INB255/INN255 Security

Lecture 9 Network Security

Outline

- Basic network concepts
- Communication protocols
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture
- Malicious Software
  - Viruses

Basic Network Concepts

- Network: A number of computers and devices, connected by communications channels, and hardware and software to enable data exchange
- The connections can be:
  - Physical
    - Examples: cable, fibre optic
  - Wireless
    - Example: Radio signal, Infrared, Satellite

Basic Network Concepts

- Network types and information security:
  - Need to secure both
    - the devices and
    - the communication channels.
  - Easier to do this for a LAN with physical connections: can provide physical protection at the location to restrict access to authorised users
    - For wireless connections and larger networks, the communication may extend beyond physical boundaries of organization

Outline

- Basic network concepts
- Communication protocols
  - HTTP authentication
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture

Outline

- Basic network concepts
- Communication protocols
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture
- Malicious Software
  - Viruses

Communication Protocols

- Communication Protocols
  - Are sets of standard rules required for data representation, authentication, error detection etc. to send information over communications channels
  - The protocols permit the communications themselves to be separated from the communication media
    - Communication is independent of whether the media is coax cable, optical fibre, wireless, etc

Communication protocols

- Protocol Stacks
  - Layered architecture for communications
    - Each layer performs different activities required to enable communications
  - ISO Open Systems Interconnection (OSI) model consists of 7 layers:
    - Application: User level data
    - Presentation: Data standardisation, blocking, compression
    - Session: Message sequencing
    - Transport: Flow control, error detection and correction
    - Network: Routing, blocking messages into uniformly sized packets
    - Data Link: Separating packets into frames, error recovery
    - Physical: Actual communication – bit transmission

Communication protocols

- Protocol Stacks
  - Transmission Control Protocol/Internet Protocol (TCP/IP) can be considered as four layers:
    - Application: Prepares messages from users
    - Transport: Converts messages to packets
    - Internet: Converts packets to datagrams
    - Physical: Transmission as bits
  - TCP packet: data structure containing information such as sequence number, source and destination port numbers, data
  - Different applications have different port numbers. For example:
    - HTTP – port 80
    - SMTP – port 25

Communications Protocols

- Network-related security protocols in common use include:
  - Transport Layer Security (TLS):
    Used extensively on the web and is often referred to in privacy policies as a means of providing confidential web connections.
  - IP Security (IPSec):
    Provides security services at the IP level and is used to provide Virtual Private Network (VPN) services.

Outline

- Basic network concepts
- Communication protocols
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture
- Malicious Software
  - Viruses

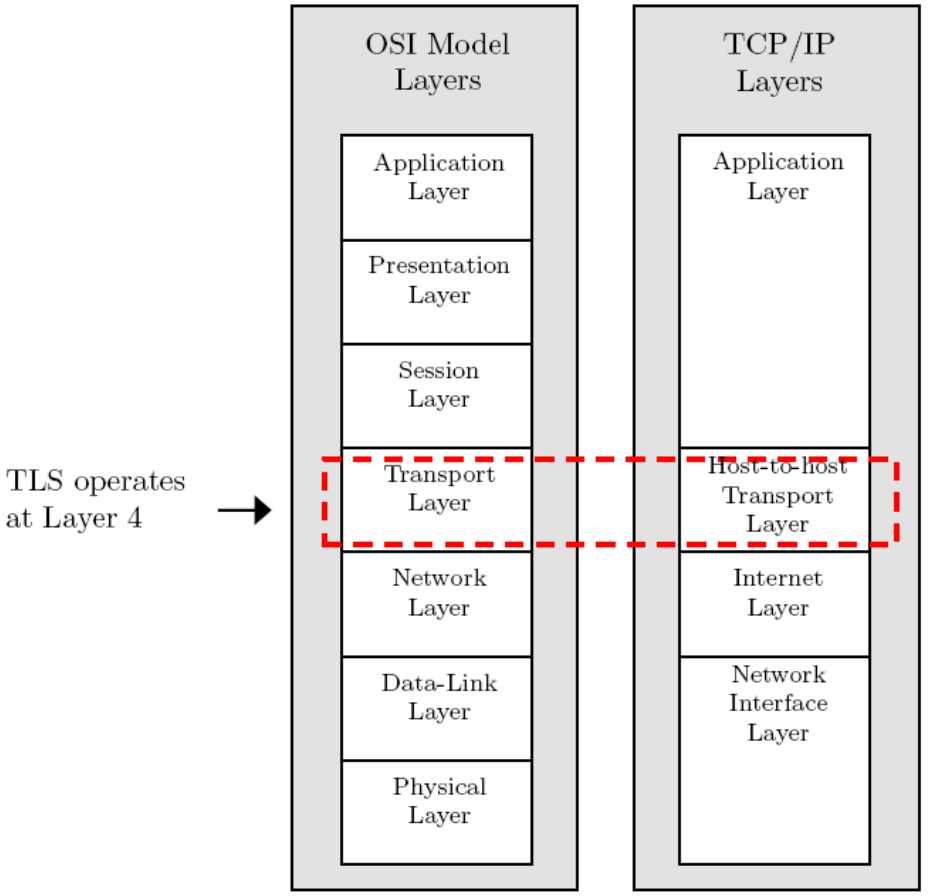
SSL/TLS

- History:
  - Originally Netscape's **Secure Sockets Layer (SSL) protocol**
  - SSL Versions: SSLv2 in 1995, SSLv3 in 1996
  - Standardized as **Transport-Layer Security (TLSv1)** by Internet Engineering Task Force (IETF) in RFC2246
- TLS versions:
  - TLSv1.0 specified in RFC2246 in 1999
  - TLSv1.1 specified in RFC 4346 in 2006
  - TLSv1.2 specified in RFC 5246 in 2008

SSL/TLS

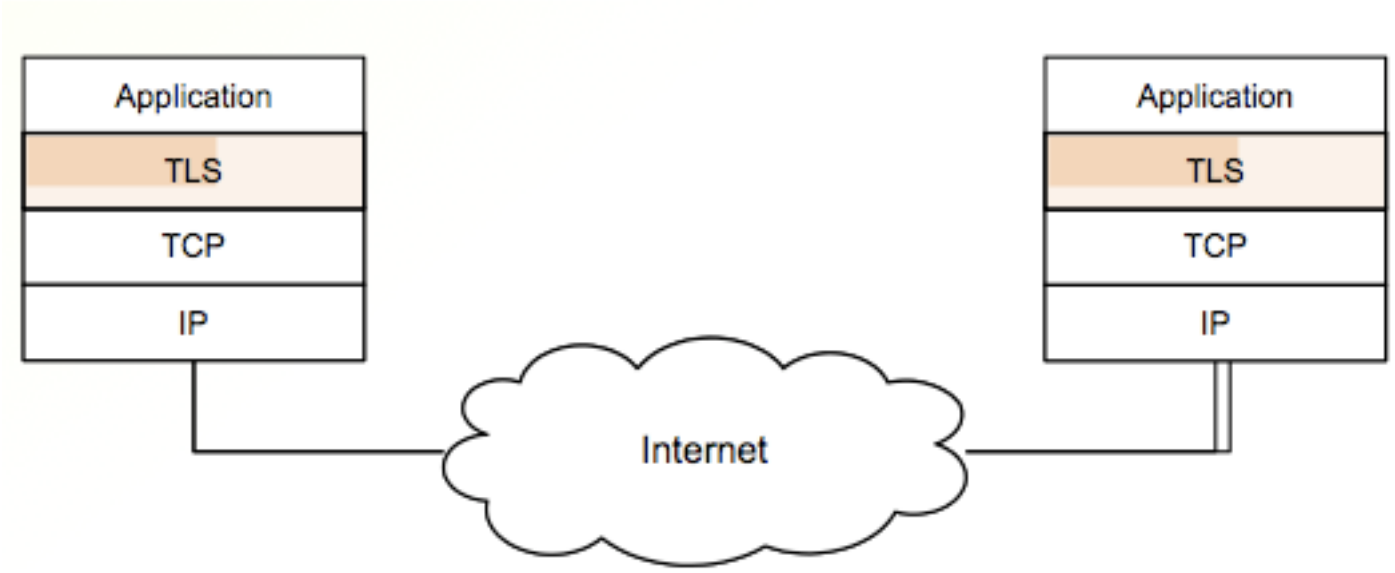
- Transport Layer Security (TLS) is a cryptographic protocol that operates at the transport layer (actually, above the transport layer)
  - Say, on top of Transmission Control Protocol (TCP)
- Uses encryption and PKI to provide protection for network communication protocols operating at higher levels
  - For example, to protect HTTP communications
  - Use X.509 certificates to obtain public keys
  - Can be used to provide confidentiality and authentication

TLS
Transport Layer Security Protocol



TLS

- Encryption and authentication layer added to the protocol stack between TCP and applications.



Source: Tuomas Aura, http://research.microsoft.com/en-us/people/tuomaura/

TLS and HTTP

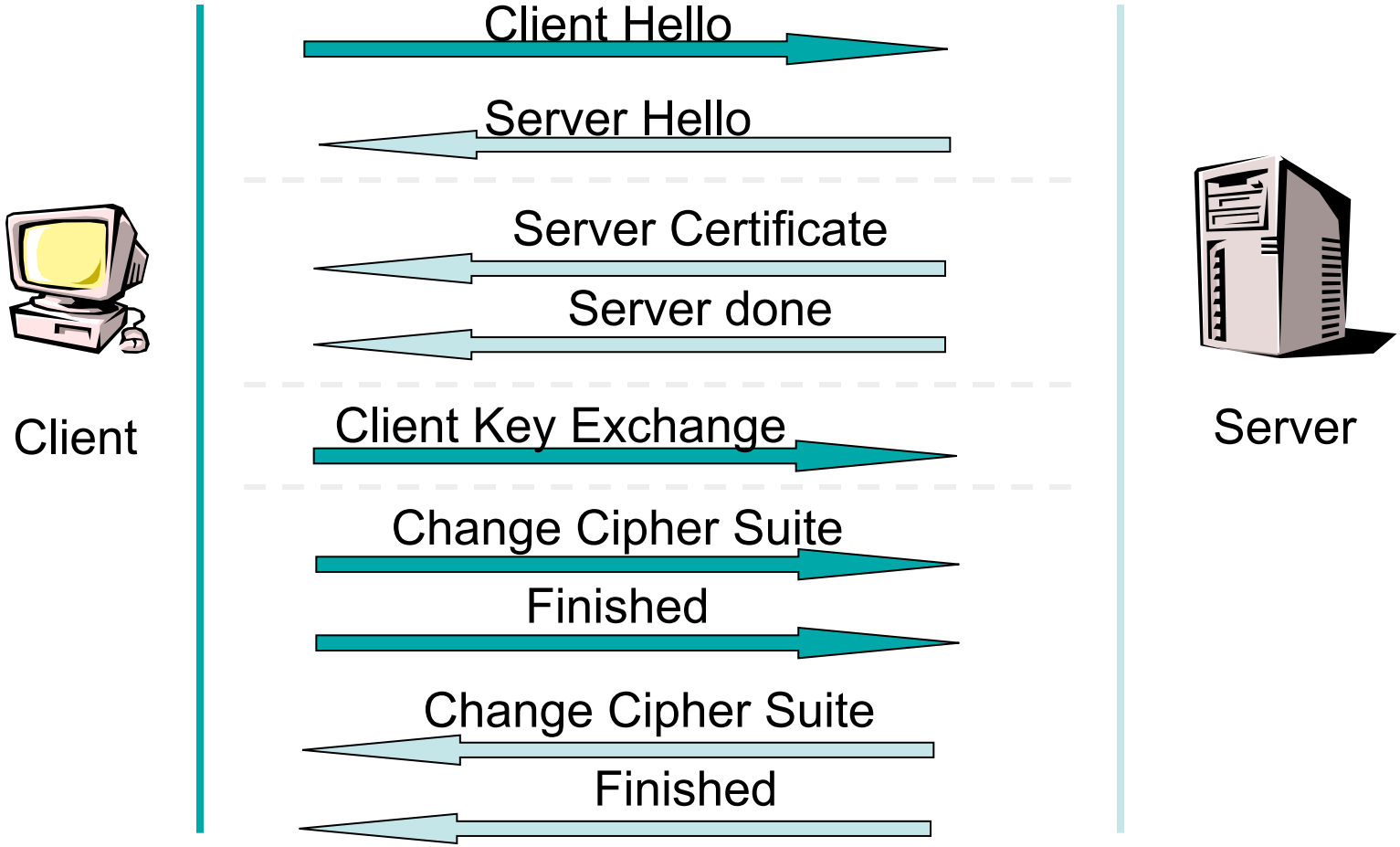
- SSL/TLS is the most commonly used encryption standard for Internet communications
  - Fast adoption because it is built into web browsers – Safari, Firefox (TLSv1.0), IE8 (TLSv1.2)
  - Intended to facilitate web commerce - used to encrypt credit card numbers and passwords sent to web sites
- TLS can be used to provide protection for HTTP communications:
  - Port 443 is reserved for HTTP over TLS
  - HTTPS is the name of the URL scheme used with this port.
  - http://www.develop.com implies the use of standard HTTP using port 80.
  - https://www.develop.com implies the use of HTTP over TLS using port 443.

TLS: Architecture Overview

- TLS Handshake Protocol: When establishing a TLS connection, the client and server must establish the version of TLS and the CipherSuite – a set of cryptographic algorithms that will be used to secure transmissions
- TLS Record Protocol: the format for TLS records to provide basic services to higher level protocols
- Other TLS Protocols include:
  - TLS Alert Protocol – error messages
  - TLS Change Cipher Spec Protocol – turn on encryption or update keys

Diagram

TLS: Simplified Handshake
RSA-based



TLS: Simplified Handshake
RSA-based

- Client hello
  - Advertises available cipher suites
  - Most common cipher suite: RSA for key establishment, 3DES for encryption and HMAC-SHA1 for data authentication)
- Server hello
  - Returns the selected cipher suite (choose from list sent by client)
  - Server adapts to client capabilities
- Server Certificate
  - X.509 digital certificate sent to client.
  - Client verifies the certificate including that the certificate signer is in its acceptable Certificate Authority (CA) list.
  - Now the client has the server's certified public key.

TLS: Simplified Handshake
RSA-based

- Server done
  - To indicate that the server has finished sending messages.
- Client Key Exchange
  - Client selects a random ‘pre-master secret’
  - Client encrypts the ‘pre-master secret’ using the server’s public key
  - Client sends the encrypted ‘pre-master secret’ to the server.
  - Server decrypts using its private key to recover the ‘pre-master secret’.
  - Both parties now compute the master secret using the pre-master secret and other exchanged values.

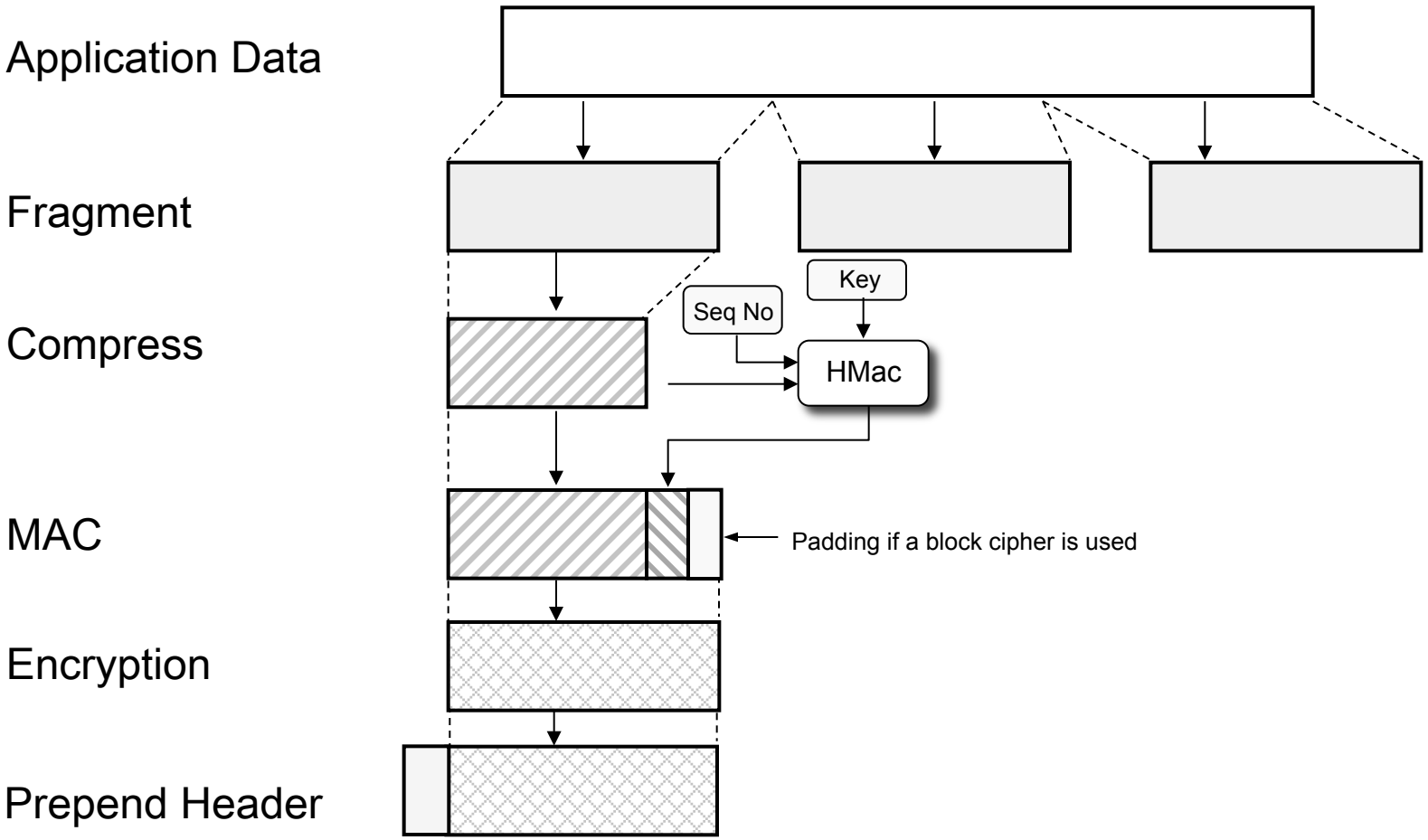
TLS: Simplified Handshake
RSA-based

- Completion
  Both client and server exchange
  - change_cipher_spec to indicate subsequent messages are encrypted and MAC'ed
  - finished message (already protected) to complete

TLS: Record Protocol Overview

- Provides two services for TLS connections.
  - Message Confidentiality:
    - Ensure that the message contents cannot be read in transit.
    - The Handshake Protocol is used to establish a symmetric key to be used to encrypt SSL/TLS payloads.
  - Message Integrity:
    - Ensure that the receiver can detect if a message is modified in transmission.
    - The Handshake Protocol establishes a shared secret key used to construct a MAC.

TLS: Record Protocol Operation



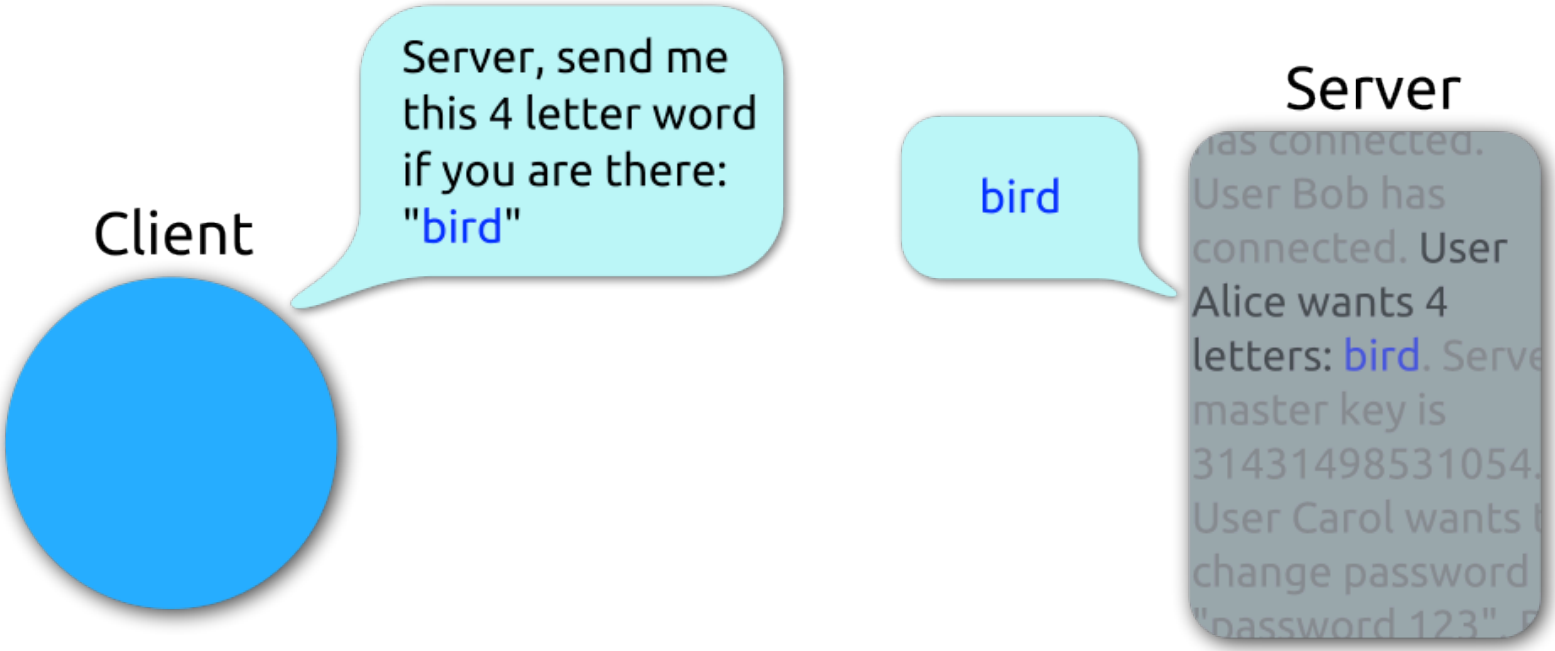
TLS security considerations

- Trust and digital certificates:
  - TLS uses public keys – provided in digital certificates
  - Certificates should be verified – requires tracing certificate pathways
  - Web browsers come with pre-configured lists of root certificates but users can add or remove root CAs
- One-way or mutual authentication?
  - Authentication is usually of server to client only, not mutual
  - Users usually do not have client certificates
  - Typically, authentication of users is not performed in handshake
  - Instead, password authentication over server-authenticated HTTPS channel

The Heartbleed Bug

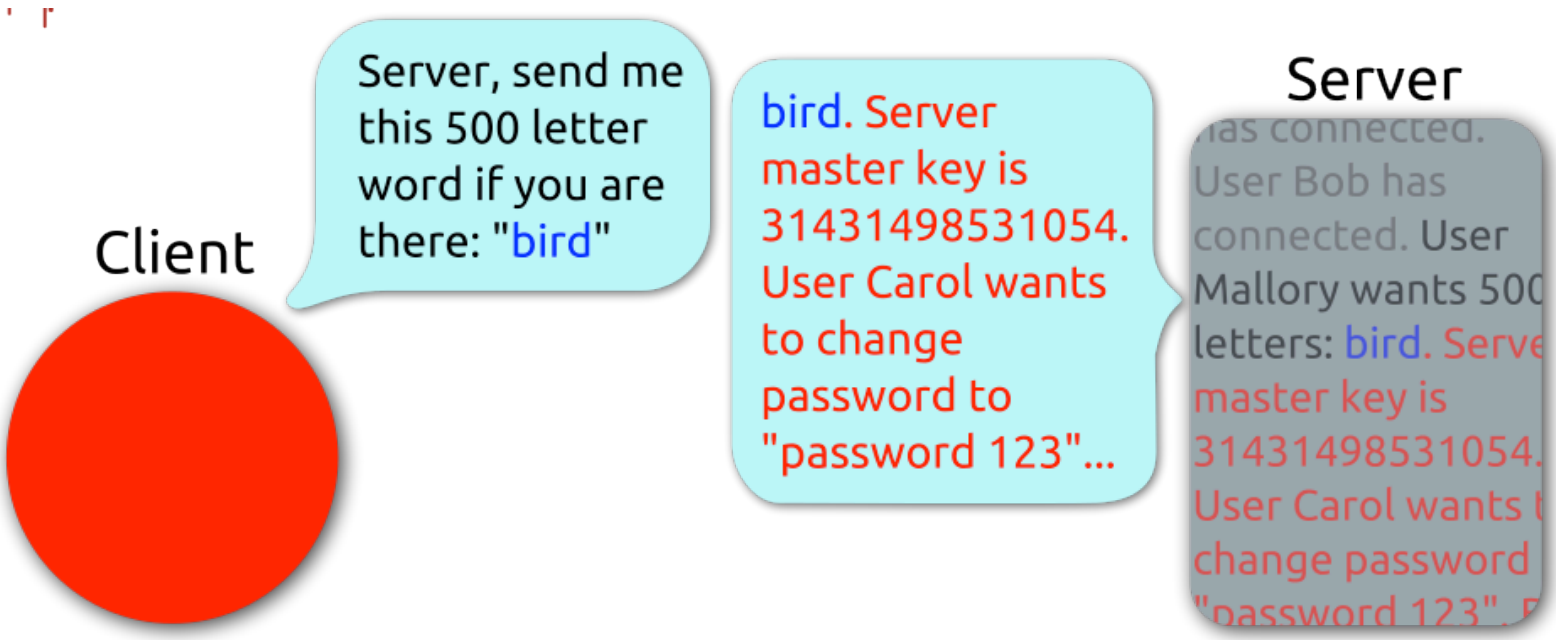
- The Heartbeat Extension for the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols
- These protocols are extremely widely used from security vendors products to secure web browsing (when you log in to a site and see https://)
- Published and implemented in 2012
- Contains a buffer overflow bug that allows up to 64Kb of memory to be returned to malicious

SSL Heartbeat Message



http://en.wikipedia.org/wiki/File:Simplified_Heartbleed_explanation.svg

Malicious Heartbleed Message



http://en.wikipedia.org/wiki/File:Simplified_Heartbleed_explanation.svg

Heartbleed Bug Issues

- Affected versions of OpenSSL are OpenSSL 1.0.1 through 1.0.1f (inclusive)
- Patch as soon as possible
- After patching, private keys need to be renewed and passwords should be changed
- Many servers have been patched but clients are also vulnerable

Outline

- Basic network concepts
- Communication protocols
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture
- Malicious Software
  - Viruses

IPSec: Introduction

- Internet Protocol Security (IPSec) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks
- Operates at the Network or Internet layer, so can secure application and transport layer communications, including arbitrary TCP and UDP sessions.
- Uses encryption, authentication and key management algorithms to provide end-to-end security
- Specified in RFCs by Internet Engineering Task Force (IETF) Working Group
- URL: http://www.ietf.org/html.charters/ipsec-charter.html
- Provides a security architecture for both IPv4 and IPv6

IPSec: Security Services

- Message Confidentiality.
  - Protects against unauthorised data disclosure.
  - Accomplished by the use of encryption mechanisms.
- Traffic Analysis Protection.
  - A person monitoring network traffic cannot know which parties are communicating, how often, or how much data is being sent.
  - Provided by concealing IP datagram details such as source and destination address.
- Message Integrity.
  - IPsec can determine if data has been changed (intentionally or unintentionally) during transit.
  - Integrity of data can be assured by using a message authentication code (MAC).

IPSec: Security Services

- Message Replay Protection.
  - The same data is not delivered multiple times.
- Peer Authentication.
  - Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate.
  - Ensures that network traffic is being sent from the expected host.
  - IP addresses are used as host identifiers.

IPSec: Protocol Types

- Encapsulating Security Payload (ESP)
  - Confidentiality, authentication, integrity and replay protection
- Authentication Header (AH)
  - Authentication, integrity and replay protection. However there is no confidentiality
- Internet Key Exchange (IKE)
  - negotiate, create, and manage security associations

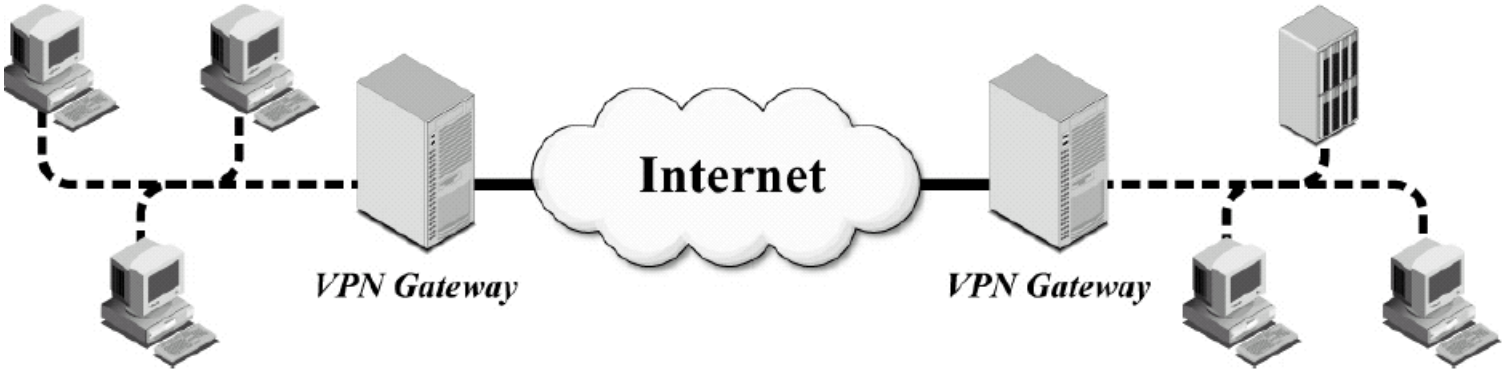
IPSec: Modes of operation

- Each protocol (ESP or AH) can operate in transport or tunnel mode.
- Transport mode:
  - Operates primarily on the payload (data) of the original packet.
  - Generally only used in host-to-host architectures.
- Tunnel mode:
  - Original packet encapsulated into a new one, payload is original packet.
  - Typical use is gateway-to-gateway architecture.

IPSec: Common Architectures

- The endpoints for communications secured using IPSec can be either hosts or gateways to secured networks.
- Combinations of these form three common architectures:
  - Gateway-to-gateway
  - Host-to-gateway
  - Host-to-host

IPSec: Common Architectures
Gateway-to-Gateway

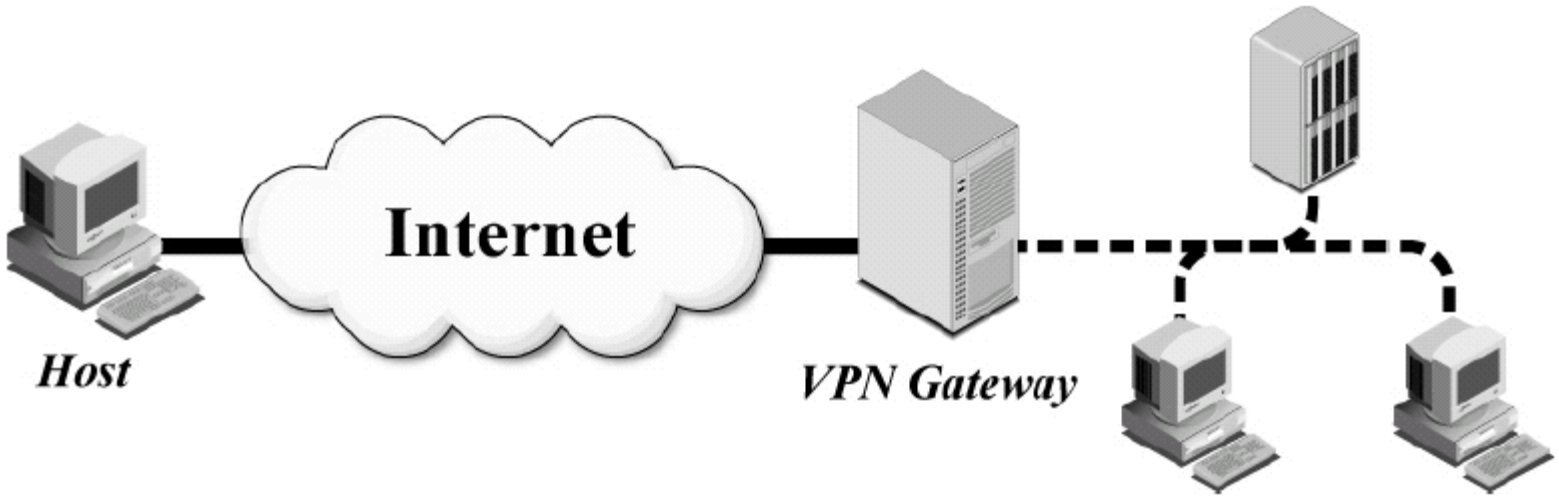


Source: NIST Special Publication 800-77

IPSec: Common Architectures
Gateway-to-Gateway

- Provides secure network communications between two secure networks. Network traffic is routed through the IPsec connection, protecting it appropriately.
- A VPN connection is established between the two gateways.
- NOTE: This only provides protection for data between the two gateways.
- Commonly used for connecting two secured networks as an alternative to the more costly private wide area network (WAN).
- Example: linking a branch office to headquarters over the Internet.

IPSec: Common Architectures
Host-to-Gateway

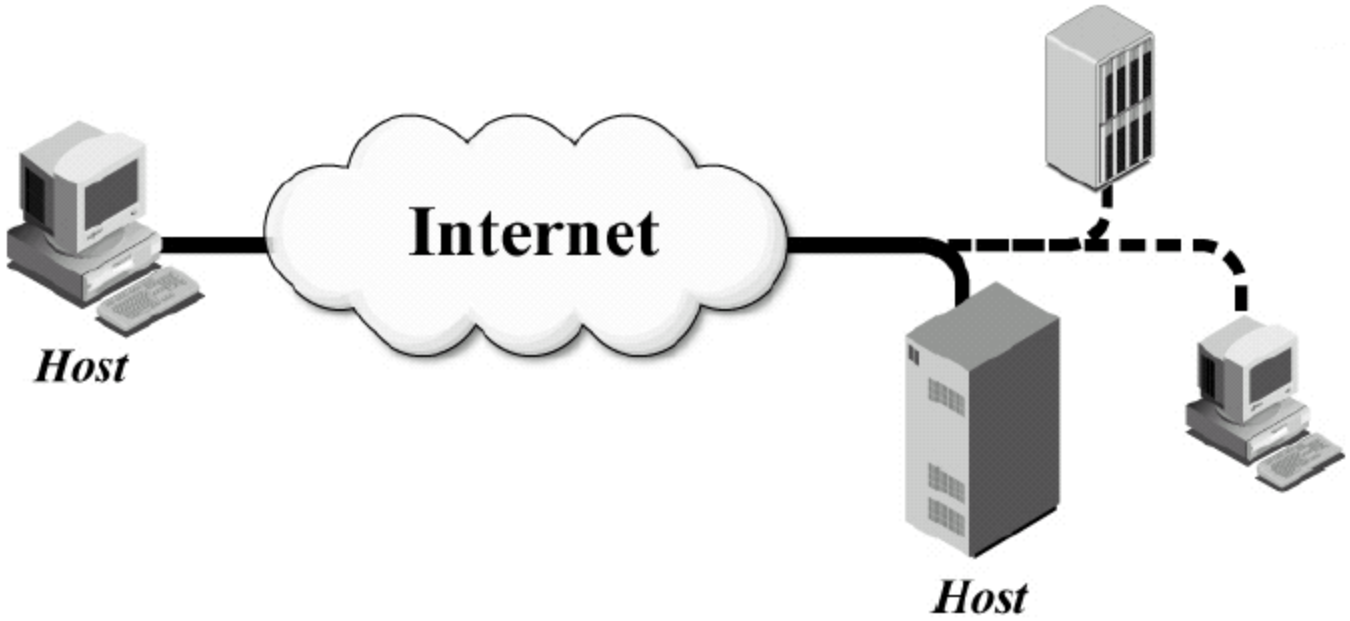


Source: NIST Special Publication 800-77

IPSec: Common Architectures
Host-to-Gateway

- Provides secure communications over an insecure connection between a single host and a secure network.
- A VPN connection is established between the host and the gateway to the network.
- NOTE: This only provides protection for data between the host and the gateway – within the network the transmissions are not protected.
- Commonly used to provide secure remote access for a single user connecting over an untrusted network to resources on a secure company network.
- Example: providing access over the Internet for employee working from home (their local computer is the host) to resources located within the company headquarters.

IPSec: Common Architectures
Host-to-Host



Source: NIST Special Publication 800-77

IPSec: Common Architectures
Host-to-Host

- This is the only architecture that provides protection for data throughout its transit.
- All user systems and servers that will participate in VPNs need to have VPN software installed and/or configured.
- Key establishment is often accomplished through a manual process.
- Resource-intensive to implement and maintain in terms of user and host management
- Example: Could be used for special purpose, such as system administrators performing remote management of a single server.

IPSec: Benefits

- Is transparent to applications
  - Operates at Network/Internet layer so applications are not aware of its operation.
- If applied at a network gateway (firewall/router), strong security applies to all traffic crossing this boundary.
  - Internal workstations need not be reconfigured.
- Can be transparent to end users.
  - System administrator configures IPSec; the end user is not involved.

Outline

- Basic network concepts
- Communication protocols
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture
- Malicious Software
  - Viruses

Firewalls

- Firewall: component or set of components
  - placed at the interface between two networks with differing security requirements
  - aims to control the flow of network traffic between a protected network and other networks.
- Frequently used to prevent unauthorized Internet users from accessing private networks (Intranet).
  - All messages entering or leaving the intranet pass through the firewall
  - Each message is examined, and those that do not meet the specified security criteria are blocked.
- Can be implemented in hardware, software, or a combination of both.

Firewalls

- Firewall categories:
- Firewalls can be categorized according to two criteria:
  1. the highest layer data in the network communication protocol stack (OSI or TCP/IP) the firewall can examine; and
  2. whether or not the communication terminates at the firewall:
  - If the connection does not terminate, the firewall is a **filter**.
  - If the connection terminates, the firewall is called a **proxy**.

Firewalls:
Firewall categories

- Basic firewalls examine data associated with lower TCP/IP layers only.
  - Example: Simple packet filters operating at network level
- More sophisticated firewalls can examine application layer data.
  - Example: Application level gateway

Outline

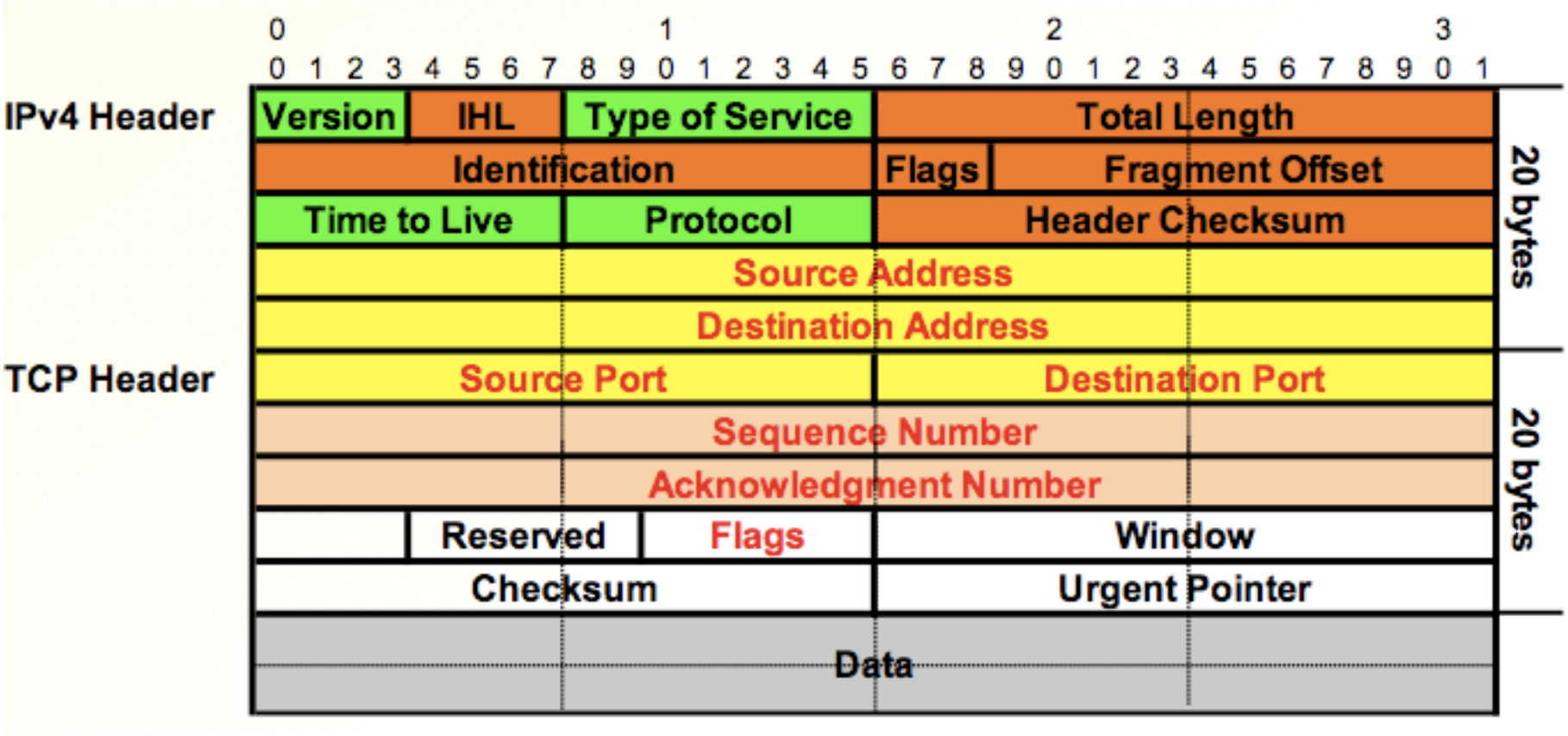
- Basic network concepts
- Communication protocols
  - HTTP authentication
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture

Firewalls:
Simple packet filters

- A packet filter is a device or program that operates at the network layer
- Simple packet filters examine each packet independently of other packets
  - Even if they are part of the same connection
- The packet filter decides whether to pass or drop each packet
- Decisions based on information in packet headers, such as
  - IP header fields (Source or Destination IP Addresses)
  - The Protocol (UDP, TCP or ICMP)
  - TCP/UDP port numbers (Source or Destination Port Numbers)
  - Direction the packet is travelling (into/out of the internal network)

Firewalls:

Information layers - IPv4 and TCP headers



- Which fields should a firewall use for filtering?

Source: Tuomas Aura http://research.microsoft.com/en-us/um/people/tuomaura/teaching/network-security-firewall.pdf

Firewalls:
Simple Packet Filters

- Routers are commonly used as packet filters, in addition to performing normal routing duties
- To perform simple packet filtering a set of rules is required that specifies what sort of action to take for a given set of conditions.
- These rules should be consistent with the organisation's information security policy
- The rules are generally recorded in table form.

Firewalls:
Simple Packet Filters

- A rule table specifies how to filter network traffic:
  - Each rule consists of conditions and an action
  - For each packet, the first matching rule is found
  - Two possible actions: allow or block
- Example rule table: inbound traffic to email (SMTP) server 1.2.3.10

Protocol	Src IP	Src port	Dst IP	Dst port	Action	Comment
TCP	4.5.6.7	*	1.2.3.10	25	Block	Stop this spammer
TCP	*	*	1.2.3.10	25	Allow	Inbound SMTP
TCP	1.2.3.10	25	*	*	Allow	SMTP responses
*	*	*	*	*	Block	Default rule

Source: Tuomas Aura http://research.microsoft.com/en-us/um/people/tuomaura/teaching/network-security-firewall.pdf

Firewalls:
Simple Packet Filters

- Decision making can also consider the direction the packets are travelling:
  - Ingress filtering: filtering inbound traffic
  - Egress filtering: filtering outbound traffic
- To reduce the possibility of transmitting packets with spoofed addresses, a simple rule to implement is:
  - Ingress filtering: drop inbound packets with source addresses that belong to the local network
  - Egress filtering: drop outbound packets with source addresses that are not local

Outline

- Basic network concepts
- Communication protocols
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture
- Malicious Software
  - Viruses

Firewalls:
Stateful Packet Filters

- Stateful packet filters operate in the same way as simple packet filters
  - examining headers and comparing to ruleset to see if the packet transmission is allowed under the firewall rules
- BUT stateful packet filters are more 'intelligent' than simple packet filters
  - Also keep a 'state table' noting the state of each connection:
  - Is the connection being established, in use, or terminated?
- Stateful packet filters examine the state in the context of the of the conversation
  - If header values contradict the expected state, the packet will be dropped

Firewalls:
Stateful Packet Filters

- Sometimes called dynamic packet filters due to their ability to add rules 'on the fly'.
- For example:
  - Can recognise an outgoing connection request being sent from an internal client to an external server,
  - Will add a temporary rule to allow reply traffic back through firewall.
  - When session is finished, the temporary rule is deleted.
- Common software packages for stateful packet filters include:
  - IPTables for Linux
  - Checkpoint Firewall-1
  - Cisco PIX (integrated hardware & software)
  - Microsoft Internet Security and Acceleration Server

Firewalls:
Packet Filters

- Strengths:
  - Low overhead
  - High throughput
  - Operates at lower layers, so supports almost any application
- Weaknesses:
  - Do not examine application layer data/commands
    - May allow insecure operations to occur
    - Cannot perform content filtering or user authentication
  - Allow direct connections between hosts inside & outside firewall
  - Simple (stateless) packet filters only:
    - less secure (can be susceptible to IP spoofing)
    - more difficult to write complex rules

Firewalls:
Personal Firewalls

- A personal firewall is a software program that is designed to protect the computer on which it is installed.
  - Frequently used by home users to provide protection against unwanted Internet traffic.
- Usually these are stateful packet filters.
- Examples:
  - Windows XP, Vista and Mac OSX all include a personal firewall.
  - Vendors such as ZoneAlarm, and Sygate provide a free version of their product for personal use.
- Some products include anti-virus software as well (maybe at extra cost).

Outline

- Basic network concepts
- Communication protocols
  - HTTP authentication
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture

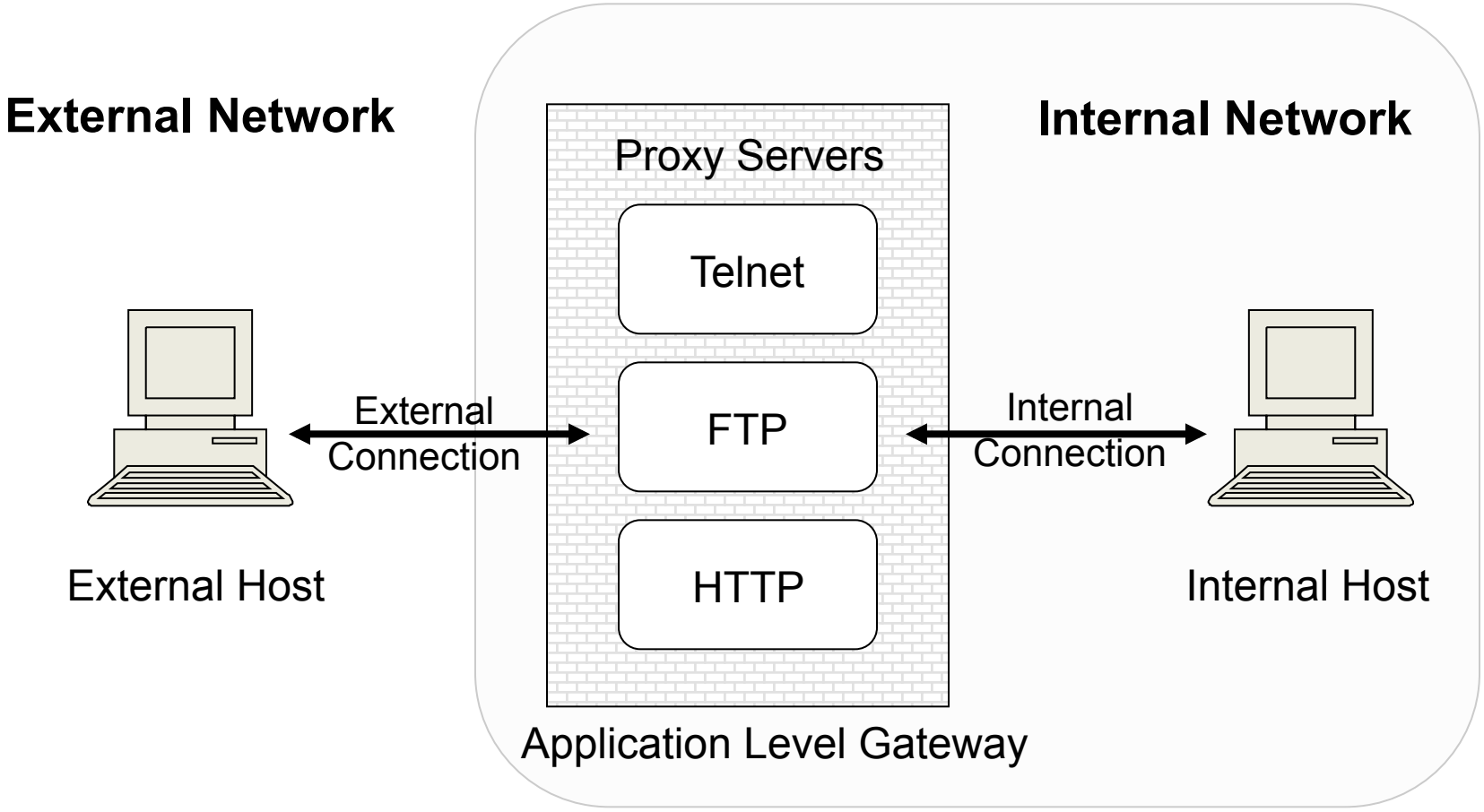
Firewalls:
Application Proxy Gateway

- Application level gateway filters traffic based on application data
  - Can examine application data, not just header info such as protocol and port numbers
- Known as an application proxy because the firewall needs to act on behalf of the client.
  - All connections terminate on the firewall.
  - Instead of a direct connection from client to server, the application proxies have an internal and external interface.
  - Two connections are made: connection from client to proxy and, if request is permitted, connection from proxy to requested destination
  - The proxy accepts the incoming connection, analyzes contents of packet and protocol to be used, determines if rules allow connection and, if connection is permitted, initiates a connection

Firewalls:
Application Proxy Gateway

- Usually configured to support only specific applications or specific features of an application:
  - each application (email, web browser) must have its own proxy (specific gateway) in the firewall
  - If proxies are designed specifically for that protocol, they understand whether the traffic flowing is following the protocol and allowed by the policy rules
- Application layer firewalls have proxies for the most commonly used protocols
- Some ‘generic’ gateways can be used if a specific gateway does not exist, sometimes called circuit level gateways

Firewalls:
Application Proxy Gateway



Firewalls:
Application Proxy Gateway

- Strengths:
  - Provides potential for best security through control of application layer data/commands
  - Better logging and audit of traffic
  - Allows content filtering and user authentication
- Weaknesses:
  - Slower than packet filters – requires time to examine packet data in details, so may be unsuitable for real-time applications
  - Limited support for new applications – additional time requirement for vendor to write new gateways for new applications
  - Requires one additional connection (including processing resources) for each new connection

Firewalls:
Dedicated Proxy Servers

- To deal with load problems in an application proxy gateway dedicated proxy servers can be used
- These are typically
  - Deployed behind traditional firewall platforms
  - Dedicated to one type of traffic such as HTTP, SMTP, FTP
- Can perform authentication and audit as well as filtering for content such as:
  - Active code such as Java applets
  - Email attachments of certain types
  - Viruses

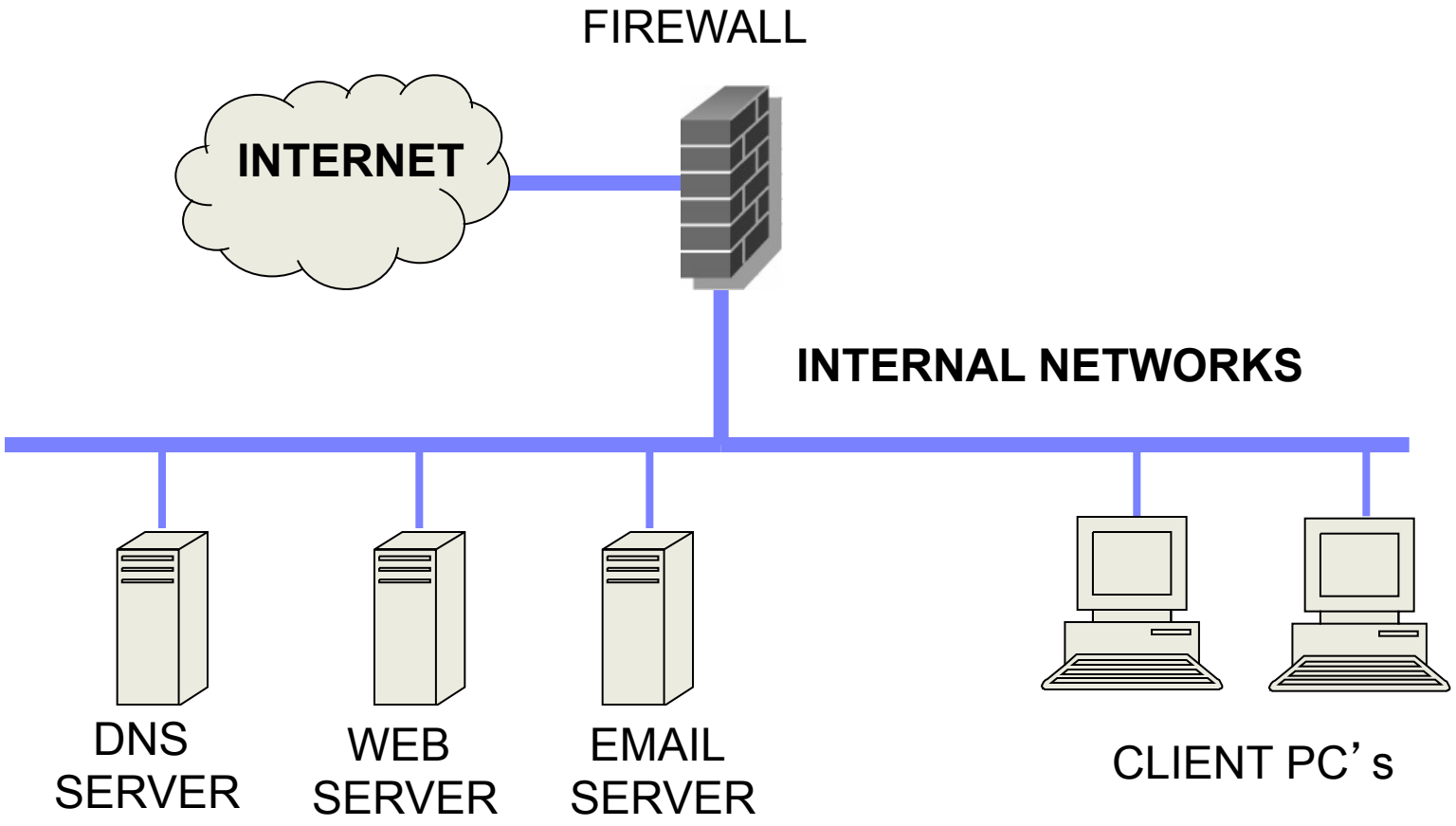
Outline

- Basic network concepts
- Communication protocols
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture
- Malicious Software
  - Viruses

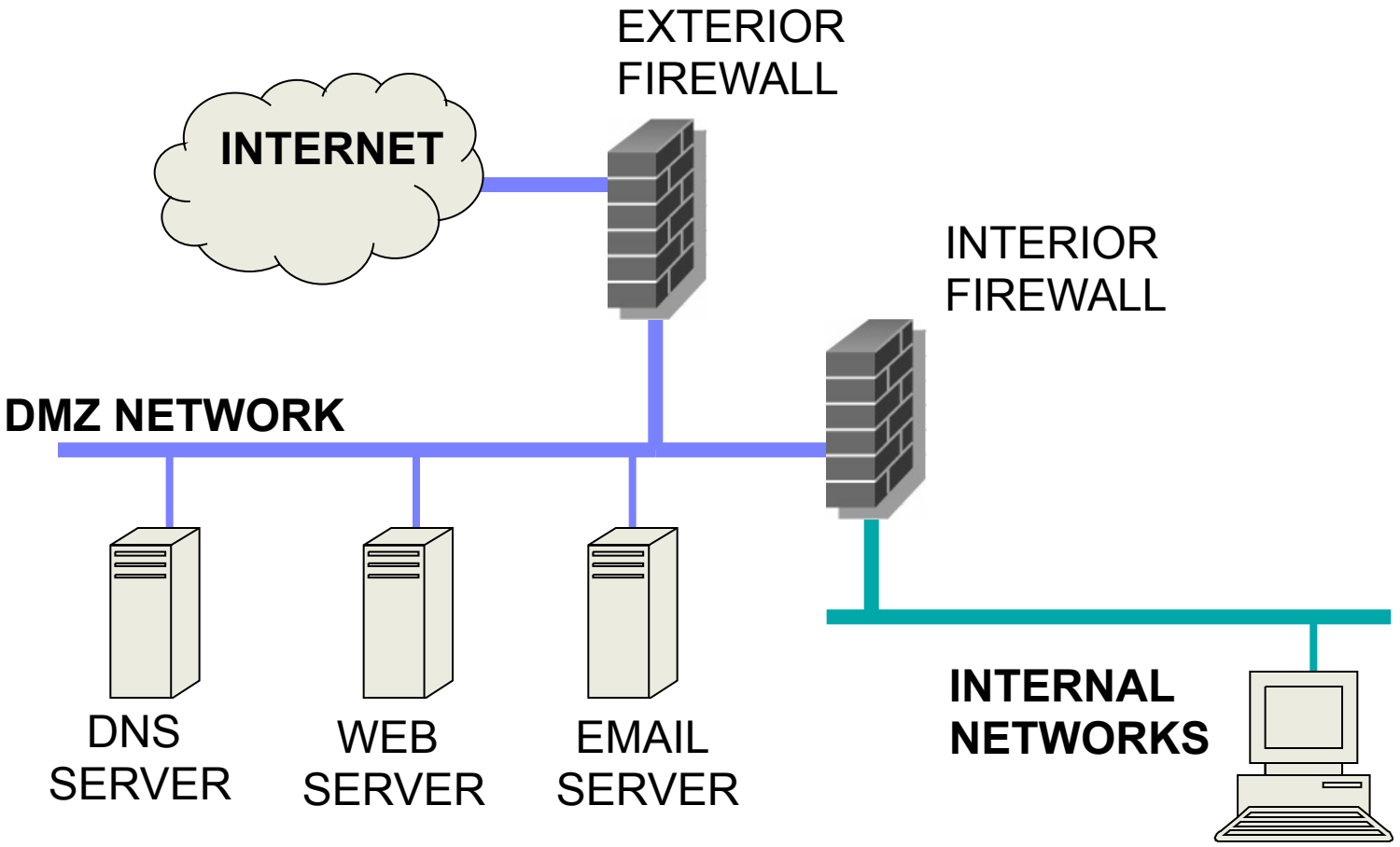
Diagram

Firewalls:

Simple Firewall Architecture



Firewalls:
DMZ Architecture



Firewall issues

- Firewalls are only effective if:
  - they are set up to implement a well formulated security policy.
  - That is, the most important aspect of a firewall is a clear conception of what it is meant to protect.
  - they are effectively administered, updated with the latest patches and monitored.
- The security policy must clearly define acceptable traffic
  - Only that traffic allowed to pass through the firewall;
  - everything else is considered unacceptable and must be blocked

Firewall issues

- Filtering should be performed on traffic in both directions:
  - Outbound connections should be filtered to prevent:
  - internal users accessing untrusted services or dangerous content
  - compromised internal machines spreading viruses to the Internet, or being used as part of distributed attacks
- Firewall rules can be difficult to configure
  - Order of rules matters
  - Configurations are usually fragile
  - Administrators can be afraid to modify configurations in case something breaks

Firewall issues

- Using firewalls to provide perimeter defence has serious limitations:
  - Errors in firewall configuration are common
  - There are other unfiltered communication routes, for example:
    - dial-up modem connections
    - unauthorised wireless access points
    - Unprotected laptops, USBs, etc move in and out of the intranet
  - In large networks there are often compromised nodes inside
  - Many new applications `bypass' firewalls by disguising as web traffic, using TCP port 80 and 443. For example, skype, bittorrent
- Given these limitations, firewalls should be complemented with intrusion detection systems

Outline

- Basic network concepts
- Communication protocols
  - SSL/TLS
  - IP Layer Security (IPSec)
- Firewalls
  - Simple packet filter
  - Stateful packet filter
  - Application-layer firewalls
  - And Network Architecture
- Malicious Software

Malicious Software

- Malware are programs that exploit system vulnerabilities.
- Types:
  - program fragments that need a host program
    - e.g. viruses, logic bombs, and backdoors
  - independent self-contained programs
    - e.g. trojan horses, worms, bots
  - replicating or not
- Sophisticated threat to computer systems !

Viruses

- A Virus is a piece of software that infects programs(host)
  - modifying them to include a copy of the virus
  - so it executes secretly when host program is run
- Usually specific to operating system
  - taking advantage of their details and weaknesses
- A typical virus goes through phases of:
  - Dormant: idle (not found in all viruses)
  - Propagation: copy itself into other programs/disk areas
  - Triggering: activated (date, file, disk limit)
  - Execution: perform the intended function(message, damage.

Virus Structure

- Components:
  - Infect - enables replication
  - Trigger - event that makes payload activate
  - Payload - what it does
- May be prepended, postpended or embedded
- When infected program invoked, executes virus code then original program code

Infection strategies

- Nonresident viruses:
  - Search for other hosts that can be infected,
  - Infect those targets,
  - Transfers control to the infected program
- Resident viruses
  - Do not search for hosts when they are started. Instead, it loads itself into memory on execution and transfers control to the host program.
  - The virus stays active in the background and infects new hosts when those files are accessed by other programs or the operating system itself

Propagation

- Using infected programs the virus is executed every time the program is executed.
- Using interrupts that occurs each time an external disk drive or a DVD is inserted into a USB port. Once this interrupt occurs, the virus is executed as part of the interrupt-handling routine and it tries to infect the newly inserted volume.
- As an email attachment.
- Through infected software. Embed a virus or a Trojan horse in a useful program (a calculator, a nice clock, or a beautiful screen saver)

Trigger

- Any event in the PC can be used as a trigger by a virus
  - Date or time
  - Number of boots
  - Generation counter of the virus
  - Number of keypresses on the keyboard
  - Amount of free space on the hard drive
  - Amount of minutes the machine has been idle

Virus Payload

- The Virus Payload is the malicious "task" of a virus.
- Performed when the triggering condition is satisfied.
- Examples:
  - Display a message, such as "Gotcha," a political slogan, or a commercial advertisement
  - Read a certain sensitive or private file. Such a virus is in fact spyware.
  - Slow the computer down by monopolizing and exhausting limited resources.
  - Completely deny any services to the user.

Virus Payload

- Erase all the files on the host computer
- Select some files at random and change several bits in each file, also at random.
  - referred to as data diddling and may be more serious, because it results in problems that seem to be caused by hardware failures, not by a virus.
- Random change of permissions.
- Produce sounds, animation.

Virus Classification by Target

- **Boot sector:** Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
- **File infector:** Infects executable files
- **Macro virus:** Infects files with macro code that is interpreted by an application.

Virus Classification by Hiding Method

- **Encrypted virus:** creates a random encryption key, stored with the virus, and encrypts the remainder of the virus. Then, the virus uses the stored random key to decrypt the virus. Virus replicates, a different random key is selected.
- **Stealth virus:** designed to hide itself from detection by antivirus software. By restoring the size, modification date, and checksum of the infected file

Virus Classification by Hiding Method

- **Polymorphic virus:** Mutates and infects each new file as a different string of bits making detection by the "signature" of the virus impossible.
- **Metamorphic virus:** As with a polymorphic virus ,a metamorphic virus mutates with every infection but rewrites itself completely at each iteration, increasing the difficulty of detection

Virus Classification by Hiding Method

- **Compression virus:** In addition to mutating, a virus may hide itself in a compressed file in such a way that the bits with the virus part depend on the rest of the infected file and are therefore always different.

E-Mail Viruses

- e.g. Melissa
  - exploits MS Word macro in attached doc
  - if attachment opened, macro activates
  - sends email to all on users address list
  - and does local damage
- Then saw versions triggered reading email
- Much faster propagation

Virus Countermeasures

- Anti-virus
- Prevention - ideal solution but difficult
- Need:
  - Detection
  - Identification
  - Removal
- If detect but can't identify or remove, must discard and replace infected program

Anti-Virus Evolution

- Virus and antivirus technologies have both evolved
- Anti-Virus generations
  - First - signature scanners
  - Second – heuristics rule (structure)
  - Third - identify actions and unusual behaviour
  - Fourth - combination packages

Types of Malware

- **Spyware**
  - Programs, cookies, or registry entries that track your activity and send that data off to someone who collects this data for their own purposes
  - The type of information stolen varies considerably
    - email login details
    - IP and DNS addresses of the computer
    - users' Internet habits
    - bank details used to access accounts or make online purchases etc…

Types of Malware

- **Adware**
  - Software that is installed on your computer to show you advertisements
  - These may be in the form of pop-ups, pop-unders, advertisements embedded in programs, or placed on top of ads in web sites, etc
- **Key loggers**
  - A program that captures and records user keystrokes
  - E.g. whenever a user enters a password, bank account numbers, credit card number, or other information, the program logs the keystroke
  - The keystrokes are often sent over the Internet to the hacker

Types of Malware

- **Rootkit**
  - A set of tools and utilities that a hacker can use to maintain access once they have hacked a system.
  - The rootkit tools allow them conceal their actions by hiding their files and processes and erasing their activity
- **Bot/Zombie**
  - These are programs that are inserted on computers by attackers to allow them to control the system remotely without the user's consent or knowledge
  - Botnets: Groups of computers infected by bots and controlled remotely by the owner of the bots
  - Computers that are infected with a bot are generally referred to as zombies

Types of Malware

- **Exploit**
  - A piece of software, a command, or a methodology that attacks particular security vulnerability
  - Takes advantage of a particular weakness e.g. OS, application programs
- **Phishing**
  - is not an application. It's the process of attempting to acquire sensitive user information with fake websites.
  - It's an example of social engineering techniques used to fool users
  - Common targets for phishing
    - Online payment systems such as e-bank, e-commerce are

Types of Malware

- **Spam**
  - is unsolicited bulk e-mail which is sent in massive quantities to unsuspecting Internet email users.
  - Most spam tries to
    - Sell products and services.
  - A more dangerous category of spam tries to
    - Convince the recipient to share their bank account numbers, credit card numbers, or logins & passwords to their online banking systems/services
  - It is also used for phishing and to spread malicious code

Summary

- Networks are computers and devices, connected by communications channels, and hardware and software to enable data exchange
- Different networks have different security requirements
- Defence in depth
  - Security for networks should consider both the perimeter and the interior of the network
- Firewalls
  - Remember these require understanding of policy, not just technology