CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2021-05-31, 08:30 – 12:30

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) There are different ways for an attacker to perform DoS attacks, one way is to exhaust system resources. Give an example of such an attack and the reason why it can become problematic for a server! (2p)

Many answers are possible, for example SYN flooding of a server where its connection table fills up and other legitimate connections are refused.

b) Another possibility for an attacker to perform a DoS attack is to try to trigger implementation bugs in protocols. How can this be done? Give two practical examples! (2p)

Abuse header fields, for example send TCP segments with invalid lengths that differ from the real length, or send IP packets with the source address equal to the address of the receiver. [See IP and TCP lectures for other examples]

c) What can be a possible reason for an attacker to send TCP segments with both the SYN and FIN flag set at the same time? (2p)

To test the stability of the IP stack by sending illegal and malformed packets and observe its behavior. Smaller devices with optimized network stacks may crash or system resources may be allocated without ever being freed.

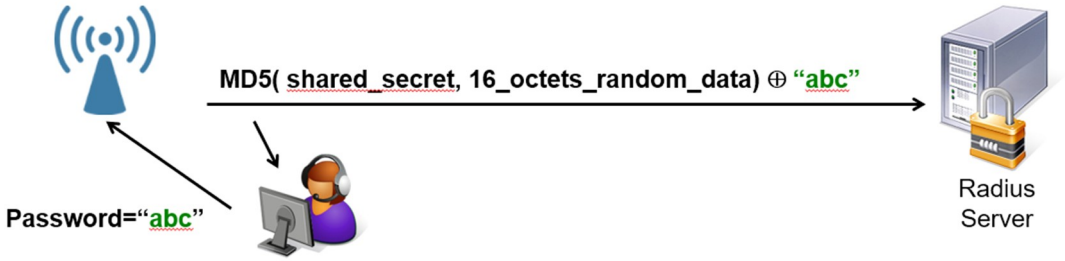
d) What is required for an attacker to be able to insert data into another user's ongoing TCP session to a web server if the attacker cannot see the traffic between the parties (i.e. the attacker is not a MITM)? Assume the connection is not encrypted and that the attacker is able to guess the IP addresses of the two parties, how easy or complicated is it to perform such an attack and succeed in inserting own data to their session? (2p)

The attacker must guess the TCP sequence numbers the parties are using to be able to insert a segment into the receiver's window. In addition, the source port-number must be guessed but since it is a web server, the destination port number is known (80).
So what must be guessed is a 16-bit port source number and the 32-bit seq. number. If we assume the receiver's TCP window = 64kB, then 16 bits remain to be guessed. This means that the attacker must send 2^32 = 4 billion packets to be sure to hit the receiver window. (This would take 5 hours on a 100 Mbps link to transmit.)

e) Is it easier or harder to do this attack if the communing parties are located on different continents than very close to each other? Assume that the connection speed is more or less equal. Explain your reasoning! (2p)

It will be easier. A connection with longer delays and high speed must allow for more packets to be in transit to optimize performance (bandwidth-delay product). It also means that such a connection has a larger receive window, thus maybe only 8 bits of the TCP sequence number has to be guessed.

2. Authentication, WLAN



a) In the picture above, we can see an attack against a Radius server. What is the purpose of this attack? What is it the attacker tries to do? Explain! (2p)

The only unknown in the request to the Radius server is the "shared secret" and it may be possible to do (an exhaustive) search to find the secret. The secret could be a word from a dictionary, for example.

b) Can a rainbow table be of help to the attacker in the example above? Why/why not? (2p)

It is not useful since the hash (MD5) contains random data. This data is known by the attacker but it is impossible to create pre-calculated tables since each message is unique.

c) WPA3 is the latest WLAN security protocol and it guarantees that all session keys are unique for the session and that they are not in any way related to other session keys. However, the current and most used protocol today, WPA2, does not have this property.
What is this property called? Why is this a good property?
Also explain how this is normally achieved and what "mistake" WPA2 does! (3p)

The property is called (perfect) forward secrecy and means that older and future sessions should not be compromised if a session keys ever broken.
This is normally done by using Diffie-Hellman key agreement to make session keys unique and never reused.
WPA2 calculates session keys from the master key which is derived from the SSID + Password/shared secret (and by an attacker some known random values). If the password is revealed, session keys for all other sessions can be recalculated.

d) Kerberos is a good protocol performing both authentication and authorization. It has some advantages and at least one disadvantage:
1: it uses symmetric keys;
2: the tickets handed over to the clients contains its internal state;
3: however, it requires applications to be Kerberized.

Explain these concepts and what the advantages and disadvantage mean! (3p)

1. Symmetric keys are easier to work with than asymmetric keys and eliminates complicated calculations.
2. This makes servers stateless and many servers can share the workload without consulting each other or a common database
3. Applications must understand the ticket concept and how they should be used

3. Secure Protocols

a) IPsec can operate in both Tunnel and Transport mode. In Tunnel mode, a new IP header has to be inserted. Why?
Also, the new address is not protected by the MAC. Why is this not needed? (2p)

A new header is needed since it is not at the datagram's final destination it is decrypted. The address to the system decrypting the datagram can be modified by someone (MITM) and it will be sent to another destination. However, it is encrypted and useless for the receiver.

b) How is freshness of data packets guaranteed by the TLS record layer protocol? There are no sequence numbers in the header. (2p)

It uses implicit sequence numbers, i.e. both sides counts number of packets and this counter is included when calculating the MAC. This ensures that replays are not possible and that packets are not replays from the past.

c) SSH uses a (keyed) MAC which is calculated from the plaintext data to protect against modification. What is the drawback/danger of using with this method? (2p)

It means that the receiver must decrypt the packet before the MAC can be checked. This is the "Encrypt-and-MAC" method which may cause additional work for a receiver if garbage packets are sent to it. It can also be dangerous (may trigger bugs) if the receiver has to process data packets before it knows they are authentic and correct.

d) What other two alternatives to the SSH method above exist? What are the pros and cons of these? (2p)

We also have MAC-then-Encrypt (as in TLS) with the same problem as in SSH, and Encrypt-then-MAC (as in IPsec and TLS 1.3). The latter offers ciphertext integrity but no plaintext integrity but should not really be a problem. [see slide 49 in TLS lecture]

e) Diffie-Hellman key negotiation is computationally expensive which means that an attacker can trigger such computations in order to cause excessive load on a server. Some protocols have protection against this. Mention one such method! (2p)

IPsec is one example where the server sends a cookie to the client requesting an IPsec session (using IKE). The cookie contains a hash of the source and destination IP addresses, port numbers and a secret. This must be returned by the client and guarantees that the sender has received the packet (prevents use of random IP addresses).

4. Firewalls and IDS systems

a) In the course, we have discussed that it is becoming increasingly important to help the main border firewall by moving protection to the endpoints. What are the arguments behind this change? What has happened now that motivates a new way to think when protecting corporate networks? How should we think in the future? (4p)

See the slides about network design and "The Jericho Forum" and how to replace the medieval ring-wall architecture. In short: users are no longer located only inside at the corporate network, we have WLANs, users should have different roles at different servers and applications, access may have to be different based on what device is being used, etc.

b) A stateful firewall must maintain a list of filter rules and also a state table. Give an example of what the state table should contain for TCP and UDP traffic! (2p)

TCP: port numbers of communicating parties, TCP sequence numbers, TCP state
UDP: port numbers and a timer for when to terminate the connection

c) Suppose you can choose between using either a stateless screening router as a firewall or a NAT gateway to secure your home network. Which would you choose? Compare the two solutions, what advantages and disadvantages they have? Motivate your decision!
(There is no right or wrong answer, motivating your decision is what is important.) (4p)

The stateless firewall can inspect contents of packets, including some application-layer protocols but will not see the relation between packets and cannot check TCP sequence numbers, for example. It will not be very secure and it may cause some security problems.

The NAT gateway on the other hand will only give access to systems found or listed in the translation table. However, it does not inspect traffic to servers so allowed traffic will not be inspected at all.

5. Link layer security and VPN systems

a) On a local network, it may be possible for an attacker to pretend having lots of MAC addresses to confuse more intelligent switches. Why? What could be the reason an attacker performs this action? (2p)

More intelligent switches can learn where hosts (MAC addresses) are located and will normally not forward private traffic between two ports to any other ports. The attacker's goal is to overflow the switch memory with garbage MAC addresses to make it forget the real MAC addresses and force it to broadcast all traffic to all ports. This enables the attacker to listen to all ongoing conversations.

b) An attacker on a local network may be able to redirect traffic from other hosts to his/her own computer. Give two examples of how such attacks can be done! (2p)

It is possible to fake ARP packets on the network with other hosts IP addresses. Another possibility is to send false replies to DHCP requests to become the default route for systems.

c) What is the main difference between using VLAN technology and IPsec to secure a network? Would you use VLAN to create a virtual course lab at Chalmers with lab computers at different locations in the EDIT building? Motivate your answer! (2p)

VLAN does not encrypt nor protect the messages against modification. But it may be a good solution if the purpose is to separate the course lab traffic from other types of traffic. VLAN can be used to make sure that traffic from the lab is not forwarded to office computers and servers but still be sharing the same physical network.

d) What protocol would you select when building a VPN system for remote users who need to access various services inside an office? TLS, SSH or IPsec? There may be several acceptable solutions to this question so please motivate your answer! (2p)

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

e) What would the purpose of using the 802.1X protocol in a switch be? (2p)

To implement user authentication before network access is granted.

6. Misc. short questions

<u>One short sentence</u> is enough to motivate the answers of (a) to (e).
Question (f) to (j)only require "True" or "False" as an answer, no motivation is needed.
1p per question, incorrect answer = 0p

a) Why do we often see nonces in security protocols?

To guarantee freshness and prevent replays of older sessions

b) Why do we (sometimes) see time stamps in security protocols?

Also to guarantee freshness and prevent replays of older sessions

c) TCP segment reassembly can be problematic to an IDS system. Why?

It may not know how the receiving host reassembles overlapping fragments

d) IPsec has sequence numbers. Why?

To make sure duplicates are not delivered (which could cause problems for, for example UDP which lacks sequence numbers)

e) UDP scanning is often harder to do than TCP scanning. Why?

TCP responds with a SYN/ACK to a connection request but UDP just delivers the data to the application and we don't know how it will react.

f) Diffie-Hellman guarantees that two parties share a common secret but not who the other party is.

TRUE

g) WEP allows the same IV to be reused. This makes it possible to reuse key streams.

TRUE

h) Disabling SSID broadcasts in an access point is only "security by obscurity", not really something offering good security.

TRUE

i) TTL in an IP datagram can be used by an attacker to see if a host is available.

FALSE

j) Circuit-level gateways/proxies remove all headers and replace them with new fresh headers to make sure packet modification attacks do not work.

FALSE (works on transport level, application level headers are not touched)

Headers and pictures that may be useful