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

Dipl.-Inform. Heiko Niedermayer

Exercises for Lecture „Netzsicherheit“
Assignment 1, WS09/10

Hand-out:	Thursday October 29th 2009
Deadline:	Thursday November 12th 2009
Exercise course:	Thursday November 19th 2009

Registration:
For the exercises it is necessary to register at the website of our department
http://www.net.in.tum.de/de/lehre/ws0910/vorlesungen/network-security/

Your homework: There will be 6 assignments, roughly every 2 weeks. Two students are allowed to work together and hand-in one solution. The deadline is usually Thursdays, and new assigments are usually also released on Thursdays. We hand them out, but you can also download them from the website.

Grades:
If you succeed in the exercises, you get a benefit of 0.3 in the exam. Success means:
• Regular and active participation in the exercises
• 75% of the tasks in the assignments have to be worked on. We do not correct your work, but we will check if you tried to solve a task.
• Each participant has to present a solution in the exercise.

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 the security services?
b) Argue why confidentiality cannot guarantee that data has not changed without noticing.
c) The designers of the system want. What can they do to detect an attack that delays messages 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 bruteforce 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 tries for a user, e.g. no delays after false authentication.
a) All users only use small letters and they use them in a uniform and random way. How much time does the attacker need on average?
b) Now assume that also capital letters, numbers and 31 ASCII special characters are used, so-called strong passwords. What is now the average time the attacker needs?

Task 3: Ping-of-Death

The application ”ping“ can be used to check wheather 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“ that is no problem anymore. However, there are also other reasons why ICMP may be blocked like hiding the network structure.

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

---- turn page ----

Task 4: The Network „sniffer“ Wireshark

For this task you need to install the paket sniffer Wireshark[1] onto your system.You should also check its functionality, like the definitionen of ”Capture Filters“. Now capture and start your Internet browser. You should now observe your http webtraffic. Wireshark will present a lot of information about packets on various layers, e.g.. IP, TCP, HTTP.

a) What is the risk when data is transmitted over the Internet unencrypted?
b) Now, open a website with HTTPS. Is it stilll possible to see the content on application layer. What information is available about this application layer content?
c) The connection to the webserver 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 session with the webserver.
    Find these packets with wireshark. What „Flags“ SYN, ACK, RST and FIN are all set with these three messages.

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