CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

2011-08-25, 08:30 - 12:30

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

CTH Grades:	30-38 → 3	39-47 → 4	48-60 → 5
GU Grades:	30-47 → G		48-60 → VG

1. Attacks and firewalls

Assume you are given the task to test a new firewall on the market. It is supposed to be a good deep packet inspection firewall and your task is to give a verdict of it and whether it can be used as a firewall to protect a mid-size company (500 users or so). You can make no assumptions about the firewall's abilities without testing it.

a) How would you perform the tests? Outline a series of tests you would perform! (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]

Now assume that the company you work for decide to use this firewall. It should only allow access to the company's web and mail (SMTP) servers from the outside and also allow remote access (IPsec) to a separate VPN server on a DMZ network. Inside users should have full access to the Internet.

b) Draw a picture of how you would do the installation. (2p)

c) Show using a reasonable syntax what firewall rules you would place in the firewall! (2p)

2. Wireless LANs

a) In WEP, the server authenticates a client by sending a long random string to the client to be encrypted. Explain why and how it is possible to use this message by an attacker! (4p)

WEP uses the same algorithm for authentication and packet encryption and IVs can be reused.
The authentication process starts with sending a challenge in cleartext which is encrypted by the client and the ciphertext is sent back. An attacker can derive the cipher stream used for encryption from these two messages: $c1 = p1 \oplus stream$. Then everyone can construct arbitrary messages with that stream since IV's may be reused.

b) WEP uses a linear CRC function to check packet integrity. Why is this not sufficient? Explain! (2p)

A linear checksum makes it possible to predict how the checksum changes if any bit in the message changes. Since the message + checksum is XORed with the key stream, it is therefore possible to change arbitrary bits in the message and create a valid checksum even though the message is encrypted.

c) What does the TKIP (temporal key integrity protocol) present in WPA do to enhance security? Give some details about what it does! (4p)

TKIP makes sure encryption keys change over time. It extends the IV (with a new field EIV) and 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.

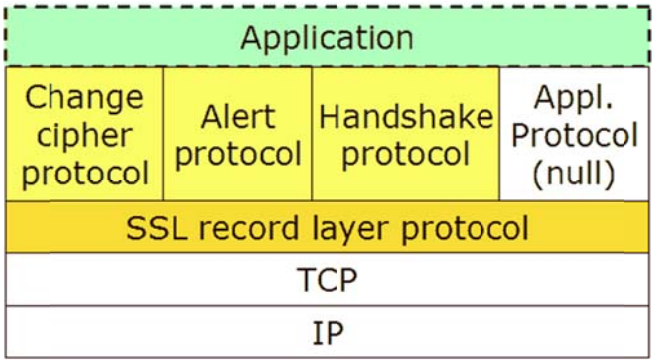
3. SSH and SSL

a) SSH (Secure Shell) offers a concept called "port forwarding". What is it? What functionality does it offer? Explain with 2-3 sentences, not more. (2p)

The SSH client opens a local port (e.g. 80) and local applications can connect to it. All data written (and read) is sent encrypted to the SSH server which decrypts it and forwards it to the final target (in this case, a web server at the other end).

b) When port forwarding is used, SSH opens a number of ports. This may enable attacks by other users, local and remote. Explain! (2p)

Ports normally have no access control which means that any application and any user at the local host can connect to it and send data to the remote server. (This is especially a problem on multi-user systems where all users can make connections. It may even be the case that other computers can connect to the local port and communicate with the remote server…)



The picture above shows the SSL protocols.

c) Explain the purpose of the SSL record layer protocol and what it does! (2p)

Fragmentation, (compression), adding MAC, encryption

d) SSL creates six different keys from the Master secret: Server write key, Client write key, Server MAC key, Client MAC key, Server IV and Client IV. Why are six different keys used? What happens if the Client write key is cracked? (2p)

e) SSL has a special message to close a connection. Why is this message present, why not just send a TCP FIN segment? (2p)

Anyone may insert a false FIN message. When received, TCP closes the connection (in that direction) and the rest of the conversation is truncated and data may be lost. This situation may not be detected by the communicating parties.

4. Authentication and encryption

a) What is the purpose of Radius? What services does a Radius server offer? Explain *briefly* what happens when a user wants to connect to a service that uses Radius for authentication. (2p)

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

When the client contacts the server to authenticate a user, it sends:

- *Request code* (1 = access request)
- *ID* (sequence number)
- *Length*
- *MD5(shared_secret, 16_octets_random_data)* $\oplus$ *password*

and

- *MD5(full_message, shared_secret)*

b) Explain the purpose of the two hashes, their parameters and why they exist! (4p)

Shared secret = crypto key – a secret the client and the Radius server share.
16_octets_random_data = data making the transmitted data packet unique.

The first MD5 field enables the server to check the password. Since the packet is not encrypted, the shared secret makes it impossible to retrieve the password if someone is listening to the communication.

If the second MD5 field does not match, the Radius server will not respond to the request (silent drop). Only clients knowing the secret may request authentication.

c) What is Diffie-Hellman key agreement used for? Give a simple example with numbers! (4p)

d) Is Diffie-Hellman vulnerable to MITM attacks? Explain! (2p)

Yes, there is no authentication. It is possible to agree on a common secret with someone (e.g. an encryption key) but it is not possible to know who the other party is.

5. Link-level security

a) 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 types of network devices can handle it! (4p)

VLANs use tagged link headers (it's a link-level protocol) to isolate/separate traffic between different LANs. It is not primarily designed for security. All packets sent out can have a tag identifying it (tagged VLAN) or without tags if the devices keep track of where packets are received (interface/port). It can be handled by switches and routers as well as by individual workstations (computers). In short, it governs how packets are sent on the network and who can communicate with who, thus allows the creation of "workgroups".

b) ARP spoofing is possible to do by someone who has access to the physical network (or access to a wireless network). What is ARP and ARP spoofing? What is the goal with this attack? How can a host, at least partly, protect itself against such attacks? (2p)

ARP spoofing is a way to erroneously send or respond to ARP queries on the network ("who has IP address 1.2.3.4?") and make computers send IP messages to the attacker's computer instead of to the correct destination. Most systems will accept the first answer they get and treat it as valid. This way it is possible to spawn man in the middle attacks. Possible protection can be to define important IP-address to MAC address translations as static.

c) Switches can be self-learning when it comes to MAC addresses. Explain this feature. Is this good or bad from a security point of view? How much trust can we place on it? (2p)

6. Mixed questions

Only a short answer is needed (normally a couple of sentences only), although a motivation must be given to see that you understand the concept.

a) The IEEE 802.1x standard describes "port based authentication". What is it? (2p)

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

c) Many security protocols have a variable-size padding field. Why (2p)

d) Give one example of why fragmentation can be problematic for a firewall. (2p)

e) Mention two different ways to, at least to some degree, protect a system against SYN-DoS attacks. (2p)

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.