CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers)
DIT071 (GU)

Monday 2011-04-26, 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.**

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 DoS

a) One type of attack is SYN flooding. Explain how it works and why it can be problematic for the attacked hosts. Also explain three different methods hosts can use to protect themselves against SYN attacks! Explain with enough detail to show how and why the method may be effective. (6p)

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:
- start freeing pending connections (decrease timeout values, drop older entries),
- allocate micro-records (16 bytes typically, source+dest IP address and port numbers + ISN + options)
- use SYN-cookies (for details, see slides from lecture).

b) Give an example of a DDoS attack that is hard to trace and stop! Motivate your solution! (Several answers may exist to this question.) (2p)

See for example the slide "DDoS Attacks through Handlers and Zombies".

c) What is stealth scanning? Give an example! (2p)

2. Authentication and WLAN

a) Both LDAP and Radius can be useful in situations where users should be authenticated. Describe what functionality each protocol offers!
In your answer, make sure you highlight the differences between them and that it is clear to the reader when the respective protocol can or should be used! (4p)

LDAP is a protocol used to access directory listings (user accounts). It is a way to retrieve information about a user and is not in itself an authentication protocol. The user password may be stored (encrypted) in the database, but the end-system (client) needs to perform the authentication, i.e. to check the password, not the LDAP server.

Radius is a good protocol for networked devices (clients) without their own account database to connect to an authentication server and ask it to authenticate a user. The Radius server may either have its own database or use LDAP to retrieve records about the users it authenticates.

b) A system that wants to authenticate a user (a client) over a network is designed to request the client to encrypt the *username* + *password* with the system's public key and then send it to the server. We can assume the private key is at all times kept secret and that the encryption algorithm cannot easily be broken. Is this a good solution or not? Explain! (2p)

What is sent over the network is encrypted, but it can be used in replay attacks by an attacker. Nothing makes it unique and it can be used over and over again.

c) Challenge-response authentication is generally a good security solution. However, the implementation in WEP turned out to be not so good. Why? (4p)

WEP uses the same algorithm at authentication as it does for packet encryption. This means that the attacker gets a 128-byte cleartext challenge and a 128-byte ciphertext

from the authentication procedure. By XORing these values, he/she gets a 128-byte keystream that can be used for transmitting own messages via the access point.

3. TCP and Firewalls

a) Explain why a firewall and a host receiving a fragmented IP packet may end up with two different results. Show with a picture how this is possible. Is this problem possible to solve? (4p)

Overlapping fragments can be reassembled in different ways. See slides. Solution can be that firewall always reassembles all packets or that fragments always are dropped.

b) Can or should a firewall to a corporate network filter out (drop) all incoming ICMP messages? Motivate your answer! (2p)

c) Explain how TCP fingerprinting works, i.e. how a system's identity can be determined. Give some examples of what it *may* look like! (4p)

By inspecting TCP traffic from a system, it is possible to determine its type based on values in different TCP header fields, such as TTL, Window size, TOS and DF bit. Different operating systems will use different options and set for example TTL to different values. The attack can work just by trying to establish a connection and watching the first TCP reply. The applications do not need to be involved, i.e. no accounts on the server have to be available.

4. IPsec, SSH and SSL

a) IPsec can be used in both tunnel and transport mode. What is the difference and what is the reason two different modes were introduced? (2p)

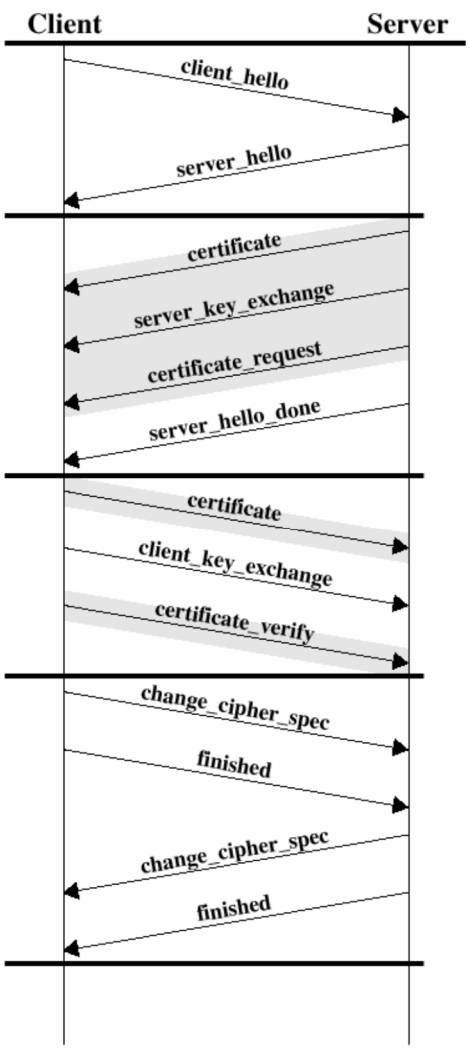
Tunnel mode is used in site-to-site VPN systems and is often used between firewalls that take incoming IP messages, encrypts them and sends them to the other end (keeps original IP header inside IPsec datagram). End systems do not have to be aware of encryption. Transport mode offers end-to-end encryption

b) In many security protocols, for example IPsec, it is possible to send messages without encryption and still be protected against packet modification (i.e. to offer integrity protection only). Describe how this is possible! (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) SSH (Secure Shell) offers a concept called "port forwarding". What is it? What functionality does it offer? Explain with 2-3 sentences. (2p)

d) The figure below shows the SSL handshake protocol and how a client and a server exchange information. The grey messages are optional and are not always exchanged. Explain the mandatory (non-grey) messages and what they contain and do! (4p)



5. Link-level security

a) ARP spoofing could be problematic on a network. What is it? What could an attacker gain from it? Explain! (2p)

b) There are several solutions against ARP spoofing that, at least to some degree, can solve the problem. Mention two possible countermeasures and explain how they work! (4p)

Use of static ARP entries.
Try old MAC address before updating entry to new address (Linux "Antidote" patch).
Don't accept changes in IP-address and MAC address mappings (manual reconfig needed).

c) MAC address flooding may cause problems in switches. Why? What could the possible gain for an attacker be with such an attack? (2p)

May overflow switch memory and make it broadcast all packets to all ports.

d) Give an example of how VLAN (802.1q) can be used to enhance security! (2p)

6. Mixed short 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) How can network address translation (NAT) be used to enhance security in a network? Mention one positive and one negative thing with implementing NAT! (2p)

c) Mention briefly two things TKIP (temporal key integrity protocol, present in WPA) does to enhance security? (2p)

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.

d) What is TLS? Mention two differences between SSL and TLS! (2p)

TLS is just SSL version 3.1 (mainly name change).
Differences (new features):
- Uses new MAC function (HMAC)
- More alert codes
- Variable-size padding
- Easier to add new ciphers and compression methods
- AES supported

...

e) Many security protocols such as IPsec, have a variable-size padding field. Why? What can it do to enhance security? (2p)

Used to hide size of payload. All packets may have the same size when encrypted.