Max Dabbs
V00892472
CSC 466
March 7th, 2025

Midterm Update/Bi-weekly Update 2

Between the previous update and now, I have mostly been deciding on what network security concepts to test, and attempting to set up and familiarize myself with GNS3.

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.	*Completed*
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.	*In Progress*
April 4th	**Present Project Presentation**	*Not Started*
April 11th	**Submit Final Report**	*Not Started*

Progress:

Test Cases:

For the security test, I plan to test the following:

MAC Whitelist:

The idea of a MAC whitelist is to only allow devices with MAC addresses that have been preapproved to successfully connect to the network via WiFi or Ethernet.

This concept should be effective in countering multiple of the risks identified in BWU1, mainly WiFi security and physical access, though this might be additionally effective in preventing user misuse and data interception due to restricting access the LAN.

As MAC addresses are spoofable, this will not prevent an attacker with enough time or existing knowledge of the network and/or approved devices to connect, but should prevent most unauthorized connections.

Network Segmentation/ ‘Guest’ Network:

Network segmentation works by dividing the network into smaller parts by controlling how traffic flows among the parts. This can a complete blocking of flow between segments, or just allowing only a limited type or destination of packets. This can be accomplished using firewalls, in addition to software configurations like Access Control List and VLAN.

By preventing devices to communicate freely between all local devices, this would potentially reduce/remove all the risks I identified in BWU1. The biggest issue with this is the additional time/equipment needed to set up and maintain, in addition to the potential for placing devices in such a way as to defeat the benefits, for example, placing the majority of devices in the same segment.

A simpler and (currently) more consumer-oriented/friendly variation of this would be placing less secure and guest/temporary devices into the guest Wi-Fi network that can be activated on all/most residential Wi-Fi routers.

MACsec:

MACsec is a point-to-point encryption over Ethernet within a network. MACsec defines secure channels to allow symmetric encrypted communication between 'nodes' over Layer 2.

While MACsec is useful, due to being designed for Ethernet connections, it cannot work over Wi-Fi. As Wi-Fi already offers encryption (WEP, WPA1/2/3), communication between Wi-Fi devices should already be obfuscated from snooping. Any communication between Wi-Fi and Ethernet communications are still exposed. AS a result, as long as the main or important devices are interconnected exclusively using Ethernet, MACsec will protect their communications from snooping.

The main risk covered by MACsec are data interception from physical access to the Ethernet network. Another alternative would be IPSec, but from what I can tell, MACsec is better suited for LAN traffic due to its lower latency.

Additional Considerations:

While weak device and Wi-Fi passwords are also a serious issue, I cannot think of a network system I can simulate that can counter this (minimum password requirements, WPA3, etc), besides countering Wi-Fi security with device whitelisting. Related to this, I initially was going to propose placing IoT/smart devices in the DMZ in the router, but my research suggests that the DMZ present on consumer routers differs from the DMZ I was aware of, making it not possible/feasible with home routers.

Security Test System:

To allow for more complicated and theoretical systems to be tested, I have decided to use a software simulation instead of a physical network. After some research online, I decided on using GNS3 due to being powerful and having ample tutorials and documentation, in addition to being free and open source.

Unfortunately, at the moment, there is issues getting GNS3 running. Since GNS3 'recommends' using a GNS3 VM, but VM networking doesn't work on my desktop, I attempted to set up the GNS3 VM via VirtualBox on my MacBook. While I was able to get the VM running after changing the Host-Only Adapter to a Host-Only Network due to depreciation in VirtualBox 7, GNS3 does not recognize the VM is running, even though this change should be supported since 2023.

Next Steps:

Next, between now and March 21st, assuming there is no further issues constructing the test environment or changes from feedback received, I will finalize getting GNS3 working and construct virtual networks in GNS3 and begin testing.

I will attempt further to get GNS3 to function on macOS, but if I cannot troubleshoot the issues, I will attempt using my ThinkPad T550 or W530 with Debian, since the documentation claims that Linux can function without the VM. While this should work, the age (10+ years vs 6 months) and lesser CPU cores (2/4 vs ‘8’) may lead to restrictions on what can be comfortably simulated.

References:

Amazon Web Services, Inc. (n.d.). *What is IPSec? - ipsec protocol explained - AWS*. What is IPSec? - IPSec Protocol Explained - AWS. https://aws.amazon.com/what-is/ipsec/

Cisco. (2024, July 30). *What is network segmentation?*. Cisco. https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html

Dubroca, S. (2016, February). MACsec: Encryption for the wired LAN. In netdev 1.1. Red Hat.

DMZ (computing). (2025, January 11). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=DMZ_(computing)&oldid=1268829795

Gargan, R. (2024, July 16). *MACsec vs IPsec - unpacking the differences*. RSS. https://www.netmaker.io/resources/macsec-vs-ipsec

Getting started with GNS3. GNS3 Documentation. (n.d.). https://docs.gns3.com/docs/

Getting started with GNS3. GNS3 Documentation - Should you use the GNS3 VM? (n.d.). https://docs.gns3.com/docs#should-you-use-the-gns3-vm

GNS3 | The software that empowers network professionals. (n.d.). https://www.gns3.com/

GNS3 VM with Virtualbox 7: Host-only adapter not available any more · issue #3472 · GNS3/GNS3-gui. GitHub. (2023, May 24). https://github.com/GNS3/gns3-gui/issues/3472

Is a MAC address whitelist good security for my network?. r/netsec - Technical Information Security Content & Discussion. (2009, September 27). https://www.reddit.com/r/netsec/comments/9on4s/is_a_mac_address_whitelist_good_security_for_my/