Sprint Retrospective Document

Date: 20/02/2019
Project acronym: PENIOT
Members: Berat Cankar
Bilgehan Bingöl
Doğukan Çavdaroğlu
Ebru Çelebi
Supervisor: Dr. Pelin Angın

Notes: There are several changes on master features of the project. We decided to change the list of protocols that we initially wanted to implement as written in our Kick-off document. We decided to implement CoAP protocol instead of the RPL protocol. Also, due to lack of hardware devices and library resources, we decided to remove Zigbee from the protocol list. However, we currently did not decide on the substitute protocol, we are working on it now. Candidates include KNX and XMPP protocols. All the master feature changes are described later in the document in a detailed way.

Sprint 5 summary

Item ID (from the previous retrospective doc)	Workpackage ID (from the Kick-off doc)	Status	Group's comments
1	4	Dropped	Due to lack of necessary equipment, the item is lasted for several sprints and still the department was not be able to get those devices, so we decided to drop the item.
2	4	Dropped	The same as above comment, we decided to drop this item.
3	7	Dropped	In semester break, we implemented all the attack set for CoAP, so we decided to integrate with fresh protocol CoAP instead of MQTT. With some changes in code structure, MQTT also needs to get overview and to be tested, so we started to structure and plan our codes for integration with CoAP for now.
-	7	Was not on the initial	We researched for python libraries to

		plan	create a graphical user interface for our project. After deciding to use Kivy library, we designed the general structure of the interface.Then, we created ‘Home Page’, ‘About Us Page’ and ‘Help Page’.
-	6	Was not on the initial plan	We implemented sniffing attack for CoAP while improving previous sniffing module of our project.
-	6	Was not on the initial plan	We created DoS attack functionality for CoAP protocol.
-	6	Was not on the initial plan	We coded two different fuzzing method for CoAP protocol; random payload fuzzing and payload size fuzzing.

Sprint 6 plan

Item ID	Workpackage ID (from the Kick-off doc)	Description	Status
1	3	Research for new protocol in order to replace Zigbee	New
2	3	Implement one attack for the new researched protocol	New
3	3	Implement example server and client for the researched protocol for testing	New
4	4	Research and implementation of an application layer IoT protocol, possibly to replace BLE protocol	New
5	7	Design and implement attack selection page	New
6	7	Design and implement attack input page	New
7	7	Integration of CoAP attacks and graphical user interface	New

Overall progress

	Sprint 1	Sprint 2	Sprint 3	Sprint 4	Sprint 5	Sprint 6	Sprint 7	Sprint 8	Sprint 9
MF1*	0	15	15	15	0				
MF2*	0	0	0	0	0				
MF3	0	0	100	100	100				
MF4	0	5	100	100	100				
MF5**	0	0	0	0	100				
MF6**	0	0	0	0	100				
MF7	0	0	0	10	10				
MF8	0	5	5	8	8				
MF9	0	10	10	10	20				
MF10	0	0	0	0	0				
MF11	0	0	0	0	0				

Master feature list

MF-1 - Sniffing Zigbee message traffic **(Change will be done, but not finalized yet)**
MF-2 - Zigbee attacks (at least 1) **(Change will be done, but not finalized yet)**
MF-3 - Sniffing MQTT message traffic
MF-4 - MQTT attacks (at least 1)
MF-5 - Sniffing CoAP message traffic **(RPL is replaced with CoAP)**
MF-6 - CoAP attacks (at least 1) **(RPL is replaced with CoAP)**
MF-7 - Sniffing BLE message traffic
MF-8 - BLE attacks (at least 1)
MF-9 - Easy-to-use menu (interface)
MF-10 - Report generation with respect to test cases
MF-11 - External module integration capability

(*) Zigbee will be dropped because we could not get the necessary hardware devices to work on Zigbee. We did not finalize the substitute protocol, but in the following sprint, we will conduct research for it.
(**) RPL is dropped because we could not find useful open source Python libraries about RPL that enables us to develop the project properly. Also, we thought it would be better if we worked on more popular and more common IoT protocols. The coding part of replaced code is done in semester break.

Notes: In order for informing concerning work packages, they are not affected by master feature changes since just the name of protocol is changed.