

# Network Security – DIGITAL

EDA491 (Chalmers)  
DIT071 (GU)

2022-05-30, 08:30 – 12:30

***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.

*Automatically corrected questions in this exam will be manually inspected if the exam is close to a grading border.* It may be that one or two bonus points from them can be awarded if the overall exam motivates it.

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

Red text is added to show automatic scoring, these texts were not printed on the exam. Note that manual checks of the system will be done to compensate for systematic errors or unfair scores.

# 1. Attacks and DoS

- a) Give an example of a link-layer attack (2p)
- b) Give an example of a Network layer attack (but not the one in question d below) (2p)
- c) Give an example of a Transport layer attack (2p)

Clearly explain how they work, what makes the attacks possible and the possible/desired results of the attacks!

Several answers are possible, for example:

a) ARP spoofing. ARP is used to get a system's MAC address given its IP address and no security is present in the protocol. An attacker can easily listen to an ARP request and quickly send a reply to the requesting host before the real receiver responds. Normally the first reply will be used by hosts.

b) The LAND attack is performed by sending a host a packet to a target with its own IP address in both the source and destination fields. Some systems (in the past) used to crash when they tried to respond to themselves.

c) A possibility is to try to exhaust the connection table of a receiving host's TCP stack by never finishing the TCP three way handshake process. By sending a SYN packet only and never respond to the SYN-ACK, the receiver waits. By sending lots of such requests, possibly from spoofed addresses, a DOS attack is possible since the table is full and no one else can open new connections.

d) The TTL (time to live) field in an IP datagram can be useful when an attacker wants to create a network map. Explain how this can be done! (2p)

Each router in a path decreases TTL in the IP packet with one, and when it reaches zero, an ICMP message is sent back to the source telling it what router discarded the message. Therefore, an attacker sending a packet with increasing values of TTL (1, 2, 3, etc.) to a host will provide info about what routers exist in the path. This may also work when traffic passes a firewall. By sending traffic to different IP addresses, different paths and networks can be mapped.

e) Describe two possible ways to address this TTL problem in a border firewall! (2p)

Drop outgoing ICMP Time Exceeded messages. Normalize TTL values for incoming datagrams in the firewall (e.g. set TTL to 255).

f) TTL and some other fields in IP and TCP headers can also be used to reveal information about the type of system returning the packet. Mention two other such fields and explain how it may be used! (2p)

Systems have different default values for many header fields such as TTL, Window size, DF bit, SYN message size, window scaling, etc. This information can be used to tell what system has generated the datagrams.

## 2. WLAN

a) When authenticating a client in WEP, the access point (AP) sends a long random string as a challenge to the client. This means that a listener gets access to both the cleartext (challenge) and the ciphertext (encrypted challenge). It makes it possible for attacker to search for the password, but there is another problem associated with this as well. Explain what this security problem is and how it can be used by an attacker. (2p)

The attacker can see both the challenge and the ciphertext encrypted with the secret (password). This makes it possible to extract the keystream using an XOR operation:  $c1 = p1 \oplus stream$ , and since the same algorithm is used for data transmission, this 128-byte keystream can be used to transmit arbitrary data. Unfortunately WEP uses the same algorithm for authentication and packet encryption and IVs can be reused.

b) WEP uses a linear CRC function to check packet integrity. Why is this not sufficient? Explain! (2p)

With a CRC function, it is possible to calculate exactly what bits in the checksum need to be changed when a bit is changed in the input (a hash requires a complete recalculation). It does not matter whether the data or CRC is encrypted, a bit change is still possible to do.

An access point has several features as seen in the figure:



Explain briefly (one or two sentences) the following features and what they do:

c) WPA2-EAP (i.e. Radius) (2p)

Radius is a standard protocol for user authentication supporting AAA (authentication, authorization and accounting). Three parties are involved: the client, the application server and the Radius server. The Radius server offloads application servers to maintain lists of users and do user authentication.

d) TKIP

(2p)

TKIP makes sure encryption keys change over time. It extends the IV (with a new field EIV). It makes sure each station uses a unique key by involving the MAC address in key calculation. It also makes sure each packet has a unique sequence number and that the key is changed every 10,000 packets.

e) A feature present in WPA and WPA2 is 802.1x – port-based authentication. What is this? What does it do? How? (2p)

Port-based authentication is a link-level mechanism where a client does not get access to the network unless authenticated and authorized. It uses Radius for central authentication and authorization. When the Radius server accepts the user, full network access is given.

### 3. Link level security and network design

a) A self-learning switch learns where hosts are located and will normally not forward private traffic between two ports to any other ports. How can an attacker see this supposedly private traffic between two other communicating parties? What could an administrator do to decrease this problem? (2p)

May overflow switch memory and make it broadcast all packets to all ports. An attacker may spoof other hosts' MAC addresses to disturb the functionality of a self-learning switch and force it into a broadcast mode of all packets.

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? And 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. The trusted ports function is that the switch only allows these ports to answer DHCP requests.

c) A link-level problem is ARP cache poisoning (spoofing) where the attacker sends faked ARP messages to confuse other systems. Why would he/she do so? Give two possible solutions to this problem! (2p)

Goal can be to become a man in the middle. Solutions may be to create smaller subnets, accept only the first reply (Solaris), the "Antidote patch" (Linux), Secure ARP (S-ARP), ...

d) VLAN is a useful link-layer technology when building networks. There are two main ways it can be used in: with or without tags. What is VLAN and a tag? Explain the difference between with and without tags! (2p)

VLANs can be used to isolate/separate traffic on a LAN into virtual LANs. All packets sent out can have a tag identifying it (tagged VLAN) or be without tags if the network devices keep track of where packets are received (interface/port).

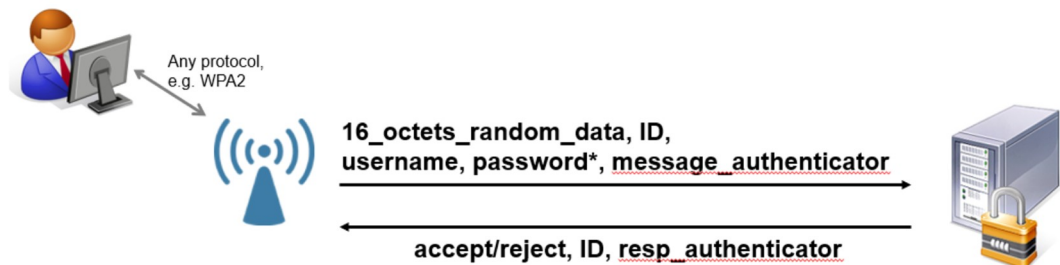
e) Is VLAN a good and secure technology? Mention one attack that it cannot protect against! (2p)

It is vulnerable against MITM attacks. If an attacker has access to a link and can insert or modify packets, it is also possible to modify tags and insert own messages. There is no integrity protection nor confidentiality in the protocol, but it is still useful knowing its limitations.

## 4. User Authentication

The picture below shows the initial dialog in Radius when an Authenticator wants the Radius server to authenticate a user.

Assume an attacker is able to both send and listen to the traffic between the Authenticator (access point) and the Radius server, and also talk to the Authenticator and ask to be authenticated. The attacker has no account and should not be allowed to log in.



$\text{password}^* = \text{MD5}(\text{shared\_secret}, 16\_octets\_random\_data) \oplus \text{password}$

$\text{message\_authenticator} = \text{MD5}(\text{packet\_contents}, \text{shared\_secret})$

$\text{resp\_authenticator} = \text{MD5}(\text{packet\_contents}, 16\_octets\_sent\_by\_client, \text{shared\_secret})$

What is true in this situation? (4p)

Note that 4p does not necessarily mean that four alternatives are correct, and that incorrect answers give lower total score.

Select one or more alternatives:

- ☐ Observing a response from the Radius server makes it possible to do an off-line dictionary attack of the password
- ☐ The message authenticator is present to authorize the supplicant to the Radius server
- ☐ By asking the Authenticator to be authenticated and capturing our corresponding access request message, it enables us to do off-line attacks of other user's passwords when observing their access request messages
- ☐ By observing two access request messages, it is possible to XOR the two Password\* fields together and the result is two passwords XORed together
- ☐ Observing a request to the Radius server makes it possible to do an off-line attack of the shared secret ✓
- ☐ This protocol has replay protection of answers from the Radius server, which means that old accept messages cannot be reused by the attacker in his/her own connection attempts ✓

2p for a correct answer, -1p for incorrect answer(s)

## 5. DDoS mitigation

There have been different solutions proposed for how DDoS attacks can be stopped. Suggestions include “traceback”, “pushback” and “centertrack”. Pair the explanations with the corresponding technology! (2p)

Please match the values:

	Pushback	Centertrack	Traceback
For each datagram forwarded by a router, the receiver may, with some small probability, also receive additional info about who forwarded it,	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓
Routing within a system (e.g. AS) may be temporarily handled by special routers that are configured to handle tracing, if an attack is seen	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Routers realizing they have to discard many datagrams to one destination can tell other routers to drop these datagrams as well.	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>

1p for each correct answer, -1p for incorrect answer(s)  
(max 2p)

## 6. Firewall Technologies

Assume we want to block all connections from the Internet to a web server, except for encrypted TLS traffic. The server also has some other services running but they should be hidden and not accessible from the Internet.

Assume the price for the firewall increases for each technology in the order listed 1-5. The cheapest being the static packet filter and the most expensive the air-gap firewall. Choose the cheapest firewall in the list that will fulfill the requirements below!

0,5p for each correct answer, no points for incorrect answers

(4p)

1. static packet filters
2. dynamic packet filters
3. deep-packet packet inspection firewall
4. circuit-level gateway
5. air-gap firewalls

NOTE that the order of firewalls is randomized below - they are not in price order!

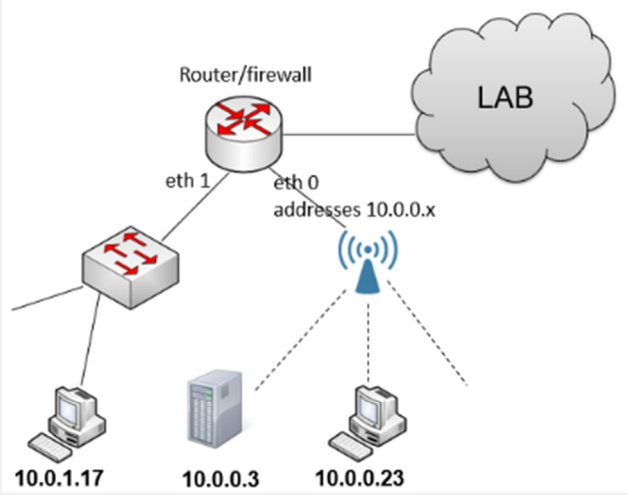
	2. Dynamic packet filter	5. air- gap firewall	4. Circuit- level gateway	None of the firewalls	3. Deep- packet inspection	1. Static packet filter
Replayed TCP segments should not reach the server	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Protect server against SYN flood attacks coming from one and the same IP-address	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
DNS requests from the web server and only corresponding replies should be allowed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
SYN-scans should not reveal the hidden services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Inspect web page requests sent to the server	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
ACK or FIN scans should not reveal the hidden services	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Hides the real IP address of the server and protects the server against scanning attacks	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Invalid IP packets with expiring TTLs should not be forwarded	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>



## 7. Firewall rules

We have a network using the full 10.x.x.x address space, and we want to give LAB access only for the hosts connected to interface eth0 except for the server 10.0.0.3.

Place the firewall rules in the correct order to achieve this! (2p for a correct solution)



Router/firewall

eth 1

eth 0

addresses 10.0.0.x

LAB

10.0.1.17

10.0.0.3

10.0.0.23

iptables -N ip\_filter

iptables -A ip\_filter -s 10.0.0.3/32 -j DROP

iptables -A ip\_filter -i eth0 -s 10.0.0.0/24 -j RETURN

iptables -A ip\_filter -s 10.0.0.0/8 -j DROP

## 8. Security protocols

What is true for the different security protocols?  
Correct answers for each protocol gives 2p.

(6p)

IPsec

- Supports perfect forward secrecy
- Transparent to ICMP and transport layer protocols
- Protects applications from dropped messages
- Suitable to build into own applications
- Uses TCP for transport
- Protects applications from duplicated messages

TLS

- Supports perfect forward secrecy
- Transparent to ICMP and transport layer protocols
- Protects applications from dropped messages
- Suitable to build into own applications
- Uses TCP for transport
- Protects applications from duplicated messages

SSH

- Supports perfect forward secrecy
- Transparent to ICMP and transport layer protocols
- Protects applications from dropped messages
- Suitable to build into own applications
- Uses TCP for transport
- Protects applications from duplicated messages

0,5p for a correct answer, -1p for incorrect answer(s)

However, assessment will be done manually to give a fair assessment of errors made so this score is only indicative.

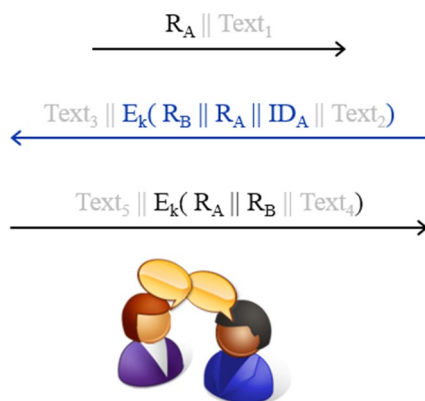
## 9. True or False?

Please answer True or False to the following statements.

**Correct** answer gives +1p, an **incorrect** answer as well as **no answer** gives -1p so please answer all questions. Most of these questions should be easy to answer which also motivates deduction of points for incorrect answers.

The total score from this question cannot be negative. (10p)

Consider the following simple user authentication scenario from the ISO 9798 standard.  
(R is a random number, Texts can be ignored.)



Are the statements below true or false?

a) Both parties know that the other is in possession of the key

True.

b) Alice knows that Bob is alive (i.e. it's a fresh session)

True. Bob could encrypt  $R_A$

c) Bob knows that Alice is alive

True. Alice could encrypt  $R_B$

d) Diffie-Hellman key exchange can to some degree identify the other party

False. All we know is that we share the secret with someone.

e) The length field of an IP datagram is 16 bits long which limits the length of a datagram to 64 kByte (65,535 bytes). However, it is still possible for an attacker to send datagrams longer than this.

TRUE - by using fragmentation

f) The ESP header in IPsec contains the fields "next header", see last page. It tells IPsec what upper layer protocol should receive the message, for example UDP.

TRUE - The original field in the IP header now contains protocol 50 (ESP) since it should receive it first, thus the original value needs to be stored somewhere.

g) The IPsec protocol IKE uses cookies when a client wants to establish a connection to protect itself against unauthorized session key calculations.

True

h) Linux can begin using SYN cookies to protect itself against DoS attacks to avoid having to calculate random sequence numbers.

False

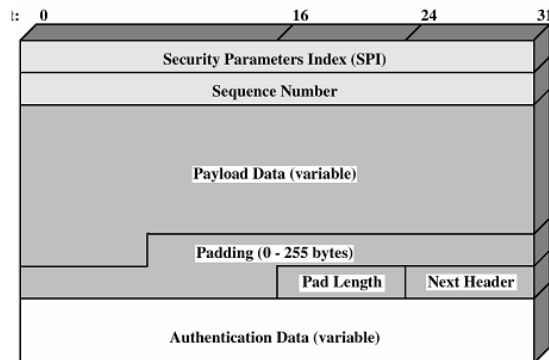
i) A master key in for example TLS is used to authenticate the other party.

False. The master key is derived from key negotiation process during connection setup. It is then used to create session keys which are used for data encryption, etc, keys that are changed regularly.

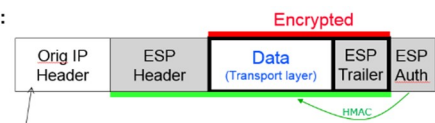
j) TLS is sensitive to NAT (network address translation)

False - it does not care

# Headers and pictures that may be useful

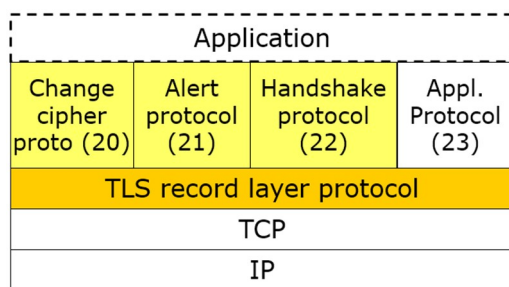
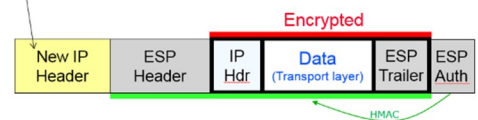


Transport mode:



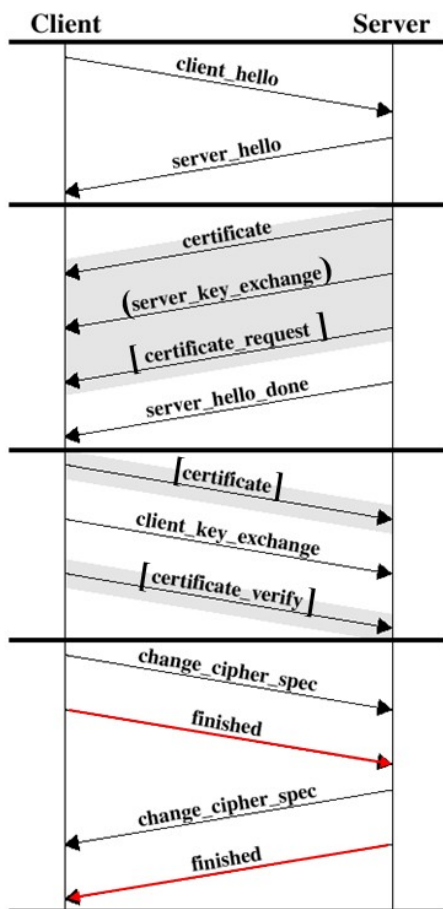
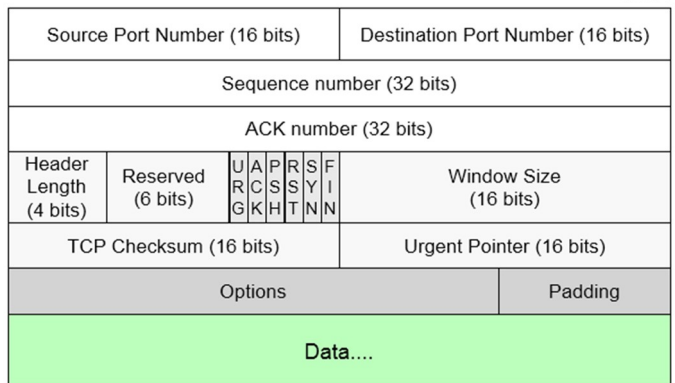
Protocol = 50 (ESP)

Tunnel mode:



Bit 0

Bit 31



Bit 0

Bit 31

