CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2021-10-08, 14:00 – 18:00

M Building

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.

Start answering each question (1, 2, 3, …) on a new page; use only one side of each sheet of paper; please sort and number the sheets in question ordering.

Write in a clear manner and motivate (explain, justify) your answers. If it is not clear what is written for some answer, it will be considered wrong. 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/explanation 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) Give an example of a network layer attack and explain how and why it works! (2p)

See lecture slides for possible answers, one example can be:

The LAND attack is performed by sending a host a packet to a target with its own IP address in both the source and destination fields. Some systems (in the past) used to crash when they tried to respond to themselves.

b) One type of attack is SYN flooding. Explain how it works and why it can be problematic for the attacked hosts. Mention three different ways to, at least to some degree, protect a system against these attacks (one point each)! (4p)

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.

Protection mechanisms (three needed):

- Variable time-out: decrease waiting time when needed.
- Allocate micro-records and do most of the work when connection completed
- Round robin, drop connections when needed.
- SYN-cookies where the server does not have to keep state.
- …

c) What is required by an attacker to do a *blind* insertion of a packet into an ongoing TCP session? Assume you are the attacker and you can see that a person in the room connects to a web server which is well-known to you. What do you have to guess to be able to insert a RST packet into the communication and tear down the connection? (2p)

In general, an attacker must guess the TCP sequence number since he/she is "blind" and cannot see the network traffic. It is enough to guess a number that lies within the current window size. In addition, IP addresses and port numbers being used must be guessed.
In this case, since you know the web server, both the destination IP address and port number are known. So the source port number and possibly some bits of the local IP address plus the TCP sequence numbers being used must be guessed.

d) The SMURF attack uses ICMP echo packets and is 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, 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? (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) A certificate can be used to identify a web server when using SSL/TLS. Describe what happens if an attacker tries to impersonate the server (for example for mybank.com) by faking the DNS reply, which causes the client to connect to the attacker's computer/IP address instead of to the correct server? 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) 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.
- …

d) The Kerberos server is stateless which means that it does not keep track of the users it has authenticated. It is still possible for a user to come back to it and request tickets to services without repeating the authentication process. How is this possible? (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.

3. Security protocols, TLS and IPsec

a) 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 older sessions. The session keys should be independent of this key.

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

b) Many security protocols support sending messages without encryption (encryption=NULL) and still protect packets against modification. Describe how this can be done! (2p)

The protocols use a cryptographic or keyed checksum (e.g. HMAC) where a key is used together with the plaintext: hash(key | text). It requires the key to be known both to verify and to create hashes. This protects the contents of the message even if it is not encrypted.

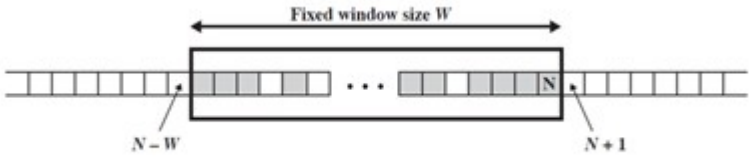
c) In TLS, a Pseudo-random function is used:

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

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)

d) IPsec uses packet numbering, see the picture. For what purpose? (2p)



It protects against replay attacks by discarding duplicates, but unlike TCP, it allows packets to be missing.

e) The ESP header differs depending on what mode is used (see header on last page). Why is it possible to keep the original header in transport mode but not in tunnel mode? (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.

4. Firewalls and IDS systems

a) Stateful firewalls maintain both a state table (connection table) and a table of rules. What is the difference between these tables, why are two needed? Which table is consulted first when an incoming packet is received? Show with an example what happens when some packets go through the firewall and how these two tables are used and what they may contain! (4p)

State table is used for established connections.
The ACL contains the rules for the firewall and is consulted when new connections are estabished.
Example:
ACL:
- Pass in from any to 1.2.3.4 port 80 # web traffic
- Block in all

When an incoming SYN packet is received from host 22.33.44.55 to port 80 on 1.2.3.4, the ACL list is consulted and a state table entry is created:
22.33.44.55 999 1.2.3.4 80 SYN-recvd
When an SYN/ACK is seen (from 1.2.3.4), the State table is directly consulted and since it contains an entry for this connection, the packet is passed on. It is now updated to:
22.33.44.55 999 1.2.3.4 80 SYN/ACK-sent

b) Give some examples of rules that a screening router likely would have to filter traffic! You may use text or your own "pseudo-language" for the filter rules as long as they are possible to understand (comments to the rules are necessary). (2p)

See slides. Examples could be private (reserved RFC 1918) addresses:
(block inout 127.0.0.1), incoming traffic to broadcast addresses (block in 1.2.3.255), outgoing ICMP packets such as ICMP echo reply, clearly erroneous incoming packets (SYN=1, FIN=1), outgoing packets not belonging to our IP address range, etc.

c) TTL can sometimes 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 can normalize incoming TTL values to a standard value, say 20.

d) What is port knocking? How can it be used to hide a service offered by a system? Explain! (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.

5. WLAN

a) The use of shared keys 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.

b) WEP has at least one problem with its handling of IVs. Explain how an attacker may use this weakness! Is this problem likely to occur? (3p)

WEP allows an IV to be reused, we will have two packets encrypted with the same byte stream (since same shared key + IV being used to create the stream). This means that an XOR operation between the cipher texts will result in an XOR of the clear-texts: $c1 \oplus c2 = (p1 \oplus b) \oplus (p2 \oplus b) = p1 \oplus p2$. Since the IV is only a 24-bit value, a busy AP is very likely to reuse IVs. In fact, a busy AP will exhaust the available space in about 5 hours.

c) The documentation of an access point tells us that it has the functionality to "*support 802.1x authentication with a Radius server*". What does this mean? How is this functionality useful for us in a WLAN environment? (2p)

Instead of using a shared key, users can now be authenticated through the Radius server using individual passwords and tokens such as SecurID.

d) Mention three improvements that have been implemented in WPA2 when compared to WEP! (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
- …

6. Link level security

a) More advanced switches can have protection against several types of link-level problems and attacks. Describe *three* different security mechanisms which may be found in switches, and what they protect against! (6p)

For example; MAC address flooding protection (limit number of addresses per port), DHCP spoofing (trusted ports), block traffic between clients (protected ports), 802.1x port-based access control, lock MAC addresses to ports, functionality to detect IP address spoofing (MAC-IP address monitoring), etc. For details, see slides.

b) An attacker on the local network may be able to redirect traffic from other hosts to his/her own computer. Give an example on link level for how such attacks can be done! (2p)

It is possible to fake ARP packets on the network.
Another possibility is to send false replies to DHCP requests.

c) VLANs (virtual LANs, IEEE 802.1q) can be used to achieve some level of security. Explain the general idea of how it works and what level of security it offers! (2p)

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 used to control how packets are sent on the network and who can communicate with who, thus allows the creation of "workgroups".
Since traffic is not encrypted, a MITM can read and alter anything on the network.

Headers and pictures that may be useful