Max Dabbs
V00892472
CSC 466
February 7th, 2025

CSC 466 Project Proposal

Much of an average person's focus and consideration for internet security and protection is aimed at protecting and obfuscating communication with and to the wider internet from interception and snooping, what about the devices within their LAN?

The Problem:

While this might not seem like a large concern, with the potential of backdoors and exploiting of the rising amount of internet-enabled devices and always-on smart home appliances in the home, the risk is increasing steadily.

Why is this an issue? Hasn't something already been done?

As network security is a never-ending matter of trying to stay ahead of intruders and exploits, there is always changes and breakthroughs in network security to consider. In addition, since arguably the majority of consumers have little to no understanding of network and device security and its importance, it is unreasonable to assume residential local network devices and infrastructure is kept up to date, nor to expect users to deal with more stringent/strict policies used by business and government networks.

My Proposed Approach:

I propose to look into not only the current risks and common security measures in the standard residential LAN, but also any emerging security risks and what existing or developing networking protocols or best practices could be employed to residential networks to increase LAN security and reduce risk. I will then test one or more of the networking protocols/best practices in a simulated residential LAN again the risks I found. This will then be analyzed by me for the security effectiveness, ease of use, and any weaknesses found.

Proposed Deliverables Schedule:

Date	Deliverable
February 7th	**Deliver Project Website & Proposal**
February 21st	Compile list of the current major issues and weaknesses of residential LAN networks, in addition to any notable emerging risks. Additionally present preliminary research into existing or emerging protocols and practices that may be applied.
March 7th	Finalize and report what plans for security system(s) and test cases.
Early March	**Present Midterm Presentation**
March 21st	Finalize construction of test system(s) (physical and/or simulated). Evaluate and potentially update requirements/testing based on any preliminary testing or restrictions found.
April 4th	**Present Project Presentation**
Mid-April	**Submit Final Report**

Website:
https://denmanmax.github.io/CSC_466/

References:
https://www.getcybersafe.gc.ca/en/blogs/network-cyber-security-introduction

https://helpcenter.trendmicro.com/en-us/article/tmka-19635