IoT Security for Home Network Enhancement

Abstract

In the event of a cyber attack on a home network, integrating additional defense mechanisms into the router is crucial. This measure helps identify the targeted hardware, pinpoint involved IP addresses, and potentially gather legal information related to the breach. Employing canaries as a preemptive measure enables prompt alerts to both end-users and network providers about unauthorized access. This safeguard also extends to detecting anomalies in IoT device data, allowing for the isolation and temporary termination of usage by affected appliances. Analyzing input/output metrics, packet arrival times, and data parameters is essential for identifying irregular patterns and triggering proactive responses.

Motivation/Problem

The growing security concerns surrounding Wi-Fi hotspots and Internet of Things (IoT) devices. With a significant percentage of Wi-Fi hotspots lacking encryption, there's an increasing risk of user traffic interception and exploitation by malicious actors.

Additionally, the rapid proliferation of IoT devices across various industries and consumer markets raises concerns about the security of sensitive data they handle.

Security issues such as DoS attacks, identity theft, and vishing further underscore the need to address these vulnerabilities to protect sensitive information from unauthorized access and exploitation.

Addressing these security threats is vital to safeguarding user privacy, protecting against financial fraud, and upholding the reliability and trustworthiness of VoIP systems in an increasingly digital and interconnected world.

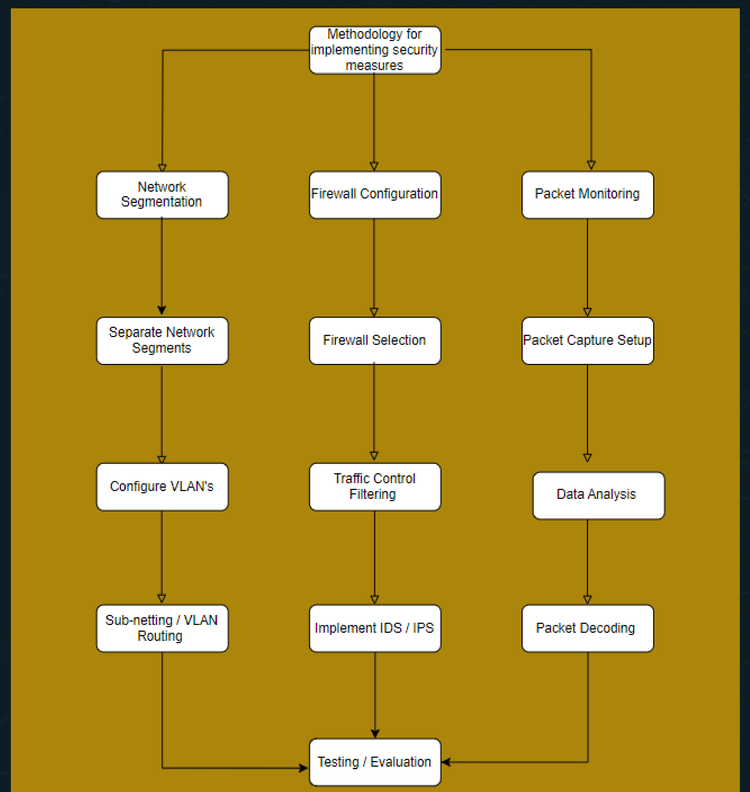
Hypothesis & Methods

Implementing network segmentation, VLAN management, firewall configuration, and IoT device monitoring in a home network can enhance security, improve performance, and control IoT devices.

- Implementation approach
  - Set up multiple VLANs to segregate traffic.
  - Deploy firewall rules for traffic control and web response filtering.
  - Integrate and monitor IoT devices in the network.
  - Evaluate effectiveness through data collection, analysis, and testing.

Objective: Assess the impact of these measures on network security, performance, and management in a home environment.

Overview



Current Work

In the current phase of the project, extensive groundwork has been laid, encompassing thorough research into network security and IoT technologies. Essential tools, including packet capture software like Wireshark, have been acquired, while necessary hardware components have been procured and await deployment. Detailed documentation and planning have been undertaken to ensure systematic execution, complemented by ongoing collaboration with peers to refine project objectives and strategies.

Future Work

Future efforts can focus on conducting experiments to test the effectiveness of security measures on various IoT devices, conducting longitudinal studies to track the long-term effectiveness of implemented measures, and exploring the integration of emerging technologies like artificial intelligence and blockchain.

Acknowledgements

Thank you to the University of Central Florida for funding this research and the DRACO Lab for continued support and guidance.

MALIA ROJAS
Malia.Rojas@ucf.edu

DRACO LAB | www.ece.ucf.edu/DRACO
Dr. Mike Borowczak, Lab Director

Dept. Of Electrical & Computer Engineering
College of Engineering and Computer Science
University of Central Florida

2023 STUDENT RESEARCH WEEK
March 27 - 31 | researchweek.ucf.edu
SHOWCASE · LEVERAGE · IMPACT · CELEBRATE

DRACO