Ministry of Higher Education and Scientific Research

University of Babylon

College of Information Technology

Department of Information Security

Study: (Morning)

Embedded Firewall-Based Raspberry pi for IoT Devices

A Graduate Project Submitted to the department of Information Security of the College of Information Technology, University of Babylon, in Partial Fulfillment of the Requirements for the Bachelor's degree in the Information Security of Information Technology

By

Sajad Abdul-Munim Habib

Supervised by

Assist. Lec. Shahad A. Hussein

2023-2024

Abstract

With the proliferation of Internet of Things (IoT) devices, the security concerns associated with them have become increasingly prominent. As these devices often lack robust built-in security measures, they are susceptible to various cyber threats, including unauthorized access, data breaches, and malware attacks. To address these vulnerabilities, this graduation project proposes the development of an embedded firewall-based system using Raspberry Pi for securing IoT devices.

The proposed system leverages the computational capabilities of Raspberry Pi to implement a firewall solution tailored specifically for IoT environments. By deploying the firewall directly on the Raspberry Pi device, it serves as a centralized security gateway for managing network traffic between IoT devices and the external network. This approach enables the implementation of customizable security policies, intrusion detection mechanisms, and traffic filtering rules to safeguard IoT networks against malicious activities.

The key components of the embedded firewall system include packet filtering modules, network monitoring tools, and a user-friendly interface for configuration and management. The packet filtering modules utilize techniques such as stateful inspection and access control lists to analyze and control incoming and outgoing traffic. Additionally, the network monitoring tools continuously monitor network activity and generate alerts for suspicious behavior or potential security breaches.

To validate the effectiveness of the proposed solution, a series of experiments and simulations will be conducted to assess its performance in real-world IoT environments. The evaluation criteria will include factors such as throughput, latency, resource utilization, and security efficacy. By demonstrating the feasibility and benefits of the embedded