TECHNISCHE UNIVERSITÄT BERLIN
Fakultät IV – Elektrotechnik und Informatik
Fachgebiet Internet Network Architectures

WirelessLab WS 2016/17
Homework 8: Wireless (In-)Security

The purpose of this exercise is to get an overview over 802.11 security mechanisms and to provide a practical understanding of the attacker model in a wireless network, in order to be able to secure it against such threats. Furthermore, it illustrates the risks of insufficiently protecting one's wireless network, e.g. by using outdated encryption schemes, to increase awareness of this issue.

Question 1: (50 Points) *Cracking WEP*

In the same room as your nodes, an Access Point that uses the outdated WEP security scheme has been set up. It is periodically exchanging encrypted traffic with a client located in the same room over its wireless interface.

In this question, you crack the Access Point's encryption, first in a passive attack by only listening, then in an active one by injecting frames to get the system to generate traffic. Your goal is to obtain the WEP key and decrypt the communication.

(a) Set up the aircrack-ng suite on your own device(s) and/or on (one of) your nodes. Describe your setup and how you distribute the tasks between the different devices that you use.

Note: For certain tasks, like injecting frames, you may need a specific chipset in your wireless network card, which is present on your nodes. For other tasks, there are no hardware requirements. Some tasks require more computing power than others.

(b) With a monitor interface, capture the WEP-encrypted 802.11 frames exchanged on the network "WirelessLab_WEP_Crack_Me" on channel 11 and perform the PTW attack on them. Do not inject your own frames yet, but just listen to the already existing traffic.

Describe all of your steps and record the date and time of your attack. Obtain the WEP key. How long did the attack take, and how many frames and IVs did you need?

If successful, decrypt the traffic and describe it. Who is talking to whom here, and what protocols do you see?

(c) Crack the WEP encryption using an active attack, injecting ARP requests to the network "WirelessLab_WEP_Crack_Me" and capturing the traffic. Try to obtain the WEP key using the KoreK attack.

Note: Some of the "hacker tools" may be buggy or broken. Specifically, the "frame injection test" of aireplay-ng is known to fail even though frame injection actually works.

Describe all of your steps and record the date and time of your attack. Did it work? If so, how long did it take? What is the difference between PTW and KoreK attack?

(d) What are the advantages and disadvantages of an active attack, compared to a passive attack?

(e) How could the two devices secure their communication, such that it is not possible to decrypt their traffic? Describe at least 2 realistic possibilities (practical ones, please, not some theoretical stuff that nobody actually uses).

Question 2: (30 Points) *Cracking WPA-PSK*

In the same room as your nodes, there is another network which has been secured using the more advanced WPA2 encryption scheme with a Pre-Shared Key ("Wifi password"). There is a client connected to it.

In this question, you analyze the security of this network and try to crack it using a dictionary attack.

(a) With a monitor interface, capture traffic on the network "WirelessLab_WPA_Crack_Me" on channel 1 until you observe at least one four-way handshake of a client authenticating to the AP. Rather than just passively listen, you may also "help" make it happen.

Examine the header fields of the beacon of the network, and the handshake messages and document your observations. In the beacon, what Cipher Suites are advertised? Which message is the first step of the authentication/association of the client? After this first message exchange, you should observe an association request and response, and then the four-way handshake within 802.11 data frames. What information is exchanged there, which is then used to construct the PTK (session encryption key)? How is the handshake secured against replay attacks? (Please show the frames that you are talking about in your documentation, e.g. as a screen shot.)

(b) Using aircrack-ng, try to crack the WPA key using a dictionary attack. (Hint: The password is an English word in lower-case.)

Describe all of your steps and record the date and time of your attack attempt. Did it work, and if yes, what is the WPA key? In any case (even if you are unsuccessful), explain why one needs to capture at least one four-way handshake to perform this attack.

Question 3: (20 Points) *How secure is eduroam?*

Eduroam is the Wireless LAN that most of us use each day when on campus.

(a) Would one of the above attacks work against eduroam? Why (not)?
(Please do not try it out!)

(b) Is there another possibility to attack a network such as eduroam, getting unauthorized access?

Submission
`https://isis.tu-berlin.de/course/view.php?id=8501`
Please submit a PDF document containing *a cover page* with your names and group ID, and *having your group number in its file name.*
The PDF should contain:

- A description of your setup and the steps that you took to crack the networks' encryption.
- The answers to the questions.

Please also include packet traces of the decrypted WEP traffic and the four-way handshake, or at least have them available for the debriefing.
Make an archive (.tar.gz, .zip) containing *a directory* with all of your files and *having your group number in its file name.* All files that belong to a specific question must have the question/subquestion in their filenames. Please try not to clutter your submission with temporary files.
Due Date: Wednesday, 11. January, 23:55.