Gateway for IoT Security

Tomáš Čejka, Marek Švepeš, Jan Viktorin
CTU in Prague, CESNET a.l.e.
{Thákurova 9, Zikova 4}, 160 00 Prague, Czech Republic

tomas.cejka@fit.cvut.cz, svepes@cesnet.cz, viktorin@cesnet.cz

Keywords. IoT, security, gateway, anomaly detection.

Abstract

In the last years, many devices and systems containing electronics were equipped with communication interfaces and it allowed people to read data from them and control the functionality of the devices remotely. Using the communication interfaces, it was possible to let devices communicate between each other without human interaction. The current state-of-the-art call this phenomenon as an Internet of Things (IoT).

This kind of automation helps people to improve their lives and therefore in many cases people can become dependent on the devices. In some cases, the security of the devices and their communication is crucial. Unfortunately, as some of the manufacturers focus on low price, many devices and technologies are not secured enough.

There is a research project called Secure Gateway for Internet of Things (SIoT) with several participants from the Czech academic institutions. The main goal of the project is a gateway based on open source technologies for secure deployment and operation of IoT devices.

2 Introduction

An Internet of Things infrastructure usually consists of lots of devices. Typically, there are special gateways, which are used as an access point for the IoT devices and connect them via special communication protocols such as LoRa, ZWave, Bluetooth and others.

Our research of the communication protocols and existing published papers shows that there are various vulnerabilities of the devices or the protocols. Therefore, this project aims to provide an improved SIoT gateway that will extend basic gateway functionality with security features.

The SIoT gateway is designed for OpenWrt, an open source linux distribution for embedded devices. The main benefit of the gateway is a capturing and collection of statistics and metadata about communication via the gateway. Besides that, the gateway is able to process captured data and perform some basic security and forensic analysis. The discovered suspicious events are reported to security teams that can take appropriate actions.

The SIoT gateway firmware must be prepared to run on even commodity devices with limited computational and storage resources. The flexible design of the proposed SIoT gateway that allows for offloading computational power needed for more advanced analysis and detection.

3 System Architecture

The architecture of the SIoT gateway is shown in Fig. 1. The gateway serves as an interconnection point between the sensors and application server(s). The modular framework for both southbound and northbound interfaces allows us to fit the gateway instance for the specific deployments as well as to extend its functionality with new protocols. Southbound interface provides connectivity with various sensors and other IoT devices communicating via protocols such as LoRa, ZWave, Bluetooth etc. Northbound interface, on the other hand, communicates with the application servers via a common IP network. The data from sensors are aggregated and exported to the application servers. Contrariwise, control messages from the servers are distributed by the gateway to the appropriate sensors.

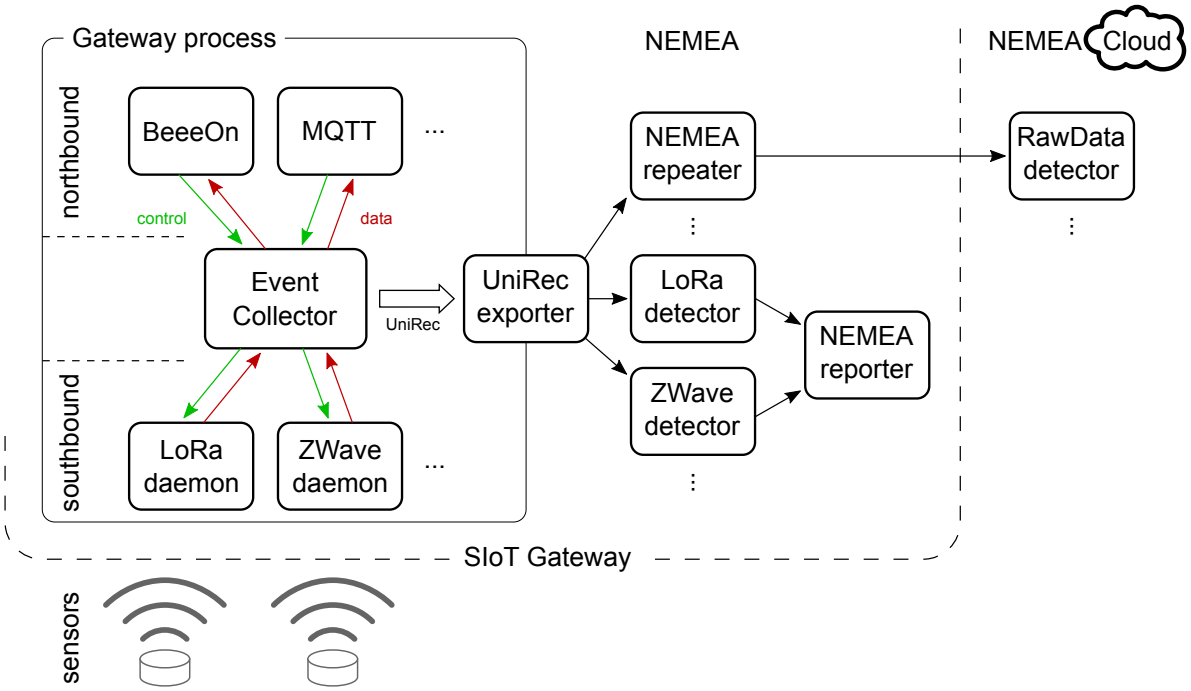

Figure 1: SIoT Gateway architecture.

Network Measurements Analysis (NEMEA) is a modular framework presented in [1]. It was originally developed for stream-wise processing flow data from high-speed computer networks in real-time. The aim of NEMEA is to provide application interface for developers of detection modules, while the framework itself handles the rest. NEMEA system, consisting of independent modules, can be easily distributed upon multiple machines. Therefore, some detection algorithms with high resource consumption can be easily offloaded from the gateway, with limited hardware resources, into NEMEA Cloud. Since NEMEA uses an efficient and flexible binary data format, it is a suitable component for security area of the SIoT project.

When a detection module, running in the gateway, discovers some suspicious behaviour or malicious traffic, it creates a special alert message. Subsequently, alerts can be handled in several ways such as passing the alert into some incident sharing system, directly to a security team via e-mail, storing into database etc.

4 Conclusion

Network connection becomes a commodity feature for many electronic device. Such devices are able to communicate with each other and this trend is called as an Internet of Things. Unfortunately, manufacturers rarely focus on security aspects and, therefore, insecure devices become a security threat. Besides that, low power requirements lead to development and usage of special communication protocols and our current research of the state-of-the-art shows some vulnerabilities of these communication protocols.

The SIoT gateway aims to provide a monitoring and analysis component which is currently missing in the IoT infrastructure. In addition to connecting several IoT devices, the SIoT gateway will contain a set of analysis and detection modules for online processing and reporting suspicious behaviour.

Acknowledgment

This work was supported by the CTU grant No. SGS17/212/OHK3/3T/18 funded by the Ministry of Education, Youth and Sports of the Czech Republic and *Secure Gateway for Internet of Things (SIoT)* project No. VI20172020079 funded by the Ministry of the Interior of the Czech Republic.

References

[1] Cejka, T. et al.: NEMEA: A framework for network traffic analysis, CNSM2016, Montreal