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**

Friday 2010-08-27 08:30–12:30 in building M

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 and DoS

The article "*DRDoS – Distributed Reflection DoS attacks, the next generation of DDoS attacks*" describes a site that appeared to be under attack from several hundred Internet core routers.

a) What is meant with a reflection attack? How was this attack done? (2p)

The attacker can instruct zombies (innocent systems) to send spoofed SYN segments to other hosts (victims) by spoofing the victims IP address in the SYN packet. The zombie systems will generate SYN/ACK messages in response and send them back to the victim that is flooded with packets.

b) What are the reasons for doing this kind of attack instead of performing a "normal" DDoS attack and just spoofing IP addresses? (2p)

Since the zombies are hosts that send legitimate and important information as well, no operator wants to block traffic from them. Traffic filters will therefore not be implemented stopping the traffic. In addition, the TCP's resend mechanism will resend the SYN/ACK messages if it does not get an answer from the victim (magnification effect).

c) There have been different solutions proposed for how attacks like the reflection attack can be stopped. Suggestions include "traceback", "pushback" and "centertrack". Explain very briefly two of these methods – just a sentence each describing its main idea! (2p)

Traceback: For each datagram forwarded by a router, the receiver may, with some small probability, also receive additional info about who forwarded it
Pushback: Routers realizing they have to discard many datagrams to one destination can tell other routers to drop these datagrams as well
Centertrack: Routing within a system (e.g. AS) may be temporarily handled by special routers that are configured to handle tracing, if an attack is seen

d) Describe <u>two</u> attacks on network level and <u>two</u> on transport level that may be successful to perform against a host! Explain! (4p)

2. Firewalls and VPN systems

a) A screening router can be used to implement ingress and egress filtering.
Give <u>four different</u> examples of rules, two ingress and two egress that should be implemented! (4p)

b) Circuit level gateways and application level gateways work differently from "normal" packet filtering/inspection firewalls. Explain how they differ! (2p)

c) What is the difference between the circuit level gateway and the application level gateway? (2p)

d) Firewalls may support encryption of network traffic, i.e.VPN functionality, to other sites. This makes it possible to connect multiple sites over the Internet securely. What protocol are the firewalls likely using to implement this functionality? Why is this protocol more suitable than, for example, SSL? (2p)

IPsec. It encrypts IP traffic and is completely transparent to the transport and application layers. SSL is better to use when securing a TCP connection between a client and a server.

3. WLAN

a) 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).

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) Mention (any) three improvements that have been implemented in WPA2 when compared to WEP! (3p)

d) 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, for example using individual passwords or tokens such as SecurID.

4. Authentication

Kerberos is a system originally developed at MIT and is used in many systems such as in Windows and Unix. In the initial communication between a client (A) and a Kerberos server (AS), a Ticket Granting Ticket (TGT), is requested:

Packets to obtain a Ticket-Granting ticket (TGT):

(1) A → AS: $ID_a \,||\, ID_{tgs} \,||\, TS_1$

(2) AS → A: $E_{Ka}[K_{a,tgs} \,||\, ID_{tgs} \,||\, TS_2 \,||\, Lifetime_2 \,||\, TGT_{tgs}]$

TGT_{tgs}: $E_{Ktgs}[K_{a,tgs} \,||\, ID_a \,||\, AD_a \,||\, ID_{tgs} \,||\, TS_2 \,||\, Lifetime_2]$

a) Explain the fields present in the TGT and their purpose including E_{Ktgs}! (4p)

b) The client is authenticated after these messages have been exchanged. Explain! (2p)

c) WEP uses shared secrets for user authentication. The authentication is implemented as a challenge response mechanism to verify the shared secret. Why? Describe how the authentication process works. Is the implementation of the authentication mechanism secure enough? Please explain the details! (4p)

It should not be possible for an attacker listening to the authentication process to repeat it, therefore just sending the password, encrypted or not, will not do. The server sends a 128-byte string to the client which is encrypted with the shared secret.

The problem with the implementation is that for the attacker, he/she gets a cleartext message and a ciphertext message for a given IV and by XORing these, he/she gets a 128 byte key stream which can be reused over and over again sending own packets.

5. Link level security

a) 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.

b) A self learning switch normally learns where hosts are located and only forwards packets to the ports where the MAC address is known to be. An attacker may still be able to make the switch forward the traffic so he/she can see the traffic. Explain how this may be possible! (2p)

By overflowing the switch with faked messages with different MAC addresses, its memory becomes full and old entries are lost. The switch now needs to broadcast traffic from other hosts to all ports.

c) Give *two* short examples of how this problem (in b) may be dealt with either by the system owner or by the switch itself! (2p)

Static configuration of important hosts/gateways in the switch.
Some switches limit number of MAC addresses per port.
Or it may just learn the first n addresses (which cannot be spoofed)

d) Is link-level authentication ever implemented? If so, give an example of how it may work and the purpose!

802.1x – port based authentication. Description…

6. Mixed short questions

a) What is MD5 and SHA-1? What makes them fundamentally different from a CRC? (2p)

b) What is the overall idea with VLAN (802.1q)? Can it be used to secure communication between hosts on a local corporate network (VPN-like functionality)? Explain! (2p)

c) Diffie-Hellman is a useful method. For what? (2p)

d) What fundamental mathematical property is Diffie-Hellman based on? (2p)

e) In IPsec, AH (authentication header) is one protocol we can use. Even though packets are not encrypted, it could still be useful. Why? What does it do? (2p)

It provides authentication and message integrity. This means that messages are protected against modification by using a keyed hash function (HMAC) which requires a secret key to be recalculated.

f) Mention 2 differences between SSL and TLS!

(2p)