Sprint Retrospective Document

Date: 19/12/2018
Project acronym: PENIOT
Members: Berat Cankar
Bilgehan Bingöl
Doğukan Çavdaroğlu
Ebru Çelebi
Supervisor: Dr. Pelin Angın

Sprint 3 summary

Item ID (from the previous retrospective doc)	Workpackage ID (from the Kick-off doc)	Status	Group's comments
1	5	Complete	We are currently able to sniff MQTT messages in order to use them for our other MQTT attacks. We also implemented our own packet parser to get internal information from those sniffed packets.
2	5	Complete	We created necessary environment for Raspberry PIs to be able to perform MQTT attacks. We implemented the previously mentioned attacks for MQTT. For replay attack, we sniff the packets of target device, then send them at a different time. For DoS attack, we implemented a continuous topic flooder to exhaust broker resources. For fuzzing attack, we implemented different cases such as malformed packet handling, maximum payloaded packet sending and also publishing to SYSTEM topics (which is forbidden in MQTT protocol). All these cases must be handled by the broker, if not they can lead to serious misfunctions. Our aim is to test this.
3	4	In progress	In this sprint, our main aim was to finish necessary functionalities for

			MQTT attacks because of a change in project timing. Also, the department has ordered the hardware devices we need for implementing BLE functionalities but they did not arrive yet. Therefore, we completely focused on MQTT and we did not improve our previous BLE sniffing capabilities. However, we will have a look at it and complete BLE sniffing at the beginning of the next sprint.
4	4	In progress	Although we have some functionalities to perform BLE attacks, we do not have any implementation yet since we could not test our sniffing module due to lack of hardware devices. After we are done with sniffing part, we will implement attacks which we decided (replay attack, fuzzing attacks). Moreover, we will continue to search for possible vulnerabilities and we will increase the number of attacks that we have.

Sprint 4 plan

Item ID	Workpackage ID (from the Kick-off doc)	Description	Status
1	4	We planned to complete sniffing of target device and packet parser for BLE protocol to get necessary information.	Left over from Sprint 3
2	4	Although we did not decide particular attacks to perform, we planned to implement two or three attacks for BLE.	Left over from Sprint 3

Overall progress

	Sprint 1	Sprint 2	Sprint 3	Sprint 4	Sprint 5
MF1	0	15	15		
MF2	0	0	0		
MF3	0	0	100		
MF4	0	5	100		
MF5	0	0	0		
MF6	0	0	0		
MF7	0	0	0		
MF8	0	5	5		
MF9	0	10	10		
MF10	0	0	0		
MF11	0	0	0		