CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2020-08-28, 14:00 – 18:00

No additional time for scanning at the end – make sure
you can upload the exam in time and when/if you need to scan
something, notify the proctor before you start ☺

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 and you may receive *a warning which can be ignored*, but **longer explanations must 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

a) When scanning a system, in some cases like for example when doing a SYN scan, the attacker may immediately send a RST after a reply is received. How about when performing an ACK scan, would there be a reason to send a RST? Explain your reasoning! (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. But when an ACK scan is performed, the receiving host will not allocate anything and it will be completely invisible and changes no state on the host.

b) Is it possible to determine type and version of an operating system by observing TCP headers? Explain! (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. Different operating systems will 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. The applications do not need to be involved, i.e. no accounts on the server have to be available.

c) Is it possible to determine type and version of an operating system by observing UDP headers from it? Explain! (2p)

UDP traffic only contains source and destination ports, a checksum and the packet length. There is no operating system dependent information in it.

d) IP has a counter field that is decremented when a router processes the packet. Give an example how it can be used to increase security! (2p)

This is the TTL, time to live field. If a border firewall normalize the TTL values for incoming datagrams (e.g. set TTL to 255), internal systems will know that this is external traffic. It also prevents the value from being decremented to 0 and a possible ICMP Time Exceeded message to be transmitted back.

e) Is it a good idea to select the initial sequence numbers for a TCP session randomly? What would the advantage (or disadvantage) be? (2p)

To prevent *blind* TCP hijacking ISNs should be random. If not, attackers may be able to guess sequence numbers used in connections and insert their own segments.

2. Security protocols

Which security protocol (SSH, SSL/TLS, IPsec) do you associate with the following terms or features? Pick the most suitable protocol for each question and motivate briefly your choice.

a) Certificate authentication (1p)

SSL/TLS. SSH uses host keys, IPsec may support it but SSL/TLS is widely used in all web browsers and all web servers have certificates.

b) Transparent access for all applications (1p)

IPsec. It is designed for transparent access and all protocols running on top of IP is supported. SSH and SSL/TLS is not that transparent, the application must be installed and requires configuration on the client side.

c) Suitable for securing own-developed client-server application (1p)

SSL/TLS. It is designed to be included in applications where only a suitable library is needed.

d) Least suitable for securing an own-developed client-server application (1p)

IPsec since it requires operating system support to encrypt traffic on IP level.

e) We have discussed the use of master secrets in the course and that they should be used as little as possible. Why? What is the master secret then used for? (2p)

The master secret is used to create other keys, for example session keys that are frequently changed. We should never use the master secret directly, for example to encrypt traffic or use it in challenge-response authentication since this gives a potential attacker the possibility to compromise it - the more it is used, the more material is given to a potential attacker.
And maybe more important, if a session crypto key is compromised, damage is limited if it is frequently changed.

f) IPsec has a window to protect against replays. Assume that it currently accepts datagrams with numbers between 100 and 200. What happens if a datagram comes in with number 90? And if a datagram with number 320 arrives? Explain! (2p)

Datagrams below 100 will be dropped to prevent duplicates. When number 320 is received, the window is moved to contain that datagram, i.e. it will now accept 220-320.

g) What is the advantage of having four different keys for encryption as in SSL/TLS? Explain with some detail! (2p)

If one key is cracked, for example the packet encryption key from A to B, it is possible to read traffic in that direction but not in the opposite direction. It is also not possible to change the contents of any packets since other keys are used to protect them.

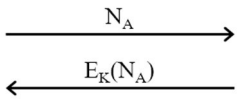
3. Authentication

a) Certificates contain several fields, for example public key, identity of the holder and an expiration date. But for a certificate system to be really useful, it must also be possible to withdraw/cancel a certificate. Why? What could likely have happened when it is necessary to withdraw it? How can cancellation be done in a real implementation? (2p)

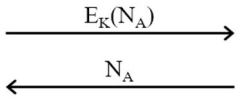
If the owners private key is disclosed, for example after a security incident, anyone can pretend to be the owner and there is no way for clients to know that it is compromised. Therefore, certificate revocation lists (CRLs) need to be distributed to clients regularly so the know what certificates no longer can be trusted.

b) Below, we have three different *authentication* methods or scenarios. For each, describe in what situations it can be useful (i.e. what it offers)!
N = random number (nonce), K = shared key, f = hash function (3p)

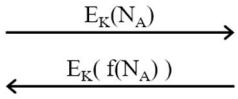
1:



2:



3:



All scenarios serve the same purpose:
Scenario 1: The receiving party (B) shows that it is in possession of the shared secret and is authenticated. B knows nothing about A since Na is a random number it knows nothing about.
Scenario 2: Similar to scenario 1: (A) knows that (B) can decrypt the nonce thus is in possession of the key.
Scenario 3: Same as scenario 1 since (B) knows nothing about now Na was selected and cannot authenticate (A). The result is still that (B) proves that it is in possession of the key K. (This scenario does not reveal Na and is likely better if the number Na is not created from a good random number generator.)

c) In example/scenario 1 above, would it be possible to replace the encryption $E_K(N_A)$ with a hash function $f(K, N_A)$ and still be secure? Explain! (1p)

It is ok. Assuming the hash function is good enough, an attacker cannot guess what the reply from B is regardless of whether it is encrypted or hashed.

d) Why are nonces used in many authentication protocols?
It may be possible to perform authentication without nonces. Give an example! What is the drawback with that method? (2p)

The nonces are used to create something that is never reused and show that the connection is fresh and not a replay (if it was reused, an attacker may know the answer

for example in scenario 1 above). An alternative could in many cases be to use timestamps but it requires all parties to have synchronized clocks.

e) Kerberos servers do not keep state. How is that possible? Give two advantages with not having to keep state! (2p)

The client gets a ticket which contains the state information the Kerberos needs. It is encrypted by the server and cannot be decrypted by anyone else. Advantages:
- There is no real limitation to number of clients it can work with. No state is stored.
- It is easy to have a cluster of servers or redundant servers that process client requests and they can be completely independent of each other – no communication or shared state is needed.
- If the Kerberos server goes down, it can be restarted and does not have to recover client information or client states
- Authentication and Authorization servers can be different entities and do not have to communicate
- …

4. Firewalls and IDS systems

a) IP fragment reassembly policies may differ between different systems on a network. This may cause problems for IDS systems. Give *two* different examples that may be a problem for an IDS system and explain how the IDS system may deal with the problems. (2p+2p)

Overlapping fragments: Depending on what kind of system receives the fragments, the datagrams will be assembled in different ways. The IDS system may not reassemble them in the same way as all end systems do. One possible solution is that the firewall knows what systems different hosts on the internal network have and how they deal with fragmentation.

Timeout: There may be long delays between the fragments and some hosts may discard already received fragments if it is too long. If the IDS system does not know this, it may keep it and end up with different contents than the end system. (Several answers possible here – many problems exist!)

Assume that you are responsible to design a firewall system for a company with 100 employees which has two offices, one in Göteborg and another in Stockholm. There are several things to consider and the task for you is to motivate some design choices that you make. *There is not just one correct answer or one possible design, so the motivations for the decisions that you make are important!*

Also note that your solutions to question b, c and d must be compatible and work well together, we don't want not three independent solutions that barely work together.

b) Should we have a main border firewall only or spend some money on a screening router? Briefly elaborate about pros and cons about the two solutions! (2p)

Not very expensive to have a screening router, the router may likely already exist. Offloads main router some work. Some protection if main router is incorrectly configured. (Many answers possible)

c) Transparent access to servers in the other office is also needed, i.e. Göteborg employees working in that office need access to servers in in Stockholm and vice versa. This may be solved with either IPsec, SSH or using VLAN technology. What would you chose? Motivate! (2p)

VLAN is not an option. It is not encrypted and will not work over the Internet.
IPsec will be transparent to the users and allow all types of access. SSH will work but needs to be configured for each service to be used so it may be an option (motivation needed if you go for this choice).

d) Remote access to the offices is needed. This means that home users and travelling users must be able to securely connect to their servers in both offices at the same time. How would you solve remote access? Explain! (2p)

SSH tunneling is a good option if a few services should be used. IPsec if universal access is needed, but then a firewall in the server end should limit what it allows to the corporate network. IPsec requires the home user to be administrator to configure the system, which may be problematic for some users. SSL/TLS may also be an option.
The important here is to get a motivation for your choice!

5. WLAN and link level security

a) Mention one attack on link level that makes it possible to become a man in the middle and receive all traffic to and from another system! Explain how and why it works. Also, mention a way to protect our network against this attack! (3p)

ARP spoofing is a possible attack. ARP spoofing is a way to erroneously send or respond to ARP queries on the network ("who has IP address 1.2.3.4?") and make computers send IP messages to the attacker's computer instead of to the correct destination. Most systems will accept the first answer they get and treat it as valid. This way it is possible to spawn man in the middle attacks. Possible protection can be to define important IP-address to MAC address translations as static (use static ARP entries), Try old MAC address before updating entry to new address (Linux "Antidote" patch). Don't accept changes in IP-address and MAC address mappings (manual reconfig needed).

b) Mention another attack on link level which could be used if the attack in question (a) cannot be used! Explain how it works and describe a way to protect the network against it! (3p)

DHCP spoofing: An attacker may also answer DHCP requests in order to become a man in the middle. The computer that asks what IP address to use and the address to the default gateway will accept the first answer it gets. Some switches have a "trusted ports function" which means that it only allows preconfigured ports to answer DHCP requests.
Other attacks also possible, MAC flooding to be able to listen to traffic, etc.

The WEP authentication method is flawed and makes it possible for an attacker to (1) crack a user's password, and (2) to use the access point to transmit messages even if the password could not be cracked.

c) How can the password be cracked? Explain! (2p)

The server sends a 128-byte string to the client which is encrypted with the shared secret. It is possible to do an off-line exhaustive search of the password (e.g. using Rainbow tables) since the attacker sees both the challenge and the response.

d) Why can the access point be used to transmit messages even if the password was not guessed? Explain with your own words! (2p)

A problem is that same method is used both for authentication and packet encryption, which means that the attacker gets a cleartext message and a ciphertext message for a given IV and by XORing these, he/she gets a 128 byte keystream which can be reused over and over again sending own packets.

6. Misc questions

Please answer True or False to the following statements. *No motivations are needed.*
Correct answer **gives +1p**, an incorrect answer gives **-1p** so don't guess!
The total score from this question cannot be negative. (10p)

a) Diffie-Hellman can be used to negotiate secrets, for example session crypto keys. It only offers weak authentication of the parties which, with few exceptions, cannot be trusted.
False – no authentication is offered at all

b) IPsec has a window to protect against replays, to make sure no duplicates are transmitted and no datagrams are lost.
False – it protects against duplicates and replays, not against reordering and lost datagrams.

c) IPsec adds its own IP header in tunnel mode which is not protected by the HMAC. If an attacker modifies this header, the result is just that another system receives a useless encrypted datagram.
True

d) TLS is not sensitive to Network address translation done by firewalls.
True – it does not deal with IP addresses at all

e) The length field of an IP datagram is 16 bits long which limits the maximum IP datagram size to 65,535 bytes.
False – fragmentation and playing with the offsets makes it possible

f) Web servers are typical targets for SYN flood attacks
True

g) Rainbow tables is a method to save CPU time but instead requires more space for storage.
False – it saves space and needs more computational resources

h) Circuit level gateways protect servers against TCP and IP packet header modification.
True

i) The main purpose of the IV present in WEP and WPA2 is to make sure two identical packets are encrypted differently.
False – it has this function but more important is to create different key streams for all packets

j) MITM attacks against virtual LAN technology is possible
True