CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2020-06-01, 08:30 – 12:30

plus 30 minutes for scanning at the end

All questions must be clearly explained using 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

Slightly changed from older exams

1. Attacks and DoS

a) When scanning a system, for example doing a SYN scan to find open ports, the attacker may immediately send a RST when a reply is received. Why? (2p)

If the port receiving the SYN is open, the host will allocate resources and wait for the three-way handshake to complete. This is visible if someone looks in the system, for example by doing a NETSTAT command. The RST resets the communication and makes it much more stealthy.

b) It may be advantageous to scan a host using different IP addresses. Why? (2p)

It may make it harder to detect by an IDS system and harder to filter out such scans in a firewall.

c) In early DDOS attacks, TCP and UDP was used to communicate with handlers. Next generation switched to ICMP echo and echo reply. Why? (2p)

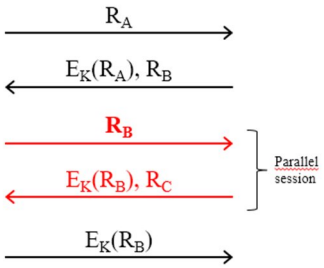
To hide their presence better. ICMP echo and echo reply are common packets sent from hosts to everywhere. In addition, they are not expected to contain useful data so they were likely not inspected by firewalls.

d) If a protocol fails to verify that the packet length field is identical to the actual length of the packet received, it can cause problems. Explain in detail two problems and what attacks this can open up for! (4p)

Packet < 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. The SSL/TLS heartbeat attack is another example.

Packet > 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.

2. Authentication, WLAN



R_A = random number (nonce) from A
K = shared key

a) The picture above shows a typical attack against a challenge response authentication protocol where a parallel session can be used to … Yes, to do what? What is the purpose of this attack? And explain how it is performed! (2p)

The red part is a new session initiated by the attacker to be able to answer the challenge the server sent above (Rb). It simply asks the server to encrypt Rb and the result can be used in the reply to the original session.

b) Nonces can be used to improve this protocol. Describe in detail how this can be done, possibly with a figure! (2p)

If each party include a nonce in the communication), it is possible to verify that the other party responds with fresh information belonging to THIS session. Responses like Ek(Ra) can be replaced by Ek(Ra, nonce) where the nonce is communicated to the other party.

c) Kerberos is implemented in such a way that it does not have to keep state, why? Describe how this is achieved! What are the advantages of this? (4p)

In the reply to a client that is authenticated, the TGT which is sent back to the client contains all the information Kerberos needs when the user reconnects and asks for access to servers (requesting SGT).
This makes it possible to have redundant and multiple servers answering requests and it does not matter who gets an SGT request, all can check that the user is authenticated by checking the TGT.

d) Kerberos offloads application servers some tasks. Explain! (2p)

They do not have to do user authentication. They also know that the user is authorized to use their service!

3. Security protocols

You are now given the task to encrypt the communication in an application like Zoom where a server offers lots of meetings with 100+ participants. Assume that the users are authenticated with a username and a password and the server has a certificate the users can download to verify its identity. We want the application to be secure and offer secrecy to their users and it should not be possible to decrypt past sessions even if the users' passwords are revealed. Assume that encryption is done user-to-server, not user-to-user.

a) How would you implement user authentication? It should guarantee that all parties are alive, i.e. that it is not a replay of another authentication session (2p)

Authenticatoin: Challenge-response authentication of users where the user's password and the servers public/private keys are used (more details needed).

b) How would you solve the problem with crypto keys for the participants and guarantee that sessions are kept secret even if all user passwords are revealed some time in the future? What is this property called? (2p)

Session keys: Use Diffie-Hellman to guarantee forward secrecy of session keys

c) In the ongoing communication, you want to guarantee protection against MITM-attacks. Encryption can be used to guarantee confidentiality, but there are more threats. Mention two other typical threats from a MITM that the protocol must protect against, and describe with some detail how to mitigate them! (2p)

MITM attacks:
- Integrity (HMAC) and replay protection (nonces, counters, timestamps)

d) Many security protocols have *implicit* sequence numbers, i.e. they are not present in the packet and are not transmitted on the network. What is the purpose of using implicit sequence numbers? How does it work? Explain! (2p)

They are used to avoid replays (and if random offer freshness). When the HMAC is calculated, the next expected number is used: HMAC(number, payload, secret) but not included in the payload. Instead both sides keep track of the current packet number.

e) Suppose you were able to influence the inventors of the IP protocol. What modifications would you have proposed to them to make it better, given what we know today about IP and security? Don't consider encryption or converting it to a security protocol, just mention two modifications you wish they had done which would make security work easier! (2p)

Fragmentation removed, most options removed (source route, …), to make it a simpler protocol, etc.

4. SSL/TLS, SSH, IPsec and WLAN

a) If you were designing a new application like an on-line game, which security protocol would you use, TLS, SSH or IPsec? Motivate your choice! (2p)

Likely TLS and use public crypto libraries since security will be built into the application. IPsec depends on the computer, SSH is a separate program (might work but you need to motivate this choice in that case…)

b) When using IPsec in tunnel mode the IP address is protected by an HMAC, but when using Transport mode it is not covered by the HMAC. Why is it protected in one mode but not in the other? (2p)

In transport mode, it is the final receiver that decrypts the packet, thus only one IP address is needed. If an attacker would modify this address, it would not reach the destination, but since it is encrypted it is useless to anyone who may receive it. However, in tunnel mode, it must be protected since this is the address of the host that receives the cleartext data.

c) If WEP would have been designed differently and had been using HMAC instead of CRC and AES instead of RC4, it would have been more secure. How secure? Would it still be vulnerable? Motivate your answer! (3p)

Still vulnerable but more secure. The user authentication process would be the same, no session crypto keys, no forward secrecy, many of the attacks would still work, etc. (details needed!)

d) Access points such as the ones mounted in the ceilings and walls at Calmers offer Eduroam acces using a Radius server. What advantage does Radius offer? Mention one security issue with this installation in some detail! (3p)

Radius offers user authentication, the AP does not have to keep track of users and users will have unique individual passwords.
Possible security problem is that a user with access to the wired network (which is in the room) can listen to the communication between the AP and the Radius server and perform one of the attacks against user passwords [described in the course].

5. Firewalls

What device or technology would you associate with the following statements?
Only one a few words is needed in the reply!

a) Can inspect all types of traffic, even understand some application layer protocols. (1p)
Stateful (deep) packet inspection firewall

b) It has problems with understanding the TCP protocol but IP is handled well. (1p)
Static packet filter (stateless) firewall

c) It can handle all application level protocols but replaces IP and TCP headers to mitigate attacks where headers are manipulated. (1p)
Circuit-level gateway

d) Hides the internal structure of the network and protects most services by changing IP addresses and port numbers. (1p)
NAT gateway

e) It separates traffic but still allows traffic to share network cables inside a company in a fairly secure way (1p)
VLAN technology

f) Coming generations of vehicles will communicate both with each other vehicles and with the infrastructure around them, with traffic signs and traffic lights and they will also use services from the Internet. If we assume that TCP, UDP and IP is used, we should be able to use conventional firewall technology to protect the vehicles from outside attacks.

Now you are given the task to test the firewall in a vehicle. You know nothing about it and how good (or bad) it is. Describe what tests you would do in order to be able to give good verdict about the quality of the protection it offers! (5p)

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

6. Misc. short questions

Please answer True or False to the following statements.
Correct answer **gives +1p**, an incorrect answer gives **-1p** so don't guess!
The total score from this question cannot be negative. (10p)

a) ARP *requests* can be a way to become a man in the middle.
TRUE – Everyone listens to the sender's address (IP and MAC) and remembers it, even if it is faked and incorrect.

b) Diffie-Hellman is vulnerable to attacks modifying the contents between the parties.
TRUE – We don't know who we are negotiating a secret with

c) If a FIN scan works through a firewall, it is stateless.
TRUE

d) If a SYN scan works through a firewall, it is stateful
FALSE

e) IVs are used in encryption to make the input match the block size of the cipher.
FALSE

f) MAC-then-encrypt is slightly better than Encrypt-then-MAC
FALSE – MAC-then-encrypt requires the receiver to decrypt the packet before the MAC can be checked.

g) IPsec needs help from UDP to pass through address translation gateways?
TRUE

h) MAC address flooding is an attack against a switch
TRUE

i) To prevent someone from hijacking a TCP session without being able to see the traffic, randomized TCP sequence numbers are useful
TRUE – If they were predictable, blind TCP hijacking would be simple

j) Rainbow tables are less useful in WPA3 than in WPA2
TRUE