CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2022-10-07, 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) There are several ways to scan networks and systems, for example with SYN and ACK scans. Explain the difference(s) between these two types and describe what the expected results from them are. It should be obvious from your answer that there is a reason why scanning tools offer different methods to scan systems. (2p)

SYN scan: shows directly what ports are open and accepts communication (SYN/ACK received) and what ports are closed (RST or no answer).
ACK scan: may work through stateless firewalls: RST means someone (a host) is there, no reply that the port is either filtered by a stateful firewall or there is not host at all.

b) Ping of death is a well-known attack. It sends IP datagrams with a size > 64 kByte. However, the maximum size of an IP datagram is 64kByte due to its 16-bit length field. Explain how is it still possible send such oversized datagrams! (2p)

A naïve implementation would assume IP datagrams never exceed 65,535 bytes since the length field is 16 bits long.
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.

c) Some systems increment TCP fragment numbers for each segment they send out. This may be useful for an attacker by using the system as a dumb zombie. Why can this be useful? Also explain with some detail how this attack can be done! (The attack is sometimes called DUMB or Idle scanning.) (3p)

An attacker who is not allowed to communicate with a server (s)he is interested in due to firewall rules, may first want to find a system that is allowed to. This system ("a zombie") can then be the first target in the attack against the server. The way to find such a trusted system is to use fragment numbers in the search for it.

We begin with sending a SYN to the zombie and record the fragment ID in the reply. Then we send a SYN to the target system with the zombie's address as the source. If the firewall allowed traffic from the zombie and the port is open, the server will reply with a SYN/ACK to the zombie, **and the zombie will respond with a RST and increase the fragment number by one**. Now we send another SYN to the zombie and the fragment number will tell whether it has communicated or not.

d) The use of of SYN cookies in Linux is a possible defense against SYN flooding DoS attacks. The defense is to store a SYN cookie in the initial serial number (ISN) selected by the server:

ISN = hash (source and destination IP-addr. and port numbers + secret + client's ISN)

What is the problem with a SYN flood attack?
Why does SYN cookies offer (some) protection to the system?
It also makes it harder for the attacker to compete the attack. Why? (3p)

Each SYN makes the receiving host allocate some internal resources (keep state) and return a SYN/ACK message. Internal resources (e.g. memory or data structures) may at some point be exhausted.

Idea with SYN cookies: The server does not save any data when a SYN is received. Instead all state information is contained in the ISN which means that it does not have to allocate any resources until it receives the ACK. Then the ISN is checked with what the client sends back.

Reason it works: The attacker must be using a valid IP address to receive the SYN/ACK with the ISN to be able to respond with a valid ACK. Only if the ACK is valid, resources are allocated. (If one or a few addresses still flood the server, a firewall could easily filter or block this IP address, manually or automatically.)

2. Authentication and Kerberos

a) Performing password authentication over networks is always problematic. Instead of sending a password in clear-text, challenge response authentication is a better method. How does it work? What is its main weakness if someone can listen to the communication? (2p)

Passwords cannot be sent in cleartext (sniffed, replayed) over the network and one solution is to use challenges that the client encrypts and sends back to the server which can verify that the client is in possession of the password. A major weakness is that an attacker can see both the challenge and the cleartext and may do an exhaustive search of the password. Another weakness is that the server needs to store the password in cleartext.

b) What is a smart card? What does it contain and how can it be used for user authentication? (2p)

It is a card, normally containing a processor and an operating system. In authentication, it is possible to send a challenge to the card which is encrypted using a stored key. The card normally requires the user to enter a PIN code before doing any operations.

c) What are the most important fields in a certificate used for authentication? (2p)

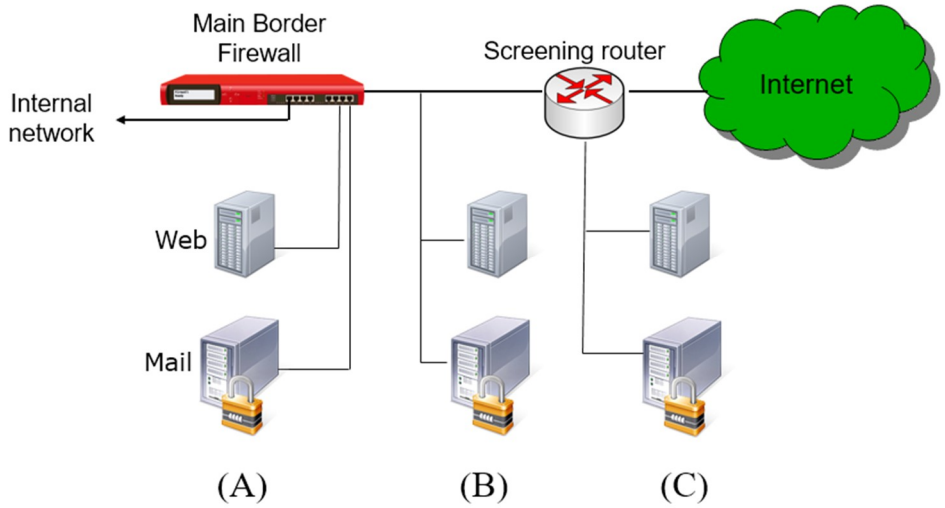
Subject, issuer, subject's public key, signature of issuer, (validity/expiration date), …

d) Kerberos is a system we have studied in some detail. Mention briefly four functions or features it has! (4p)

- One key distribution center allows the use of symmetric keys only and still each client or server only needs to keep track of one key: only n keys needed, not $O(n^2)$.
- It provides SSO functionality.
- It is highly scalable – client keeps state for the server.
- It offers both authentication and authorization.
- It can deliver crypto keys to clients and servers.
- …

3. Firewalls

We normally place external servers on a DMZ, separate from the internal network. In the picture below, we have three suggestions for where to place a web server and a server for incoming mail traffic, A, B and C:



a) Compare the three suggested locations and explain their advantages and disadvantages! (3p)

(A) is the most secure placement. The firewall can have very detailed rules about communication with the web and mail servers (ingress and egress) and can isolate them completely from each other.
(B) is the least secure solution. A cracked server (mail or Web) makes it possible for an attacker to listen to all traffic in and out from the corporate network.
(C) is better than (B) but a cracked Web server allows the attacker to listen to all email traffic since they share the network. Link-level attacks also work between these two servers. The router can have filter rules and can protect the servers from some attacks from the outside.

b) Performing ingress and egress filtering is important in a firewall. What do these terms mean? Give two examples of rules for ingress filters, and two (other) for egress filters! (4p)

Ingress = filter incoming messages, egress = filter outgoing messages.
Examples of rules can be:
- Drop incoming datagrams with internal addresses as the source
- Drop incoming datagrams with invalid flags (e.g. SYN and FIN)
- Drop outgoing ICMP echo reply messages
- Drop outgoing datagrams containing reserved addresses (10.x.x.x, etc.)

c) NAT gateways are strictly speaking not firewalls, but they are still useful and can in some situations replace a conventional firewall.
- What level of protection do they offer?
- What do they lack which normal stateful inspection firewalls have?
- Give an example of a use case where a NAT gateway can or should be used! (3p)

They hide and isolate internal systems from the outside network. 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).
NAT gateways are often used at home where only one official IP address is available and more devices are present. It is also popular by companies since they hide the internal structure of the network and the systems real IP addresses. It is often combined with "real" firewall functionality as well.

4. Encryption and WLAN

a) Diffie-Hellman is a useful method. For what? And what fundamental mathematical property is it based on? (2p)

It is used to perform public key exchange between two parties who have never met before (it also offers forward secrecy).
It is based on that factorization of large numbers is very hard.

b) Give three fundamental properties we would like to see in a hash function! (3p)

For example:

- Computationally efficient
- Must be repeatable (same input always gives same output)
- Output space should be efficiently used
- Given a hash h it should be infeasible to find any message m such that h = hash(m)
- Preimage resistant: Given an input m1 it should be difficult to find another input m2
- Collision resistance: Infeasible to find two inputs resulting in the same hash
- Any change in the input should result in a new unpredictable hash: pseudo-randomness

c) Many protocols such as WEP, WPA and WPA2 use an IV (initialization vector). Why? Explain how it is used! (2p)

The IV makes sure that two identical packets are encrypted differently. This is done with the IV+key as input to the pseudo random generator (each IV creates a different stream which is XORed with the plaintext).

d) The 802.11i framework (WPA2) offers substantially better security than WEP. Mention three improvements in this protocol! (3p)

- AES instead of RC4 encryption
- Session keys introduced
- When all IVs are used new session keys are negotiated
- Passwords are hashed 4,096 times to make it harder to do off-line searches
- Secrets not used directly
- …

5. TLS and SSH

a) The first TLS messages exchanged between a client and a server are the HELLO messages:

$$\{ ver_C \,||\, r_1 \,||\, sid \,||\, ciphers \,||\, comps \} \rightarrow \text{server}$$

$$\{ ver \,||\, r_2 \,||\, sid \,||\, cipher \,||\, comp \} \leftarrow \text{server}$$

Explain clearly what each field contains and the purpose of it (what it is used for)! (4p)

ver_c is the highest TLS version the client supports, ver is what the server decides to use.
r_1 and r_2 are nonces (random numbers) later used in key generation.
sid is session ID, a number identifying the session (a connection can have several sessions). A new session has number 0 from the client.
Ciphers is a list of algorithms the client supports (for encryption, MAC and authentication), in priority order. Cipher is the cipher the server decides to use.
Comps is a list of compression algorithm the client supports, comp is what the server decides to use.

b) A Pseudo-random function is used in TLS:

$$\mathbf{PRF(k, label, x) = HMAC_k(HMAC_k(label||x) \,||\, label||x) \;||\; HMAC_k(\ldots}$$

What is the purpose of this PRF-function? When is it used? (2p)

It is used to expand short secrets to longer blocks, for example to generate the master key from the pre_master_secret or to generate crypto-keys from the master secret:
master_secret = **PRF**(*pre_master_secret*, "**master secret**", r_c || r_s)

c) What is Secure Shell, SSH? What functionality does it offer that TLS does not have? (2p)

SSH is a program and a protocol that offers terminal access to remote systems and can tunnel and encrypt traffic invisibly for other applications which are not part of TLS. (many answers are possible)

d) Mention one advantage with using TLS instead of SSH in an application! (2p)

Several answers possible such as the use of certificates that allows for example web browsers to verify a server's identity without prior sharing of a host key as in SSH.
Or that TLS is built-in to the applications whereas SSH is a standalone program.
Etc.

6. Link level security and network design

a) A self-learning switch learns where hosts are located and will normally not forward private traffic between two ports to any other ports. What can an attacker do to see this supposedly private traffic between two other communicating parties?
What could an administrator do to decrease this problem? (2p)

May overflow switch memory and make it broadcast all packets to all ports. An attacker may spoof other hosts' MAC addresses to disturb the functionality of a self-learning switch and force it into a broadcast mode of all packets.

This can be detected by some switches, for example by limiting number of MAC addresses per port and/or to lock some MAC addresses to certain ports.

b) The documentation for a switch or an access point may tell us that it has functionality to "*support 802.1x authentication with a Radius server*". What does this mean? How can this functionality useful for us? (2p)

802.1x is port based authentication. Before a user or a device is given network access through a switch or AP, authentication needs to take place.
Instead of using a shared key, users can be authenticated through the Radius server using individual passwords or to token cards such as SecurID.

c) What protocol would you select when building a VPN system between two sites? Motivate your answer! (2p)

Most likely IPsec. Transparent for the transport layer and all application layer protocols.

d) In the course we have discussed a security paradigm (a way to think about security) called *Zero Trust* which is believed to be the type of architecture we need in the future instead of having just a traditional firewall as defense. Describe what fundamental thoughts there are behind the Zero Trust architecture! (4p)

Zero trust focuses on moving protections away from a traditional firewall at the boundary of the company to focus on users, assets and resources. This is needed since resources and users are now moved outside corporate networks. All communication should be secured, users authenticated and user authorization should be based on many factors such as role, location, device being used, etc.
In short: move protection closer to clients and services (assets).

Headers and pictures that may be useful