Computer Network Security

Lesson 3

Application and Network Attacks

Lecturer: Dr Msagha J Mbogholi, PhD

Flashback from Lesson 2

- There are several complexities to address with network security.
- The 3 major security controls are Technical, Operational and Managerial (TOM)
- There are 8 integrals of network computer security.
- FIPS 200 standard describes 17 defense mechanisms that relate to the CIA of enterprise wide information systems.
- The National Center of Academic Excellence in Information Assurance (NCAE) have described 13 principles that assist in the design of the optimal security system.
- The development of a security strategy is done by examining or rather asking 3 pertinent questions – what is the service supposed to do, how does it do it, and does it actually work?

Content

- Applications & Application Attacks
- Network Attack Mechanisms
- Protecting the Network
- Network Attack Detection
- Assessing and Responding
- Incident Handling

Part 1

Applications & Application Attacks

Web Architecture & Applications

- The World Wide Web (www) and by extension the Internet, is arguably the most widely used service in the world today. This is so much so that most users on the Internet do not really know the difference between the www and the Internet! People talk of connecting to the Internet period….this in social norms implies the use of the www.
- The Internet is the (Inter)national (Net)work, hence it is a network of networks. It is built on a mesh network topology so that the origin of the network remains unknown (mostly for security reasons).
- Every network is developed based on a certain topology (physical layout) and an architecture (logical layout).
- There are two network architectures widely available for use: peer – to – peer (P2P) and Client-Server (CS) architectures.
- The Internet runs on a client-server architecture. This means that most users on the Internet are clients seeking to use the services/resources of servers.

Web Architecture & Applications (cont'd)

- Web architecture typically refers to the different ways in which servers and clients are configured on the Internet. The differences in architecture normally occur on the server side.
- Architectures are described in terms of tiers, that is, a 1 tier, 2 tier, n tier architecture.
- Let us examine a typical 1 tier web architecture in the next slide.

Web Architecture & Applications (cont'd)

- In a 1 tier architecture there is communication between the client and the server. The latter will process requests from the client internally and send back the results of the processing to the client. This means that the server does all the processing of the request without referring to any other server, and sends results back to the client.

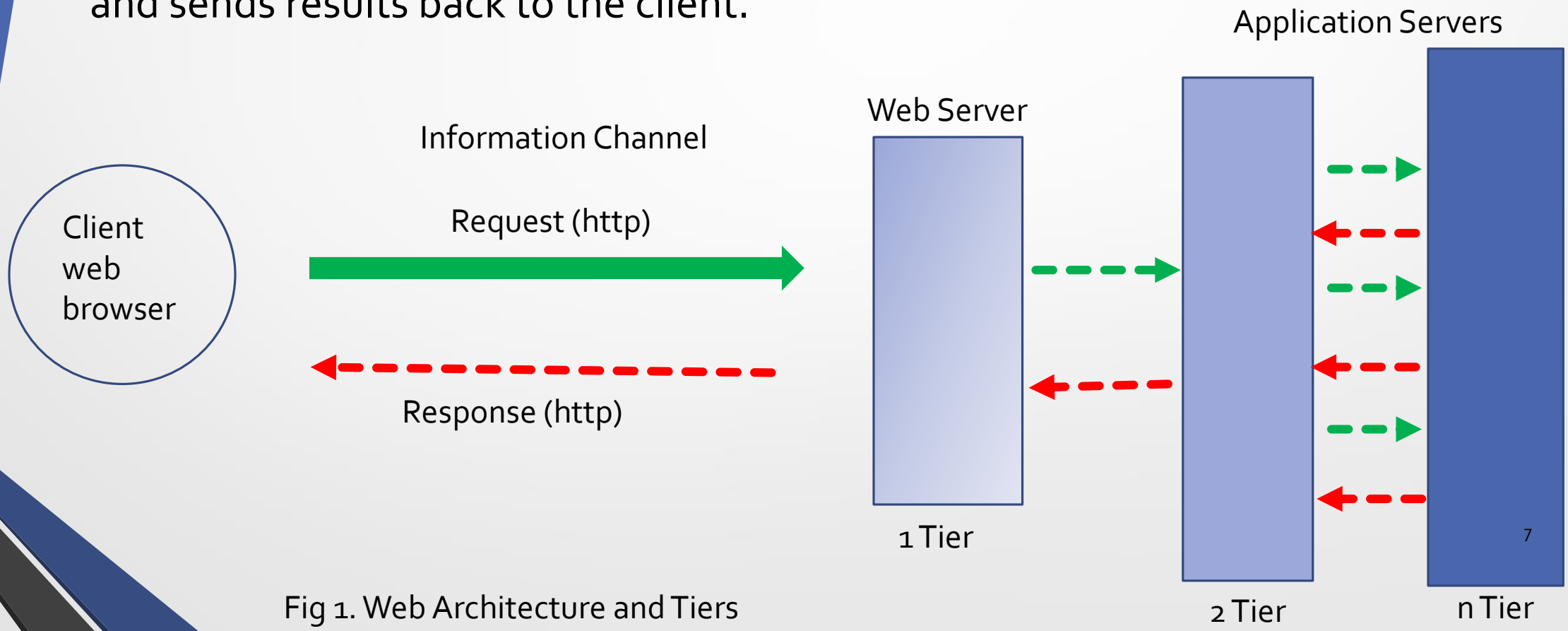

Fig 1. Web Architecture and Tiers

Web Architecture & Applications (cont'd)

- As can be seen from Fig 1 there are three key players in the transaction between a user and the web server.
- These are the client web browser/application, information channel, and the web server itself.
- The architecture shows that we can have several tiers assisting the web server in the processing of client requests. These are the application servers. The application servers can be database servers or specific application servers.
- Requests are normally processed via http over the information channel (the network); the results are sent back via the same channel.
- An attacker consequently has 3 points of attack, meaning there are 3 possible vulnerabilities: the client web browser/application, information channel (the network) and the server.

Application Attacks

- As transmission is normally done via http it is not possible to totally block http transmission; doing this would result in no communication between the client and the server! Blocking http transmission is typically a catch 22 situation; you know that http is a vulnerability but at the same time you need it to enable transmission between client and server.
- Due to this attacks will normally surround http transmission.
- The first point of vulnerability is the server end.

Application Attacks: Server Side

- Cross scripting: this kind of attack is called a cross attack as it doesn't attack the victim directly but rather via a targeted server. It takes advantage of the trust that the victim has for the server. A hacker will inject some malicious code/script into the web server with the intent of getting some sensitive/confidential information. A user then visits the server thereby triggering the malicious code. The code will then get the information the hacker wanted and forward it to him/her.
- SQL injection: as the name implies the target of this attack is the SQL database. The attacker aims to manipulate the SQL server in such a way that they can gain access to the database, thereby being able to access some desired/target information. Similar to an SQL injection is an XML injection that targets the XML used in the SQL of the database.
- Command Injection: this attack targets the operating system or a specific application at server level (tier 1) or any of the application servers (tier-n). The attacker targets to use a vulnerable application to attack the operating system of the server, thereby having control over it and its environment.
- Directory traversal attack: the attacker in this instance purposes to gain access to files in the server that they are not authorized to. The attacker identifies a vulnerable application and uses it to "traverse" from the root directory to other restricted directories.

Application Attacks: Server Side (cont'd)

- Access Rights attacks: These are attacks on the server side that target applications. These applications may be on the server or on dedicated application servers in different tiers. They are:
- Privilege escalation – this is when an attacker gives a user account higher privileges than it is supposed to have. This enables the account to perform operations that it is not authorized to. Another possibility is when the attacker uses another account with higher privilege to access the system to perform unauthorized operations.
- Transitive access – this happens when one party uses the rights of a third party to access the system. Essentially a potential attacker can use the blurry nature of transitive access to gain unauthorized use of the system.

Application Attacks: Client Side

- Drive-by download: this attack occurs when a user downloads content (code, pop ups or attachments) from a website that they trust. By clicking on a pop up window for example, a user downloads malicious code into their browser, enabling the attacker to access select information. The user is usually unaware of what has happened.
- Header Manipulation: As described in Fig 1 the communication between a server and a client occurs via http. The information (request and response) are contained in a http packet. The header manipulation attack targets the response http packet. This packet contains different parts each containing information that enables the packet to safely reach its intended recipient. The http header is part of this information; standard http header information is defined in the HTML language (see RFC 6648 and IANA Registry). In a header manipulation attack malicious code is injected into the http response header; the purpose of this is to enable the attacker to gain access to the client through the malicious code. HTTP response splitting is a common form of header manipulation attack.
- Cookies: cookies are created by a website to store user information in the client browser. The cookies help the browser to remember details about the user (name, preferences, email address and so on). Cookies are specific to the web server that created them, meaning that no web server can read cookies created by other web servers on a user machine. However, this is a possible exploit due to the information that is stored in the cookie. The different types of cookies are first-party, third party, session, tracking, secure and flash. A cookie attack can occur when the cookie is stolen and the attacker using the information stored on the cookie to impersonate the user or steal other pertinent information.

Application Attacks: Client Side (cont'd)

- Cookie poisoning: as the name implies this is a form of attack whereby an attacker aims to access a cookie with the aim of stealing information or impersonating the user. There are different forms of cookie poisoning:
- Session hijacking – this happens when the attacker accesses a session cookie and uses it to manipulate the information; the attacker may use either eavesdropping or outright theft to access the session cookie. They can then use the session cookie to access the server or even impersonate the user.
- Session fixation – difference between this and session hijacking is that the attack commences before the bona fide user logs in; the attacker aims to steal the session ID before the user starts using it.
- Buffer overflow – this attack happens when the attacker can access memory through buffer overruns and access cookies.
- Malicious add-ons – add-ons are small programs that give browsers some additional functionality. An attacker hides code in a malicious add-on which the user downloads and they get access to user information through the browser.

Application Attacks: Client & Server Sides

- There are also application attacks that may occur on either or both client and server sides; some of these attacks are worth mentioning:
  - Viruses
  - Trojans
  - Worms
  - Phishing
  - Spoofing
  - Social engineering

Part 2

Network Attack Mechanisms

Network Attacks

- Network attack mechanisms are the means by which an attacker attacks the network (information channel in fig 1).
- The purpose of the attack is to get the information as it traverses between the client and the server.
- The attacker purposes to use this information for malicious purpose, that is, to violate the CIA of the information.

Network Attacks (cont'd)

- Denial –of- Service (DoS) Attack: This is a form of attack that targets the (A)vailability of a service.
- The idea behind DoS attacks is to cripple the resource that provides the targeted service.
- DoS attacks take many forms but the overall target is to cripple a resource(s).
- In the network resources that are targeted are the bandwidth/throughput of the network or the servers (web server or application servers)

Network Attacks (cont'd)

- Types of DoS attacks include:
- Source address spoofing – with this form of attack, the attacker modifies the source address of the packet (we're at layer 3 of the OSI model). The purpose of this is to fool the server that the packets are from a legitimate source; thus the server (and router) gets flooded with requests from what appears to be legitimate sources but which are not.
- SYN spoofing - Recall the 3 way TCP handshake between a client and a server requesting to communication? The client initiates the communication using a request via a SYN packet; the server receives it and reads all information on it (details about port, address, and so on) and saves this in a table; it then responds with an ACK packet, and the client sends the ACK packet back, and the communication is established. The SYN spoofing attack uses source address spoofing to overload the server with SYN requests from random and often non existent sources. The server will attempt to service all these requests as the table gets overloaded, eventually not being able to service legitimate requests.

Network Attacks (cont'd)

Types of DoS (flooding) attacks include: note that flooding attacks target protocols used in the network channel.

- ICMP flood – this is also known as a ping attack. It is a form of DDoS attack where the attacker floods the targeted server with ICMP echo requests (pings). The server then responds, filling the network channel with responses (and more requests from the DDoS), eventually resulting in no network bandwidth being available for legitimate requests.
- UDP flood – the principle behind this is the same as the one for an ICMP attack; the only difference in this instance is that the targeted resource on the server is a UDP port identified by its number.
- TCP SYN flood – the quest is to flood the targeted system with TCP packets rather than the table in SYN flooding; this is what makes the difference between the two flooding types.

Network Attacks (cont'd)

- Distributed Denial –of – Service (DDoS) attack: a DDoS attack occurs when multiple systems attack a targeted system, unlike in a DoS attack where one system attacks the targeted system. In a DDoS the multiple systems may be made up of zombies who make up a botnet.
- SIP bandwidth flood attack – this is an application layer (layer 7) attack targeting the session initiation protocol used in VoIP. It floods the proxy server with requests (even from spoofed addresses) thus causing the proxy not to be able to keep up (due to resource intensiveness) and denying legitimate users (requests) in the network.
- HTTP flood attacks – these flood the server with http requests. A variant of this is Slowloris which floods the server threads that handle http requests.
- Reflector amplifier attacks – this attack relies on the principle of flooding a targeted system using a form of DDoS attack. In a reflector attack, the attacker sends a request to a known system (apart from the targeted one) using a spoofed source address (of the target system). The known system then replies and the reply goes to the targeted system. This makes it hard to trace the attacker and the known system is then known as a reflector (it unwittingly reflected an attack). An amplifier attack is similar to a reflector attack but generates high volume of packets in responses from the known system. Consequently, a reflector amplifier attack involves amplification and hiding the source of the attack (reflection).

Network Attacks (cont'd)

- ARP Poisoning attack – recall the role of ARP in networking; it is the protocol responsible for mapping the IP address to the MAC address of devices. This attack targets the ARP cache by an attacker modifying MAC addresses so that they point to different IP addresses. This is a form of man-in-the- middle attack. This attack may also cause a DoS attack or the attacker may actually substitute MAC address with their own (theft).
- DNS Poisoning attack – this is similar to an ARP poisoning attack; the only difference is that in this instance the IP address is directed to a different domain (device) from the one it is supposed to be mapped to, or vice versa. A domain name is given a false IP address.

Part 3

Protecting the Network

Protecting the Network: Firewalls

- Having considered all the exploits and vulnerabilities of the network it is necessary to determine the ways in which the network can be protected from all these threats.
- One of the most common protection mechanisms is a firewall.
- Firewalls come in different forms but the principle in construction, design and implementation is the same for all firewalls: keep what is bad on the outside and keep what is safe on the inside.
- This principle can be demonstrated by a simple diagram (Fig 2)

Firewalls (cont'd)

- Fig 2 shows the simple design principle behind all firewalls.

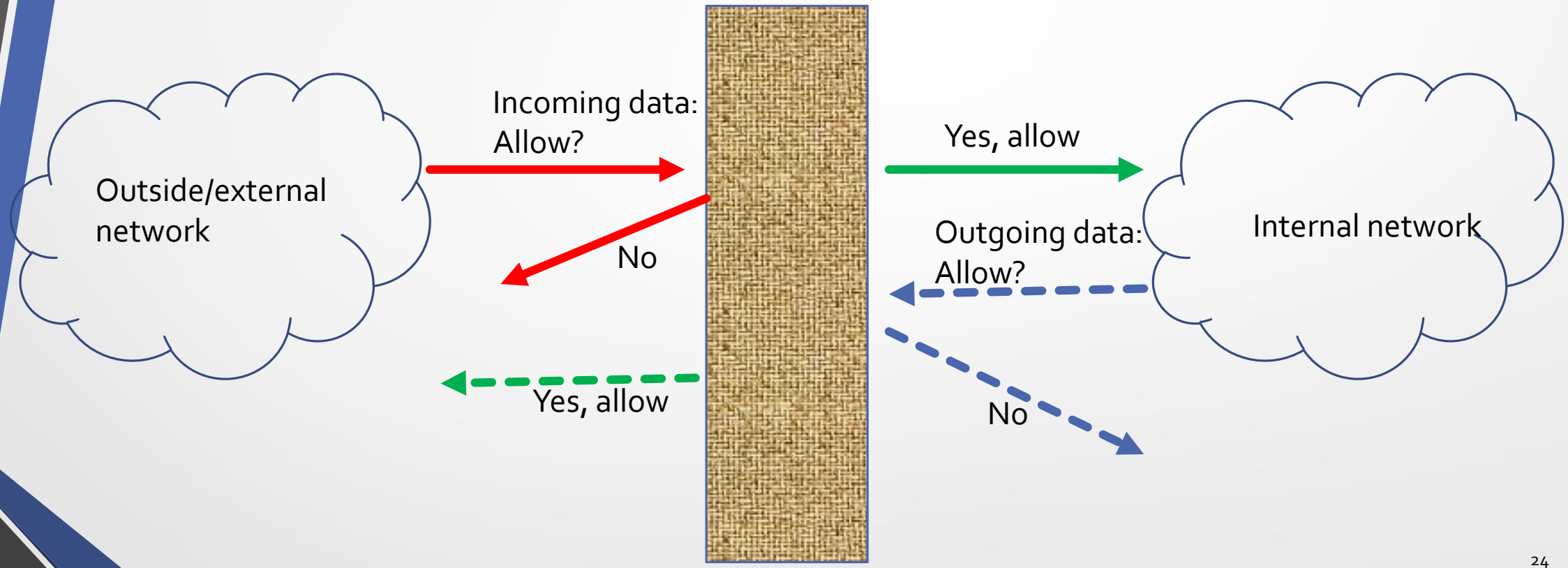

Fig 2. Firewall Principle

Firewalls (cont'd)

- Fig 2 shows the simple working of a firewall. The firewall uses some rules to assess the traffic that is coming to the network from the outside (Internet); based on these rules it will either allow the traffic to pass through or reject it.
- The same applies to traffic leaving the internal network; the firewall will apply rules to determine whether to allow the traffic to proceed outward or reject (disallow) it.
- Clearly the devil in the details is the rules and where exactly to place the firewall.

Firewalls (cont'd)

- Firewalls maybe simple packet filters or complex ones (IPS). IPS details are covered in a separate lesson.
- Packet filters work by applying a set of rules in order to allow a packet into the network. More importantly each packet is assessed independently.
- There is no ambiguity in the rules; if a packet does not satisfy the rules it is rejected (dropped).
- Cisco are the frontrunners in the design of packet filters. Their filters are based on Access Control Lists (ACLs).
- There are 2 types of ACLs; a standard ACL which examines source IP addresses only, and an extended ACL. Extended ACLs are more detailed examining even the destination IP address as well as TCP and UDP details of the packet.
- The rules of packet filters are applied in order starting from the top; thus a lot of thought must be placed in design of the rules.
- If they are not placed in proper order, then undesirable packets might pass through, or packets that were meant to pass through will not, and will be discarded.

Firewalls (cont'd)

- Packet filters do have their shortcomings. A determined hacker might still be able to find loopholes and exploit them.
- A possible solution to this is the use of proxy firewalls. These firewalls work at layer 7 in addition to layer 3 and 4 of the packet filters; further proxy firewalls have their own IP addresses so they send packets using their own IP address. They add extra protection to the network by working as a gateway between the internal and external network. It works by protecting traffic to and from the Internet. The traditional packet filter only protects from the outside.
- However, proxy firewalls have performance bottleneck among other issues, and it is desirable to have an alternative setup.
- The alternative is to have an architectural setup that is in more common use today; enter the demilitarized zone (DMZ).

Firewalls (cont'd)

- Fig 3 illustrates a simple DMZ setup.

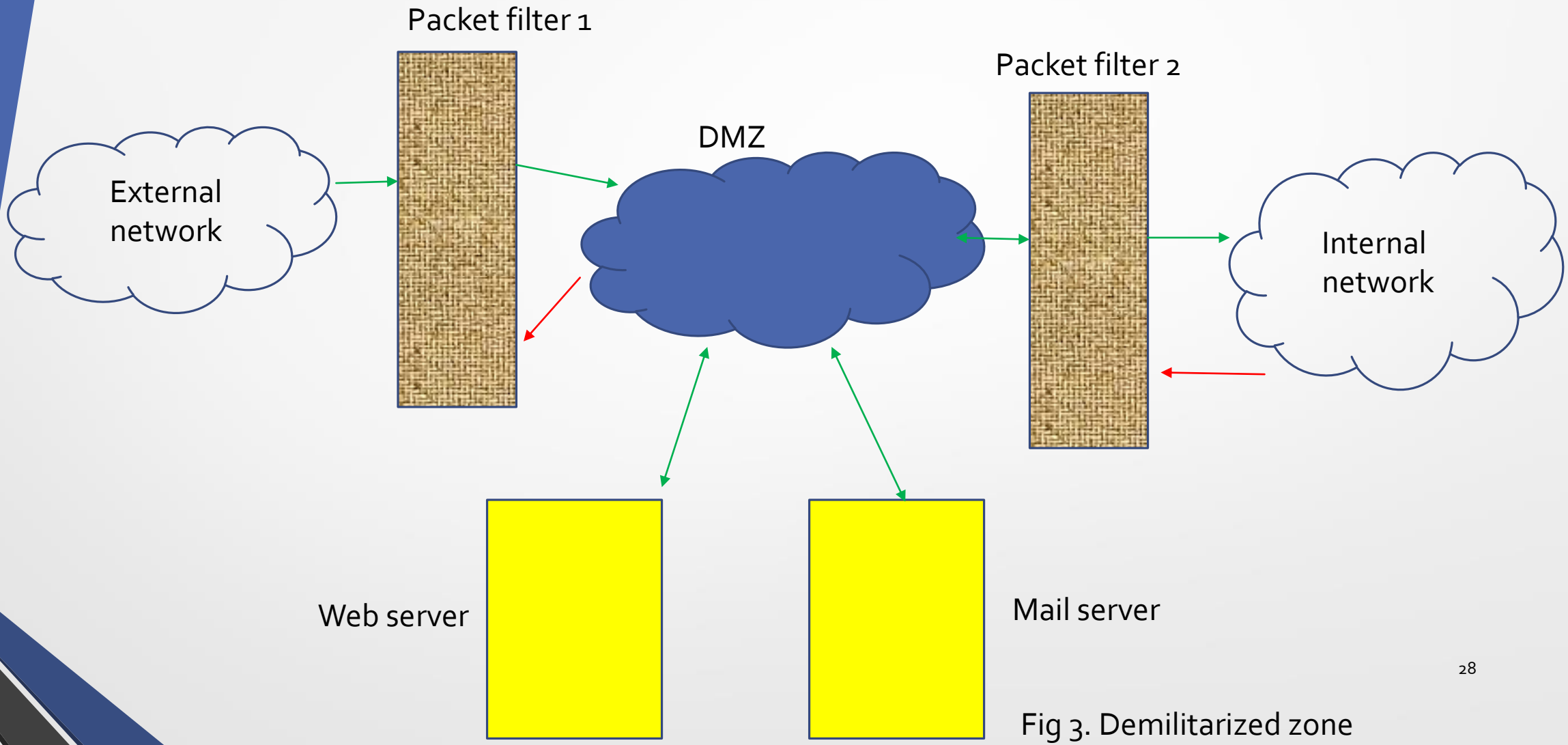

Fig 3. Demilitarized zone

Firewalls (cont'd)

- Fig 3 illustrates a typical DMZ. A DMZ can be viewed as a 'neutral' zone in the network.
- Packet filter 1 monitors all incoming traffic from the external network. If the packet passes the tests in the ACL then they are forwarded to either the mail or web server.
- Packet filter 2 monitors all packets coming from the 2 servers before they enter the internal network. The DMZ is the place where almost anyone can access; and this is where the servers are placed.
- The packet filters on either side of the DMZ serve a dual purpose of protecting the internal network as well as ensuring the external network is not aware of the existence of the internal network.
- The packet filters also monitor traffic leaving the network vide their external interfaces.

Protecting the Network: Others

- Cryptography – another way of protecting the network is through cryptography. Cryptography simply refers to the different ways in which data can be transformed so that it is only accessed and read by those who are supposed to. There are various ways of implementing cryptography and these are briefly mentioned as they will be discussed in detail in a later lesson.
- Encryption – this refers to the different ways in which data can be transformed using cryptographic algorithms. There are broadly two forms of encryption:
  - Symmetric encryption makes use of one key to encrypt (transform) the data from plaintext (unencrypted) to cipher text (encrypted).
  - Asymmetric encryption makes use of more than one key in the encryption process.

Protecting the Network: Others

- Kerberos – this is an authentication protocol that uses tickets to authenticate users and thus grant them levels of access in the network.
- IPsec (IP Security) – this protocol encrypts IP traffic between hosts and/or networks.
- SSL (Secure Sockets Layer) – this is used mostly by web browsers to secure transactions; in today's e-commerce age it is in wider use.

Part 4

Network Attack Detection

Network Attack Detection: IDS

- Even the most rigorous security system will not deter the experienced and determined attacker. It is therefore acceptable that some attacks may be successful.
- Intrusion Detection Systems (IDS) are systems that are used to monitor and detect when an attack occurs; this is to ensure that it can be contained in good time before maximum damage occurs.
- There are many types of IDS but all of them are based on 3 underlying principles.

Network Attack Detection: IDS

- Host based IDS – these are IDS that are placed in a host on the network. The IDS monitors activities on the host through tools such as logs, audit trails, system tools, and so on. By monitoring these activities they are able to detect whether an attack has occurred or in some instances whether it is still ongoing.
- Network based IDS – these monitor events on the network and hosts to detect any suspicious activities that may be taking place. They do this by examining individual packets on the network for any malicious content.
- Anomaly based IDS – these establish a pattern of normal system activity and then monitor for any deviation from the established pattern. Activities include system resource and network usage.
- All IDS have their advantages and drawbacks. Further, classification in different literature may include further sub classification of the above classifications. One of the common drawbacks associated with IDS are false positives and false negatives; thus the design of IDS requires a balance between too much generalization vs too much specifity.
- IDS will be discussed in detail in a later lesson.

Part 5

Assessing and Responding

Assessment

- Assessment of the network is done :
  - to identify any vulnerabilities existing in the network
  - Check whether all security defense mechanisms in place are working as expected.
- The assessment is done through two main activities:
  - Penetration testing – an attempt to hack into the system thereby exposing vulnerabilities
  - Vulnerability assessment – an attempt to identify vulnerabilities in the system with a view to correcting them.

Response

- Responding to an attack is also equally important. One of the most important issues here is documentation and mitigating damage that may have been caused by the attack. The organization may:
  - Alert the authority (network manager/administrator) of the attack
  - Get help (if external help is required)
  - Examine the damage and mitigate as much as possible
  - Assess why the attack was successful in the first place
  - Identify and remove the vulnerability
  - Document all the events that occurred and if necessary develop a policy that can help prevent the attack from occurring in future.

Part 6

Incident Handling

IETF RFC 2196

- The Internet Engineering Task Force (IETF) in RFC 2196 recommends the following steps to be followed in handling incidents:
  - Preparing and planning – establish goals in handling the incident
  - Notification – who to be contacted in case of an incident
  - Incident identification – severity of the incident
  - Handling – what should be done when it happens?
  - Therafters – what was the outcome/implication of past similar incidents?
  - Administrative response – to the incident

Summary

- Application attacks may occur on the server side (cross scripting, SQL/command injection, directory traversal attacks, access rights attacks, privilege attacks) or on the client side (drive-by download, header manipulation, cookies, session hijacking, session fixation, buffer overflow, malicious add-ons)
- Types of network attacks include DoS, DDoS, SIP bandwidth flood, http flood, reflector amplifier, ARP poisoning, DNS poisoning and DoS flood.
- Networks are protected using firewalls (packet filters, proxy firewalls or DMZs), cryptography, IPsec, SSL and Kerberos.
- Attack detection is achieved by the use of IDS; these are based on 3 classifications – host based, network based and anomaly detection based.
- Assessment is done through penetration testing and vulnerability assessment.
- RFC 2196 recommends steps to be followed in handling of security related incidents.

References

- Cole, E., Kurtz, R. L., & Conley, J. W. (2005). *Network security bible*. Wiley Pub.
- James, J., & McCabe, J. D. (2008). *Network security: Know it all*. Morgan Kaufmann/Elsevier.
- Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice* (5th ed.). Pearson.
- Cisco. (2017, May 7). *Access list commands*. Cisco. Retrieved October 4, 2021, from https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-0/addr_serv/command/reference/ir40asrbook_chapter1.html#:~:text=An%20access%20control%20list%20(ACL,queueing%2C%20and%20dynamic%20access%20control.
- https://datatracker.ietf.org/doc/html/rfc2196