CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2022-08-25, 14:00 – 18:00

SB Multisal

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

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

Write in a clear manner and motivate (explain, justify) your answers. 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 and explain 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) UDP scanning is harder to do than TCP scanning. Why? What is the problem? How can operating systems, at least to some degree, protect themselves against leaking information about open UDP ports? (2p)

It is hard to know whether a UDP message is accepted or silently dropped. However, if a host responds with an ICMP (port unreachable) message, it is not open. Protection can be to limit the number of transmitted ICMP messages to, for example, one per second.

b) In the Smurf attack, ICMP echo or UDP is used to do *packet magnification*. How does such an attack work? How can this problem be addressed? (2p)

It sends the messages to a broadcast address with a victim as the sender. All hosts on the network will then send an a reply message to the victim, thus one packet generates a storm of packets to the victim. Firewalls should block all external traffic to broadcast addresses to avoid its hosts to be used as senders of the traffic.

c) The goal of some DoS attacks is to try to exhaust the resources of the target, for example memory, internal tables, network, or the CPU. Briefly describe <u>two</u> possible DoS attacks targeting different resources and what weaknesses they make use of! (2p)

Examples: SYN attack (exhausts connection table), repeated requests for encrypted TLS connections (CPU exhausted), …

d) The possibility to fragment IP datagrams has shown to be problematic. Describe two different problems or attacks which exploits fragmentation and explain how they work! (4p)

* Fragment reassembly (DoS): send only one fragment per datagram making the receiver allocate buffer space for the full datagram.
* Fragment ID reveals information (OS fingerprinting).
* IDLE or Dumb scanning using a trusted system to check available resources (see slides).
* Send oversized datagrams (> 65,535 bytes) using fragments.

Etc.

2. Authentication and WLAN

a) Assume that a server which wants to authenticate a user (a client) over a network is designed to request the client to encrypt the *username* + *password* with the server's public key and send it to the server. The private key is at all times kept secret and the encryption algorithm cannot easily be broken. Is this a good solution or not? Explain! (2p)

What is sent over the network is encrypted, but it can be used in replay attacks by an attacker. Nothing makes it unique and it can be used over and over again.

b) Shared keys that are used in, for example, WLAN authentication is both good and bad. Give one advantage and one disadvantage with using it! (2p)

Easy to maintain – just one key. No individual user authentication possible. Harder to change keys – all users must change at the same time and somehow get the key.

c) Explain how encryption of data traffic is done in WEP! A figure together with explaining text is needed. You need to show how encryption is done including input and output to the system. (2p)

See the WLAN lecture and the slide explaining encryption. The answer should contain the Key, IV, CRC, PRNG, the XOR-operation and what is transmitted to the receiver.

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

See the slides for weaknesses in WEP.

3. Firewalls and IDS systems

a) If you are given the task to test whether a firewall is stateful or not, how would you do this? Describe what test you would perform and the expected result! Explain clearly why this test would work! (2p)

We could do an ACK or a FIN scan. All normal systems respond with a RST packet to non-matching ACKs (RFC 793). A reply from a system behind the firewall means that the firewall did not keep state and had to forward the ACK to the inside. A stateful firewall would silently drop the packet.

b) 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.
The firewall must also keep track of the TCP state and TCP sequence numbers.

(Real firewalls store more information but this information is at least needed for a firewall to be called stateful.)

c) What is a DMZ and what purpose does it have? (2p)

It is a dedicated network outside the internal network which host external services, such as web servers, mail servers and other systems offering services to the outside world (see lecture slides). Purpose is to avoid forwarding traffic to public servers to the internal network.

d) NAT gateways are strictly speaking not firewalls, but they are still useful and can in many situations replace a conventional firewall.
- What level of protection do they offer?
- What do they lack which normal stateful inspection firewalls have? (2p)

They hide internal systems from the outside network. In short, a service not present in its translation table is not visible/accessible from the outside.

It does not inspect traffic that is allowed to traverse (as done in a conventional firewall).

e) Firewalls must be able to handle UDP traffic, but there is a fundamental problem with it that does not exist for TCP traffic. How can a firewall handle UDP connections from the "inside" to the "outside"? Is this a good (secure) solution? Assume that the firewall does not understand the application level, thus cannot inspect these datagrams and the replies. (2p)

Unlike TCP, there are no sessions to keep track of and no sequence numbers. One outgoing datagram may result in one or more replies from the outside.
When a request packet is sent out from the trusted side, it can allow replies from the outside, but only from the same host and port number that received the first packet and only for a limited time period.

4. Cryptographic protocols

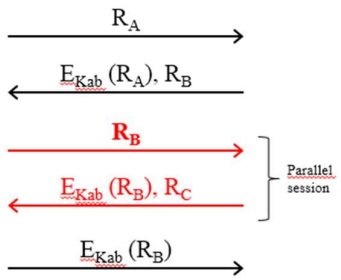
a) Even if we encrypt network traffic with the best cipher available, it is still possible to change the contents and also to replay the packets. How can this be solved? (2p)

We should use cryptographic hashes (such as HMAC) to protect the packet from modification and add freshness guarantees, for example by using sequence numbers or time stamps.

b) Some protocols create four or more keys from a Master secret, for example a Server write key, Client write key, Server MAC key and a Client MAC key.
What is the purpose of all these keys? Why so many and not just one "encryption key"? (2p)

Client and Server write keys are used to encrypt messages, Client and server MAC keys to create secure hashes i.e. the HMAC (message integrity). The client keys are used in one direction, the server keys in the other.

c) Some protocols are vulnerable against reflection attacks as shown in the figure:



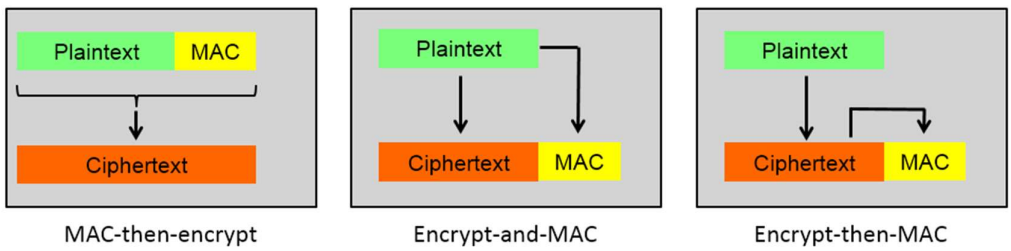
What is meant with a reflection attack? Explain how this attack works and how it can be avoided! (2p)

It is an attack where a completely symmetric protocol can use the originator (server) to answer the question it asked the client to answer. See slides from "User authentication" lecture.

d) What makes hash functions such as MD5, SHA-2, etc. fundamentally different from a CRC when protecting message integrity? (2p)

A message that is protected by a keyed hash cannot be modified without having access to the full input, i.e. the key and the message. With a CRC, it is possible to change parts of the message and predict what to change in the CRC without having access to the original message, even if the message is encrypted.

e) In the course, we discussed three different ways to add MACs: MAC-then-encrypt, Encrypt-and-MAC and Encrypt-then-MAC, see the picture below.



There are some pros and cons with each solution. IPsec uses the last method (Encrypt-then-MAC). Give an argument for or against Encrypt-then-MAC when compared to the other. Motivate clearly why this is (or is not) advantageous! (2p)

Encrypt-then-MAC makes it possible to check the integrity of the datagram before sending it for decryption. It both saves processing time but also prevents attacks against the crypto-engine with specially crafted datagrams.

5. TLS and IPsec

a) TLS consists of several protocols. Describe the functionality of the *record layer, change cipher* and *handshake protocols* (see picture on the last page). (3p)

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) 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) On the last page, there is a picture of an IPsec header. Explain what the *next header*, *SPI and padding fields* are used for and what purposes they have! (3p)

The SPI is an index that tells what SA (security association) should be used, i.e. a pointer to a data structure containing info about the type of connection, keys used, etc.
Next header tells what upper layer protocol should receive this data.
Padding: to disguise to an attacker the actual amount of data being transmitted.

d) In tunnel mode, a new IP header is created. Why? Why is this not necessary in transport mode? Explain! (2p)

In tunnel mode, it is not the final (original) receiver of the datagram that should receive the encrypted datagram. Tunnel mode is often transparent to the original sender and receiver.

6. Link level security and network design

a) What is the reason lots of link layer devices such as access points (APs) support Radius? What advantage do they get from it? (2p)

To implement user authentication without having to keep its own database.

b) VLANs (virtual LANs, IEEE 802.1q) can be used to achieve some level of security. Explain the general idea of it and how it works and what types of network devices can handle it! Also, give an example with a picture how it can be used! (4p)

VLANs can be used to isolate/separate traffic on a LAN into virtual LANs. All packets sent out can have a tag identifying it (tagged VLAN) or be without tags if the network devices keep track of where packets are received (interface/port). It can be handled by switches and routers as well as by individual workstations (computers). It can be used to control how packets are sent on the network and who can communicate with who, thus allows the creation of "workgroups".

For a picture, see the slides.

c) Some more advanced switches may have more "intelligent" functionality than a plain dumb €10 switch and can prevent some link layer attacks. VLAN technology can be one such functionality, but describe *two other* possible functions they can have and explain what attacks they protect against! (4p)

- Limit number of MAC addresses per port – protects against MAC address flooding which may force a switch to broadcast all packets to all ports
- Trusted ports – limit what ports are allowed to answer, for example, DHCP requests
- Lock MAC addresses to ports
- Functionality to detect IP address spoofing (MAC-IP address monitoring)

etc.

Headers and pictures that may be useful