CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491	**(Chalmers)**	**7,5 hec**
DIT071	**(GU)**	**7,5 hec**
EDA490	**(Chalmers old)**	**6,0 hec**
DIT070	**(GU old)**	**6,0 hec**

Tuesday 2010-04-06 14:00–18:00 in building V

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

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, 772 1688

Answers: Published on the web page after the exam

Inspection of exam: See web page for announcement

NOTE: Indicate clearly on front page if you take an older 6 credit course!

CTH Grades:	30-38 → 3	39-47 → 4	48-60 → 5
GU Grades:	30-47 → G		48-60 → VG
Older 6 credit courses:			
CTH Grades:	24-35 → 3	36-47 → 4	48-60 → 5
GU Grades:	24-47 → G		48-60 → VG

1. Attacks, DoS

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 and some other fields in the header can also be used to reveal information about the type of system returning the packet. How? (2p)

c) Finally, 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.

d) To prevent blind TCP hijacking attacks, it is important that TCP sequence numbers are randomly selected. Why does it matter? The attacker cannot see the TCP connection and the numbers being used anyway. Explain! (2p)

The attacker may send own TCP segment (for example a SYN) to the server to fake a connection and based on the sequence numbers it sees in the replies (SYN/ACK) it may be possible to predict what sequence numbers other users will get.

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.

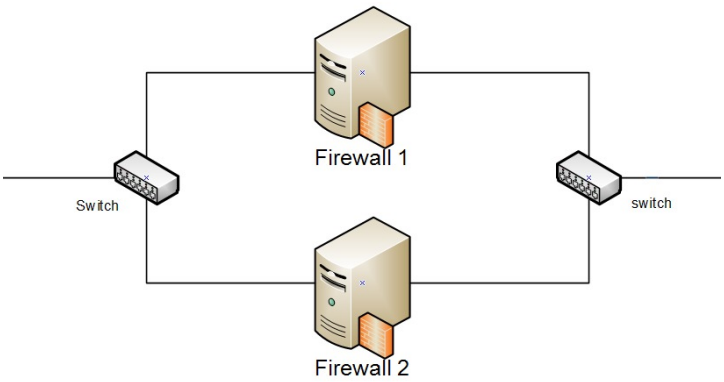
2. Firewalls

a) Explain the functionality of a circuit-level gateway and an application-level gateway. (2p)

Curcuit-level gateways are firewalls terminating the TCP connections. It opens a new TCP connection to the other side to avoid TCP and IP headers being forwarded. The application-level protocol is not touched.
Application-level gateways also terminate the application protocol such as Telnet, FTP, SMTP, etc. It extracts the data and creates a new connection to the other side with new application headers.

b) Firewalls must be able to handle UDP traffic, but there is a fundamental problem with it that does not exist for TCP traffic. What? How can a firewall handle UDP traffic in order to offer reasonable security for a network? (2p)

They should be stateful and keep track of all UDP traffic originating from the inside. When a request packet is sent out from the trusted side, it could allow replies from the outside from the same host and port number that received the first packet for a limited time period.



c) Assume someone places two firewalls (for example two Linux machines not specially designed for this purpose) in parallel as shown in the picture, believing they could handle traffic to and from a network with the intention to enhance reliability. The designer wants uninterrupted service in case one firewall fails. Would this work? List some potential problems with this approach! (3p)
Hints: think about failover, IP and MAC addresses…

Both firewalls need to see all traffic to be able to keep state, but only one is allowed to forward traffic to avoid duplicates. A self learning switch would hide the traffic for the other system.
What IP address should the firewalls have on the network, same address?
The router and switch needs to know where to send packets, to FW1 or FW2? If they are configured to use the same IP address, what MAC address would they use? Packets will still just be sent to one of them.
If they would have same MAC addresses, still problems with sending packets to both unless we place a dumb hub in front of them, sending packets to all ports.

3. SSL and VPN systems

a) Why are man-in-the-middle attacks not possible in SSL? Consider both the cleartext connection setup phase and data integrity during data communication. (3p)

1. The server normally identifies itself with a certificate (public key crypto-system) which at least makes sure the client talks to the right server. Client certificates are also supported although not that often used.
2. After connection setup and encryption is turned on, the parties exchange hashes of all messages being transmitted. This makes sure a man-in-the middle has not changed any of the cleartext data being exchanged.
3. During data transmission, encrypted data is protected by a hash, HMAC.

b) The first SSL messages exchanged between the client and the server are the HELLO messages:

$\{ ver_C \| r_1 \| sid \| ciphers \| comps \}$ → server

$\{ver \| r_2 \| sid \| cipher \| comp \}$ ← server

Explain clearly what each field contains and the purpose of it (what it is used for)! (5p)

c) SSL has a procedure for closing a connection. Why not just use TCP's FIN message to close the connection? (2p)

To prevent a third party from prematurely closing the connection and cause data to be lost. Both parties want to know for sure that it was an intentional close of the connection and this cannot be done by sending a FIN only.

d) During the connection setup phase, SSL can use either the RSA or Diffie-Hellman algorithm when negotiating the pre-master key. RSA is most often used. Why?
Also explain how the pre-master key is handled with RSA! (3p)

RSA offers server authentication, D-H only key negotiation.
With RSA, the client generates a 48 byte pre_master_secret, encrypts it with the server's public key and sends it to the server. Only the correct server will know the key.

4. WLAN

a) WEP allows the same IV to be reused several times. Why can this be useful for an attacker? (2p)

If the IV is reused in two messages, c1 and c2, we can xor them together and get p1 xor p2 from which statistical analysis may reveal both cleartext 1 and 2.

b) The authentication procedure in WEP sends a 128 byte challenge to the client. Why is this a bad idea? (2p)

It offers the possibility to get the keystream for the IV used:
p1 XOR c1 = 128 bytes of the keystream for that particular IV
This keystream and same IV can be used to send messages without knowing the key.

c) Compare WEP and SSL with respect to user authentication. Discuss differences and explain how the authentication procedure works in the two protocols! (4p)

- WEP uses shared secret, SSL supports authentication of both parties.
- WEP has no authentication of the AP, only of connecting user
- SSL: both parties involved in key negotiation, WEP: no negotiation, secret directly used
- etc.

d) What is the major difference between WEP and SSL when considering message integrity during data communication? (2p)

WEP uses a linear checksum (CRC) and SSL hash functions.

5. Authentication, link level security

a) What is Radius? What services does a Radius server offer? Explain *briefly* what happens when a user wants to connect to a service. The explanation must show clearly what parties are involved. It may help to use a figure to illustrate your thoughts! (2p)

Radius is a standard protocol for user authentication supporting AAA (authentication, authorization and accounting). Three parties are involved: the client, the application server and the Radius server. The Radius server offloads application servers to maintain lists of users and do user authentication.

b) In Radius, when the client sends the user's password, it sends:
MD5(shared_secret, 16_octets_random_data) ⊕ password
Explain the first two parameters and their purpose! (2p)

Shared secret = crypto key the authenticating server and the Radius server share. If it does not match, the Radius server will not respond to the question.
16_octets_random_data: makes sure the transmitted data packet is unique

c) The server then responds with:
Access Accept or Reject (Code=2 or 3)
A sequence number (ID)
Possible attributes (if any)
Length
A hash: *MD5(Code, ID, Length, attributes, 16_octets_sent_by_client, shared_secret)*

Explain the purpose of this hash and why each field is present in the hash! (3p)

The first four fields are included to make sure it is impossible to modify them in the message (if so, the hash will not match).
The same 16 bytes as the client sent are included again so that the application server can see it is a reply to its request and not a replay of an older reply.
The shared secret guarantees it is a reply from the Radius server and not someone else.

d) Mention three different ways to, at least to some degree, protect a system against SYN-DoS attacks! (3p)

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

6. Misc short questions

Answer the following questions with one or maximum two sentences, not more. The answer must be detailed enough to show that you understand the topic!

a) In IPsec, ESP mode has a padding field. What does padding do to enhance security? (2p)

b) What is the purpose of TKIP? (2p)

c) What is 802.1X (port authentication) used for? (2p)

d) What is the overall idea with VLAN (802.1q)? (2p)

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