Technische Universität München
Informatik VIII
Netzarchitekturen und Netzdienste
Prof. Dr.-Ing. Georg Carle

Dipl.-Inform. Ralph Holz

Exercises for Lecture „Netzsicherheit“
Assignment 1, WS10/11

Hand-out:	Thursday October 21st 2010
Submission Deadline:	Thursday October 28th 2010
Exercise Hours:	Wednesday November 3rd 2010

Registration:
To participate it is necessary to register at the website of our department:
http://www.net.in.tum.de/de/lehre/ws1011/vorlesungen/network-security/

Assignments and Exercise Hours: The purpose of the assignments is to help you deepen your understanding of the subject and get your questions answered during the Exercise Hours. We thus strongly recommend doing the assignments and also to attend the exercises. However, we will not grade your work. There will be 6 assignments, roughly every 2 weeks. Two students are allowed to work together and hand in a solution together. The deadline is usually Wednesday, and new assignments are usually also released on Wednesdays. We hand them out, but you can also download them from the Web site. Every participant will be asked to present a solution to one Task at least once in the course of the semester.

Task 1: Security Threats and Services

Given a client-server architecture with a potential attacker on the data path.
The attacker can stage the following attacks:

- Eavesdrop on messages
- Modify messages
- Delay messages
- Delete messages

Let us assume that within the protocol there are mechanisms for the following security services:

- Confidentiality
- Data Integrity

(We will present such mechanisms in the lecture, e.g. encryption algorithms and cryptographic hash functions)

a) Which of the attacks mentioned above cannot be prevented with these security services?
b) Argue why confidentiality cannot guarantee that “data has not changed” without the receiver being able to notice it.
c) The designers of the system want to provide more security. What can they do to detect an attack that works by delaying messages by more than 45s?
d) What can be done so that the server can detect the following:
    - A message was deleted by an attacker.
    - A message was re-sent (replayed) by an attacker (”Replay Attack“).

Task 2: Brute-Force Attacks on Passwords

Let us assume there is a password-based authentication system. The password has 8 characters. In a brute force attack, the attacker tries all possible passwords to find the right one.

Assume that an authentication takes 1 µs and that the authentication server is stateless and does not remember the number of authentication attempts of a user, i.e. there are no delays after false authentication.

a) Assume all users only use lower case letters (no special characters, digits, etc.). These characters appear in passwords in a uniform and random way. How much time does the attacker need on average to find a password?
b) Now assume that capital letters, numbers and 31 ASCII special characters are also used (so-called strong passwords). What is the average time the attacker needs now?
c) Which methods for password cracking are better than brute force? Give an example of a particularly promising strategy and explain under which circumstances it can be expected to work better than brute force. Hint: You can find many examples on the Web, especially on sites dealing with hacking.

Task 3: Ping-of-Death

The application ”ping“ can be used to check whether a host is reachable on the Internet or not. The program sends an ICMP ”echo request“ message to the host. The host usually replies with an ICMP ”echo reply“ message.

ICMP messages are often blocked by firewalls in companies. One reason is an old attack called ”Ping-of-Death“ (which is no problem anymore, but used to be particularly bad). In addition, there are also other reasons why ICMP may be blocked, e.g. the desire to hide the network structure.

a) Do some research on the Internet. What is the Ping-of-Death? Explain.
b) Is this attack specific to ICMP or could it also happen with other transport protocols, e.g. UDP? Justify your answer.
c) What are possible countermeasures against the attack?
d) The attack is rather old and does not work anymore. What are similar attacks against today’s systems?

---- turn page ----

Task 4: The Network „sniffer“ Wireshark

For this task you need to install the packet sniffer Wireshark[1] on your system. You should also check its functionality, like the definition of “Capture Filters“. Now start capturing and start your Internet browser. You should now observe your HTTP Web traffic. Wireshark will present much information about packets on various layers, e.g. IP, TCP, and HTTP.

a) What are the risks when data is transmitted over the Internet unencrypted?

b) Now, open a Web site with HTTPs. Is it still possible to see the content on application layer? What information is available about application layer content? What “protocol” is HTTPs?

c) The connection to the Web server is based on the transport protocol TCP (layer 4) and the application protocol HTTP (layer 7). The three first TCP packets are:

• SYN	(Client → Server)
• SYN-ACK	(Server → Client)
• ACK	(Client → Server)

They are used to establish a connection with the Web server.
Find these packets with wireshark. What „flags“ (SYN, ACK, RST and FIN) are set in these three messages?

[1] Wireshark is available for Linux as well as windows systems (http://www.wireshark.org/)