University of Mauritius

Faculty of Information, Communication and Digital Technologies

Synopsis

Name of student: Girish Dyal

Programme: BSc Computer Science level 3

Student ID: 2012046

Title of dissertation: Enhancing Wifi security in an IoT network

Introduction:

With a world of constantly emerging technologies, millions of smart devices are being manufactured and are being deployed in many areas of network. As the number of Internet of Things devices continues to increase, the security of these devices and the networks they operate on has become a growing concern. Wi-Fi is a widely used technology for connecting IoT devices to the Internet, but it is also a popular target for attackers due to its widespread use and inherent vulnerabilities.

Generally, IoT devices have limited resources such that they have a low memory and cannot support complex operations which makes it challenging to implement strong security measures such as AES or TLS which are normally used nowadays. They use lightweight protocols that are not secure to communicate and this makes it an easy prey for hackers. However, there are authentication and lightweight encryption mechanism that exist for IoT devices but this does not really solve the issue. This is because hackers can perform brute-force attack or data breach to gain the password or even decrypt the small key-size bits that are implemented in those lightweight cryptographic algorithm.

Aim: Construct a smart home IoT system and segment the network while preserving power of these devices

Objectives:

1. Create separate network for each group- IoT devices, authorized computer and traditional computers on the network
2. Set up a password-protected gateway with WPA2 protocols
3. Configure switch to create VLANs & router to create logical interfaces for VLANs
4. Configure password parameters on both switch and router

Proposed Methodology:

This project aims to segment the local network in a smart home IoT ecosystem. The first step is to explore suitable platforms and visualize the IoT network. Once the IoT network has been set up, VLANs will be implemented in order to segment the IoT device from the main network and authorized only one PC to monitor or control these IoT devices. All the other traditional computers will be connected to the main network.

Expected Output:

A secure smart home IoT system where all IoT devices will connect wirelessly and communicate with a central gateway whilst protecting privacy of sensitive data.

Proposed Plan:

	NOV 2023	DEC 2023	JAN 2023	FEB 2023	MAR 2023	APR 2023	MAY 2023	JUN 2023	JULY 2023
Literature Review	×	×	×	×					
Analysis				×	×				
Design and Implementation				×	×	×	×		
Testing							×	×	
Evaluation								×	
Introduction and Conclusion									×

Cost: Not applicable since simulator will be used

Supervisor's name: Dr. Avinash Mungur