Sprint Retrospective Document

Date: 28/11/2018
Project acronym: PENIOT
Members: Berat Cankar
Bilgehan Bingöl
Doğukan Çavdaroğlu
Ebru Çelebi
Supervisor: Dr. Pelin Angın

Sprint 2 summary

Item ID (from the previous retrospective doc)	Workpackage ID (from the Kick-off doc)	Status	Group's comments
1	2	Complete	We gave a list of devices to buy to the department and this list was approved. This week we will order these devices and we will wait for them to arrive. We also installed the main software tools we predict we will need during this project. If we need more software tools during our implementation, we can download them on the run.
2	3	In progress	We implemented sniffing functionality, it scans environment, then finds the devices in a short range. We wrote the code in order to sniff the found devices (collecting the messages and analyzing them) with respect to API of Zigbee framework; however, we could not try our code since we could not obtain the proper hardware devices to test our code. We will order these devices this week with the help of department Also, we started to implement basics of attack. For example, we wrote

			packet dumper for captured packets and reader for reading dumped packets which will be used while performing replay attack. Also, we wrote a packet parser which extract specific information from the obtained packet. With this, we will be able to perform beacon frame flood attack by using those information like coordinator id, personal area network id of the captured packets.Because of some problems related to devices (we could not find a device called RzRaven. The site says it is sold out.We checked other sites as well,but it seems that it is very difficult to find one),we will continue with BLE and MQTT attacks until we find a solution for that problem.
	4	Was not on the initial plan (timing changed)	Since we did not have any devices for Zigbee protocol, we decided to move on with BLE protocol which requires less devices. We simply implemented scanning functionality and some functions which returns specific information about a BLE device such as services and characteristics it provides. We will have a look at sniffing a BLE message traffic and try to implement one or more attacks such as replay attack.
	5	Was not on the initial plan (timing changed)	We got our Raspberry Pis from the department. Therefore, we decided to implement some functionalities which enable us to attack a MQTT network.Since there will be a demo at the end of December, we want to have something real until that time. According to our initial plan, we would like to implement some attacks for Zigbee,but we encountered some problems related to devices, we have to add these two items (this one and the above one) to Sprint 2.

Sprint 3 plan

Item ID	Workpackage ID (from the Kick-off doc)	Description	Status
1	5	We will try to provide sniffing functionality on the devices found in local area.	New
2	5	Since we have Raspberry PIs, we will try to perform replay and fuzzing attacks for this sprint.	Left over from Sprint 2
3	4	We have implemented some functionality for sniffing BLE, but we will improve and add more features related to it.	New
4	4	We will try to create infrastructure for BLE attacks, also try to implement one of the attacks that we promised in WP description.	Left over from Sprint 2

Overall progress

	Sprint 1	Sprint 2	Sprint 3	Sprint 4	Sprint 5
MF1	0	15			
MF2	0	0			
MF3	0	0			

MF4	0	5			
MF5	0	0			
MF6	0	0			
MF7	0	0			
MF8	0	5			
MF9	0	10			
MF10	0	0			
MF11	0	0			