Project Proposal

INSE 6170: Network Security Architecture & Management

Concordia Institute for Information Systems Engineering

Concordia University, Montreal, Canada

Fall 2024

NAME: Ashiqul Hoque Chowdhury

ID: 40228852

Project Proposal: IoT Device Access Point Application (Default project)

Introduction: The goal of this project is to create computer software that serves as an Internet of Things access point. The program finds linked IoT devices and gives comprehensive information, such as their IPv4, IPv6, MAC address, and vendor details, when the device's hotspot function is activated. Additional features of the program will include device information management, packet capture, and a rudimentary Intrusion Detection System (IDS).

Platform and Implementation: Since Python has robust libraries for data processing and network analysis (such as Scapy for packet capture), I intend to use it to develop computer-based apps. The program will be developed from the ground up, utilising pre-existing Python packages to provide the necessary features:

a. **IoT Device Detection**:

When the PC serves as a hotspot, use libraries like scapy and psutil to identify connected IoT devices. By using public MAC address databases, this module will gather and show the IP addresses (IPv4 and IPv6), MAC addresses, and device vendors.

b. **Device Data Administration**:

   Users have the ability to modify and store extra device details (such as name, model, and version), which are kept locally in a database (such as SQLite).

c. **Capturing packets**:

   Give the user the ability to utilise Scapy to capture packets from particular IoT devices. Captured data is recorded in.pcap files, and the quantity of packets and duration of the capture are both customisable. Captures can be stopped or resumed at any moment by users.

- **System for Detecting Intrusions (IDS):**

  By keeping an eye on the data rate of linked devices, you may implement a simple IDS. The average data rates will be computed using a moving average. An alarm is set off when a device's data rate surpasses the configurable threshold, which is twice the average. This anomalous behaviour is then recorded, and the user is notified either email or push notification.

  Historical data rates will be tracked for the last 7 days to enable examination of prior behavior.

  File Administration:

  Users of the software will have the option to remove all or just some of the recorded records (device details, packets that were captured, etc.).

  Initial Architecture Design: The program will be organised as follows:

  Frontend (UI): A basic Tkinter-developed graphical user interface (GUI)

  Backend: Python modules for IDS, packet capture, and device detection
  Database: SQLite to store device information and data rate logs.

Timeline:

Week 1: Study, set up the environment for development, select the network analysis libraries, and create the database schema. Create the module that manages device information and detects Internet of Things devices.

Week 2: Start using the packet capture feature. Create the alerting system and IDS.

Week 3: Compile all functionality and polish the user interface in week three. Both testing and troubleshooting.

Week 4: Get ready for the demo of your work.

Work on the final report and presentation throughout the last weeks.

In summary, the project will deliver a flexible instrument for overseeing and controlling Internet of Things devices linked to a local area network. Users will be able to detect gadgets, record network data, and spot unusual activity with the finished solution. To improve network security for IoT devices, a simple intrusion detection system will be added.

Reference:

a. https://www.youtube.com/watch?v=LvaII2PEwcQ
b. https://www.youtube.com/watch?v=girsuXz0yA8
c. https://www.youtube.com/watch?v=uNmJppc-gR8&list=PLJ8t3BKaQLhOp2lgeRkyGrlIu4vnGsOT3
d. https://github.com/abhinav-bhardwaj/IoT-Network-Intrusion-Detection-System-UNSW-NB15