Cardiff University
School of Computer Science and Informatics

Evaluating Intrusion Detection Systems in IoT

Initial Plan

Author:
Haya Alsultan

Student Number:
1558069

Supervisor:
Philipp Reinecke

Moderator:
Charith Perera

Table of Contents

Project Description:

Introduction:

Internet of Things (IoT) is a recent paradigm that integrates physical objects and the Internet. It combines connectivity with devices, sensors, and people, allowing a form of conversation between human and machine, software and hardware. These conversations can enable devices to predict, react, and improve the physical world similarly to how the internet currently uses networks and computer screens to improve the information world. One of the main aims of IoT is to enhance the quality of human life in terms of comfort and efficiency. It is applied in several domains, such as smart environments, automation of homes, and environmental monitoring. It is estimated that by 2020, the market will have approximately 30 billion connected devises (EY Global 2019). Although the potential for IoT is vast, its practical execution still remains in its beginnings. Therefore, despite its many benefits, it also introduces security issues due to its security vulnerabilities, which could affect its applications. Intrusion Detection Systems (IDS) have been an important tool for the protection of information systems and networks. IDS perform intrusion detection by comparing observable behaviour against suspicious patterns in network resources and detecting irregular behaviour and abuses (AM 2017). However, due to the particular characteristics of IoT devices such as their specific protocols and limited capabilities concerning storage and computing, applying traditional IDS techniques may not be suitable for IoT environments (Zarpelaoa et al. 2017).

Brief Description:

Therefore, this project will focus on evaluating the use of traditional intrusion detection systems, such as Snort and Bro, in an IoT environment. Two main measures for evaluation will be used. Firstly, the overall effectiveness of the IDS, where this measure represents the ability of the system to differentiate between intrusive and non-intrusive activities. Secondly, efficiency and performance, where this measure deals with the resources needed to be allocated to the system such as CPU cycles and main memory. Additionally, an attempt to automate the evaluation process will be made. Finally, based on the evaluation results, analysis of the systems will be done in order to judge their performance and classification accuracy, in addition to a comparison with an IDS specifically created for IoT by a PhD student.

Project Aims and Objectives:

This section will illustrate the main aims and objectives of the proposed project throughout the time frame of the project.

1. **Establish a background in several areas relevant to the project.**
    - Understand Intrusion detection systems and how to use them.
    - Understand the different evaluation techniques and metrics.
    - Understand the basics of IoT and its devises.
2. **Perform evaluation of an intrusion detection system in an IoT environment.**
    - Gain an understanding of the IoT device used to simulate an IoT environment.
    - Perform evaluation of the intrusion detection systems in terms of detection quality and overall performance by simulating attacks.
    - Acquiring evaluation results.
3. **Produce an analysis of the intrusion detection system in terms of detection quality and overall performance of the systems.**
    - Discuss and illustrate evaluation results.
    - Perform evaluation of an IDS specifically created for IoT by a PhD student and compare results.
4. **Produce and submit the final report, which will include all information relevant to the project and previous background search.**
    - Provide a final report for the project, that discusses the different aspects of the project such as the approach used to achieve the project and the evaluation results. It will also include a self-reflection section, including improvements that can be made in future work.

Supervisor Role:

A weekly meeting will be arranged with the supervisor, Dr Philipp Reinecke, for an approximate duration of 30 minutes. The purpose of the meetings will be to discuss the project's progress, where guidance, support, and feedback will be offered.

Ethics:

Ethical approval is likely not required for this project as the data and devices used do not utilize personal information and does not involve human participation. However, there will be ethical consideration while working on the project and writing the final report.

Work Plan:

The following work plan is developed in order to manage the various stages of this project and the final report. Additionally, weekly meetings with the supervisor will be carried out to discuss and monitor the progress of the project. The work plan is subject to change as the project progresses.

Week 1:

- Begin writing the initial plan.
- Research about relating projects.
- Meet with the supervisor for further clarification of the project aims and objectives.
- Produce and submit the initial plan, considering the supervisor's comments.

Milestone 1:

- Submit initial plan (4th February 2019).

Week 2-4:

- Background research about different aspects of the project.
- Set up intrusion detection systems and IoT device.
- Research and decide on evaluation technique and traffic generator.
- Produce first draft of background section of the final report.
- Meet with the supervisor to discuss progress.

Milestone 2:

- First draft of background section of the report.

Week 5-7:

- Begin evaluation process of IDS in an IoT environment.
- Document evaluation results.
- Research automation techniques and begin automation of evaluation process.
- Begin first draft of approach section in the final report.
- Meet with the supervisor to discuss progress.

Milestone 3:

- Acquire evaluation results.

Week 8-11:

- Continue development of automation of evaluation process.
- Test automation.
- Evaluate the IDS created with consideration to IoT by PhD student.
- Analyse and compare evaluation results.
- Meet with the supervisor to discuss the final report before Easter break.

Milestone 4:

- Complete automation of evaluation.

Easter break:

- Establish conclusions based on results.
- Produce first draft of the final project.

Milestone 5:

- First draft of final report.

Week 12:

- Review and finalise the final report.

Milestone 6:

- Submission of the final report.

Viva Week:

- Prepare for the VIVA of the final year project.

Milestone 7:

- Completion of the project.

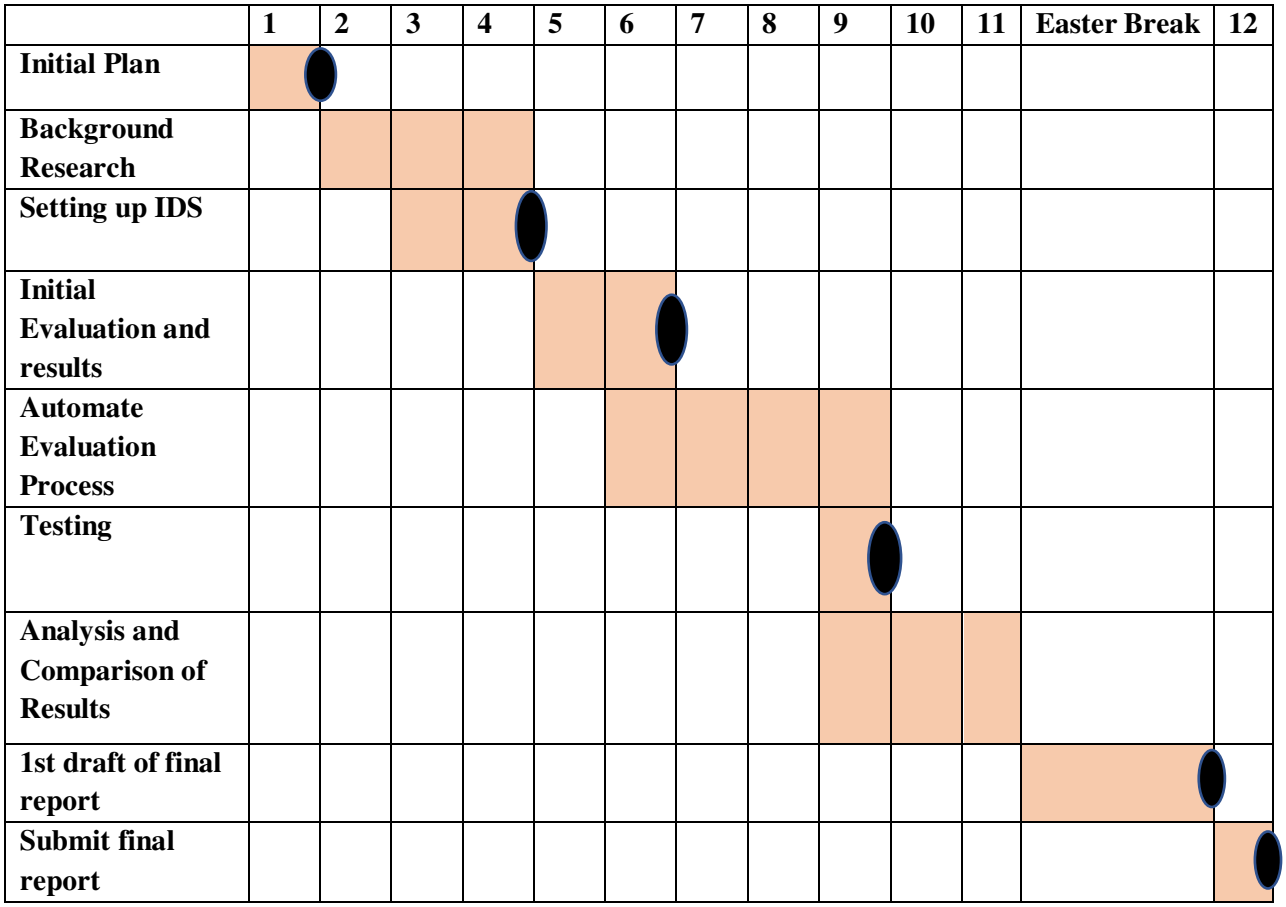
Milestones and Deliverables:

This section will outline the most significant milestones and deliverables of the project, derived from the work plan above.

- Submission of initial plan.
  - Submit the initial plan, which includes a project description, the project's aims and objectives, a work plan, and risk management section.
- First drafts of several sections of the final report:
  - Background
  - Approach
  - Results and Analysis
  - Future work.
- Acquire evaluation results for traditional intrusion detection systems in IoT environment.
- Complete automation of evaluation process.
- First draft of the final report.
- Submission of final report.
- Complete VIVA demonstration.

Gantt Chart:

The following Gantt chart illustrates the work plan graphically, where the black circles represent the milestones for the project. It also identifies the time, in terms of weeks, needed to complete each task.



Risk Management:

The risk plan illustrated below is created to ensure efficient risk management and preparation for any obstacles that might be faced while working on this project.

Risk	**Risk level** (Low, Medium and High)	**Likelihood of event** (Certainty, Likely, Somewhat Likely and Unlikely)	**Solution**

Data loss	High	Somewhat Likely	Have multiple backups of the project stored and update them frequently with each stage of the project.
Falling behind the work plan	Medium	Likely	Start tasks as soon as each week starts and provide time in the following week to finish left over tasks in the case of falling behind.
Hardware failure (such as IoT device)	Medium	Unlikely	Make sure similar devices are available in the case of failure and identify their locations and the process of acquiring them.
Inability to complete automation of evaluation process	Medium	Somewhat Likely	Perform evaluation of IDS manually in every iteration and record results.
Illness	Low	Somewhat Likely	Make sure the workload is distributed in such a way that would make it manageable to get caught up with the work plan in the case of falling behind.

Conclusion:

To conclude, this report discussed the proposed final year project. It provided a project description, project aims and objectives, and a work plan, including a Gantt chart. It also illustrated the supervisor's role in the project, some ethical consideration, and a risk analysis.

References:

AM, R. 2017. Intrusion Detection System Techniques and Tools: A Survey. Scholars Journal of Engineering and Technology 5(3), pp. 122-133.

EY Global. 2019. [online] Available at: https://www.ey.com/Publication/vwLUAssets/ey-m-e-internet-of-things/$FILE/ey-m-e-internet-of-things.pdf [Accessed 31 Jan. 2019].

Zarpelaoa, B., Miani, R., Kawakani, C. and Alvarenga, S. 2017. A survey of intrusion detection in Internet of Things [online]. Available at: http://www.download-paper.com/wp-content/uploads/2017/11/2017-elsevier-A-survey-of-intrusion-detection-in-Internet-of-Things.pdf [Accessed 1 Feb. 2019].