CHALMERS | GÖTEBORGS UNIVERSITET

Network Security – DIGITAL

EDA491 (Chalmers)
DIT071 (GU)

2023-05-29, 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.

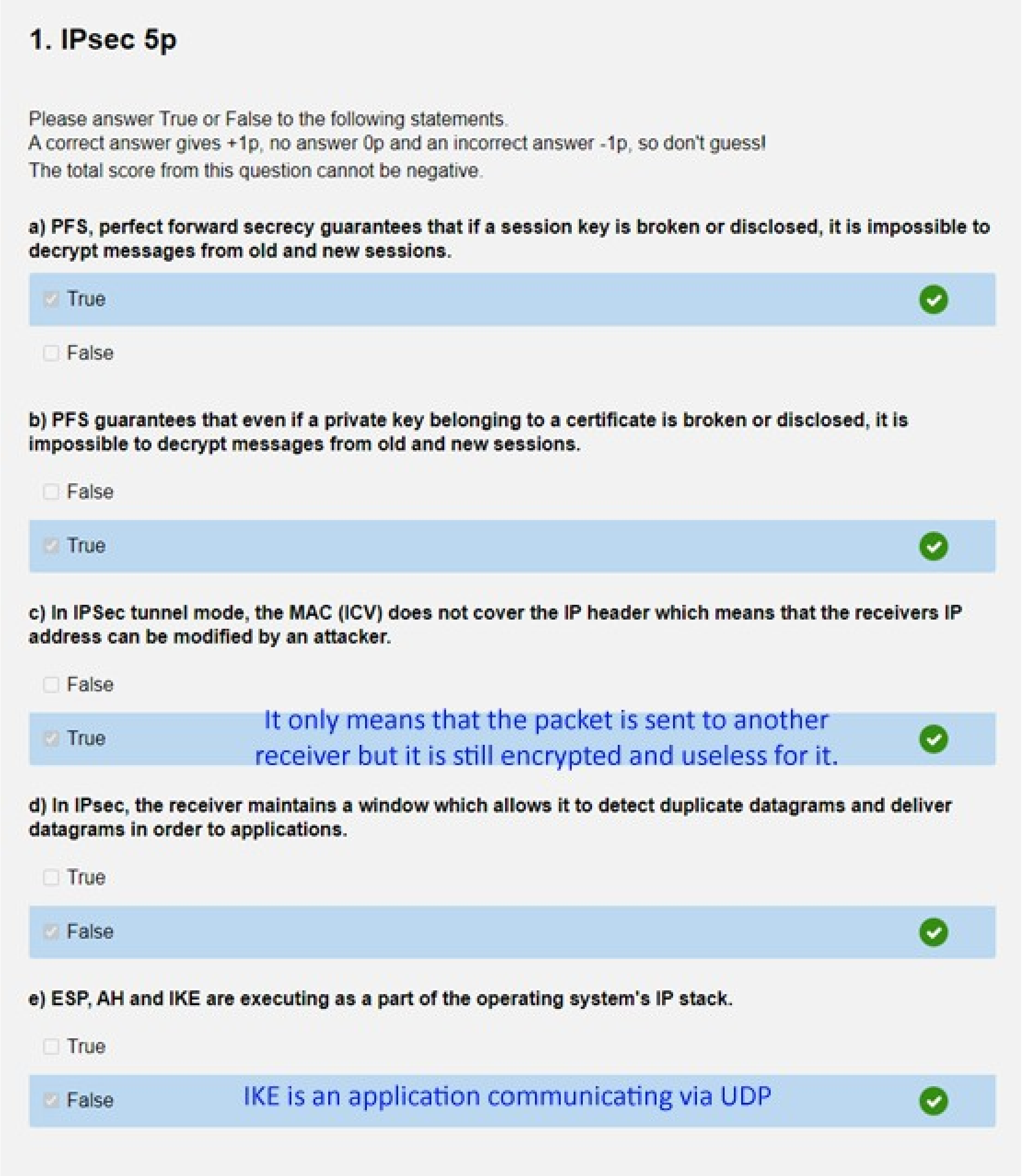
A good rule-of-thumb for how much detail to provide, is to include enough information and explain so that a person who has not taken this course can understand the answer.

Automatically corrected questions will be manually inspected if the exam is close to a grading border. It may be that the rules for the automatic correction need to be updated if they turn out to be too strict.

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. IPsec 5p

Please answer True or False to the following statements.
A correct answer gives +1p, no answer 0p and an incorrect answer -1p, so don't guess!
The total score from this question cannot be negative.

a) PFS, perfect forward secrecy guarantees that if a session key is broken or disclosed, it is impossible to decrypt messages from old and new sessions.

☑ True ✓

□ False

b) PFS guarantees that even if a private key belonging to a certificate is broken or disclosed, it is impossible to decrypt messages from old and new sessions.

□ False

☑ True ✓

c) In IPSec tunnel mode, the MAC (ICV) does not cover the IP header which means that the receivers IP address can be modified by an attacker.

□ False

☑ True ✓

It only means that the packet is sent to another receiver but it is still encrypted and useless for it.

d) In IPsec, the receiver maintains a window which allows it to detect duplicate datagrams and deliver datagrams in order to applications.

□ True

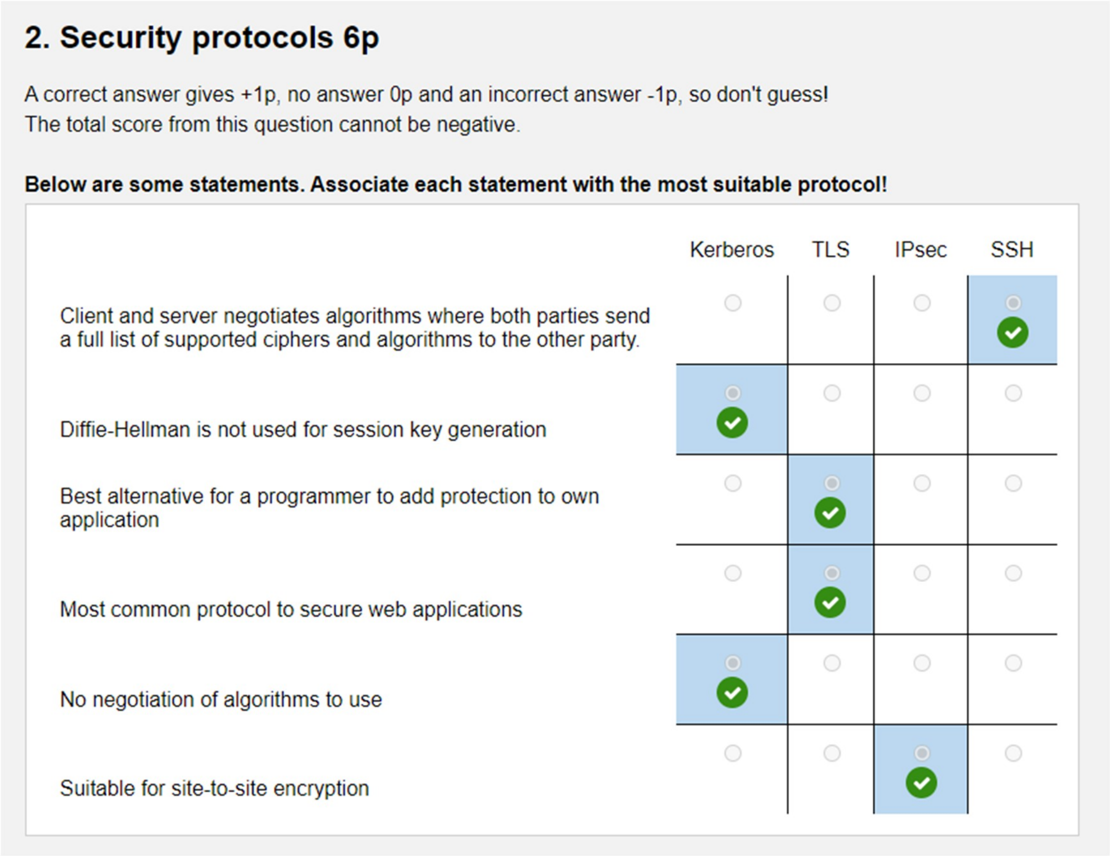
☑ False ✓

e) ESP, AH and IKE are executing as a part of the operating system's IP stack.

□ True

☑ False ✓

IKE is an application communicating via UDP



2. Security protocols 6p

A correct answer gives +1p, no answer 0p and an incorrect answer -1p, so don't guess!
The total score from this question cannot be negative.

Below are some statements. Associate each statement with the most suitable protocol!

	Kerberos	TLS	IPsec	SSH
Client and server negotiates algorithms where both parties send a full list of supported ciphers and algorithms to the other party.	○	○	○	● ✓
Diffie-Hellman is not used for session key generation	● ✓	○	○	○
Best alternative for a programmer to add protection to own application	○	● ✓	○	○
Most common protocol to secure web applications	○	● ✓	○	○
No negotiation of algorithms to use	● ✓	○	○	○
Suitable for site-to-site encryption	○	○	● ✓	○

3. WLAN 8p

Below are some statments about wireless protocols. Mark what alternatives are true.
Each correct answer gives +1p and an incorrect answer -1p.

Total score from this question is 8p but it does not necessary mean that 8 alternatives are correct (it could be fewer or more). The total score from this question cannot be negative.

What alternative(s) are correct regarding WEP:

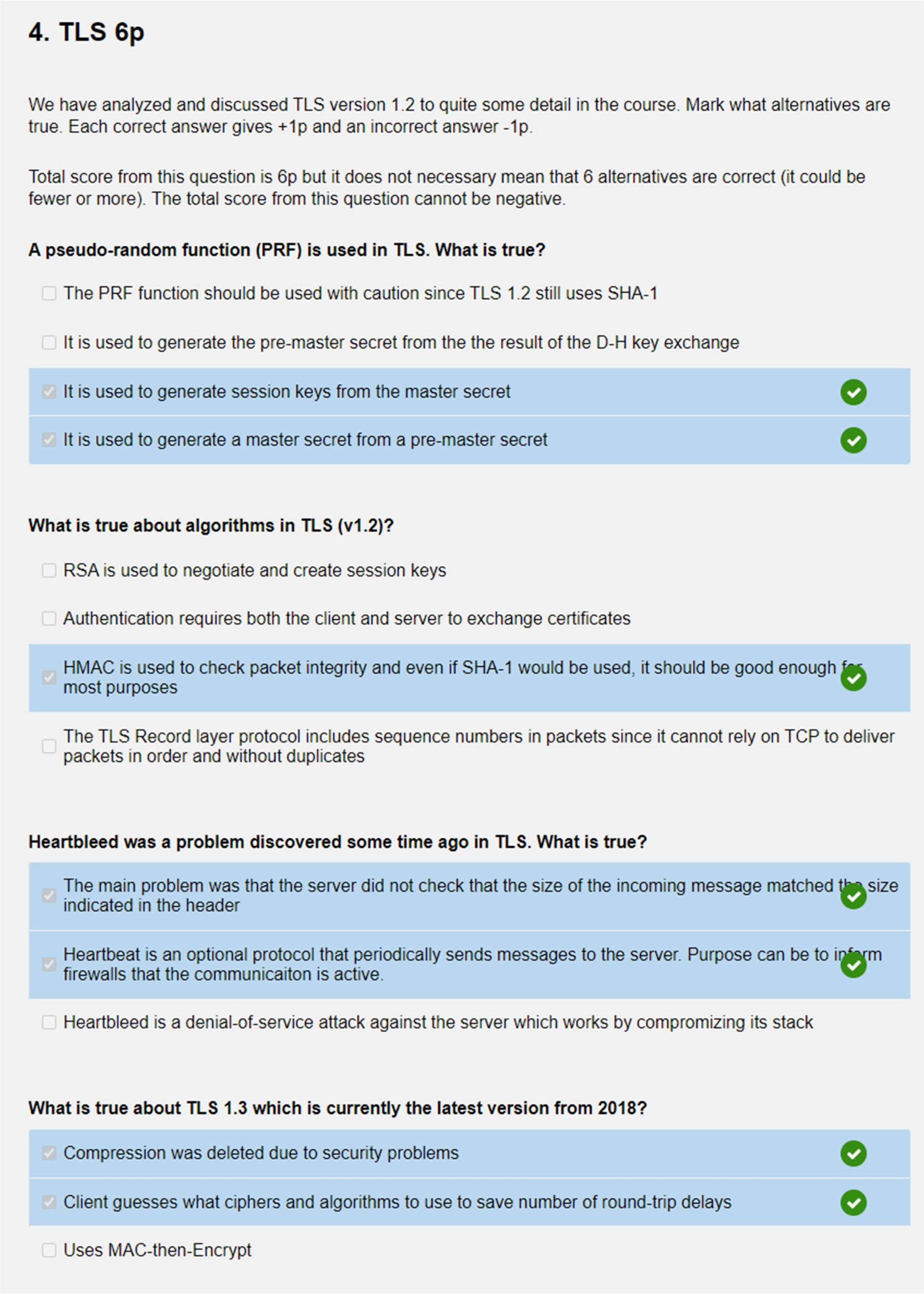
- ☑ Encryption keys are never changed during a session ✓
- ☑ Does not offer any freshness guarantees during communication, replays are possible ✓
- ☐ Uses sequence numbers to prevent replays and duplicates of old packets
- ☐ Does not offer any freshness guarantees during authentication, replays are possible
- ☑ Uses challenge-response authentication ✓

What is correct for WPA2:

- ☑ Group transient keys are shared between all users and used for example when ARP broadcasts a question. ✓
- ☐ Diffie-Hellman key exchange is supported
- ☐ Group transient keys (GTK) are created which are shared between all users and are changed each time a new user connects or disconnects
- ☑ Port-based network access control (IEEE 802.1x) is a link-level protocol used by WPA2. It makes sure that a client does not get access to the network before being authenticated. ✓
- ☑ Individual session keys (PTK, pairwise transient keys) are unique for each station even if all stations share the same pre-shared key for authentication ✓

Misc WLAN questions:

- ☑ WPA3 offers perfect forward secrecy even in open networks where no password is needed ✓
- ☐ WEP was updated with TKIP (temporal key integrity protocol) before WPA arrived, when it was discovered that the IV space was too short. When the IV space now is exhausted, new keys are generated.
- ☑ WPA and WPA2 does not allow the same IV to be reused which makes it impossible to reuse key streams ✓
- ☐ Rainbow tables can be used to help cracking a session key for WEP, WPA2 and WPA3 if the station uses a well-known SSID
- ☐ Disabling SSID broadcasts is a security feature that means that no new clients can connect until it is enabled again



4. TLS 6p

We have analyzed and discussed TLS version 1.2 to quite some detail in the course. Mark what alternatives are true. Each correct answer gives +1p and an incorrect answer -1p.

Total score from this question is 6p but it does not necessary mean that 6 alternatives are correct (it could be fewer or more). The total score from this question cannot be negative.

A pseudo-random function (PRF) is used in TLS. What is true?

- ☐ The PRF function should be used with caution since TLS 1.2 still uses SHA-1
- ☐ It is used to generate the pre-master secret from the the result of the D-H key exchange
- ☑ It is used to generate session keys from the master secret ✓
- ☑ It is used to generate a master secret from a pre-master secret ✓

What is true about algorithms in TLS (v1.2)?

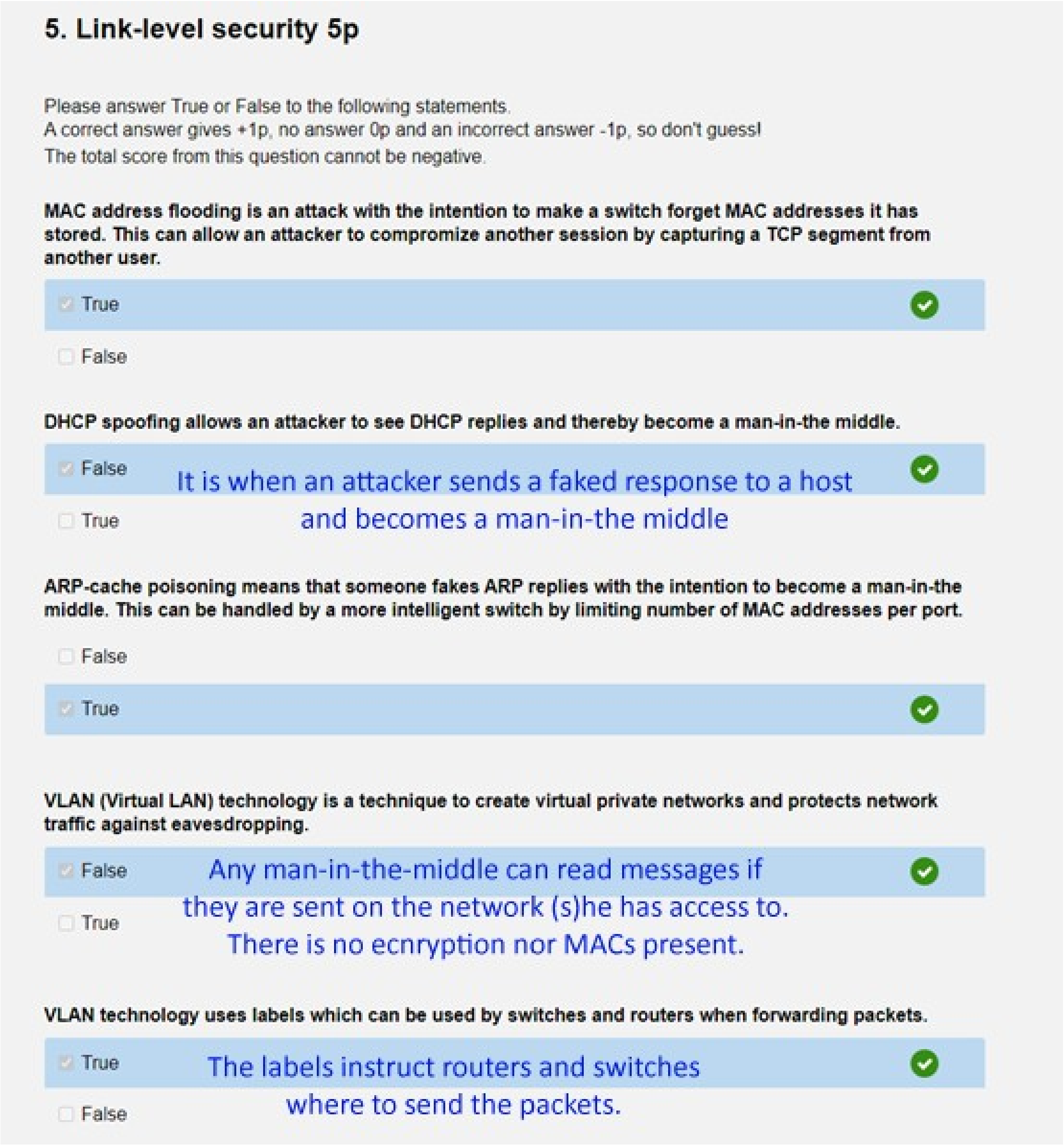
- ☐ RSA is used to negotiate and create session keys
- ☐ Authentication requires both the client and server to exchange certificates
- ☑ HMAC is used to check packet integrity and even if SHA-1 would be used, it should be good enough for most purposes ✓
- ☐ The TLS Record layer protocol includes sequence numbers in packets since it cannot rely on TCP to deliver packets in order and without duplicates

Heartbleed was a problem discovered some time ago in TLS. What is true?

- ☑ The main problem was that the server did not check that the size of the incoming message matched the size indicated in the header ✓
- ☑ Heartbeat is an optional protocol that periodically sends messages to the server. Purpose can be to inform firewalls that the communicaiton is active. ✓
- ☐ Heartbleed is a denial-of-service attack against the server which works by compromizing its stack

What is true about TLS 1.3 which is currently the latest version from 2018?

- ☑ Compression was deleted due to security problems ✓
- ☑ Client guesses what ciphers and algorithms to use to save number of round-trip delays ✓
- ☐ Uses MAC-then-Encrypt



5. Link-level security 5p

Please answer True or False to the following statements.
A correct answer gives +1p, no answer 0p and an incorrect answer -1p, so don't guess!
The total score from this question cannot be negative.

MAC address flooding is an attack with the intention to make a switch forget MAC addresses it has stored. This can allow an attacker to compromize another session by capturing a TCP segment from another user.

☑ True ✓

☐ False

DHCP spoofing allows an attacker to see DHCP replies and thereby become a man-in-the middle.

☑ False ✓

☐ True

It is when an attacker sends a faked response to a host
and becomes a man-in-the middle

ARP-cache poisoning means that someone fakes ARP replies with the intention to become a man-in-the middle. This can be handled by a more intelligent switch by limiting number of MAC addresses per port.

☐ False

☑ True ✓

VLAN (Virtual LAN) technology is a technique to create virtual private networks and protects network traffic against eavesdropping.

☑ False ✓

☐ True

Any man-in-the-middle can read messages if
they are sent on the network (s)he has access to.
There is no ecnryption nor MACs present.

VLAN technology uses labels which can be used by switches and routers when forwarding packets.

☑ True ✓

☐ False

The labels instruct routers and switches
where to send the packets.

6. Attacks and DoS

a) Explain how TCP fingerprinting works, i.e. how a system's identity can be determined. Give two examples of what it *may* look like! (2p)

By inspecting TCP traffic from a system, it is possible to determine its type based on values in different TCP header fields, such as TTL, Window size, TOS and DF bit. (Note that sequence numbers should be random and therefore useless here.)

Different operating systems use different options and set for example TTL to different values. The attack can work just by trying to establish a connection and watching the first TCP reply.

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

Drop outgoing ICMP messages (port unreachable, …)
Drop malformed TCP packets
Change some fields (e.g. normalize TTL or window size) to make packets less useful.

c) Why could it be problematic for a system to deal with a packet that has an incorrect (i.e. faked) IP or TCP length field that differs from the real physical packet length? Describe two possible scenarios! (2p)

Length field > actual length: old contents of buffer can be used and sent to receiver. Example is a router that forwards an IP datagram, it may take the old contents in the buffer and forward (a part of) another packet's payload to the receiver.

Length field < actual length: may cause a buffer overrun if the receiver dynamically allocates buffers based on the header length. It may overwrite stack contents and change program behavior.

d) 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. By not responding to the SYN/ACK and not finishing the three-way handshake, the queue of pending connections will be filled up and no new legitimate connections will be accepted.

Faked IP addresses: to hide own address and using multiple addresses is to make it hard for the receiver to know what addresses are faked and part of a DoS attack.

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.
- …

7. Authentication

a) Describe in detail the process of how an (X.509v3) certificate is used, i.e. how someone's identity can be verified by a web browser or by an application you have created!
What steps does the receiver of the certificate have to take to verify the identity?
Are there any restrictions in the way it can be distributed to the receiver?
Hint: think about the contents of the certificate and how you use it. (4p)

- The certificate's signature of the CA is checked using the CA's public key (a hash of the certificate is created and the encrypted and compared with the hash in the certificate)
- The validity period and whether the certificate has been revoked (CRL) are checked.
- The owner's identity is checked, for example by giving it/him/her a challenge to encrypt with the private key which we can decrypt with the public key found in the certificate.
- It does not matter how it is distributed since the full contents and the authenticity can be checked using the CA signature.

b) Both LDAP and Radius can be useful in situations where users should be authenticated. Describe what functionality each protocol offers! In your answer, make sure you highlight the differences between them and that it is clear when the respective protocol can or should be used! (4p)

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 good protocol for networked devices (clients) without their own account database 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.

c) Using passwords to generate session crypto keys does not guarantee PFS, Perfect Forward Secrecy. Why not? Give an example of how it can be achieved? (2p)

PFS is a way to guarantee that if a session key is compromised, it should not be possible to decrypt any other sessions, past of future. The session keys should be independent of this key, thus independent of for example a password.

Using Diffie-Hellman or Elliptic Curve key exchange guarantees unique keys for each session.

8. Firewalls and IDS

a) In the course we have looked at different types of firewalls such as

- Static packet filters
- Dynamic packet filters
- Stateful packet inspection

Explain with one or two sentences for each type what it is and what it does! Make sure your answer makes it possible to distinguish the firewalls from each other. (3p)

Static packet filter firewalls just compare the IP addresses and port numbers in each packet with a static table of what should be allowed or dropped. It should just be used as a complement to a "real" firewall (a screening router).

Dynamic packet filters are similar to static filtering, but the firewall may modify its own rules based on some events (e.g. when an outgoing UDP message is seen, it may add a rule to allow a response).

Stateful packet inspection firewalls understand and keep state of at least TCP and UDP. The ACL list is only consulted when a TCP connection is established. It is therefore both more secure and faster than static filters.

b) Explain why a firewall and a host receiving a fragmented IP packet may end up with two different results. Is this problem possible to solve? (2p)

Overlapping fragments can be reassembled in different ways. See slides. Solution can be that the firewall always reassembles all packets or that fragments always are dropped.

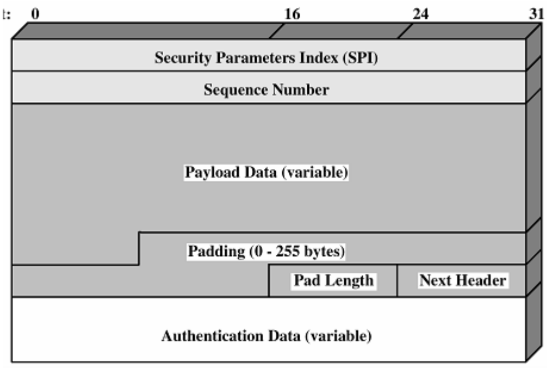
c) NAT gateways are strictly speaking not firewalls, but they are still useful and can in some situations replace a conventional firewall.
- What level of protection do they offer?
- What do they lack which normal stateful inspection firewalls have?
- Give an example of a use case where a NAT gateway can or should be used! (3p)

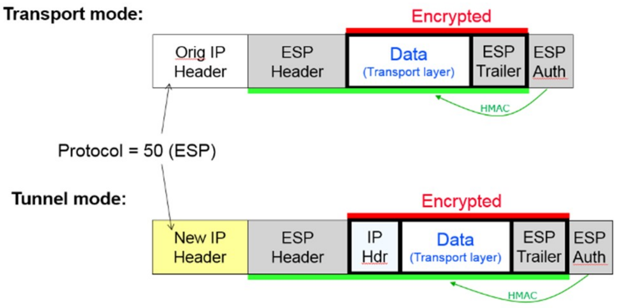
They hide and isolate internal systems from the outside network. A service not present in its translation table is not visible/accessible from the outside.
It does not inspect traffic that is allowed to traverse (as done in a conventional firewall).
NAT gateways are often used at home where only one official IP address is available and more devices are present. It is also popular by companies since they hide the internal structure of the network and the systems real IP addresses. It is often combined with "real" firewall functionality as well.

d) 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.

Headers and pictures that may be useful

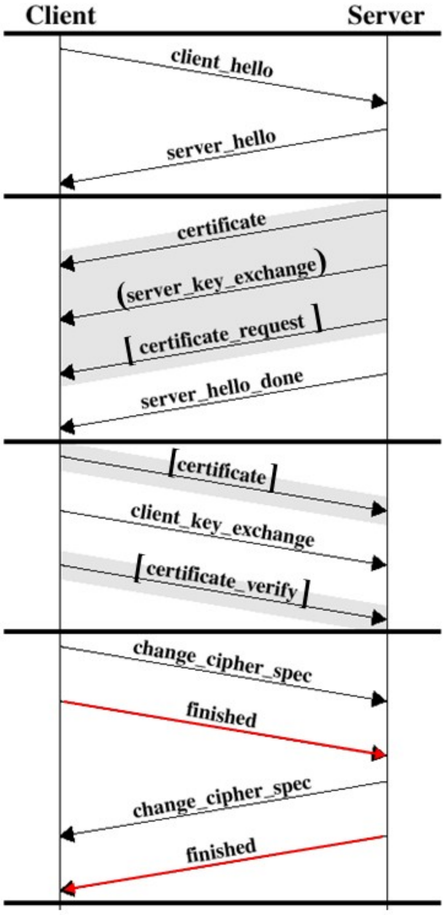




Application			
Change cipher proto (20)	Alert protocol (21)	Handshake protocol (22)	Appl. Protocol (23)
TLS record layer protocol			
TCP			
IP			

Bit 0 Bit 31

Source Port Number (16 bits)								Destination Port Number (16 bits)
Sequence number (32 bits)								
ACK number (32 bits)								
Header Length (4 bits)	Reserved (6 bits)	URG	ACK	PSH	RST	SYN	FIN	Window Size (16 bits)
TCP Checksum (16 bits)								Urgent Pointer (16 bits)
Options								Padding
Data....								



Bit 0 Bit 31

Version (4 bits)	Header Length (4 bits)	QoS (8 bits)	Total Length (16 bits)	
Fragment identification (16 bits)			Flags (DF, MF)	Fragment Offset (13 bits)
Time to Live (8 bits)		Protocol (8 bits) 1=ICMP, 6=TCP, 17=UDP, 50=ESP, ...	Header Checksum (16 bits)	
Source IP Address (32 bits)				
Destination IP Address (32 bits)				
Options (if any)				Padding
Data....				