CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2019-03-06, 08:30 – 12:30

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

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

Give clear answers. Your thoughts and ways of reasoning must be clearly understood! Questions must be answered in English.

Teacher: Tomas Olovsson
Dept. of Computer Science and Engineering

Questions during exam: Tomas Olovsson, 031 - 772 1688

Inspection of exam: See web page for announcement

CTH Grades:	30-38 → 3	39-47 → 4	48-60 → 5
GU Grades:	30-47 → G		48-60 → VG

1. Attacks

a) The TTL (time to live) field in an IP datagram can be useful when an attacker wants to create a network map. Explain how this can be done! (2p)

Each router in a path decreases TTL in the IP packet with one, and when it reaches zero, an ICMP message is sent back to the source telling it what router discarded the message. Therefore, an attacker sending a packet with increasing values of TTL (1, 2, 3, etc.) to a host will provide info about what routers exist in the path.

b) TTL can sometimes also be used to fool firewalls and intrusion detection (IDS) systems. How? Mention a possible protection mechanism against this attack. (2p)

Low TTL values may cause some datagrams to be discarded by routers which in turn may result in that the IDS system and the receiving hosts having different meaning of what has been communicated over the network. Border routers could normalize incoming TTL values to a standard value, say 20.

c) An attacker may try to flood a server with SYN packets using faked IP addresses. Why would he/she try to do so? What would the gain be? Mention two possible remedies to this attack! (2p)

d) RFC 793 requires that TCP initial sequence numbers (ISNs) always differ and are unique in order to detect duplicates from retransmitted segments. For security reasons, we have higher demands than ISNs just being unique. What are these? Why? (2p)

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

e) The SMURF attack uses ICMP echo packets and is called a magnification attack. Explain how it works and how firewalls connected to the Internet should be configured to prevent such attacks. (2p)

It sends ICMP echo messages to a broadcast address with a victim as the sender. All hosts on the network will then send an ICMP echo 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.

2. Authentication

a) In radius, when a client contacts the server to authenticate a user, it sends:

- Request code 1 (access request)
- ID (sequence number)
- Length
- **MD5(shared_secret, 16_octets_random_data) ⊕ password**

and

- **MD5(full_message, shared_secret)**

Explain the purpose of the two hashes! Also explain their parameters (shared_secret, 16_octets_random_data) and why they exist! (4p)

Shared secret = crypto key, a secret the client and the Radius server share.
16_octets_random_data = data making the transmitted data packet unique.

The first MD5 field enables the server to check the password. Since the packet is not encrypted, the shared secret makes it impossible to retrieve the password if someone is listening to the communication.

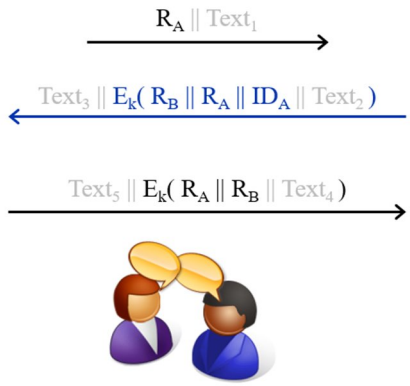
If the second MD5 field does not match, the Radius server will not respond to the request (silent drop). Only clients knowing the secret may request authentication.

b) What is Diffie-Hellman key agreement used for? (2p)

c) Is Diffie-Hellman vulnerable to MITM attacks? Explain! (2p)

Yes, there is no authentication. It is possible to agree on a common secret with someone (e.g. an encryption key) but it is not possible to know who the other party is.

d) ISO 9798-2.4 describes three-pass mutual authentication using symmetric key encryption between two parties who share a common key:



Explain the purpose of the messages and what is achieved in the steps! (2p)

A sends a random number to B who responds with encrypting it with the shared key together with a new random number. This proves to A that B is in possession of the shared key and is alive (it is not a replay of an old session). A now decrypts the contents and sends back B's random number encrypted to prove that A is also in possession of the key and is alive.

3. Secure protocols

a) SSL/TLS has a special message to close a connection. Why is this message present, why not just send a TCP FIN segment and let TCP close the session? (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.

b) An SSL/TLS certificate can be used to identify a web server. What happens if an attacker manages to spoof the DNS response (for example for *mybank.com*) which causes the client to connect to the attacker's address instead of the correct IP address? What happens? Motivate your answer! (2p)

The web browser checks that the domain name in the certificate matches what the user typed in the web client and the server needs to prove it is in possession of that certificate's private key. (If the server authentication fails, the web browser displays a warning message.)

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

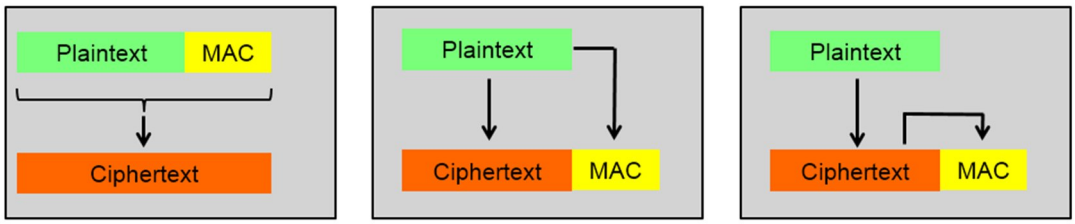
In tunnel mode, it is not the final receiver of the datagram that should receive the encrypted datagram but a host that decrypts it and forwards it to its final destination. Tunnel mode is often used for transparent site-to-site encryption.

d) What is (Perfect) Forward Secrecy? How can it be achieved? (2p)

It is a way to guarantee that if the main key (e.g. an asymmetric key belonging to a certificate) is compromised, it should not be possible to decrypt other sessions. The session keys should be independent of this key.

Using Diffie-Hellman or Elliptic Curve key exchange guarantees unique keys for each session.

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.



MAC-then-encrypt Encrypt-and-MAC Encrypt-then-MAC

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.

4. Firewalls and remote access

a) Suppose you are responsible for a small company network with 15 employees, and you want to connect it to the Internet. You are considering two different firewall configurations:

1: A stateful "deep packet inspection" firewall

2: A NAT gateway as the firewall

Compare the two solutions and discuss advantages and disadvantages with them. Discuss what types of attacks they may be vulnerable against, if any. (3p)

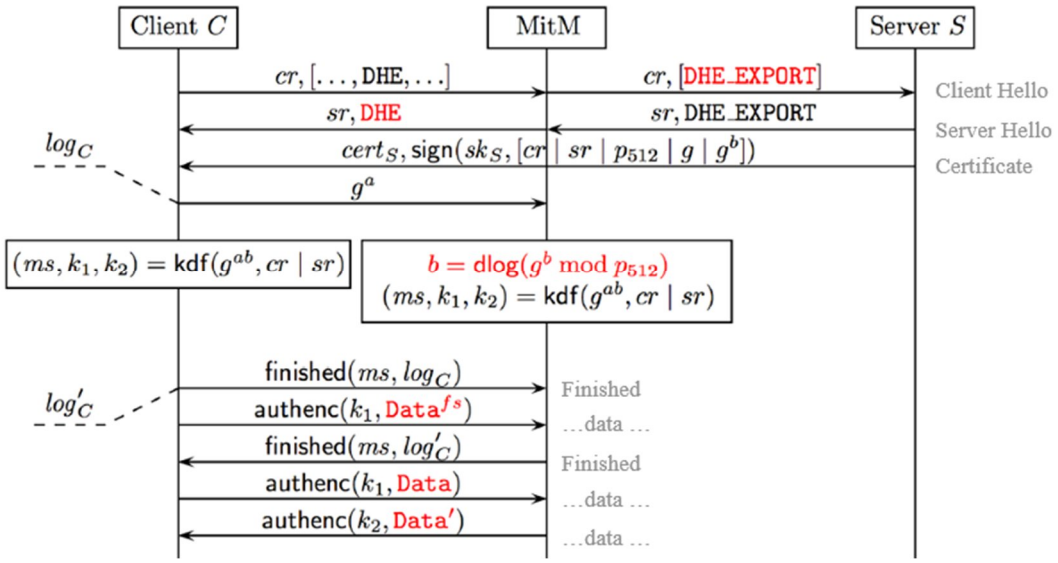
The firewall can inspect contents of packets, including some application-layer protocols including the relation between packets and will check TCP sequence numbers, for example.

The NAT gateway will only give access to systems found or listed in the translation table. However, it does not inspect traffic to servers.

b) Screening routers can be useful to offload a main border firewall some work. Give four filter rules addressing *different* types of problems that you recommend should be implemented! (2p)

c) Give four different filter rules that a main border firewall could/should have! (2p)

d) The figure below shows a MITM attack against SSL/TLS that we have discussed in the course. Explain how it is performed and what makes the attack possible! (3p)



This is the Logjam attack. In short, the MITM degrades the D-H key exchange (msg #2) to become a weaker Export-grade key exchange with short primes (p and g) that can be cracked. It works since most clients do not check the size of the numbers, they just assume normal ephemeral D-H is used. When the attacker has cracked the weaker master secret (ms), it can create a faked finished message to make the client happy. It is now a MITM who can read and send data packets since the session key is known.

5. Link level security and WLAN

a) More advanced switches can have some security enhancing functionality. Mention three different security mechanisms that we may find in such switches. Explain each function clearly, what problem it solves and how! (6p)

- Port based authentication (802.1x),
- VLAN (802.1q) functionality
- Limit number of MAC addresses per port – protects against MAC address flooding which may force a switch to broadcast all packets to all ports
- Lock MAC addresses to ports
- Trusted ports – limit what ports are allowed to send, for example, DHCP answers
- Functionality to detect IP address spoofing (MAC-IP address monitoring)

etc.
(More details needed to explain the selected functions)

b) How does WEP prevent packets from being modified? Is this mechanism sufficient, or does it result in any (known) security problems? Give some details! (2p)

WEP uses a linear CRC function to check packet integrity. With a CRC function, it is possible to calculate exactly what bits in the checksum need to be changed when a bit is changed in the input (a hash requires a complete recalculation). It does not matter whether the data or CRC is encrypted, a bit change is still possible to do.

c) Challenge-response authentication is generally a good security solution. However, the implementation in WEP turned out to be not so good. Why? (2p)

WEP uses the same algorithm at authentication as it does for packet encryption. This means that the attacker gets a 128-byte cleartext challenge and a 128-byte ciphertext from the authentication procedure. By XORing these values, he/she gets a 128-byte keystream that can be used for transmitting own messages via the access point.

6. Mixed questions

Only a short answer is needed (one sentence or two), although a motivation must be given to see that you understand the concept.

a) What is port knocking? How can it be used to hide a service offered by a system? (2p)

A way to request a firewall to allow a client to connect to a service. Done by sending for example SYN packets to different port numbers in a special sequence known only by the authorized user.

b) What is the reason many wireless access points support Radius? (2p)

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

c) Why does IPsec have problems with NAT? (2p)

NAT replaces the IP address and the port numbers with its own, but no port numbers are present in IPsec messages.

d) Give one situation where SSL may be more appropriate as a VPN solution than IPsec! Motivate briefly your answer. (2p)

When lots of different client types must be supported, for example mobile clients. IPsec requires support in the operating system, configuration can be more problematic, SSL is more light-weight, etc. For home users, NAT is often used which creates problems with IPsec.

e) Many security protocols have a variable-size padding field. Why? Give a real-world problem when this could be useful! (2p)

To hide the length of the payload.
An attacker may know the sizes of all pages and objects on a web site. Then when looking at a secure (encrypted) SSL/TLS connection, the size of messages may reveal what the user is doing.

Headers and pictures that may be useful