CHALMERS | GÖTEBORGS UNIVERSITET

Network Security

EDA491 (Chalmers) 7,5 hec
DIT071 (GU) 7,5 hec

Monday 2010-12-13, 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

An attacker has the possibility to attack a system on many different protocol levels. Give an example of an attack that either works today or has worked in the past for each of the following layers. Explain how it works, why the attack is possible and the possible result from the attack!

a) Link level (2p)
b) Network level (2p)
c) Transport level (2p)

a) ARP spoofing. An attacker can easily listen to an ARP request and quickly send a reply to the requesting host before the real receiver responds. Normally the first reply will be used by hosts.

b) The LAND attack is performed by sending a host a packet to a target with its own IP address in both the source and destination fields. Some systems used to crash when they tried to respond to themselves.

c) A possibility is to try to exhaust the connection table of a receiving host's TCP stack by never finishing the TCP three way handshake process. By sending a SYN packet only and never respond to the SYN-ACK, the receiver waits. By sending lots of such requests, possibly from spoofed addresses, a DOS attack is possible since the table is full and no one else can open new connections.

d) What is required by an attacker to do a *blind* insertion of a packet into an ongoing TCP session between two other users? What is the countermeasure we have in TCP against it? Is the solution good enough? How likely is the attacker to succeed? (4p)

The attacker must guess the sequence numbers selected by one of the parties in a TCP session. New sessions begin with the parties selecting a random number for the TCP numbers exchanged during the initial three-way handshake. The attacker must therefore guess the sequence number assuming he/she is "blind" and cannot see the network traffic. It is enough to guess a number that lies within the current window size.

An estimation of the number of packets needed: 32-bit seq. numbers, assume window > 64kB, then less than 16 bits remain. In addition: port numbers of the parties, 16+16 bits and IP addresses (which may be guessed?) must be guessed. This may be more or less impossible(?) unless the numbers to some degree can be predicted.

2. Firewalls

2a) IP fragmentation is problematic in many situations. Consider a firewall or IDS system inspecting the traffic and mention three problems related to fragmentation that may affect security. Describe the problems and what situation they may result in! (6p)

Needs reassembly to inspect contents, overlapping fragments may produce different results in different hosts, short fragments may overwrite already inspected headers, fragments may be used to create oversized IP messages, …

b) What kind of information is used by a typical static packet filtering firewall? What are the shortcomings of such a firewall when compared to a stateful inspection firewall? (3p)

c) What is an air-gap firewall? Give an example how it may work! (2p)

3. WLAN and VLAN

a) WEP is not a secure protocol anymore. The reuse of initialization vectors (IVs) is one problem. Explain in some detail how this can be used by an attacker! (3p)

Reuse of IV allows us to reuse a keystream if we know it. It can be retrieved for example by looking at the authentication messages, or …

b) This problem is addressed in WPA by using TKIP. What is TKIP? Mention three of its features! (3p)

Longer IVs, unique sequence numbers, change keys every 10,000 packets, CRC replaced by MIC, etc.

c) Another feature added in WPA and WPA2 is 802.1x – port-based authentication. What does this mean? Explain briefly! (2p)

d) VLAN is a useful link-level technology. There are two main ways it can be used in: with or without tags. Explain the difference! Is VLAN a good and secure technology? Motivate your answer! (3p)

4. SSL and VPN systems

a) The SSL record protocol performs 4 major (but optional) tasks, which? (2p)

Fragmentation, compression, adding MAC and encryption

b) A possible weakness in SSL is that a man-in-the-middle may alter the contents of the first negotiation phase to become a weaker cipher than the client really wanted. How do later versions of SSL make sure the packets sent during the handshake phase are not altered? Explain! (2p)

Since no encryption or MAC checking can be done before crypto-keys and ciphers are agreed upon, the client and server makes a hash of all important information being transmitted in the end of the handshake protocol. If the hash does not match the information the other party has received, the connection is terminated.

c) What protocol would you select when building a VPN system between two sites? Motivate your answer! (2p)

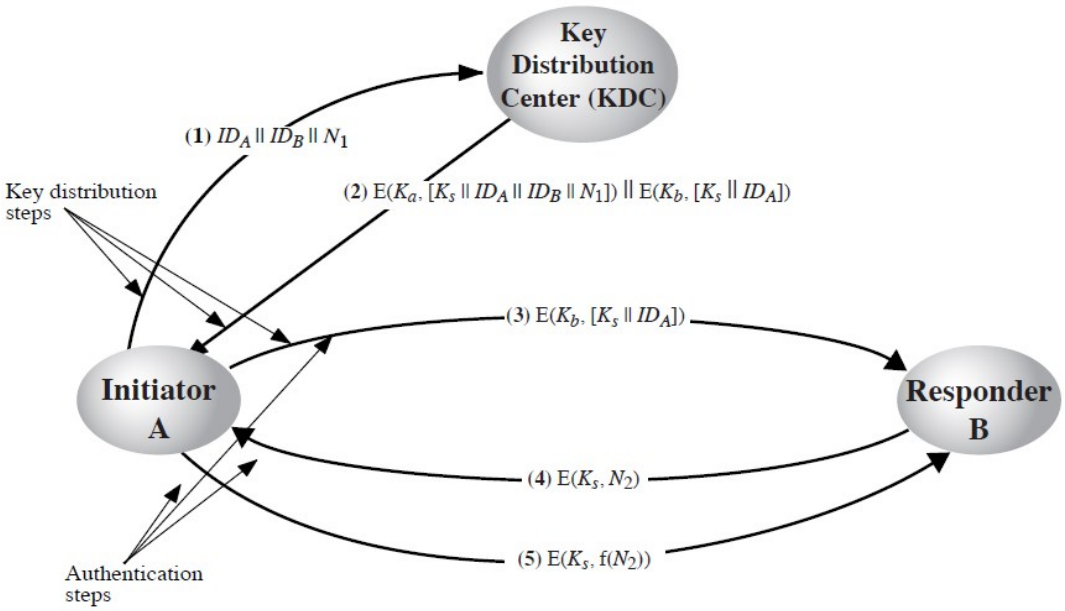
Most likely IPsec. Transparent for the transport layer and all application level protocols.

d) What protocol would you select when building a VPN system for remote users who need to access various services inside an office? There may be several solutions to this question. Please motivate your answer! (3p)

Most likely SSH or SSL. Easy to configure, client can run as an application without administrative privileges, etc.

5. Authentication

The following picture shows a proposed authentication method using a key distribution center (KDC). In the picture, encrypting something with *Key a* is written E(K_a, …).



a) Explain on a fairly high level how this protocol works! Don't just repeat what the picture tells but explain the purpose and outcome of each step! (4p)

See the book, picture 14.3 and explanation in chapter 15.2.

b) What is the advantage of using a KDC instead of using public/private key-pairs between the communicating parties? (2p)

Central authentication and authorization. Individual nodes do not have to care about users and user rights. Only one key to manage for a server (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) This protocol is not entirely secure although it is probably secure enough for most practical purposes. What is its main weakness (which is eliminated in Kerberos)? Propose a solution! Is there a drawback with this solution? (3p)

Attacks are possible with replays if the session key is broken or stolen from A's computer. Keys never expire – can be used and reused forever.

Use timestamps! Problem is that clocks must be synchronized and keys renewed regularly. Long sessions may be interrupted when keys expire.

6. Mixed short questions

Only a short answer (max 5 sentences) is needed when answering these questions, although a *motivation must be given* to see that you understand the concept.

a) Diffie-Hellman is vulnerable to MITM attacks. Explain what a man in the middle may do! (2p)

b) What is the reason lots of link level devices such as access points (APs) support Radius? What advantage do they get from it? (2p)

Central user account database. Easier administration.

c) What is the difference between a master key and a session key? Why are both needed? (2p)

Master keys derived from key negotiation process during connection setup. Master key then used to create session keys which are used for data encryption, etc,. and are changed regularly.

d) Is NAT useful as a firewall for a smaller office? Explain! (2p)

Ok. Hides internal structure (IP addresses). Only connections initiated from the inside can get reply traffic from the outside. If no entries exist in the connection table, all traffic from the outside is discarded.

e) What are the most important fields in a certificate used for authentication? (2p)

Subject, issuer, subject's public key, signature of issuer, (validity/expiration date), …