CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2023-08-24, 14:00 – 18:00

***No extra material* is allowed** during the exam except for an English language dictionary in paper form.

The last page of this exam contains pictures of some protocols and headers that *may* be useful in some questions.

Write in a clear manner and motivate (explain, justify) your answers. If an answer is not explained/justified, it will get significantly lower or zero marking. If you make any assumptions in your answer, do not forget to clearly state what you assume.

A good rule-of-thumb for how much detail to provide, is to include enough information and explain 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:	30-38 → 3	39-47 → 4	48-60 → 5
GU Grades:	30-47 → G		48-60 → VG

1. Attacks and DoS (10p)

a) The length field of IP is 16 bits long which means that a datagram can have any length between 0 and 65,535 bytes. It is still possible to send larger IP datagrams, for example a datagram which is 75,000 bytes long. How? (2p)

A naïve implementation would assume IP datagrams never exceed 65,535 bytes since the length field is 16 bits long.
An oversized IP datagram can be created that exceeds this size by sending a fragment with an offset and a length extending the datagram beyond this limit, for example by setting offset to 65,000 and length to 1,000 bytes.

b) An attacker may try to flood a server with SYN packets using faked IP addresses. What is the purpose of this attack? Why use multiple faked IP addresses? Also mention two possible remedies to this attack! (4p)

Purpose: 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.
Faked IP addresses: (to hide own address and) when using multiple addresses, it is hard for the receiver to know what addresses are faked or part of a DoS.

Protection mechanisms (two needed):

- Variable time-out: decrease waiting time when needed.
- Allocate micro-records and do most of the work when connection completed
- Round robin, drop connections when needed.
- SYN-cookies where the server does not have to keep state.
- …

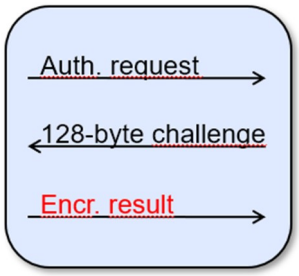
c) Assume you have been given the task by a friend to test the security of a networked IoT device. Give a high-level description of *how such a security analysis should be done* and what general tests should be performed. Assume that you know nothing about the device and its protection system and existence of a possible firewall in advance. All you know is its IP address. (4p)

A penetration test of an unknown system can be done, for example, by:

- Do a port scan to identify possible services available
- Try to detect the operating system being used (OS fingerprinting)
- Try to see if there is a (stateless?) firewall protecting the system
- Listen to traffic and see what services exist and to what level they are protected. MITM attacks may work?
- Test with well-known attacks against different network layers
- Test the stability of the system with some DoS attacks

2. Authentication and WLAN (10p)

a) WEP uses challenge response authentication, and the first message in WEP is the 128-byte random challenge that authenticates the client:



Why is this mechanism flawed? Two reasons! (3p)

It uses the same method (engine) for encryption as is used later for packet encryption. An attacker listening to the authentication procedure can see both the challenge and the encrypted challenge. By XORing them with each other, the 128 byte key stream is obtained which can be used to transmit own messages through the AP.

It also makes it possible to guess the user password off-line, for example using rainbow tables.

[Other answers: RC4 is flawed, no mutual authentication, …]

b) Both WEP and WPA2 use IVs when encrypting data packets. Why? What would happen if there were no IVs present in the packets? (2p)

It guarantees that different key streams are created for each packet. Without IV:s, the same key stream would always be used. If no IV was present, identical datagrams would have the same crypto text.

Also, XORing two messages having the same IV (or no IV) with each other would result in two plaintext messages XORed with each other.

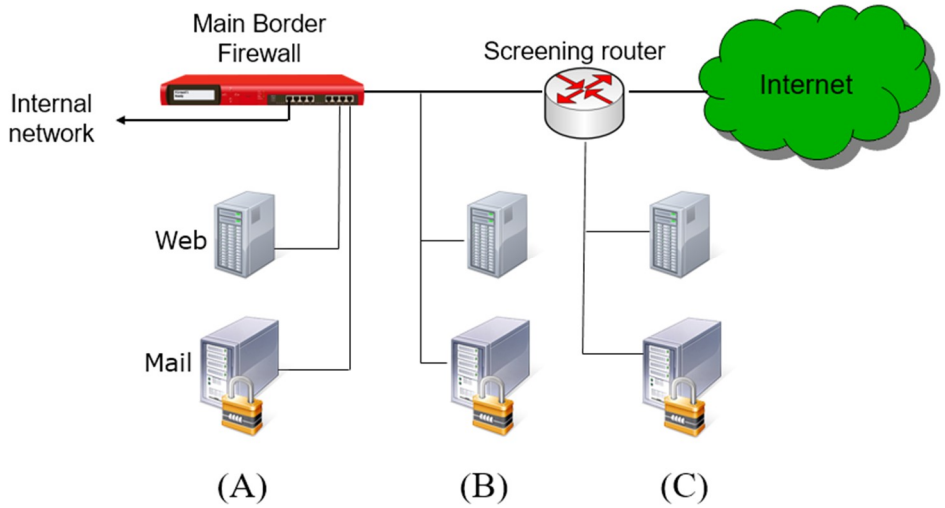
c) WPA2 derives a pairwise master key (PMK), a pairwise transient key (PTK) and a group transient key (GTK). What are these three keys used for? (3p)

The PMK is the master secret used to create all other keys.
The PTK is a session key between a station and the AP.
The GTK is a key shared between all stations and used for broadcast messages that should reach all stations.

d) When are GTK keys changed? (2p)

Each time a station leaves/disconnects, a new key is generated. Some systems also change this key at a regular time interval.

3. Firewalls and IDS systems (11p)



a) Compare the three suggested locations for an external web and mail server and explain their advantages and disadvantages! (3p)

(A) is the most secure placement. The firewall can have very detailed rules about communication with the web and mail servers (ingress and egress) and can isolate them completely from each other.
(B) is the least secure solution. A cracked server (mail or Web) makes it possible for an attacker to listen to all traffic in and out from the corporate network.
(C) is better than (B) but a cracked Web server allows the attacker to listen to all email traffic since they share the network. Link-level attacks also work between these two servers. The router can have filter rules and can protect the servers from some attacks from the outside.

b) What is the purpose of a screening router? Why not just use a good deep packet inspection firewall to take care of all traffic? (2p)

To offload the main firewall from obvious garbage traffic. It is a *cheaper alternative* and can offload the main firewall from more trivial work.

c) Why can network address translation (NAT) be used to enhance security in a network? Mention one positive and one negative thing with implementing NAT! (2p)

They hide and isolate internal systems from the outside network. A service not present in its translation table is not visible/accessible from the outside. Also, since many internal addresses will be translated to one (or a few) external addresses, it is not possible to figure out the size of the internal network by counting IP addresses.

One downside is that it does not inspect traffic that is allowed to traverse (as done in a conventional firewall). Another that some protocols, for example those that expect to see the real IP address of the internal system in the packets, will not work.

d) IP datagrams with overlapping fragments can be problematic, for example for IDS systems and firewalls. Why? Describe one problem by giving an example! (2p)

If datagram 1 = AAAAAA and datagram 2 = BBBBBB and they overlap by 50%, a firewall or IDS system does not know how the receiving system reassembles the datagram. It may become AAABBBBBB or AAAAAABBB.

e) An active IDS system (IPS) may have a rule that blocks an IP address when it detects that someone is doing a port scan. This may lead to other problems. Explain! (2p)

An attacker can fake the IP address in the port scan and thereby cause another user to be locked out.

4. TLS and Cryptographic protocols (8p)

These questions only require "True" or "False" as an answer, no motivation is needed. If in doubt, you may write a small motivation about how you reason, but it is not needed!
+1p per correct answer, -1p for an incorrect answer, so don't guess!

a) A pseudo-random function (PRF) is used in TLS to generate a master secret from a pre-master secret and to generate session keys from the master secret.

True – it is a function used to generate key material from an initial value (e.g. a master secret)

b) The TLS Record layer protocol uses implicit sequence numbers, which means that the sequence numbers are not present in the packets transmitted. These numbers are needed since it cannot rely on TCP to deliver packets in order and without duplicates.

True

c) The heartbeat protocol is an optional protocol that periodically sends messages to the server. Its purpose can be to inform firewalls that the communication is active.

True

d) Heartbleed is a denial-of-service attack against the server which works by compromising its stack.

False – Heartbleed send a packet which is smaller than its length field and hope to receive old contents from the buffer

e) TLS is sensitive to NAT, network address translation

False

f) In TLS 1.3 compression was deleted due to security problems

True

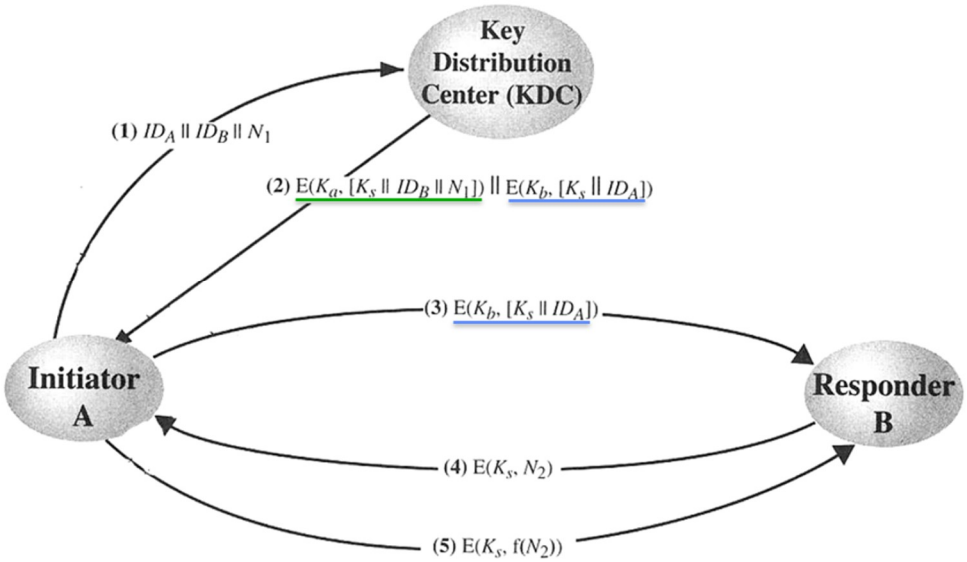
g) In TLS 1.3 the client guesses what ciphers and algorithms to use to save number of round-trip delays

True

h) Diffie-Hellman enables two parties that have never met to authenticate each other and to securely negotiate a secret such as a session crypto key.

False - they can negotiate a secret, but they don't know who the other party is

5. Kerberos (11p)



The picture shows a possible authentication method using a key distribution center (KDC). In the picture, encrypting something with *Key a* is written $E(K_a, \ldots)$.

a) In the second message, A gets two things back, the first which is highlighted in green, and a second highlighted in blue. Explain the contents and purpose of the blue message! (2p)

It contains the session key to be used when B talks to A. It is encrypted with a key K_b which only B and the KDC know thus B knows that the KDC has approved the communication. (A cannot decrypt it but it will be forwarded to B in message 3.)

b) In the fifth message, explain the purpose of the function "f" and give an example of what could it be! (2p)

To guarantee freshness: A proves that she is alive and can decrypt N_2 with the session key by sending a (by B known) reply which could be $N_2 + 1$.

c) The real Kerberos protocol adds time stamps to the messages. There are at least two reasons for this. Please explain! (2p)

To guarantee freshness and to make sure that keys expire and are not valid forever.

In Kerberos, the first two messages look like this:

Authentication Service Exchange: To obtain Ticket-Granting Ticket

(1) A → AS: $ID_a \| ID_{tgs} \| TS_1$

(2) AS → A: $E_{K_a}[K_{a,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| TGT_{tgs}]$

TGT_{tgs}: $E_{K_{tgs}}[K_{a,tgs} \| ID_a \| AD_a \| ID_{tgs} \| TS_2 \| Lifetime_2]$

d) What is the purpose of the TGT_{tgs} ? Why is it sent to the client? Also explain its contents! (3p)

TGT is a ticket granting ticket and is encrypted with a key only known by the Kerberos server and shows that the client is authenticated. It is the state information it needs to know that A is authenticated, but instead of keeping it, it lets all clients keep these tickets which makes it stateless.

It contains the session key for A and the TGS, their identities, A's address, a tipmestamp (TS) and the lifetime of this ticket.

e) Does Kerberos support Perfect Forward Secrecy, PFS? Explain what PFS is and your reasoning! (2p)

PFS means that if one session key is broken, no older or future sessions should be compromised. Since the KDC generates session keys, we have to assume that all keys are randomly generated and do not depend on a common secret.

6. Link level security and VPN technology (10p)

a) On a local network, it may be possible for an attacker to pretend having lots of MAC addresses and to send lots of messages using these to confuse more intelligent switches. Why? What could be the reason an attacker performs this action? (2p)

More intelligent switches can learn where hosts (MAC addresses) are located and will normally not forward private traffic between two ports to any other ports. The attacker's goal is to overflow the switch memory with garbage MAC addresses to make it forget the real MAC addresses and force it to broadcast all traffic to all ports which enables the attacker to listen to all ongoing conversations.

(This can be detected by some switches, for example by limiting number of MAC addresses per port and/or to lock some MAC addresses to certain ports.)

b) DHCP spoofing is a problem advanced switches can deal with. What is DHCP spoofing? How can it be dealt with by a switch? (2p)

An attacker may answer to DHCP requests in order to become a man in the middle. There is a function (often called "trusted ports function") telling the switch to only allow certain trusted ports to answer DHCP requests.

c) What is the main difference between using VLAN technology and IPsec to secure a network? Would you use VLAN to create a virtual course lab at Chalmers with lab computers at different locations in the EDIT building? Motivate your answer! (2p)

VLAN does not encrypt nor protect the messages against modification. But it may be a good solution if the purpose is to separate the course lab traffic from other types of traffic. VLAN can be used to make sure that traffic from the lab is not forwarded to office computers and servers but still be sharing the same physical network.

d) Firewalls may support encryption of network traffic, i.e.VPN functionality, to other sites. This makes it possible to connect multiple sites over the Internet securely. What protocol are firewalls likely using to implement this functionality? Why is this protocol more suitable than, for example, TLS? (2p)

IPsec. It encrypts IP traffic and is completely transparent to the transport and application layers. TLS is better to use when securing a TCP connection between a client and a server.

e) What is the reason lots of link layer devices such as access points (APs) support Radius? What advantage do they get from it? (2p)

To implement user authentication without having to keep its own database.

Headers and pictures that may be useful