21st Academic Sessions 2024
University of Ruhuna
Matara, Sri Lanka
https://www.ruh.ac.lk/index.php/en/
ISSN: 2362-0412

User-centric Security Monitoring for IoT Devices

G.A.R.S. Ediriweera, E.W.T.K. Wickramadhara, R.A.A.G. Wickramasinghe and K.L.K. Sudheera

Faculty of Engineering, University of Ruhuna, Sri Lanka.

Abstract

The Internet of Things (IoT) has rapidly expanded in the last five years, bringing numerous benefits along with increasing security concerns. The simplification of human interaction to different tasks brought IoT closer to humans. User-centric security monitoring for home network systems is a user-friendly tool and interface that can effectively manage and monitor the security of IoT devices. This approach empowers users to make informed decisions about device anomalies. There are many network security monitoring tools available at the enterprise level. Nevertheless, many homeowners lack advanced technical knowledge about networking and information security. Most of which are plug-and-play (PnP) devices that lack regular updates and security patching. Therefore, a user-centric approach should be designed with simplicity in mind to ensure that anyone can use it effectively. In this work, we propose a software platform that can automatically identify the IoT devices in a network and analyze security-related issues. Device fingerprinting is a crucial step in IoT threat analysis. Because each IoT device's network traffic is different to find the advanced vulnerabilities of each IoT device. Once devices are identified, it is easier to identify vulnerabilities based on the device type in the identification of weak credentials and potentially vulnerable ports. The system will keep monitoring the incoming traffic with a predefined threshold. If the incoming traffic crosses the predefined threshold, it will raise alerts for DoS (Denial of Service) attacks. It further identifies the connected services for each IoT device through reverse DNS (Domain Name System) traffic analysis and presents them in a user-friendly manner.

Keywords: DoS, IDS, IoT, PnP

*Corresponding Author: *eg183499@engug.ruh.ac.lk*