CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2019-08-30, 14:00 – 18:00

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 Dept. of Computer Science and Engineering
Questions during exam:	Tomas Olovsson, 031 - 772 1688

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 FIN and NULL scans. Explain the purpose of these two types and describe what the expected results from them are. (2p)

FIN 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.

NULL scan: this is an invalid packet and could trigger unexpected behavior in the recipient since such packets should normally not be present on the network.

b) UDP scanning is harder to do than TCP scanning. Why? How can operating systems, at least to some degree, protect themselves against this type of scanning? (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.

c) An attacker on the 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.
Another possibility is to send false replies to DHCP requests.

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 allocation of SYN cookies 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)

Explain why SYN cookies can offer protection and why it works (i.e. its advantage)! Are there any drawbacks or problems with this method? (2p)

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.

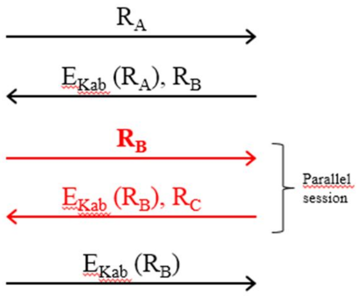
Idea with SYN cookies: The server does not save any data when a SYN is received. Instead all state information is contained in the ISN which means that it does not have to allocate any resources until it receives the ACK. Then the ISN is checked with what the client sends back.

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.)

Drawbacks: problems to remember if TCP options (such as window size) that were negotiated in the SYN and SYN/ACK packets since they are not saved by the server. Another drawback may be that the computation of the hash may take some time, a fact that may be utilized by the attacker.

2. Authentication, Kerberos

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



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.
Mitigations, examples:
- Protocol may start with the server giving the initiator a challenge.
- Response could include both a client challenge and Ek(both challenges)
- Include a nonce in each new connection which is used in calculations

b) Kerberos uses a Key Distribution Center. Mention two advantages of using a KDC instead of using public/private key-pairs distributed to the communicating parties? (2p)

Central authentication and authorization where individual nodes do not have to care about users and user rights.
Only one key to manage for clients and servers (the key to the KDC) – no need to store and distribute public keys between the parties.
No session crypto key negotiation needed such as D-H (faster).

c) TGT and SGT are two different types of tickets in Kerberos. Explain the difference between them and show a scenario when/how they are used (a picture may help)! (2p)

The TGT, ticket granting ticket, is a proof that the user is authenticated and contains encrypted state information the Kerberos needs when the user requests tickets to services. The SGT is a service granting ticket which is a proof that can be sent to a server showing that the user is authorized to for a particular service.

d) Describe in detail the process of how a certificate is used, i.e. how the owner's identity can be verified by another party! What does the receiver of the certificate do? How is it distributed to the receiver? (4p)

• The certificate's signature of the CA is checked using the CA's public key (a hash of the certificate is created and the encrypted and compared with the hash in the certificate)
• The validity period and whether the certificate has been revoked (CRL) are checked.
• The owner's identity is checked, for example by giving it/him/her a challenge to encrypt with the private key which we can decrypt with the public key found in the certificate.
• It does not matter how it is distributed since the full contents and the authenticity can be checked using the CA signature

3. Secure protocols

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) A Pseudo-random function is used in TLS:

PRF(k, label, x) = HMAC$_k$(HMAC$_k$(label||x) || label||x) || HMAC$_k$(…

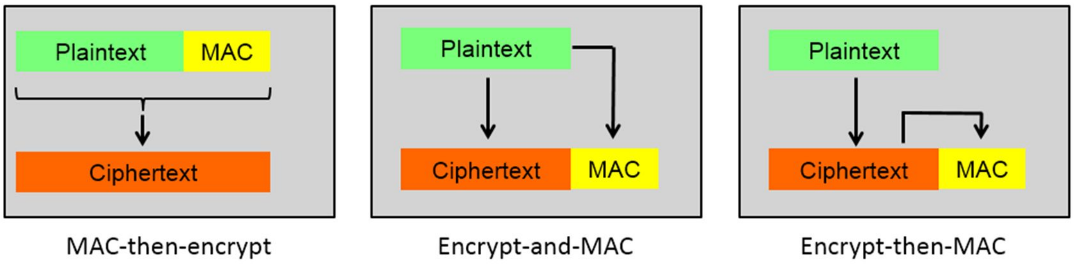
What is the purpose of this PRF-function? When is it used? (2p)

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) SSL/TLS consists of several protocols. Describe the functionality of the record layer, change cipher, alert and handshake protocols (picture on last page). (4p)

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.

d) 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.

4. Firewalls

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) Assume you are given the task to test a new firewall. It is supposed to be a good deep packet inspection firewall and you should give a verdict of it and whether it can be used as a firewall to protect a mid-size company. You should make no assumptions about the firewall's abilities without testing it.

How would you perform the tests? Outline a series of tests you would perform! (This question may have many different answers.) (6p)

There are several possible answers to this question. One possibility is to set up the firewall in front of a system offering some services, and then test its functionality by:

- Port scanning to see that blocked services are blocked (i.e. test filter rules)
- Test if strange options (source routing, …) and clearly invalid packets (IP, TCP, …) are removed
- Test if it is stateful (ACK scanning for example)
- Test its handling of fragmentation (ping of death, Teardrop, …)
- Test fragmentation and if headers can be changed (small fragments)
- Test flooding attacks against firewall and protected systems (SYN flooding)
- Use tools to test attacks against application level protocols (e.g. HTTP, SMTP, …)
- Test logging abilities
- etc.

At least some of the attacks should be described at some level to show that you understand what the attack tests and how the test is done.
[1p for each test]

5. IDS systems

a) What are the two main types of IDS systems (or detection methods) we normally choose between? Explain how each type works! Also mention at least one advantage and one disadvantage with each type! (4p)

Signature-based detection: The system has signatures of known attacks and observes network traffic and try to match them. All known attacks will be detected with few false alarms, but it cannot detect new types of attacks for which there are no signatures yet. (Compare with anti-virus software.)

Anomaly detection: The system knows what activities are normal and tries to detect anomalies, deviations, from this behavior. It is not trivial to learn these systems what is normal activity, and there is a relatively high risk of having too many false alarms. An advantage is that this system may be able to catch new types of attacks. (Compare with an anti-spam system.)

b) In the course we have discussed several ways to evade IDS systems and firewalls, and there are several problems we face if we want to fully understand the traffic between communicating systems. Give at least three different examples of how IDS systems and/or firewalls can be confused by malicious traffic, i.e. how they may end up with different views of the communication than the communicating systems have.

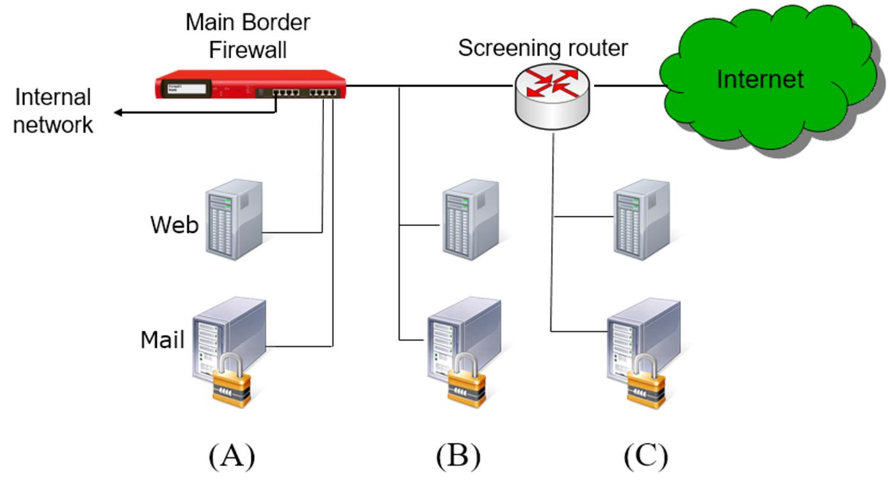
Motivate clearly why the examples you provide are problematic, and what the IDS system or firewall should do to deal with the problems. If there are other solutions to the problems (outside the IDS or firewall), please describe! (6p)

Examples of problems: Overlapping IP fragments changing already inspected data, overlapping fragments which may be reassembled differently by different systems, overlapping TCP segments with different reassembly algorithms, expiring TTLs, send datagrams with a timing that may expire either in the end-host or in the IDS system, experiments with the DF (don't fragment) bit, etc.

More details are needed when explaining the attacks you select.

6. Secure network design and WLAN

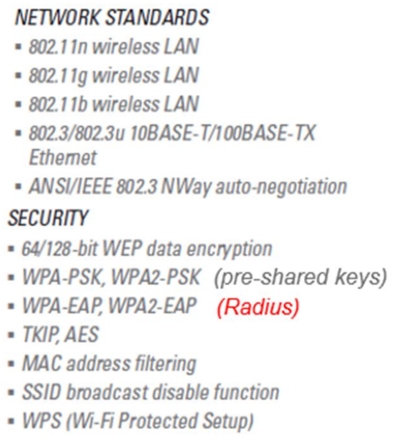
We normally place external servers on a DMZ, separate from the internal network. In the picture below, we have three suggestions for where to place a web server and a server for incoming mail traffic, A, B and C:



a) Compare the three suggested locations and explain their advantages and/or 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.

An access point has several features as seen in the figure.



NETWORK STANDARDS
- 802.11n wireless LAN
- 802.11g wireless LAN
- 802.11b wireless LAN
- 802.3/802.3u 10BASE-T/100BASE-TX Ethernet
- ANSI/IEEE 802.3 NWay auto-negotiation

SECURITY
- 64/128-bit WEP data encryption
- WPA-PSK, WPA2-PSK (pre-shared keys)
- WPA-EAP, WPA2-EAP (Radius)
- TKIP, AES
- MAC address filtering
- SSID broadcast disable function
- WPS (Wi-Fi Protected Setup)

Explain briefly (one or max two sentences) the following features and what they do. The answer should show that you know what the feature is:

b) WPA2-EAP (i.e. Radius) (1p)
c) TKIP (1p)
d) MAC address filtering (1p)

It performs authentication and offloads the server from maintaining a list of user accounts.

TKIP makes sure encryption keys change over time. It extends the IV (with a new field EIV). It makes sure each station uses a unique key by involving the MAC address in key calculation. It also makes sure each packet has a unique sequence number and that the key is changed every 10,000 packets. (shorter answer ok)

MAC address filtering is a simple filter functionality in the AP to only allow a limited set of authorized MAC addresses to connect. All other devices are rejected.

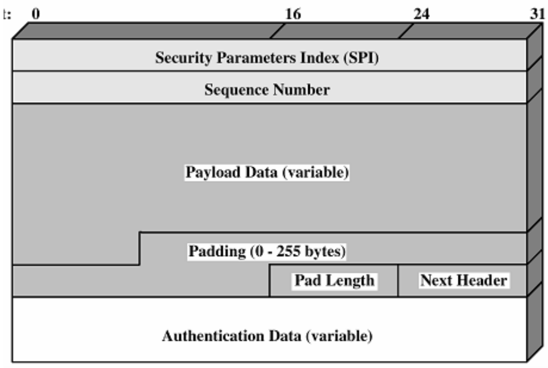
e) When authenticating a client in WEP, the access point (AP) sends a long random string as a challenge to the client. This means that a listener gets access to both the cleartext (challenge) and the ciphertext (encrypted challenge). It makes it possible for attacker to search for the password, but there is another problem associated with this as well. Explain what this security problem is and how it can be used by an attacker. (2p)

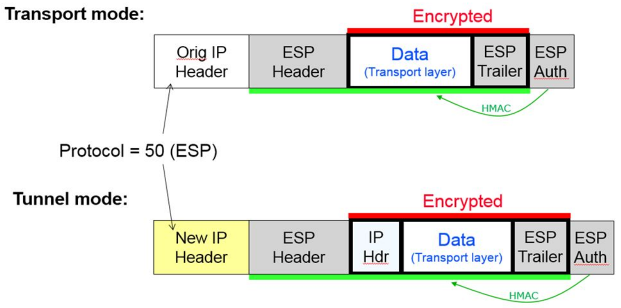
The attacker can see both the challenge and the ciphertext encrypted with the secret (password). This makes it possible to extract the keystream using an XOR operation: $c1 = p1 \oplus \textit{stream}$, and since the same algorithm is used for data transmission, this 128-byte keystream can be used to transmit arbitrary data. Unfortunately WEP uses the same algorithm for authentication and packet encryption and IVs can be reused.

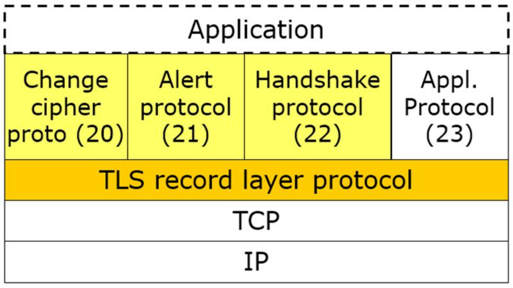
f) Give a suggestion of how this problem can be eliminated. (2p)

Use a different dedicated IV for authentication or use different algorithms for authentication and data transmission.

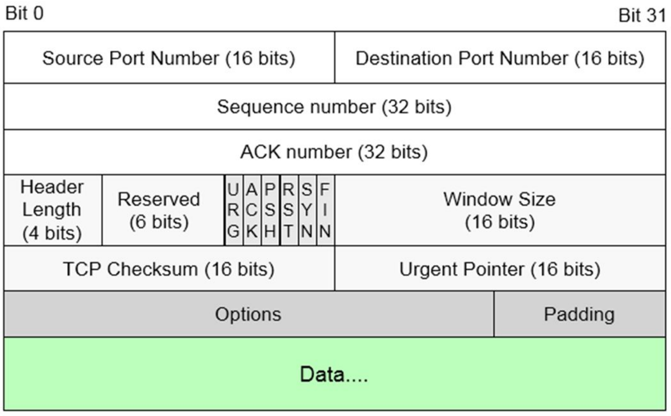
Headers and pictures that may be useful



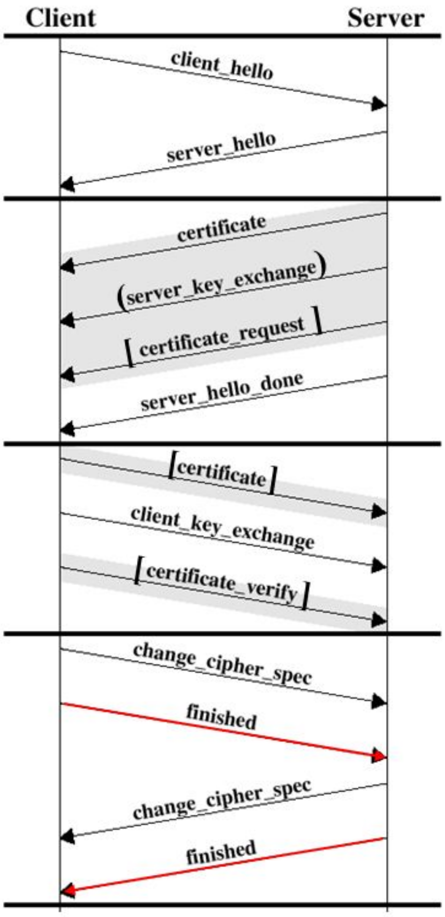


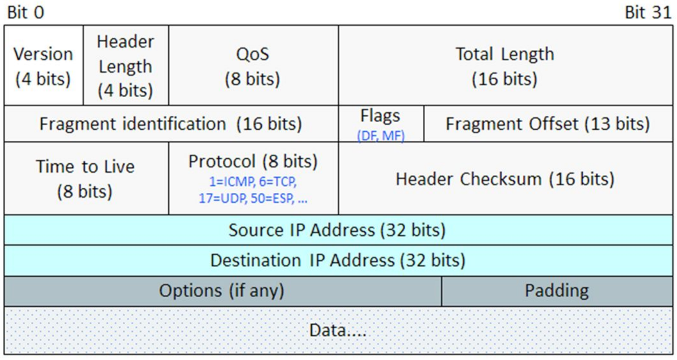


Application			
Change cipher proto (20)	Alert protocol (21)	Handshake protocol (22)	Appl. Protocol (23)
TLS record layer protocol			
TCP			
IP			



Bit 0								Bit 31
Source Port Number (16 bits)								Destination Port Number (16 bits)
Sequence number (32 bits)								
ACK number (32 bits)								
Header Length (4 bits)	Reserved (6 bits)	URG	ACK	PSH	RST	SYN	FIN	Window Size (16 bits)
TCP Checksum (16 bits)								Urgent Pointer (16 bits)
Options								Padding
Data....								





Bit 0					Bit 31
Version (4 bits)	Header Length (4 bits)	QoS (8 bits)		Total Length (16 bits)	
Fragment identification (16 bits)			Flags (DF, MF)	Fragment Offset (13 bits)	
Time to Live (8 bits)		Protocol (8 bits) 1=ICMP, 6=TCP, 17=UDP, 50=ESP, ...		Header Checksum (16 bits)	
Source IP Address (32 bits)					
Destination IP Address (32 bits)					
Options (if any)				Padding	
Data....					