METU

DEPARTMENT OF
COMPUTER ENGINEERING

CENG 49x - Computer Engineering Design

Project Proposal Form

Important Notes

1. Please read carefully, and follow the instructions below to fill in this form.
2. A project could be proposed by (i) a student or a student group, (ii) a company, or (iii) a faculty member of the department by filling in this form and submitting it to 49x-proposal@ceng.metu.edu.tr by e-mail. For a project proposal, there might be a sponsoring company supporting the project and providing some form(s) of resources for the project.
3. Each project will be carried out by a group of 4 students over the course of 7.5 months, which amounts to 30 person*months. It is very important that your project's workload is around 30 person*months. Please make sure that you have at least a rough justification about the workload of the project.
4. The reader won't necessarily be an expert in the project's field. So, please avoid jargon and if you use an abbreviation, make sure to include its expanded form. The proposal should be understandable by a 3rd year CENG student.
5. If your proposal might contain a patentable idea or any type of intellectual property, please first make sure to follow the appropriate steps (apply for a patent, etc.) before sending your idea to us. Once this form is received from you, the instructor(s) and the department has no responsibility regarding the intellectual properties of your project/idea.
6. All sources and documentation developed for this course are assumed to be public domain (GPL, CC or similar license) by default. If you need any exception for license and disclosure of project work, please specify this in detail in "Intellectual Property" section of the form.
7. Please note that source codes, documents and issue tracking will be kept in department servers. No restrictions can be requested for limiting faculty and assistants access to student work.
8. Instructions to fill in this form are given in italic fonts and in parentheses. To provide an input for a section of the form, delete the instruction and provide your input in place of the deleted instruction. In the final form that you will submit, there shouldn't be any instructions left over.
9. If you feel that a particular instruction is not relevant to your project proposal, please use a proper explanation for this, rather than ignoring the instruction.
10. The final form should not exceed 5 pages including everything (even this page). Please use Arial, Normal, 11pt fonts and single line spacing.
11. The final form should be submitted as a PDF file.

Acronym and Title

PENIOT: A Penetration Testing Tool for Internet of Things

Target

[ ] This proposal can be announced to all student groups. It can be assigned to any student group.
[X] This proposal is restricted to the following students/groups: Berat Cankar, Bilgehan Bingöl, Doğukan Çavdaroğlu, Ebru Çelebi (e209885@metu.edu.tr, e217136@metu.edu.tr, dogukan10cav@gmail.com, eebrucelebii@hotmail.com)

Proposer Information

Names(s):	Berat Cankar Bilgehan Bingöl Doğukan Çavdaroğlu Ebru Çelebi
Email(s):	e209885@metu.edu.tr e217136@metu.edu.tr dogukan10cav@gmail.com eebrucelebii@hotmail.com

Supervisor

[X] The project will be supervised by Dr. Pelin Angın.
[ ] The project can be supervised by any faculty member. Suggestions: _____

Project Description

This project aims to develop an extensible penetration testing tool for the Internet of Things (IoT). The IoT paradigm has experienced immense growth in the past decade, with billions of devices connected to the Internet. Most of these devices lack even basic security measures due to their capacity constraints and designs without security in mind due to the shortness of time-to-market. Due to the high connectivity in IoT, attacks that have devastating effects in extended networks can easily be launched by hackers through vulnerable devices. In this project, we will develop a penetration testing tool that automates the process of security testing for various IoT devices and network configurations by launching selected IoT-specific attacks (e.g. attacks on the BLE protocol, 6LoWPAN protocol, RPL protocol, distributed denial of service, man-in-the-middle etc.) on devices through an easy-to-use menu with attack parameters set by the user. The end product will be a penetration testing tool that IoT software and hardware developers can utilize to test the security of their products against common/new attacks on IoT-specific protocols and devices. The tool can also be extended by security engineers to integrate additional tests as new IoT devices/protocols and corresponding exploits are launched.

Tentative Plan

WP0: Literature review of IoT attacks and finalization of system requirements [4 PM]
WP1: Test environment setup with necessary IoT equipment [4 PM]
WP2: Implementation of selected IoT security tests/attacks [12 PM]
WP3: Testing of implemented security tests in the IoT environment and fine-tuning [6 PM]
WP4: Implementation of modular tool integrating implemented security tests [4 PM]

WP0 should be implemented first, followed by WP1. WP2 and WP3 will take place in an iterative manner, with feedback from WP3 used to guide WP2. WP4 will take place last, after all security tests have been written.

Similar Products/Projects

Metasploit [1]: Metasploit is an open source, modular penetration testing tool that provides tremendous help to security experts. In some sense, it is an automation attempt for general penetration testing. However, IoT support was non-existent. Recently (in 2017), Rapid7 (the company that acquired Metasploit in 2009) started adding IoT support to it, but this is still at an initial stage.

Expliot [2]: Expliot is a framework to perform security testing and exploitation of IoT infrastructure and IoT devices. It is an open source project, but it is just newly created (June 2018) and it is not complete yet (still at the very beginning).

There are quite a few companies that offer IoT testing services (an example is [3]). However, all of them employ an ad-hoc and manual approach. There are very few penetration testing tools in the IoT field. We could only find two such tools and one of them is just starting, while the other is just expanding to the realm of IoT. They are not comprehensive.

Contributions, Innovation and Originality Aspects of the Project

Most of the existing automated penetration testing tools have been designed for traditional networks and devices, and do not test for IoT-specific vulnerabilities caused by use of various new protocols (e.g. MQTT, DTLS, CoAP, BLE, Zigbee etc.), resource constraints in IoT devices etc. There are a few IoT penetration testing products in the market, as mentioned above, however these are usually limited in their testing functionality for specific protocols or devices and do not provide a comprehensive test set. Comprehensive IoT pentesting is usually performed manually by companies specializing in this field, however those tests are not available to be run in an automated manner by companies developing or utilizing the IoT devices.

The main contribution and advantage of our tool over similar products will be that it will provide automated tests for IoT-specific attacks for a variety of devices and networks. While it is not possible to implement security tests for all kinds of IoT devices and communication protocols during the project period, the tool developed will have a modular architecture to provide easy integration of other security tests in the future. As a side effect of the project, we plan to construct an attack dataset that could be useful for IoT security researchers.

Success Measures

The success of the project will be evaluated through the following measures:

- The system should be capable of launching at least 5 different IoT-specific attacks on appropriate devices/networks and showing that the attacks succeed on vulnerable IoT devices/networks
- The system should be capable of easily integrating different attacks on IoT for future extensibility.
- The tool should provide menus that are easy-to-use for novice pentesters and be easy to extend for expert users.

Project Development Environment

We plan to develop the tool on Linux using python. Although we do not expect to need major software/hardware tools for the development of the attacks (perhaps other than open-source network packet sniffers like Wireshark), we will need low-cost IoT devices and networking equipment to test the attacks on vulnerable IoT devices/networks. Major IoT devices and networking equipment needed for the tests are available at the WINS lab, with which Dr. Angın is affiliated. However, depending on the attack set we determine, additional IoT equipment may be needed.
Our plan is to study major IoT-specific attacks posing significant risks to their subjects, as determined by the Open Web Application Security Project (OWASP) [4], and implement a subset of them. An isolated IoT test environment will be setup with the available equipment, attacks will be launched on the vulnerable devices and implementation will be refined until effective.

External Support

Our supervisor has talked to the Arçelik Teknokent office, which is supportive regarding the testing of their IoT products with the tool we will develop. At the start of the project, we will discuss the availability of their tools and can plan the penetration test implementation set accordingly.

Intellectual Property Information

The group members and the academic advisor will have IP rights to (re)use and/or modify and/or share the project material (source code, program, data etc.) without restrictions. In case a publication made from the project material, the project members contributing to the paper (in terms of research content) will receive credit.

Major Risks and Risk Plan

Major risks for the success of the project and contingency plans are as follows:

- Some of the initial set of attacks on IoT that we decide to implement/test may prove difficult to implement given our resources. In that case, we will replace that attack with another one from the extended list, making sure we have the required resources for implementation and testing.
- We may not be able to purchase the equipment needed for testing of specific attack implementations or may experience delays in the purchase. Delays can be resolved by changing the implementation schedule. For required equipment, we may be able to get help from Arçelik as discussed above.

References

[1] https://www.metasploit.com/
[2] https://linuxsecurity.expert/tools/expliot/
[3] https://www.attify.com/
[4] https://www.owasp.org/

/ End of the proposal */*