CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2020-10-09, 14:00 – 18:00

No extra time for scanning at the end

All questions must be clearly explained with your own words. Answers are automatically sent to Urkund before they are corrected and Urkund assigns a similarity index (in percent) with respect to other exams and known documents. Copied answers will not count. Shorter answers will likely look similar, but longer explanations need to be your own!

Write in a clear manner and motivate (explain, justify) your answers. If it is not clear what is written, it will be counted in the least favorable way and if an answer is not explained/justified, it will get significantly lower or even zero marking. If you make any assumptions in your answer, do not forget to clearly state what you assume. With good motivations, other answers than what was expected could be considered correct!

A good rule-of-thumb for how much detail to provide, is to include enough information so that a person who has not taken this course can understand the answer.

Questions must be answered in English.

Teacher: Tomas Olovsson, 031 – 772 1688
Dept. of Computer Science and Engineering

CTH Grades:	30-39 → 3	40-49 → 4	50-60 → 5
GU Grades:	30-49 → G		50-60 → VG

1. Attacks and DoS

a) If you want to investigate if a firewall is stateful or stateless and you can chose between SYN, ACK, FIN, SYN/ACK and a SYN/FIN scans. Which of these scan(s) would work? Explain for each scan why it works or does not work! (4p)

SYN is accepted for open ports but does not reveal whether the firewall is stateful or not.
ACK, FIN, SYN/ACK scans will work through stateless firewalls – the firewall does not know whether it is part of an ongoing connection or not.
SYN/FIN is invalid and should be dropped by all firewalls.

b) The maximum size of an IP datagram is 65,535 bytes since the length field in the header is 16-bit long (max length = 0xffff = 65535). It is still possible to send longer datagrams to confuse receivers. How? (2p)

Packet fragmentation can be used. By creating a fragment with an offset of for example 65,000 and a length of 1000 bytes, the total length would be 66,000 bytes.

c) Why could these oversized datagrams be a problem to receivers? (2p)

The standards does not allow creation of such oversized datagrams, and there is a risk that the receiver does not check the length and that its buffer space is overwritten (a buffer overflow attack).

d) TCP has a window field in the header which tells the sender how much data it can send until the receiver's buffer is full. How can this field be abused by an attacker? (2p)

The attacker opens lots of connections to a server (e.g. a web server) and sets its receiver window to 0. This keeps the connection alive but the server can never send any data to the client, thus occupies resources and may fill internal buffers affecting legitimate users.

2. DoS and Authentication

a) Give an example of a DDoS attack that is hard to trace and stop! Motivate your solution! (Several answers may exist to this question.) (2p)

See for example the slide "DDoS Attacks through Handlers and Zombies".

b) TCP numbers all segments to make sure the receiver knows where each segment fits in the data stream. The numbering normally starts on a random value. Why? (2p)

To prevent blind TCP hijacking attacks, i.e. to make it harder for an attacker who cannot see the TCP sequence numbers to guess what numbers will be accepted by the receiver.

c) Some systems and servers select the first sequence number in the following way:

hash *(source and dest IP addr, source and dest port #, secret, client's selected number)*

What is the reason they select the starting number this way? Explain (1) what problem it solves, (2) why it works and (3) potential drawbacks with this method! (4p)

Each SYN makes the receiving host allocate some internal resources (keep state) and return a SYN/ACK message. Internal resources (e.g. memory or data structures) may at some point be exhausted.

This method is used by Linux and called SYN cookies: The server does not save any data when a SYN is received. Instead all state information is contained in the ISN which means that it does not have to allocate any resources until it receives the ACK. Then the ISN is checked with what the client sends back.

Reason it works: The attacker must be using a valid IP address to receive the SYN/ACK with the ISN to be able to respond with a valid ACK. Only if the ACK is valid, resources are allocated. (If one or a few addresses still flood the server, a firewall could easily filter or block this IP address, manually or automatically.)

Drawbacks: problems to remember if TCP options (such as window size) that were negotiated in the SYN and SYN/ACK packets since they are not saved by the server. Another drawback may be that the computation of the hash may take some time, a fact that may be utilized by the attacker.

d) Radius and LDAP may look rather similar at a first glance. Explain briefly the fundamental difference for an application or a system who wants to authenticate a user! (2p)

LDAP is a protocol used to access directory listings (user accounts). It is a way to retrieve information about a user and is not in itself an authentication protocol. The user password may be stored (encrypted) in the database, but the end-system (client) needs to perform the authentication, i.e. to check the password, not the LDAP server.

Radius is a protocol which allows applications and devices to connect to an authentication server and ask it to authenticate a user. The Radius server may either have its own database or use LDAP to retrieve records about the users it authenticates.

3. Encryption and WLAN

a) In the course, we have seen a method where two parties can agree on a session crypto key over a network even if there are other parties listening to the conversation. How is this possible? Explain on a high level, maybe with a short (text) example. (2p)

Using the Diffie-Hellman (D-H) algorithm. See lecture slides for examples.

b) This method is vulnerable to a specific type of attack. Which? Explain! (2p)

Man in the middle attack. Alice believes she talks to Bob but Eve intercepts the messages and exchanges numbers with her until they agree on a secret. Then she does the same with Bob. D-H has no authentication.

c) A basic encryption problem is that encrypting two identical packets with the same key results in identical cryptotexts. How is this problem solved in WEP? Explain! (2p)

Another number, an IV is used together with the key to encrypt the packet. The IV is then sent in clear to the other side so it can use the same IV when it decrypts the packet (the key is not transmitted, both sides keep it secret).

d) The way WEP implemented this solution (in question c) was problematic. Why? (2p)

The IV space was too short and would eventually be exhausted. A too short IV means that used numbers have to be reused. If so, two ciphertexts will be encrypted with the same keystream, and XORing them together will remove the keystream and result in two plaintext XORed with each other.

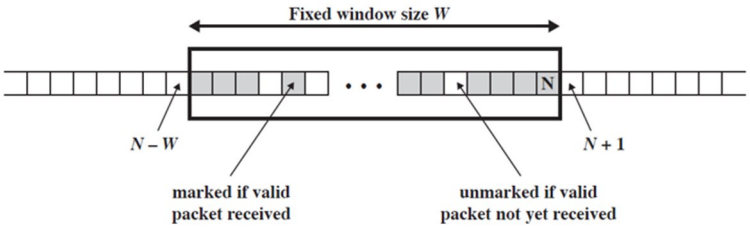
e) WPA2 is much better than WEP and contains many improved functions. However, it is still important to choose a network name that is not that common, for example at home. Why? (2p)

The key used to encrypt packets is HASH(SSID, password) which means that if the SSID, the network name, is commonly used, it is likely that a rainbow table exist which can be downloaded making it relatively easy to look up a user's password.

4. IPsec, SSL/TLS, SSH

a) IPsec has a window similar to TCP. Explain how it works and what problem(s) it addresses! (2p)

It protects against replay attacks by discarding duplicates, but unlike TCP, it allows packets to be missing.



b) When IPsec is used in tunnel mode, it adds a new IP header. This header is not protected by the HMAC which means it can be modified by anyone. Is this a problem? Explain! (2p)

If an attacker modifies this header, the result is just that another system receives a useless encrypted datagram.

c) Some security protocols may be sensitive to network address translation done by a firewall. Explain why (or why not) the following protocols care about this:
IPsec, SSL/TLS and SSH? (2p)

IPsec cannot be used together with NAT. NAT modifies the IP address and the port number being used, but there is no visible port number in IPsec packets. (NAT-T solves the problem where IPsec packets are tunneled in UDP.)
SSL/TLS and SSH don't care about the IP address being used nor the port number, they work above both IP and TCP.

d) What is Perfect Forward Secrecy? How can it be achieved? Does TLS support it? (2p)

It is a way to guarantee that if the main key (e.g. an asymmetric key belonging to a certificate) is compromised, it should not be possible to decrypt other sessions. The session keys should be independent of this key.

TLS supports it: Diffie-Hellman or Elliptic Curve key exchange guarantees unique keys for each session.

e) A common function in many secure protocols is to include padding of variable size. Why? (2p)

Used to hide size of payload. All packets may for example have the same size when encrypted.

5. Firewalls and IDS systems

a) Can or should a firewall to a corporate network filter out (drop) all incoming ICMP messages? Motivate your answer! (2p)

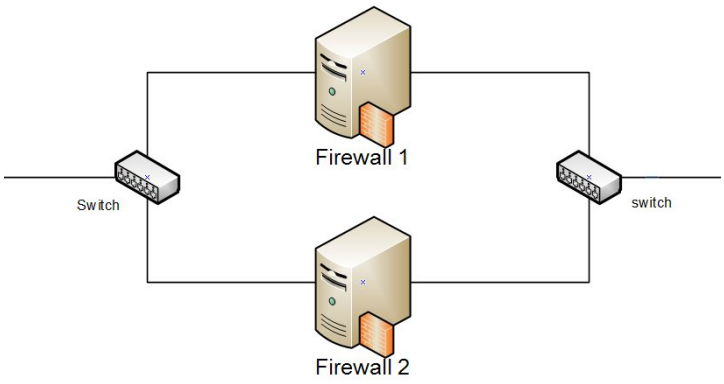
Not if the company is not extremely paranoid. It results in performance problems. Internal users will not immediately be notified if external servers are down, it is impossible to Ping other systems, TCP will have problems to figure out MSS – maximum segment size the network supports, etc.

b) Explain why overlapping TCP segments can be problematic for a firewall or an IDS system! Give two examples of potential problems! (2p)

It is not well-defined how overlapping TCP segments should be handled. When segments overlap, e.g. in the beginning or in the end with other segments, different systems have different reassembly policies and an IDS system may not understand how the target system will act.

c) Give an example of a situation (a use case) when you would use the following firewall types together with a short(!) motivation:
(1) deep packet inspection firewall
(2) NAT gateway
(3) application level proxy
(4) air-gap firewall (4p)

d) Assume you would like to increase availability to a network by placing two standard firewalls (like the ones we have used in the course) in parallel like in the picture below. The idea is that there will always be at least one firewall that will be up and running even if the other would crash or have hardware problems. Would it work? If not, how can it be made to work? (2p)



It will not work. It means that both receive the same incoming packets and send them out, i.e. we get twice as many packets on the other side. TCP may survive but not many other protocols and performance will be hit.

The solution can be to have functionality that makes sure that one firewall is the one forwarding the packets and the other is passive. When the passive sees that the other does not forward packets, it becomes the active firewall instead.

6. Link level and mixed questions

a) Explain how ARP *requests* can be a way to become a man in the middle. How can that be prevented/mitigated? (2p)

ARP spoofing is a way to send (or respond) to ARP queries using the wrong IP-address/MAC address information. Other systems will learn the information they see, so if one system fakes the IP address using its own MAC address – even in a request – other systems will learn and cache this information.

This way it is possible to spawn man in the middle attacks. Possible protection can be to set important IP-address to MAC address translations as static (use static ARP entries) or to have a system (IDS system) that monitors IP-address and MAC address usage and blocks systems that behave incorrect.

b) Give a good example (*a scenario*) at Chalmers when you would use VLAN technology. Motivate clearly *what problem it solves* for you, *how it works*, and why it is a better alternative than encrypting traffic! (4p)

Many solutions possible – the motivation is important.

c) Give an example of when authentication on link-level is used! What technology (or standard) is normally used to implement it? Explain briefly how it works! (2p)

802.1x – port based authentication: Before a user or a device is given network access through a switch or an access point, authentication needs to take place.

d) 10-15 years ago, it was enough to secure a company by placing a firewall between the corporate network and the Internet. This has changed and is not really the case today and many consider such a firewall to be outdated since it cannot offer full protection. Why not? What has changed? Explain! (2p)

Services are located both on internal networks and on external (cloud) servers, and users are located both on the inside and on the outside. It is therefore impossible to control security with only a border firewall that only sees a small part of all traffic. Since cloud services increase in popularity, data is now also moving outside of the corporate network. The solution is to move protection closer to the end-points: toward the users/client systems and to application servers.