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

ARTEMIS: A Near Real-Time Monitoring and Intrusion Detection System for IoT

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.
Ataberk Dönmez, Mert Erdemir, Mert Kaan Yılmaz, M. Ege Çıklabakkal (e217154@metu.edu.tr, e209953@metu.edu.tr, e209897@metu.edu.tr, e217150@metu.edu.tr)

Proposer Information

Names(s):	Ataberk Dönmez Mert Erdemir Mert Kaan Yılmaz M. Ege Çıklabakkal
Email(s):	e217154@metu.edu.tr e209953@metu.edu.tr e209897@metu.edu.tr e217150@metu.edu.tr

Supervisor

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

Project Description

The Internet of Things is now being used increasingly in transportation, health, agriculture, smart home and city systems. Even if they are produced and used at constant speed, IoT devices that are expected to reach 50 billion devices all over the world by 2020, are required to be deployed at 1 million devices per hour. Taking into account commercial pressures, production and deployment at this rate show that a very important layer, i.e. security, will either be completely neglected or have significant shortcomings. Since IoT devices do not have sufficient security, a variety of cyberattacks are being launched, which can result in major damages.

The goal of this project to develop a high-performance monitoring and intrusion detection system for the Internet of Things (IoT), taking into consideration protocols such as MQTT, CoAP, DTLS, LoRaWAN, BLE etc. specific to the IoT domain. Due to the variety of protocols and devices used in IoT, our tool will focus on the most commonly used and commonly attacked ones, which will be determined through literature review. The system will process large amounts of data gathered from a heterogeneous IoT network composed of low-power IoT devices and high-capacity servers in near-real time using mostly unsupervised machine learning algorithms and create alarms in case of detection of deviations from the normal behavior of the system. The end product will be an extensible monitoring and intrusion detection tool for IoT systems, that supports plugging in different data sources (IoT devices, networks, protocols) and anomaly detection algorithms. The tool will be demoed with the setup of a realistic IoT scenario and launching intrusions on the system using open source attack tools.

Tentative Plan

WP0: Literature review regarding major IoT attacks and finalization of software requirements [4 PM]
WP1: IoT equipment purchase and environment setup [4 PM]
WP2: Streaming architecture development for IoT data collection [6 PM]
WP3: Identification of anomaly detection algorithms and implementation [6 PM]
WP4: Identification of open source IoT attack tools and performance of tests with them [3 PM]
WP5: Intrusion detection tests and implementation refinement [7 PM]

WP0 should precede all packages, followed by WP1 and then WP2. WP4 can go in parallel with WP3. WP5 should be last.

Similar Products/Projects

SVELTE
SVELTE is a real-time intrusion detection system for the IoT that primarily targets routing attacks such as spoofed information, sinkhole, and selective-forwarding. It is the first attempt to develop an IDS for the IoT. SVELTE makes use of signature based detection, also, anomaly based detection is possible through extensions of the project.

Security Onion
Security Onion is a network security monitoring tool with sniffing, intrusion detection systems, analysis tools coupled together. It uses Snort or Suricata programs for Rule-driven Network Intrusion Detection Systems (NIDS) and Bro IDS for Analysis-driven NIDS. Also, it supports Host Intrusion Detection Systems (HIDS) by using OSSEC program.

Hogzilla
Hogzilla is an open source Intrusion Detection System (IDS) supported by Snort, SFlows, GrayLog, Apache Spark, HBase and libnDPI, which provides Network Anomaly Detection. Hogzilla also gives visibility of the network. Hogzilla can detect port scans, various attacks, tunnels and more.

Contributions, Innovation and Originality Aspects of the Project

While legacy IT intrusion detection system (IDS) is a well-known and used technology, real-time intrusion detection solutions are much newer in the IoT world (and in compliance with IoT standards). Realization of these solutions is an important necessity for the safety of a large number of products, fast produced and inexpensive (without additional security software / hardware). Today's intrusion detection systems (antivirus, firewall, etc.) cannot be used on these devices due to low processor power and memory capacity of IoT devices. The methods used in intrusion detection systems are different in mobile devices, local networks, and wireless networks. Since IoT has a heterogeneous structure, there is a need for intrusion detection systems to be designed to solve this problem. IoT involves various protocols and types of devices, all of which have different vulnerabilities not addressed by existing IDS for traditional networks. Also, most existing IDS rely on rule-based systems, which are incapable of detecting attacks outside their signature set. The contribution of this project will be the creation of a framework for addressing the near real-time monitoring and intrusion detection problem in heterogeneous IoT networks, focusing particularly on IoT-specific protocols and devices as opposed to legacy IDS. Through developing an anomaly-based detection approach with machine learning, the developed tool has the goal of detecting intrusions without using attack signatures, which will also prove useful for zero-day attacks.

Success Measures

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

- The developed system should be capable of collecting and processing network packet data and IoT device data in near real-time.
- The developed system should be capable of detecting anomalies in the IoT network with at least 90% precision and 90% recall.
- The system should be capable of easily integrating different anomaly detection algorithms and data sources for future extensibility.

Project Development Environment

We plan to use Apache Spark for streaming and processing of the data from the IoT devices and the Apache Spark MLLib (which provides APIs for Python, Java, R and Scala) for development of anomaly detection algorithms. In order to gather packet-level data in the network, we plan to utilize open-source packet sniffing tools like Wireshark and extensions for sniffing BLE packets. We will need to setup a simple IoT scenario involving a gateway (router), a few sensors and an IoT device like a Raspberry Pi to show real-world applicability of the system’s operation. For realizing intrusions, we will utilize open-source attack tools for different protocols in the IoT domain.

Since the intrusion detection process will be anomaly-based, we plan to generate the dataset regarding the normal operation of the IoT network ourselves under controlled conditions. An external machine learning dataset use is not planned at this point, but should there be problems with dataset generation, we can utilize some well-known intrusion detection datasets like KDD Cup’99 and UNSW-NB15.

External Support

The bulk of the networking equipment (such as routers) we need for the project will be provided by the WINS lab, with which Dr. Pelin Angın is affiliated. We will need a server on which we will install Spark and run the anomaly detection tasks. In the event that we are not able to find open source packet sniffing tools for IoT network protocols like BLE, we may need to purchase low-cost software (not to exceed $25). We may also need an IoT kit including sensors supporting the radio communication technologies we decide to focus on in the project, should these not be available in the WINS lab.

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 (concepts, algorithms, source code, program, 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 project and contingency plans are as follows:

- We may not be able to achieve the intended precision/recall rate with the primarily selected machine learning algorithms. In that case we will switch to different algorithms guided by our literature review and possibly try an ensemble learning approach.
- We may not be able to achieve the intended performance in terms of speed, in data processing and intrusion detection due to factors like the large size and dimensionality of data. If that is the case, we will try utilizing data sampling and dimensionality reduction algorithms to preprocess the gathered data.
- There might be issues using the open source attack generation tools for IoT. In that case, we might need to reduce the set of attacks with which we will perform our intrusion detection tests, but we will still be able to show the functionality of the product.

References

Raza S., Wallgren L., Voigt T. (2013). SVELTE: real-time intrusion detection in the internet of things. *Ad Hoc Networks, 11*(8), pp. 2661-2674.
Security Onion : https://securityonion.net/
Hogzilla : http://ids-hogzilla.org/

/ End of the proposal */*