Author: Ruxandra F. Olimid
Computer Science Department, University of Bucharest

- Laboratory Assignment -
WiFi Security - WPA

Disclaimer: During this course/lab you will be introduced to various notions of computer security, with the aim of learning how to secure systems. All notions and exercises are presented for didactic purposes, even if sometimes you are supposed to think like an adversary. Do not use these techniques for malicious purposes! They may have legal consequences in the event of committing crimes, for which you become fully responsible!

For this laboratory assignment, you need to use wpa-Induction.pcap from [1]. It is a 802.11 capture with encrypted WPA data. As indicated at [1], use the password *Induction*.

1. *Inspect capture and decrypt WPA encrypted traffic*

Download and inspect the capture. Reference [2] might be of help.

a) Download and inspect the capture
b) Enter the WPA key and decrypt the traffic
c) Identify a client and an Access Point (AP). Find the corresponding MAC addresses.
d) Identify the broadcast messages sent by the AP. Which is the SSID? Which is the beacon interval?
e) Search for HTTP traffic. Find and follow a TCP or HTTP stream. Name a website the client visits.

2. *4-Way Handshake*

Look into the EAPOL handshake. References [3,4] might be of help.

a) Identify the four frames of the EAPOL handshake.
b) Find the values of the two nonces further used in the key agreement.
c) Find the value of the GTK.
d) Which of the four frames is integrity protected?
e) Which of the four frames contains encrypted data? Why?
f) Find the values of the two EAPOL keys *Key Confirmation Key (KCK)* and *Key Encryption Key (KEK).* What are these used for?

References

1. Wireshark *Sample captures*. Available at: https://wiki.wireshark.org/samplecaptures
2. S.Bowne. *Project 22: WPA/WPA2 Decryption.* Available at: https://samsclass.info/123/proj14/p22-WPAdec.html
3. Network Lessons. *Introduction to WPA Key Hierarchy*. Available at: https://networklessons.com/wireless/introduction-to-wpa-key-hierarchy
4. Network Lessons. *WPA and WPA2 4-Way Handshake*. Available at: https://networklessons.com/wireless/wpa-and-wpa2-4-way-handshake