CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2019-10-11, 14:00 – 18:00

SB multisal

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

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

Start answering each question (1, 2, 3, …) on a new page; use only one side of each sheet of paper; please sort and number the sheets in question ordering.

Write in a clear manner and motivate (explain, justify) your answers. If it is not clear what is written for some answer, it will be considered wrong. 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/explanation 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

a) Give an example of a Transport layer attack (2p)

See lecture slides for possible answers. Many answers are possible.

b) 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.

c) 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. How? (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.

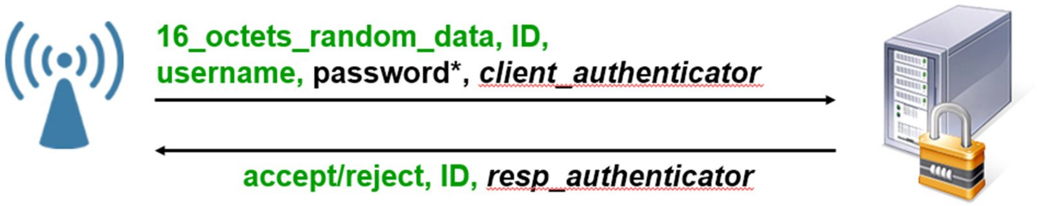
d) Describe two possible ways to address this TTL problem in a border firewall! (2p)

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

e) Ping of death is a well-known attack. It sends IP datagrams with a size > 64 kByte. However, the maximum size of an IP datagram is 64kByte due to its 16-bit length field. Explain how is it still possible send such oversized datagrams! (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.

2. Authentication,



16_octets_random_data, ID, username, password*, *client_authenticator*

accept/reject, ID, *resp_authenticator*

password* = MD5(shared_secret, 16_octets_random_data) ⊕ password

client_authenticator = MD5(packet_contents, shared_secret)

resp_authenticator = MD5(packet_contents, 16_octets_sent_by_client, shared_secret)

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

a) Explain the purpose of the *shared_secret*! (2p)

Shared secret = crypto key the authenticating server and the Radius server share. If it does not match, the Radius server will not respond to the question.

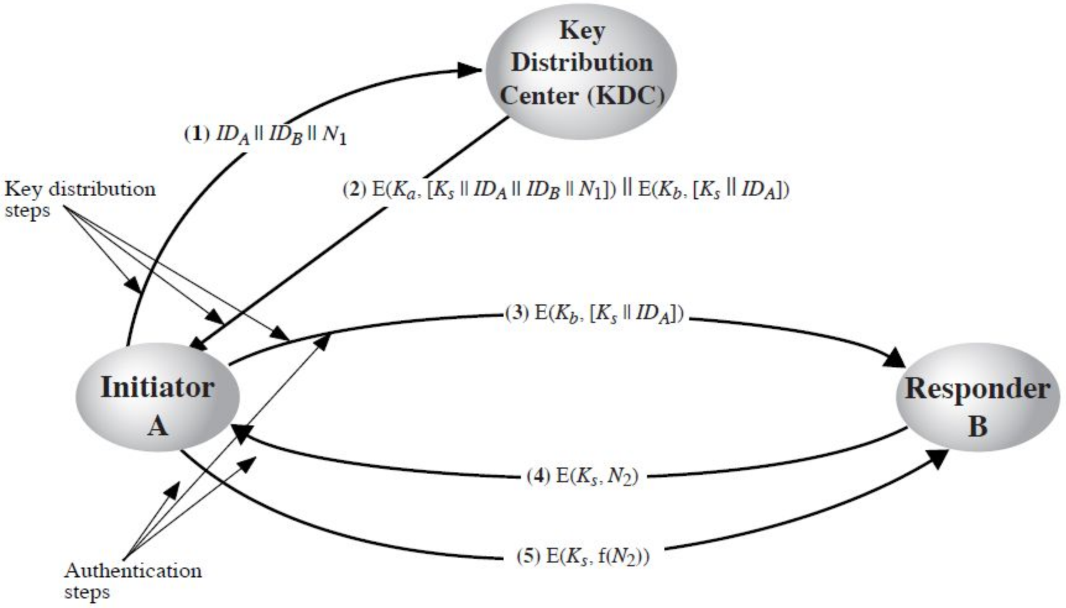
b) What is the purpose of the Authenticator (*16_octets_random_data*)? What happens if it is not random and is reused? (2p)

It makes sure the transmitted data packet is unique. See for example attack 3.5 in the reading material or in the slides.

c) If a dishonest supplicant can both send and listen to the traffic between the Authenticator and the Radius server, it is possible to do a number of attacks. Give one example of an attack against the shared secret! (2p)

See for example attack 3.1 in the reading material or in the slides.

The picture below shows a Kerberos-like protocol:


Key Distribution Center (KDC)
(1) $ID_A \| ID_B \| N_1$
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s \| ID_A])$
Key distribution steps
(3) $E(K_b, [K_s \| ID_A])$
Initiator A
Responder B
(4) $E(K_s, N_2)$
(5) $E(K_s, f(N_2))$
Authentication steps

d) Explain on a fairly high level how this protocol works! Don't just repeat what the picture tells but explain the purpose and outcome of each step! (2p)

See the book, picture 14.3 and explanation in chapter 15.2.

e) This protocol is not completely secure although it is probably secure enough for most practical purposes. What is its main weakness? How does Kerberos address this weakness? (2p)

Attacks are possible with replays if the session key is broken or stolen from A's computer. Keys never expire – can be used and reused forever.

Use timestamps! Problem is that clocks must be synchronized and keys renewed regularly. Long sessions may be interrupted when keys expire.

3. TLS and IPsec

a) SSL/TLS consists of several protocols. Describe the functionality of the record layer, change cipher, alert and handshake protocols! (2p)

Record layer performs fragmentation -> compression -> adding MAC -> encryption.
Change cipher tells the other side to change to the last security parameters negotiated (and turn on encryption).
The alert protocol sends warnings and error messages to the other side.
The handshake protocol negotiates ciphers, keys and performs authentication.

b) SSL/TLS has a special message to close a connection. Why is this message present, why not just send a TCP FIN segment? (2p)

To prevent truncation attacks. We don't want an attacker (for example a MITM) to be able to prematurely terminate a connection between the client and the server by faking a FIN in each direction (doing a perfectly normal TCP close). This could result in both sides believing that all data has been sent and received even if some data at the end was removed by the attacker.

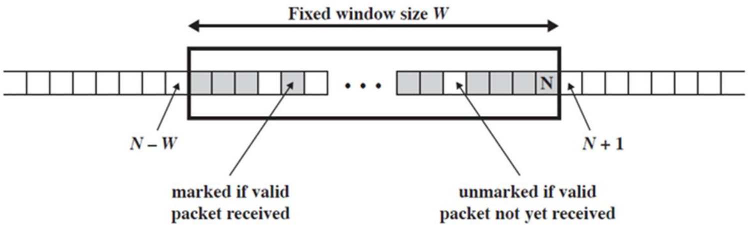
c) In TLS, a Pseudo-random function is used:

$$\mathbf{PRF(k, label, x) = HMAC_k(HMAC_k(label||x) \;||\; label||x) \;\;||\;\; HMAC_k(\ldots}$$

What is the purpose of this PRF-function? When is it used? (2p)

It is used to expand short secrets to longer blocks, for example to generate the master key from the pre_master_secret or to generate crypto-keys from the master secret: ***master_secret*** = **PRF**(*pre_master_secret*, "**master secret**", r_c || r_s)

d) IPsec uses packet numbering, see the picture. For what purpose? (2p)


Fixed window size W
N
N – W
N + 1
marked if valid packet received
unmarked if valid packet not yet received

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

e) The ESP header in IPsec differs depending on what mode is used (see header on last page). Why is it possible to keep the original header in transport mode but not in tunnel mode? (2p)

4. Firewalls and IDS systems

a) Describe briefly how a stateful firewall works! What information does the firewall (at least) need to save for TCP connections? (2p)

Source and destination IP addresses, source and destination ports, TCP state (according to the state machine), TCP sequence numbers. (Real firewalls store more information but this information is at least needed for a firewall to be called stateful.)

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

To offload the main firewall from obvious garbage traffic. Cheap alternative to offload the main firewall from work.

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

Hides internal structure (IP addresses). Only connections initiated from the inside can get reply traffic from the outside. If no entries exist in the connection table, all traffic from the outside is discarded.

d) Explain the functionality of a circuit-level gateway and an application-level gateway. (2p)

Circuit-level gateways are firewalls terminating the TCP connections. It opens a new TCP connection to the other side to avoid TCP and IP headers being forwarded. The application-level protocol is not touched.

Application-level gateways also terminate the application protocol such as Telnet, FTP, SMTP, etc. It extracts the data and creates a new connection to the other side with new application headers.

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

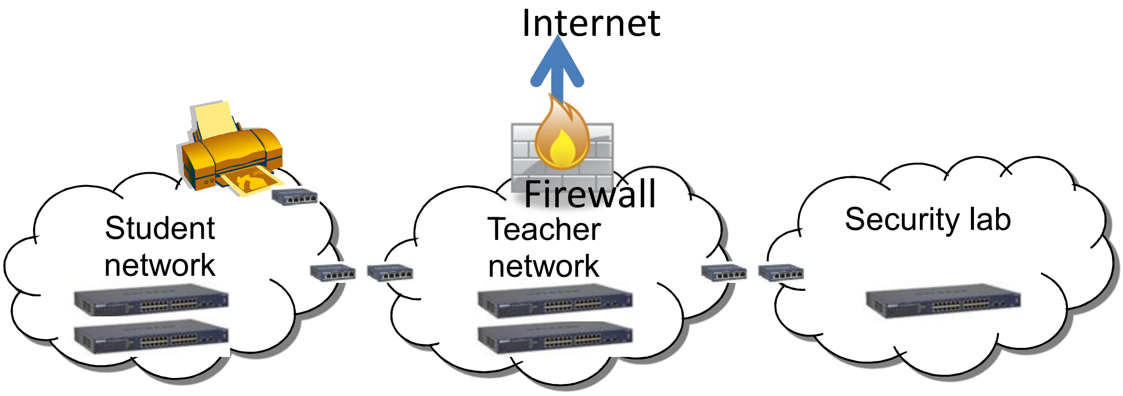
If datagram 1 = AAAAAA and datagram 2 = BBBBBB and they overlap by 50%, a firewall or IDS system does not know how the receiving system reassembles the datagram. It may become AAABBBBBB or AAAAAABBB.

5. Network design

a) Assume you are a systems administrator at a school and you need to create a link level solution using only switches. There are three networks available: a student network, a teacher network and a security lab connected as shown in the picture. There are some security requirements you need to consider:

- *The traffic between the networks should never be mixed*: students should not be able to access the teachers' computers or security lab computers. Same for teachers; no access to student computers or the security lab.
- *The traffic from the lab should never leave the lab network except to a printer* located in the students' network to allow students in the lab to print reports. This printer should only be available for people in the security lab.
- *Both teachers and students should have Internet access* but not the security lab.

Assume there are around 100 computers on each network. The users are connected to the large switches in the picture; routers or switches are used to connect networks. How would you implement your solution? (4p)



The technique to base the solution on is VLAN separation where the switches set the tags to make sure that traffic passing through the teacher network is kept isolated. Explain where tags are set, what VLANs are assigned, etc.

b) What protocol would you select when building a VPN system for remote users to the student network above? There may be several possible solutions to this question so please motivate your selection! (2p)

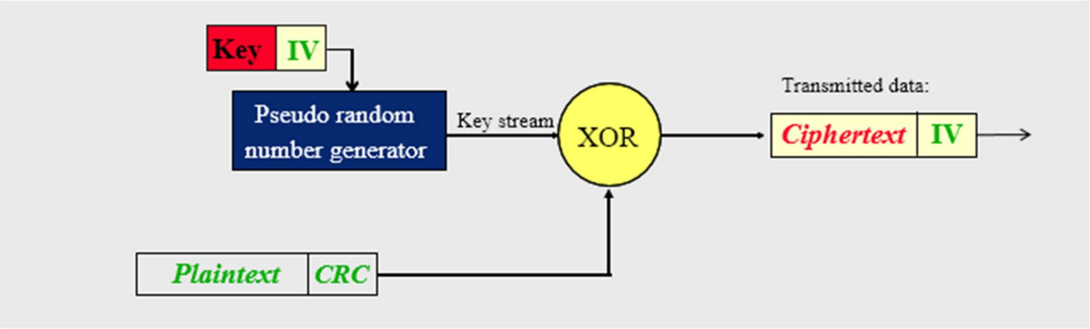
Most likely SSH or SSL. Easy to configure, client can run as an application without administrative privileges, etc.

c) We have discussed the Jericho Forum during the course. The idea they propose is to move protection closer to the end-points. Does it make sense? Explain your thoughts with some details! (4p)

Services are located both on internal networks and on external (cloud) servers, and users are located both on the inside and on the outside and also bring laptops and other devices from the outside. WLANs also extend the range of the networks outside the physical network boundaries. It is therefore impossible to control security with only a border firewall that only sees a small part of all traffic. The solution is to move protection closer to the end-points: toward the users/client systems and to application servers.

6. WLAN

a) Explain how encryption of data traffic is done in WEP! A figure together with an explanatory text is needed. (4p)



The answer should explain the purpose of the different parts.

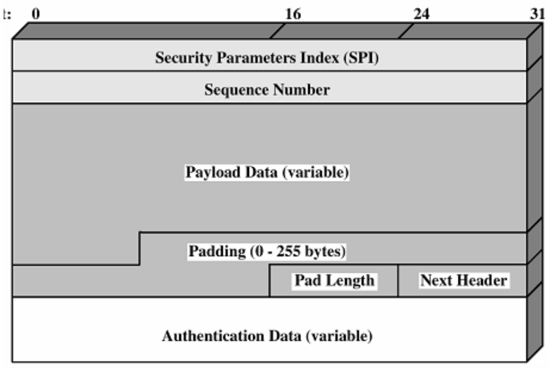
b) WEP is not known for its good security. Describe two vulnerabilities or possible attacks against it! (4p)

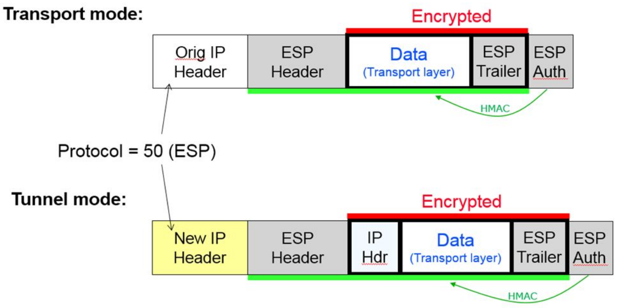
Possible answers can be: reuse of IVs, using the same method for user authentication reveals a usable key stream, the Caffe latte attack, etc.

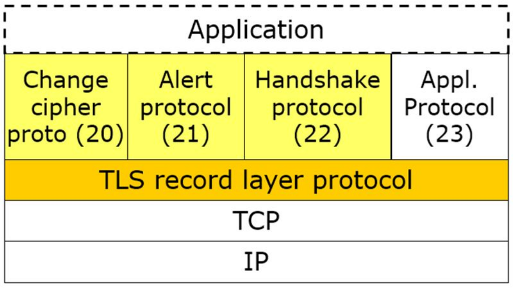
c) A feature added in WPA and WPA2 is 802.1x – port-based authentication. What does this mean? What does it do? Explain! (2p)

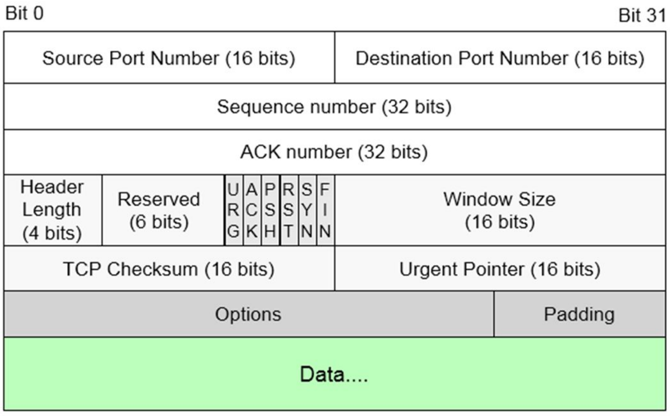
Port-based authentication is a link-level mechanism where a client does not get access to the network unless authenticated and authorized. It uses Radius for central authentication and authorization. When the Radius server accepts the user, full network access is given.

Headers and pictures that may be useful



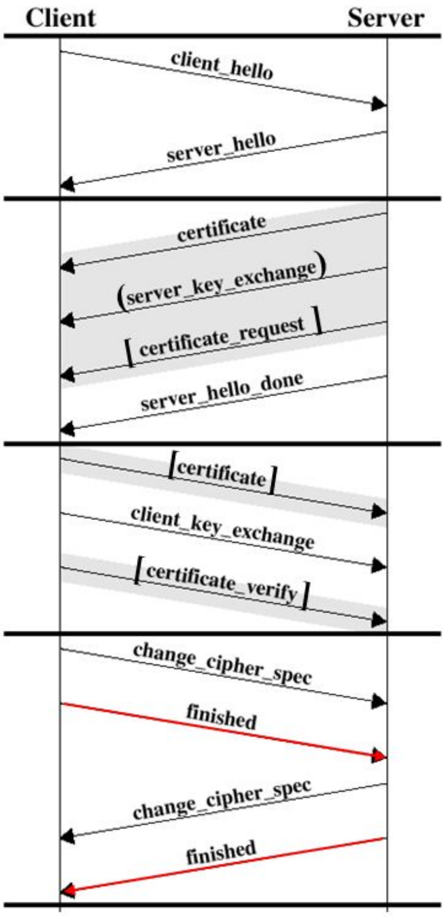


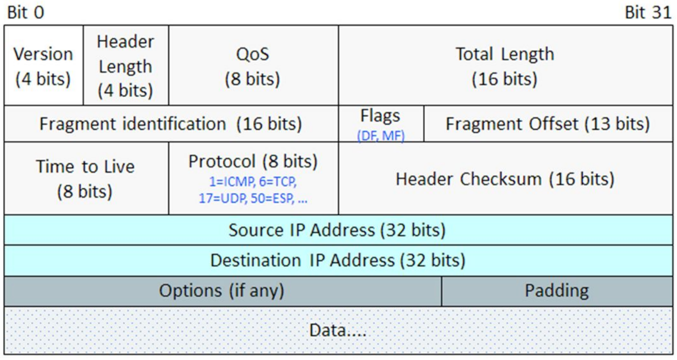




Bit 0 — Bit 31

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)	U R G	A C K	P S H	R S T	S Y N	F I N	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....				