Linnaeus University
Computer Science
Ola Flygt

2021-11-29

2DV703 Mobile and Wireless Data Security

Assignment #4

A. Theoretical part (complete before the seminar Monday 6 December)
As theoretical task this week you should read the following articles;

- "Client-based Intrusion Prevention System for 802.11Wireless LANs" by Zhang and Sampalli
- "Undesired Relatives: Protection Mechanisms Against The Evil Twin Attack in IEEE 802.11 by Analyzing Network Traffic Characteristics" by F. Lanze, A. Panchenko, I. Ponce-Alcaide and T. Engel
- "Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks" by Lazos and Krunz

You will find the articles in MyMoodle. Read them carefully. We will discuss these articles on the seminar 6 December. Come well prepared!

B. Practical part (completed at latest Friday 16 December)

For this assignment you will again have to make a proper lab report that describe all your findings and answer the specific questions posed in the assignment. Submit the lab report in MyMoodle.

B.1 VPN
Look into VPN alternatives. You may use your ASA5510, your internal windows server or a separate VPN Server. The decision should be done taking into account security, ease of implementation and management. The same radius server handling the authentication for the WPA Enterprise WiFi should be used for the authentication.

When you have a solution, you should implement and test it by connecting to the network using different mobile clients (laptop, iOS and Android mobile devices all available in the lab) from the outside. You might have to set up an open WiFi network on the outside for some of the clients.

B.2 Indoor positioning
Implement the AnyPlace indoor positioning system (https://anyplace.cs.ucy.ac.cy) or a similar system of your choosing in the lab using the access points we have there. You may during this task move some of access points out to other places in the D building to get better coverage. The idea here is to have a client on a mobile device being able to see her position on a map while walking around indoors. Evaluate the system to see how accurate it is. Does it require you to first fix the position of a number of access points or can it do it by itself? How is the precision changed if you use one, two or more access points as reference points?

Linnaeus University
Computer Science
Ola Flygt
2021-11-29

B.3 Locate the AP's

Use two different applications to map wireless access points in the building you have been allocated. Options include, but are not limited to:

- AnyPlace, using the floor plans provided with the Architect and View features
- Acrylic Wi-Fi HeatMaps (https://www.acrylicwifi.com/en/blog/free-student-license/)
- Ekahau HeatMapper (https://wifi.ekahau.com/heatmapper)

Your task is to detect all wireless access points and exactly identify the location of all the APs within a building. Compare the results from the two solutions and evaluate how precise they are but also how easy they are to use. You may limit yourself to only check the ground floor if you wish.

You may use the floor plans found provided in MyMoodle.

Group 1: B Building
Group 2: D Building
Group 3: K Building
Group 4: Library
Group 5: K2 Building

In the report you should describe:

- How did you locate them?
- Is there any AP that you think is in the building, but you could not exactly locate?
- Are any of them considered to be rouge access points (malicious or non-malicious)?
- Are any of them considered to be a security problem (even if not a rouge AP?

B.4 Find the Brands on mobile devices

We will now see what types of devices are on different locations of campus and how to find this out. Each group member shall capture (“dumps”) 10-15 min of wireless traffic at different times on crowded locations within the area where your group located APs. Parse out the MAC addresses and show their brand: e.g. http://wintelguy.com/bulkmac.pl

You might find a large number of devices of the type “Locally administered MAC address” or other MAC addressed you may find it hard to map to a brand. Why do some devices have this label? Are there any security problems or advantages with this? Can you somehow find out or guess what actual device type is behind this label?

Each group then makes a graphical representation that shows the quantity of the 5 largest represented brands and “other”. Also present other relevant information such as number of MAC addresses acquired, length of capture etc. We will then compare the results from the different groups.

Don't forget to also properly document your methods on certain decisions you may have to take such as, how to handle duplicates.

Linnaeus University
Computer Science
Ola Flygt

2021-11-29

Voluntary work:
When you scan for Wi-Fi access points you may find other types of devices e.g. IoT devices. In many cases they are not using Wi-Fi, instead they could be using Bluetooth or 6LoWPAN. This mean you you will have to scan these types of networks as well. Can you find any such devices and are they mobile or stationary?

Good luck!