CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2021-08-27, 14:00 – 18:00

No extra time for scanning at the end

All questions must be **clearly explained using your own words**. Answers are automatically sent to Ouriginal before they are corrected and it 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 and you may receive a warning when submitting your answer which can be ignored, 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

1. Attacks and DoS

a) When performing a SYN scan against a system, it may be possible to detect this activity at the target computer by a user or by an administrator. How? And what can an attacker do to make it harder to detect the scan? Explain! (2p)

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

b) Why could it be problematic for a system to deal with a packet that has an incorrect (faked) TCP length field that differs from the link-layer length? Describe two possible scenarios! (2p)

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.

c) Some port scans can be used to get information about the firewall that protects a system. Give an example and explain! (2p)

If an ACK or a FIN scan works through a firewall, it has to be stateless since it does not know whether the ACK or FIN packet belongs to a valid session or not. A stateful firewall would drop it unless the sequence number is valid.

d) Randomizing TCP sequence numbers is good from a security perspective. Why? What problem does it address? (2p)

It makes blind TCP guessing attacks (blind session hijacking attacks) much harder. If the numbers are predictable, it is much easier for remote attackers to insert valid data packets into an existing TCP stream.

e) The length field of IP is 16 bits long which means that a datagram can have any length between 0 and 65535. It is still possible to send larger IP datagrams, for example a datagram which is 75,000 bytes long. How? (2p)

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, WLAN

a) Encrypting traffic is not enough to guarantee freshness. Explain why not! Also mention two different ways to guarantee freshness! (2p)

Freshness is to make sure packets are not replayed which is possible even if they are encrypted. Including time stamps, sequence numbers or nonces can make it impossible to replay old packets. (Many answers possible here)

b) Kerberos can create session crypto keys to two parties who want to communicate. Why is it better to have the Kerberos server to do this than having the parties do it themselves? (2p)

The Kerberos server can create symmetric session keys which is easy to do (just random numbers) which can be sent securely since it shares a secret with both the applicant (client) and the server. If the client and server had to create session keys, they need to do complicated Diffie-Hellman calculations to agree on a key.

c) Both WEP and WPA2 uses 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, thus XORing two messages with each other would result in two plaintext messages XORed with each other. Also, identical datagrams would always have the same crypto text.

d) The first message in WEP is the 128-byte random challenge that authenticates the client. Why is this mechanism flawed? (2p)

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.

e) The Radius protocol is used in the Eduroam system. Why do you think it was selected? Is this a good choice? (2p)

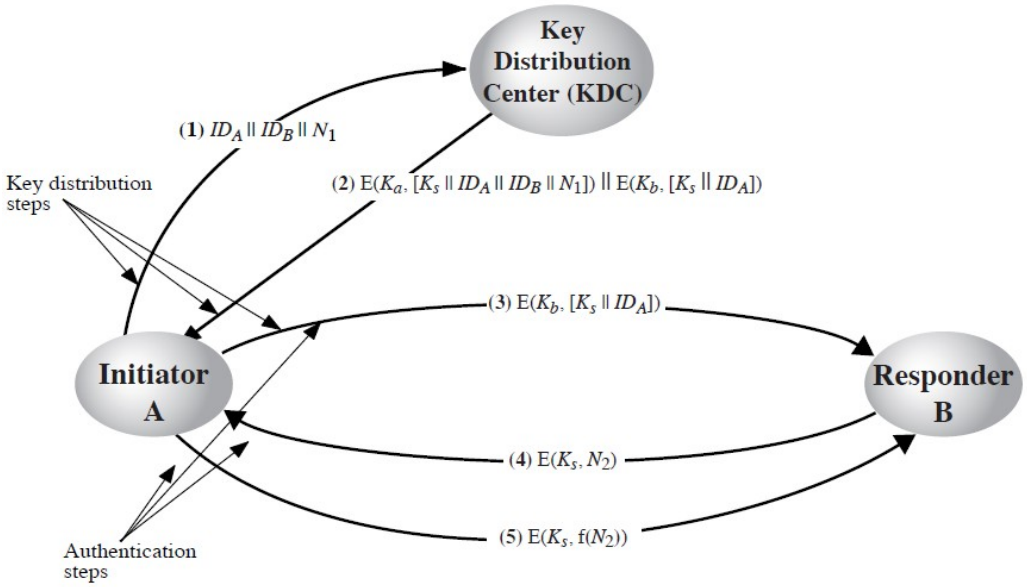
Radius offers user authentication, thus the AP does not have to keep track of users and their unique individual passwords. It is also organized in a tree structure which makes it easy to connect different subtrees (countries and organizations) together. This is a good example of where usability was prioritized and security to some extent was sacrificed (Radius is "relatively secure").

3. DoS and Secure Protocols

a) In the latest version of TLS, session establishment is faster due to the introduction of one-round-trip-time negotiation. Why is this faster? How is this possible? (2p)

Each round trip takes time and introduces a delay. It is achieved by letting the client guess what cipher suites the server accepts and what will be used. If the guess is correct, the negotiation can skip one step.

b) The picture below describes a Kerberos-like protocol. Describe with some detail each message that is transmitted and its purpose. Just repeating what is in the picture is not enough (like "a nonce is transmitted") but an explanation is needed for why it is transmitted and what the purpose of the message is. (4p)



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

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

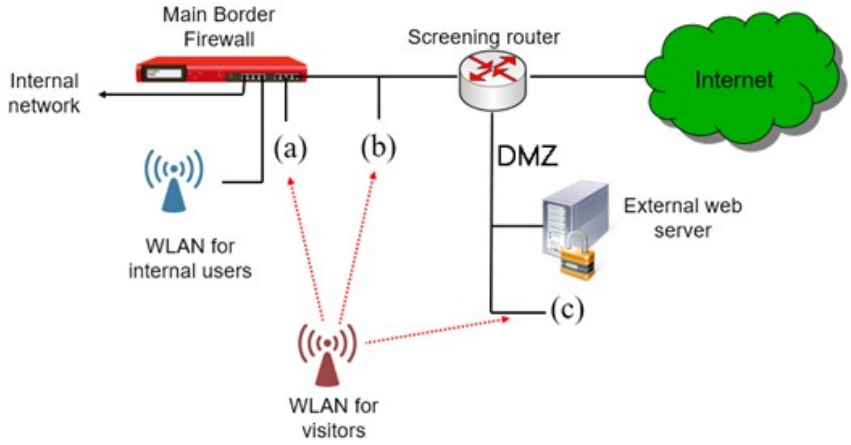
To guarantee freshness and that keys expire and are not valid forever.

d) What fundamental mathematical property is Diffie-Hellman based on? (2p)

That factorization of large prime numbers is time consuming (the discrete logarithm problem).

4. Firewalls and IDS systems

a) The picture below shows a company network with a firewall, a screening router, a web server and an access point for employees (internal users). Now they want to add another access point for visitors coming to the office and consider placing it at one of the positions (a), (b) or (c). The visitors should only be offered Internet access. Where would you place it? Motivate your answer and explain why you would or would not place it at (a), (b) and (c)! (3p)



(a) is the most secure location since the firewall can inspect the traffic and also make sure all traffic goes to the Internet. (b) is not good since it allows visitors to listen to the in- and outgoing traffic to the company (sniff the traffic). And (c) may allow visitors to monitor all traffic to the web server.

b) UDP traffic is in general harder to protect by a firewall than TCP traffic. Why? (2p)

TCP is a stateful protocol and includes sequence numbers and a well-known protocol for session setup. A firewall can check that this procedure is followed and that segments that are received fits into the communication stream. UDP has no setup procedure nor any sequence numbers so the firewall has no way to know whether a datagram with a faked IP address is legitimate or not but has to pass it to the receiver unless it understands the application level protocol.

c) Fragmentation of IP packets is a well-known problem for firewalls since they may not know how the receiving host will reassemble the datagram. Please give a longer explanation for why this is problematic! (2p)

If the firewall does not know how the end host will reassemble overlapping datagrams, it will either be making mistakes or it has to try all possible combinations to be on the safe side, but this is resource consuming and probably not realistic to do.

d) What could a solution to this problem be? (1p)

Either to know what systems it protects and how they reassemble fragments, or to drop all fragmented datagrams.

e) An active IDS system 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.

5. SSL/TLS and IPsec

a) A well-known problem in many security protocols is that an attacker in a short time can request lots of sessions with faked IP addresses and force a server to constantly calculate new session keys that are never used. IKE has protection against this. Explain how it works! (2p)

It stores the IP addresses and port numbers in a cookie which must be returned by the client before it starts calculating any keys. This makes sure that the receiver has not faked the IP address. The cookie is simply: hash(IP addresses, port numbers, secret). A client that requests lots of sessions from the same IP address can be blocked temporarily.

b) SSL/TLS has a "close session" message which is used when they want to quit. Why is it needed? Why not just tear down the TCP connection instead? TCP already has a mechanism to close connections. (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.

c) SSL/TLS has both master and session keys. What is the difference? How are they related? When are they created? (2p)

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

d) IPsec has a field "Next Header" as shown on the last page, which tells what upper layer protocol should receive the datagram. IP has a field called "Protocol" with the same purpose. Why does IPsec not use that field? (2p)

When IPsec encrypts a datagram, it replaces the receiving upper layer protocol in IP (such as TCP or UDP) with its own number and places the original content in its Next Header field. This means that the receiver in the other end will be IPsec, and when it decrypts the datagram it can restore the original Receiver field in the IP datagram.

e) Padding is an option present in many security protocols and can be used to make all datagrams of the same size (or of random size). Is this really needed? Give an example of when the absence of padding could be useful for an attacker! (Many answers are possible) (2p)

Access to a web server could reveal what pages the user is accessing by observing the amount of data being transferred.
Another example was in WEP where it was possible to identify ARP messages which could be exploited to inject own messages.

6. Misc. short questions

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) ARP can be used by an attacker to become a man in the middle on a local network.

TRUE

b) The use of VLAN offers encryption but it is not strong enough to be fully trusted.

FALSE (it does not encrypt anything)

c) An air-gap firewall does not support TCP.

TRUE (no responses/ACKs are allowed)

d) Diffie-Hellman enables two parties that have never met to securely negotiate a secret.

TRUE (they can negotiate a secret, but they don't know who the other party is)

e) In challenge response authentication, it is possible to encrypt the challenge with the user's password, or instead of using encryption, use a hash function. Both offer good security.

TRUE

f) Random numbers are often used in security protocols and are relatively simple to create.

FALSE

g) The Radius protocol is capable of protecting its traffic without help of, for example, IPsec.

FALSE (see slides)

h) The IP header does not have to be protected against modification when IPsec is used in transport mode.

TRUE

i) A Kerberos server is stateless and does not have to store any information about its current users.

TRUE

j) A self-learning switch may be fooled by someone who fakes lots of MAC addresses.

TRUE

Headers and pictures that may be useful