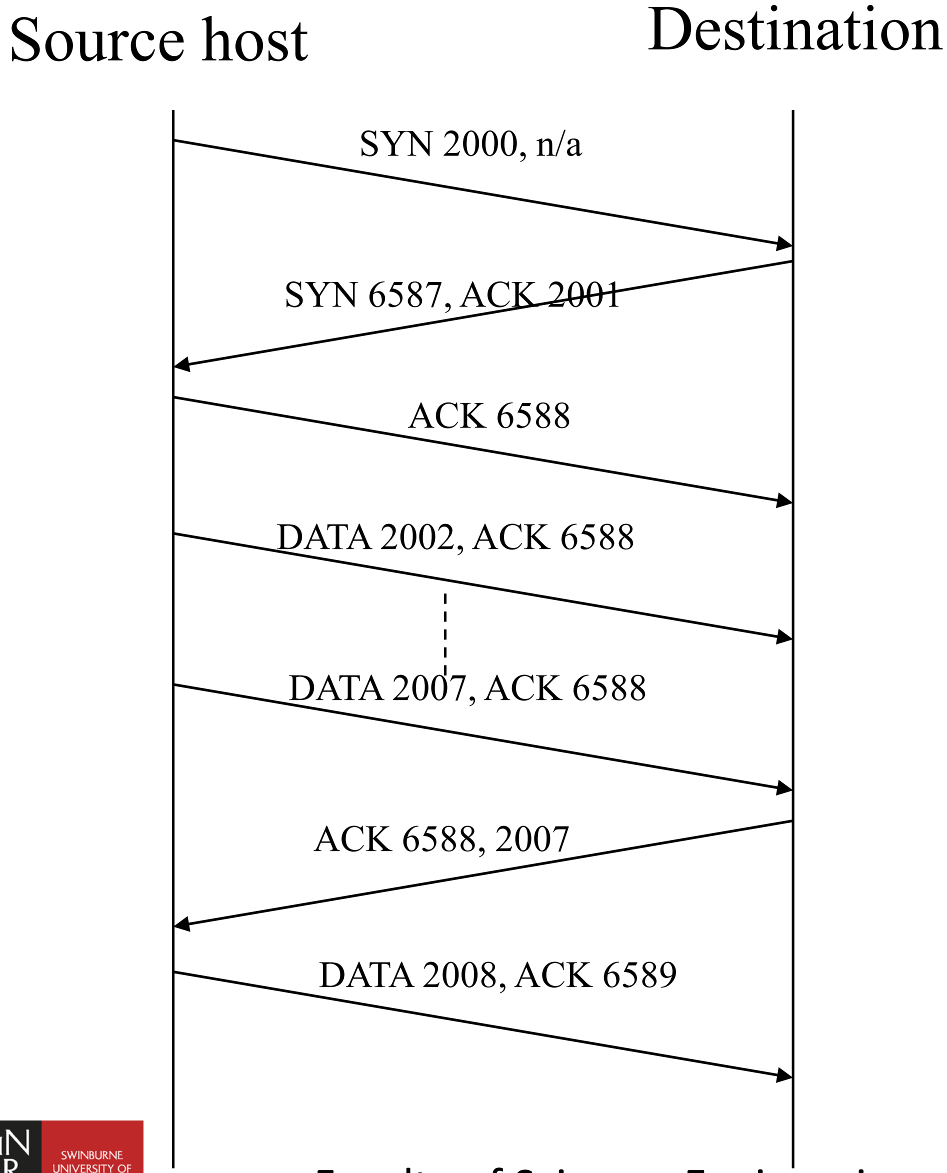
Data

Receive ACK

# Question

- A source host has an initial sequence number (ISN) of 2000 while a destination host has an initial sequence number of 6587. What will be the values of SYN and ACK transmitted in each of the handshake exchanges?

# TCP data exchange



# Security implications

- TCP is very susceptible to attacks
  - TCP sources can be spoofed so that a destination believes it is communicating with a source that it trusts
  - TCP sessions can be hijacked once they have been established
  - The TCP three-way handshake is used in a common Denial of Service attack
    - SYN flooding
- It is important that you understand TCP three-way handshake and the exchange of data after the connection has been established

# Domain Name System

- Maps domain names to IP addresses
- An hierarchical system
  - local / national / global servers
- Some security weaknesses
  - spoofing of domain names (‘phishing’ scams)
- DNSSEC a secure DNS
  - Although not widely deployed yet

# Domain Name System

- Lots of security and privacy issues associated with DNS
- DNS servers can be spoofed
  - We will look at some attacks in the next few lectures
- DNS has issues for privacy, especially with respect to compulsory metadata collection by government
  - IP addresses of end points of servers and users change continuously
    - Not a problem since we have the DNS to give us the current IP address corresponding to a domain name
    - BUT that is metadata and it is (probably) recorded somewhere
    - The fact that we visited dodgywebsite.com may not be captured, but the fact that we generated a DNS request asking for the IP address of dodgywebsite.com is (probably) recorded!!!
  - Well worth reading Geoff Huston on this topic
  - http://www.potaroo.net/ispcol/2015-08/gvi.html

# Network Address Translation

- Network Address Translation (NAT) and Network Address Port Translation (NAPT)
- Maps internal (non-routable) addresses and ports to external (routable) addresses and ports
- Driven by a number of needs
  - re-use of IP addresses
  - making system administration easier
    - don’t need to renumber the whole network when a new IP address is acquired
  - Security side effect of hiding internal IP addresses from external network

# Network Address Port Translation

- Overloading port number
- Used when number of IP addresses inadequate
  - Can allocate multiple conversations to the one IP address but with different port numbers
- Both NAT and NAPT
  - Dynamic and Static operation
    - usually Dynamic
  - Dynamic operation
    - maintains a set of state tables which map internal and external IP addresses
  - maps IP address and port numbers
  - permits multiple connections via small number of external IP address

# Security implications

- Complicated to run IPSEC through NAT
  - Motivation for “tunnel” mode in IPSec
- Some protocols across NAT very messy
  - Eg ftp contains explicit addresses (in text) that have to be modified
  - Fortunately ftp rarely used now
- Loss of end-to-end significance of IP addresses with some possibilities of spoofing and man in the middle attacks
- Configuration can be complex leading to likelihood of errors and reduced resilience

# Autoconfiguration via DHCP

- Bootstrapping of a computer to obtain an IP address, subnet mask, default gateway (router) and name server (DHCP)
- Dynamic Host Configuration Protocol (DHCP)
  - Upon startup,a host transmits a DHCPDISCOVER message containing its MAC address to the broadcast address to find DHCP servers
  - DHCP servers that receive the request send a DHCPOFFER to the client
  - The client then transmits a DHCPREQUEST to one of the servers (usually the first it receives)
  - The server then sends DHCPACK whereupon the IP address is 'leased' to the host for a certain period

# Security implications

- No default authentication of host's MAC addresses
  - Can provide IP address to a possibly unauthorised host
- No default authentication of validity of DHCP server
  - could issue bogus IP addresses with a resulting Denial of Service
- No default controls on the number of IP addresses requested
  - could write malicious code that continually requests IP addresses with fabricated MAC addresses with a resulting Denial of Service
- However, usually proprietary solutions
  - Authentication provided in Windows Server 2003 and subsequent releases
  - Cisco switches and routers provide some defense mechanisms

# IP addresses as temporary tokens

- DHCP, NAT and DNS have changed the nature of IP addresses
- IP addresses were originally long lived identifiers
- Now temporary tokens which are allocated by DHCP and translated by NAT and in the case of cloud servers, mapped by DNS
- Has security implications
  - Increased importance of DNS
    - Needs to be made very secure
  - Challenges for law enforcement
    - Knowing an IP address is not enough. Need to know DHCP and (possibly) DNA mapping

# Remote logins

- telnet, rlogin, ssh
- Provides character terminal emulation across the network
- telnet and rlogin are very susceptible to attack
  - Should be avoided
    - older versions transmitted passwords in plaintext
  - sessions can be hijacked once authentication completed
- Secure shell
  - much more secure
  - uses digital certification to provide authentication and encryption

# Electronic mail

- SMTP
  - simple mail transfer protocol
- POP
  - post office protocol
  - contains mailboxes for collection and transmission of mail
- IMAP
  - Internet message access protocol
  - alternative to POP with more control over mailboxes and partial retrieval
- MIME
  - multipurpose internet mail extensions
  - allows non ascii characters to be sent

# WWW

- World Wide Web
- Uniform Resource Locator
- HTML
- HTTP
  - HyperText Transfer Protocol
  - GET request
  - Error messages
- Many security implications
  - Use of port 80 for many traffic types other than HTML
    - Eg SOAP allows remote procedure calls through port 80

# Realtime applications

- Realtime Transfer Protocol (RTP)
  - Mostly VoIP but also video conferencing and (less so nowadays) video on demand
- Based on UDP
  - Realtime applications can (usually) tolerate loss but not delay
  - TCP guarantees no loss but with variable and unpredictable delay
- RTP Control Protocol (RTCP)
  - used primarily to synchronise streams and carry signalling messages
- Signalling protocols
  - SIP and H.323
  - RSVP

# SNMP

- Simple Network Management Protocol
  - Used to monitor and control network nodes and links
- Based on the exchange of Management Information Base
  - contains information as to a nodes configuration, capacity and recent errors
- Some security implications
  - MIBs exchanged in plain text
  - No authentication of message sources
    - could force a node off-line
  - Gives lots of information about the structure and  of a network
  - SNMPv3 includes authentication and encryption

# IPv6

- Many more security features built in to the protocol
- IPv6 protocol stacks guaranteed to support IPSec
  - Still needs configuration
- ICMPv6 much more secure
  - encryption and authentication
- More later in the subject

# Conclusion

- Review of the TCP/IP protocol suite with a high level overview of its security weaknesses
- Many areas of potential security weakness
- TCP/IP services overview and their security weaknesses