

Project Proposal

by Rhys Davies

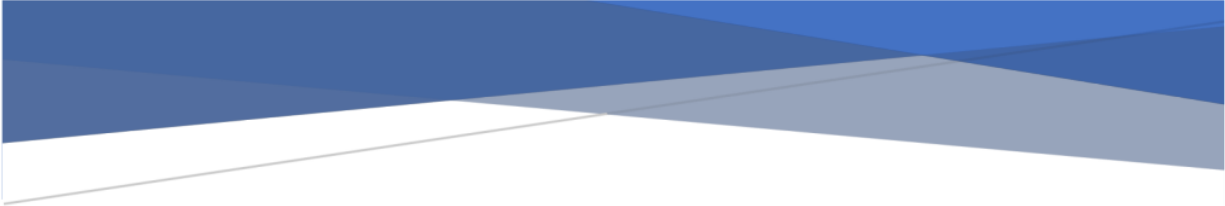
Submission date: 17-Oct-2023 10:28PM (UTC+0100)

Submission ID: 213626934

File name: 31250_Rhys_Davies_Project_Proposal_508662_1786675404.docx (175.48K)

Word count: 2169

Character count: 11591



DEMONSTRATING IOT DEVICE VULNERABILITIES AND RISKS

Research Proposal

Rhys Davies
Carlene Cambell

Table of Contents

1. Introduction	3
2. Background to the Proposed Research.....	4
3. Aims & Objectives	5
4. Methodology	5
4.1 Research Methodology	5
4.1.1 Philosophy.....	5
4.1.2 Approach.....	6
4.1.3 Strategies	6
4.1.4 Risks & Limitations	6
4.1.5 Ethical Issues	6
4.1.5 Validity, Reliability & Generalisability	6
4.1.6.1 Validity	6
4.1.6.2 Reliability	6
4.1.6.3 Generalisability	6
4.1.6 Data Evaluation Methods.....	6
4.1.7.1 Data Collection	6
4.1.7.2 Data Evaluation.....	6
5 Resources and Planning	7
5.1 Hardware Resources	7
5.2 Software Resources	7
5.5 Project Plan	7
References	8

Figure 1 Image of Gantt chart created in Microsoft Excel.....7

1. Introduction

The project I will be carrying out will start with scanning and stress testing a network to find potential vulnerabilities, find potential solutions for the network weakness and demonstrate how dangerous these vulnerabilities can be for an individual or an organisation. IoT devices have improved significantly over the years due to technological advancements with AI and breakthroughs in terms of design and software.

At the beginning of the project, it will begin by explaining the latest cybersecurity news about recent data breaches, security holes found in the technology of IoT devices and the most common cybersecurity threats that affect all types of computers. A section of the project will cover the security measures that should be in place for most devices and IoT gadgets and which measures are not there.

I am planning to perform a thorough literature study of the body of knowledge regarding IoT security and cybersecurity to accomplish these goals. I will also run several tests to check the security of various IoT devices and assess the efficacy of various security precautions.

2. Background to the Proposed Research

IoT device development has created more cybersecurity challenges, though. IoT devices frequently lack adequate security protections, leaving them open to cyberattacks. [1] Data breaches, financial losses, and in some cases, physical injury are just a few of the serious repercussions that these attacks may have. [2] To safeguard IoT devices and their users, it is crucial to establish appropriate cybersecurity solutions. [1]

For the upcoming project there are several other researchers in the field that have studied and published their work about IoT devices their names are “Giuseppe Bianchi, Roberto Di Pietro, and Antonio Vetrò” [3], after reading through their paper it grasps a great understanding of IoT devices, how they have become popular in the last few years and how they can be dangerous when exploited. [3]

Another great few researchers are named “Armin Ziaie Tabari, Xinming Ou, Anoop Singhal” [4] this paper demonstrates the importance of proper security protocols which was also mentioned in [3], this paper mentions a popular but complicated security practise called honey pots [4], honey pots are separate from a companies or users main network which is used to lure in attackers and trick them into thinking they have breached the main network when in fact it’s a dummy network which contains useless files. This is used to capture the traffic of the attacker to understand what tools and hardware they may be using. [3] [5]

One of the first few big theories in IoT security is called “Defence-in-Depth,” this involves implementing many different layers of security that are needed to protect an organisation's network from future attackers and regular internal network security testing. [6] The benefit of having multiple layers of security in place can be beneficial, if one of the layers were to fail there would be many other layers that would still be active and defend against an active attack. Due to there being multiple layers, this allows a network administrator to have detailed controls of the network, [7] [8] such as being able to control a firewall to stop an employee or guest from accessing certain websites or blocking specific traffic from coming in and from going out. [9] An IDS system (Intrusion Detection System) is like a firewall in which its purpose is to monitor network traffic, but it has a unique ability to flag any unauthorised or malicious activities that may pass through the network and the network administrator may act upon. [9] [10]

In the cybersecurity space, there is also a big theory called “Zero Trust” [11], this word has become very popular in recent years due to the ever-increasing number of data breaches, data leaks and poorly secured hardware. [12] The whole purpose of this new security model is to never trust anything, such as treating every other device and user as an attacker (Guilty until proven innocent). [13] By default, a zero-trust device and or service also needs verification to be unlocked, this can be done using biometric authentication, security keys and or iris scanners to bypass the security. A downside but also an upside to this security model is it requires constant verification when being accessed, this is beneficial for security purposes but for convenience, this is very unproductive due to an employee or user constantly needing to re-authenticate to regain access to a device or service. [14]

Lastly, the biggest and most important theory for any security professional is “Attack Surface Theory.” This involves trying to minimise an attack service as much as possible by implementing backups, finding vulnerabilities in a network, and eliminating unnecessary features that may act as a backdoor. A paper published by [15] demonstrated the importance of reducing the attack surface by reducing the number of entry points to the network [15], it lowers the risk of a future security breach and or a network getting compromised. [15]

3. Aims & Objectives

Aim: To demonstrate the effectiveness of modern cybersecurity on IoT devices and recommend potential improvements to protect a network from a possible cyber-attack.

- **To identify several types of vulnerabilities in IoT devices and how demonstrate how to secure a network from them.**
- **Observe and analyse the security risks, threats and privacy violations that may occur with these vulnerabilities.**
- **Analyse and go in depth of the different security protocols and methods that IoT devices may or may not already be using.**
- **Carry out a task to perform a scan and investigate a preset IoT device to understand how secure they may be.**

4. Methodology

4.1 Research Methodology

In the first section of the project will be a literature review, this will involve analysing and discussing already published literature, understand their findings, and improve upon what they have learned. To find this information the researcher will need to use keywords to find the appropriate papers such as “IoT” and “Security Breaches.”

There will be a data collection section which will involve screenshots of the network the researcher will use and the physical room they will carry out the scans, they will carry out a few different scanning and analysis methods such as network scanning which will be done to identify the IoT devices on a given network and report back the findings. After the network scanning section has been finished will move on to vulnerability scanning, capture packets on a network and a small sample of penetration testing.

When the data has been collected it will be analysed to determine if the network was secure in the first place and was the researcher able to compromise the network, the researcher will then compare the findings to industry standards and if they need to be improved upon.

Lastly the researcher will give a recommendation of potential security improvements if anywhere discovered during the project.

4.1.1 Philosophy

For this project Positivism is the best approach, this allows a researcher to analyse and collect data with being influenced by any biases the researcher may have, this is extremely important when discussing issues about security vulnerabilities or risks on a network as they may have a personal preference on equipment used.

The researcher may use the advantages of the philosophy by using many different methods to collect diverse types of data from IoT devices on a network, they will utilise statistical to analyse the data that has been collected and measure the severity of the risks.

To combat the disadvantages the philosophy may bring is to use a mixed methods approach. Use qualitative data to provide a description to the quantitative findings, which will result in understanding the limitations and exceptions to generalizations easier.

The data collection aspect of the project will use qualitative data, storing and using lots of data that may or may not benefit the research may increase the chances of data privacy issues if the data that was collected was stolen by a cybercriminal.

4.1.2 Approach

For the approach for the project, the research will use a Deductive approach, this the best approach for this project, before this project begins it will need a hypothesis and then evaluate that hypothesis to see if it is true or false.

4.1.3 Strategies

The researcher will implement a literature review as part of the project, this would allow them to examine real world cybersecurity attacks that were written and published by other trusted authors, another strategy is to perform a case study which will involve studying an in-depth knowledge of real risks and vulnerabilities. Lastly a document review to focusing on specific documents that are related to IoT risks and weak points.

4.1.4 Risks & Limitations

An external factor that might make the project more difficult if the testing hardware which is the router does not work properly or cannot initiate a handshake with the researcher's device resulting in a more challenging task. This can be prevented by using a different router.

4.1.5 Ethical Issues

The same issue persists with the risks, due to using network scanners and such data logs will be collected although they do not hold or contain any personal information.

4.1.5 Validity, Reliability & Generalisability

4.1.6.1 Validity

Performing the research itself will provide a more accurate image of the data and its quality.

4.1.6.2 Reliability

If a different researcher were to perform the problem the outcome will be the same as there is only 1 or 2 possibilities.

4.1.6.3 Generalisability

The results can be applied to problems related to IoT security, like finding backdoors or security issues.

4.1.6 Data Evaluation Methods

4.1.7.1 Data Collection

The data that the researcher is planning to collect are data logs from the computer network using specialised software.

4.1.7.2 Data Evaluation

The data will be evaluated using Microsoft excel to show a better understanding of the different threat levels.

5 Resources and Planning

5.1 Hardware Resources

The hardware that will be used to create this project will be a DELL Windows 11 Laptop and a Windows 11 Desktop computer.

5.2 Software Resources

In the project the researcher will be using kali linux on virtual box with their laptop which will be running Windows 11

5.5 Project Plan

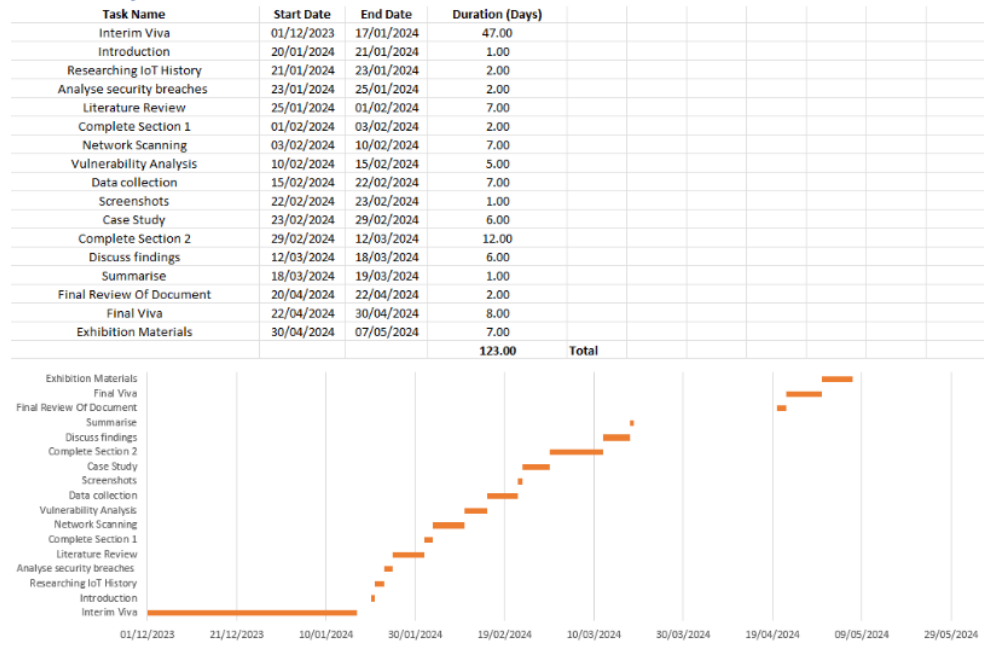


Figure 1 Image of Gantt chart created in Microsoft Excel

In this document, several different topics were discussed such as the different methods of data collection, data analysis to demonstrate vulnerabilities and security risks. The evaluation of qualitative data collection and technical data collection. The next section will delve into the history to help shape the research process.

References

- [1] N. Yousefnezhad, "Security in product lifecycle of IoT devices: A survey," *Journal of network and computer applications*, vol. 171, p. 102779, 2020.
- [2] Rawat, "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things," *IEEE Internet of Things Journal*, vol. 9, pp. 8229-8249, 2022.
- [3] Evenchick, *Up Close and Personal: Cybersecurity in Medical IoT Devices*, 2016.
- [4] A. Z. Tabari, "What are Attackers after on IoT Devices? An approach based on a multi-phased multi-faceted IoT honeypot ecosystem and data clustering," 2021.
- [5] Sridhar, "Design of routing protocol with the internet of things devices over mobile ad hoc networks," *Signal, image and video processing*, vol. 17, p. 4522, 2023.
- [6] Dazahra, "A Defense-in-depth Cybersecurity for Smart Substations," *International Journal of Electrical and Computer Engineering*, 2018.
- [7] Alexander, "Reducing Threats by Using Bayesian Networks to Prioritize and Combine Defense in Depth Security Measures," *Journal of Information Security*, 2020.
- [8] Stanzone, "Explainable Artificial Intelligence in CyberSecurity: A Survey," vol. 10, pp. 93575-93600, 2022.
- [9] M. Lee, "A Novel AI-based Methodology for Identifying Cyber Attacks in Honey Pots," in *AAAI Conference on Artificial Intelligence*, 2021.
- [10] M. Jahandar, "Indoor Organic Photovoltaics for Self-Sustaining IoT Devices: Progress, Challenges and Practicalization," *ChemSusChem*, vol. 14, p. 3474, 2021.
- [11] B. Do, "Zero-Trust Cybersecurity Approach for Dynamic 5G Network Slicing with Network Service Mesh and Segment-Routing over IPv6," *2022 International Conference on Development and Application Systems*, pp. 105-114, 2022.
- [12] Zanasi, "A Zero Trust approach for the cybersecurity of Industrial Control Systems.," *EEE 21st International Symposium on Network Computing and Applications*, 2022.
- [13] Al-Ayed, "Zero-Trust Model of Cybersecurity: A Significant Challenge in the Future," *2021 International Conference on Computational Science and Computational Intelligence*, pp. 852-854, 2021.
- [14] E. S. Saeed, *Handbook of research on cybersecurity issues and challenges for business and FinTech applications*, Hershey, Pennsylvania: Business Science Reference, 2023.
- [15] Casey, "Reducing Attack Surface by Learning Adversarial Bag of Tricks," 2022.

Project Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

70/100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student Rhys Davies
(2104756) _____ Mark
70 _____

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	14
The introduction delivers a concise overview of the project, emphasizing the focus on scanning and stress testing a network for vulnerabilities. It underscores the relevance of the project by acknowledging the significance of IoT devices and their advancements. A summarizing		

statement effectively captures the identified problem and highlights the importance of addressing it.		
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts. The background effectively highlights the cybersecurity challenges posed by IoT devices, supported by references to credible sources. It discusses key researchers and their contributions to understanding IoT risks and security practices. Clearly state how your project contributes to or extends the existing knowledge discussed in the literature. The aims and objectives are clearly defined and aligned with the project's focus on demonstrating the effectiveness of modern cybersecurity on IoT devices. Consider rephrasing the objectives for better clarity and consistency.	20	16

Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed. The research methodology is well-structured, involving a literature review, data collection, and analysis. It appropriately justifies the choice of positivism and a deductive approach. The mention of potential risks and ethical issues demonstrates awareness. As you have mentioned the importance of data and the risks around it, it would be recommended to expand on this to ensure privacy and security both physical and virtual.	30	20
Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices The specifications for hardware and software resources are clearly outlined, with a concise justification as to why the specified hardware and software resources were chosen. The project timeline is visually	15	11

represented through the Gantt chart showing the timeframe for the project as well as listing the task that should ensure the project is completed. Throughout the proposal, the deliverables are implied throughout the document in the context of achieving the project's objectives and goals.		
Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit The document is well-structured, presenting ideas in a logical sequence. Spelling and grammar meet acceptable standards. It is recommended for future work to maintain consistent use of terminology and carefully review for the use of acronyms without first stating what it stands for.	15	9
TOTAL	100	70

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9
