Max Dabbs
V00892472
CSC 466
February 21st, 2025

Bi-weekly Update 1

Between the proposal and this update, I was mostly researching risks beyond the handful of risks commonly mentioned (“*3 common threats to Home Network Security”, 2024).*

Date	Deliverable	Status
February 7th	**Deliver Project Website & Proposal**	*Completed*
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.	*Completed*
March 7th	Finalize and report what plans for security system(s) and test cases.	*In Progress*
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.	*Not Started*
April 4th	**Present Project Presentation**	*Not Started*
April 11th	**Submit Final Report**	*Not Started*

Progress:

Security Risks:

In my research, I found the following risks (Sophos Ltd., 2025) (Khoussainov & Patel, 2000) (Bialy, 2024) (More, 2009):

Risk	Description
Physical Access	If an attacker can physically access the Ethernet/network equipment, they can tamper with the network or add devices.
User Misuse	Legitimate user either intentionally or unintentionally misusing their access.
Misconfigured Network Equipment	If network equipment (router, switches, etc) or firewalls are misconfigured, it opens exploits to attackers.
Weak WiFi security	Weak WiFi passwords can easily be brute-forced to gain access.
Network Services	Services like file sharing and remote desktop could contain security exploits and weaknesses.
Viruses and Malware	If a device on the network is infected, it can spread to other devices on the network, or give attackers access inside the network.
Data Interception	If the LAN data is not encrypted, it can be read by a attacker in transit.
Weak Passwords	Like with WiFi passwords, weak admin passwords on devices are easy to break.

Shared Credentials	If multiple devices share login credentials, a compromised device's credentials can be used to access other devices.

Practices:

In trying to find risks, I came across a U.S. Cybersecurity and Infrastructure Security Agency webpage discussing home network security (Cybersecurity and Infrastructure Security Agency [CISA], 2023). The page listed 11 ways a person could improve the security of their home network; most of them were had to do with preventing weak passwords, out-of-date software, and phishing, but one section goes somewhat into depth into various ways to improve Wi-Fi security (CISA, 2023), which could be useful to my proposal.

Next Steps:

Next, between now and March 7th, I will narrow down what exactly I will test. I will also come up with some test cases, and what metrics to evaluate the results against.

References:

Book, V. (2023, October 16). *How to secure your lan network*. Tufin. https://www.tufin.com/blog/how-to-secure-your-lan

Bialy, M. (2024, August 16). *LAN security and how it is hacked*. Grandmetric. https://www.grandmetric.com/lan-security-attacks/

Cybersecurity and Infrastructure Security Agency. (2023, March 23). *Home Network Security*. https://www.cisa.gov/news-events/news/home-network-security

Khoussainov, R., & Patel, A. (2000). LAN security: problems and solutions for Ethernet networks. *Computer Standards & Interfaces*, *22*(3), 191-202.

More, A. T. B. (2009). 10 Major Security Threats. https://www.ipa.go.jp/en/security/vulnerabilities/gg76us0000008owo-att/000016942.pdf

Sophos Ltd. (2025, February 19). *LAN security: Local Area Networks explained*. https://www.sophos.com/en-us/cybersecurity-explained/local-area-network-lan

T.N. Locke Communications. (2024, September 9). *3 common threats to Home Network Security*. https://www.tnlockecommunications.com.au/3-common-threats-to-home-network-security