Home Lock-Down

**Senior Design Team Contract**

University of Cincinnati

College of Education, Criminal Justice, and Human Services

School of Information Technology

Haley Mason

Wayne Lecky

Adra Smith

Griffin Dickerson

Trevor McDonough

Table of Contents

[Intent 3](#_Toc147142259)

[Senior Design Contract 4](#_Toc147142260)

[Project Summary 4](#_Toc147142261)

[Problem Statement 4](#_Toc147142262)

[Solution 4](#_Toc147142263)

[Contact Information 5](#_Toc147142264)

[Project Source 5](#_Toc147142265)

[Project Objectives/Goals 5](#_Toc147142266)

[Team Members and Responsibilities 5](#_Toc147142267)

[Project Scope 6](#_Toc147142268)

[Quick Project Timeline 6](#_Toc147142269)

[Technologies Used 7](#_Toc147142270)

[Ethical and Legal Considerations 7](#_Toc147142271)

[Team Rules 7](#_Toc147142272)

[Team Signatures: 8](#_Toc147142273)

[References 9](#_Toc147142274)

# Intent

The following contract was written and agreed upon by Haley Mason, Wayne Lecky, Griffin Dickerson, Adra Smith and Trevor McDonough. The contract provides expectations, objectives, and results for developing and deploying Home Lock-Down.

The contract is effective for all team members participating in the Senior Design Capstone class series in the 2023-2024 academic year.

# Senior Design Contract

## Project Summary

The project "Home Lock-Down" aims to address the issue of inadequate knowledge among home network users on securing IoT (Internet of Things) devices on their home networks, leaving them vulnerable to cyber-attacks. The project involves identifying the current security gaps in their device’s network settings and proposing effective strategies and providing tools to secure the device and protect the privacy and security of users' data.

The project will include the following steps:

1. Research and Analysis: Conduct research on the current state of device’s network security, identify common vulnerabilities and potential cyber threats to specific IoT devices and analyze the user behavior that contributes to these vulnerabilities.
2. Development of Effective Strategies and Tools: Develop effective strategies and tools to secure specific IoT devices, such as enabling strong passwords, keeping firmware up to date, enabling network encryption, and implementing firewalls.
3. Implementation and Evaluation: Implement the proposed strategies and tools, evaluate their effectiveness, and make necessary adjustments.

This project's goal is to improve the security of specific IoT devices on home networks, protect users' privacy and data, and ensure safe and uninterrupted use of internet-connected devices.

## Problem Statement

The problem in securing home networks is the lack of awareness and knowledge among home network users on how to secure their home networks, this leaves them vulnerable to cyber-attacks. Specifically, IoT devices. Users often lack awareness of IoT security risks and may not take necessary precautions, such as changing default settings or updating device firmware (source: "The Internet of Things: Security Research Study," PwC, 2015). Additionally, manufacturers often ship IoT devices with default usernames and passwords that users may not change. Attackers can easily exploit these defaults (source: "Internet of Things (IoT) Security: Current Status, Challenges, and Countermeasures," Symantec, 2017). This problem affects all individuals and families who use home networks to connect to the internet and have sensitive information and devices on their network. The need for this to be fixed is urgent, as the number of cyber-attacks on home networks is increasing, and the consequences can be severe. It is crucial to fix the problem of securing home networks as it helps protect users' privacy, personal data, and devices from cyber-attacks. A secure home network also ensures the safe and uninterrupted use of internet-connected devices, which have become an essential part of daily life.

## Solution

Our solution is to create a program that allows home users to secure specific IoT devices that they are using on their home network. The program will use different scripts to scan and identify IoT devices on a home network. The program will allow the user to select the IoT device and allow the user to configure different security settings such as renaming device, creating strong passwords, updating firmware, etc. When the user is selecting these different configurations, the program will provide best practices and explanations as to why we implement them.

## Contact Information

|  |  |  |  |
| --- | --- | --- | --- |
| Team Member | Degree + Track | Email | Phone Number OR Other Contact Info |
| Wayne Lecky | BS-Cyber | Leckywm@mail.uc.edu | 513-331-5780 |
| Adra Smith | BSIT - Cyber | Smit4ar@mail.uc.edu | 614-531-5386 |
| Haley Mason | BS-CYBER  BSIT – Networking | masonha@mail.uc.edu | 513-441-7806 |
| Griffin Dickerson | BS-Cyber | dickerga@mail.uc.edu | (513) 846-1852 |
| Trevor McDonough | BSIT-Networking  BS-Cyber | mcdonotj@mail.uc.edu | (513)-444-3798 |

## Project Source

One of the team members' grandparents inspired this project. They have personally experienced attacks on their network due to lack of awareness and education. We formed a team prior to choosing a project so we all participated in the requirements analysis. The team was formed by combining common interests.

## Project Objectives/Goals

* Create a resource for securing IoT devices on a home network
* Protect IoT devices and the sensitive data they store
* Demonstrate the implementation of security tools and strategies to protect IoT devices on home networks

## Team Members and Responsibilities

Researcher: Wayne Lecky

* Responsible for conducting research on the current state of IoT device security
* Responsible identifying common vulnerabilities and potential cyber threats to specific IoT devices.
* Responsible for analyzing user behavior that contributes to these vulnerabilities.

Security Analyst 1: Adra Smith

* Responsible for developing effective strategies and tools to secure specific IoT devices on home networks.
* Responsible for best practices for passwords.
* Responsible for keeping firmware up to date, enabling network encryption, and implementing firewalls.

Security Analyst 2: Griffin Dickerson

* Responsible for developing effective strategies and tools to secure specific IoT devices on home networks.
* Responsible for best practices for passwords.
* Responsible for keeping firmware up to date, enabling network encryption, and implementing firewalls.

Implementation Specialist: Trevor McDonough

* Responsible for implementing the proposed strategies and tools,
* Responsible for evaluating their effectiveness.
* Responsible for making the necessary adjustments where practicable.

Project Manager & Graphic Designer: Haley Mason

* Responsible for overseeing the project's progress.
* Responsible for coordinating with team members.
* Responsible for managing timelines and budgets.
* Responsible for communicating with stakeholders and ensuring that the project is completed successfully and on time.
* Responsible for creating visual text and imagery concepts

## Project Scope

Our team will develop a program to secure specific IoT devices on home networks. We will be creating a program that contains different configuration methods with best practices to ensure specific IoT devices are secure. This program will be free and easy for anyone to use regardless of aptitude.

## Quick Project Timeline

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Task #* | *Task Name* | *Duration* | *Start Date* | *End Date* |
| 1 | Research Web | 1 week | TBD | TBD |
| 2 | Outline Web | TBD | TBD | TBD |
| 3 | Refurnish Web | TBD | TBD | TBD |
| 4 | Research How-To’s | 1 week | TBD | TBD |
| 5 | Choose How To’s | TBD | TBD | TBD |
| 6 | Implement How To’s into Program | TBD | TBD | TBD |
| 7 | Refine Program | 1 week | TBD | TBD |
| 8 | Workout any fine details | 1 week | TBD | TBD |

## Technologies Used

Visual Studio Code

Github

FireZilla (TBD)

Azure

Server Host (TBD)

## Ethical and Legal Considerations

1. The project will ensure the protection of information for the team and users in accordance with the Privacy Act of 1974.
2. The program will ask for the correct permissions from users to access their network and devices.
3. The program will notify the user of the steps we are taking during the process to be fully transparent in what it is doing and accomplishing.
4. The program will include a liability claim that states if there is an attack on their network or IoT devices, that the program or creators cannot be held liable.
5. The program will not harm a user’s network or IoT devices.
6. The Terms and Services Agreement will include everything above and will notify the user that accepting the Terms and Services Agreement acts as a contract that the user will not hold the program or creators liable in the case that an attacker breaches their network.

## Team Rules

1. Plagiarism will not be tolerated. Any team member that plagiarizes will be subject to university policies and a team meeting will be called.
2. Each team member will stay current on their tasks to ensure the project milestones are met. If an event conflicts that will affect the completion of a deliverable, the team member will notify the other team members at least 24 hours in advance of the scheduled due date.
3. If a group member is absent on class days or for an extended period, they will notify the other team members and the instructors.
4. All team members must attend all scheduled meetings and provide updates to the acting project manager. If a team member cannot make a scheduled meeting, they must notify all team members at least 4 hours in advance and provide an update via messenger or email.
5. All team members will review the oral presentation and final report.
6. All team members will respect the opinions and ideas of each team member, other students, and faculty.

# 

# **Team Signatures:**

**Project Manager** **Security Analyst**

Signature: Signature:

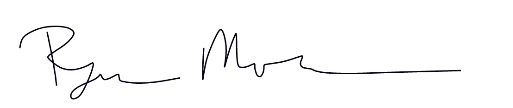
Date: \_\_\_\_\_\_\_\_10-02-2023\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_10-02-2023\_\_\_\_\_\_\_\_\_\_

**Researcher** **Security Analyst**

Signature: \_\_\_\_\_\_Wayne Lecky\_\_\_\_\_\_ Signature: \_\_\_\_Griffin Dickerson\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_10-2-2023\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_10-2-2023\_\_\_\_\_\_\_\_\_\_\_

**Implementation Specialist Project Advisor Signature: (Ryan Moore)**

Signature:  Signature: 

Date: \_\_\_\_10-2-2023\_\_\_\_\_ Date: \_\_\_\_\_\_\_10-2-2023\_\_\_\_\_\_\_\_\_

# References

Best practices for keeping your home network secure - DNI. (n.d.-a). <https://www.dni.gov/files/NCSC/documents/campaign/NSA-guide-Keeping-Home-Network-Secure.pdf>

*Home Network Security: CISA*. Cybersecurity and Infrastructure Security Agency CISA. (2023, September 29). <https://www.cisa.gov/news-events/news/home-network-security>

Introduction - hubspot. (n.d.-b).<https://cdn2.hubspot.net/hubfs/486579/Avast_Threat_Landscape_Report_2019.pdf>

Journal of Digital Forensics, security and law - commons.erau.edu. (n.d.-c). <https://commons.erau.edu/cgi/viewcontent.cgi?article=1444&context=jdfsl>

Namestnikova, M. (2021, May 13). *Router Security Report 2021*. Securelist English Global securelistcom. <https://securelist.com/network-security-2021/106711/>

*The repository @ st. cloud state*. Site. (n.d.). <https://repository.stcloudstate.edu/>

Slandau. (2022, July 1). *Wide range of routers under attack by unusually sophisticated malware*. CyberTalk. <https://www.cybertalk.org/2022/07/01/wide-range-of-routers-under-attack-by-unusually-sophisticated-malware/>

Spadafora, A. (2022, September 29). *Your Router’s security stinks: Here’s how to fix it*. Tom’s Guide. <https://www.tomsguide.com/us/home-router-security,news-19245.html>

Tressler, C., Miranda, C., Rose, R., Méndez, R., & Hopkins, M. (2023, March 14). *How to secure your home Wi-Fi Network*. Consumer Advice. <https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network>

Insureon Staff, *What You Need to Know About Software Liability | Insureon*. (n.d.). Www.insureon.com. Retrieved October 2, 2023, from <https://www.insureon.com/blog/what-you-need-to-know-about-software-liability#:~:text=Current%20software%20liability%20laws&text=For%20someone%20to%20successfully%20sue>