Pierluigi Locatelli

EDUCATION AND TRAINING

10/09/2014 – 21/05/2018 Italy

BSC IN COMPUTER ENGINEERING Sapienza Università di Roma (ROMA)

Java application that allows users to sign and verify documents according to European standards provided by CEF Digital.

Field of study Computer Engineering | **Final grade** 104/110 | **Thesis** PGSign&Verify

10/10/2018 – 14/07/2021

MSC IN CYBERSECURITY Sapienza Università di Roma (ROMA)

We discovered and analyzed a new vulnerability in the LoRaWAN protocol which results in blocking downlink communications between the network and the end device. We implemented the attack over a real network and discussed possible ways to detect and mitigate this vulnerability.
Presented at IEEE Globecom 2021, titled "Hijacking Downlink Path Selection in LoRaWAN"

Field of study Cybersecurity | **Final grade** 110L/110 | **Thesis** Time-based Wormhole Replay (TWR) Attack

01/11/2021 – CURRENT Italy

PHD IN ICT Sapienza Università di Roma

Field of study Information and Communication Technologies

WORK EXPERIENCE

15/03/2019 – 15/06/2019 Rome, Italy

"STUDIO DI MECCANISMI PER LA SINCRONIZZAZIONE DATI RETI CLOUD E GATEWAY WIRELESS PER IOT" – BANDO N. 02/2019 - SCHOLARSHIP SAPIENZA UNIVERSITÀ DI ROMA

The work focused on optimizing data synchronization between Medical Gateway devices and the Cloud in an IoT-based medical network. Using Octodiff, derived from the rdiff algorithm, the goal was to reduce data transmission by sending only modified file portions. We developed an adaptive chunk-size algorithm that adjusts based on "copy" and "data" instructions, minimizing delta file size iteratively. For specific devices like pulmonary ventilators that append data, a direct transmission method bypassing Octodiff is more efficient. Tests confirmed that our adaptive approach significantly improves synchronization efficiency compared to a fixed chunk-size method.

01/07/2019 – 30/11/2019 Rome, Italy

BACKEND DEVELOPER AUENDUO S.R.L.

Co-Author of middleware and backend server for communication and storage of data produced by several medical devices.
The middleware is developed using Node.js/Express, the backend is developed using C# .NET-core.

01/12/2019 – 31/12/2019 Rome, Italy

WEB DEVELOPER CUSTOMCUBIX

Co-Author of the 3D rendering and photo section for CustomCubix site, developed using the Three.js framework and HTML5/CSS/JS.
Site can be found at http://www.customcubix.com/

LANGUAGE SKILLS

Mother tongue(s): **ITALIAN**

Other language(s):

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken production	Spoken interaction	
ENGLISH	B2	B2	B2	B2	B2

Levels: A1 and A2: Basic user; B1 and B2: Independent user; C1 and C2: Proficient user

DIGITAL SKILLS

Microsoft Office | Operating Systems (Windows, Linux) | C / C++ / C# | Ruby | HTML5/CSS, Javascript | Android Development (Kotlin, Java) | Java | MongoDB, MySQL | Backend: NodeJS, Express, socket.io | React ecosystem: ReactJS, React Router, Redux, Typescript | Web-development front-end (Bootstrap, HTML) | React React-Native | Wordpress | bash-script | GIT & Github | Visual Studio & Visual Studio Code

PUBLICATIONS

2019

BE-Mesh: Bluetooth Low Energy Mesh Networking

We propose and discuss BE-Mesh-Bluetooth low Energy-Meshed network, a new paradigm for BLE (Bluetooth Low Energy) that enables mesh networking among wirelessly interconnected devices, both in a single hop and multi-hop fashion. Starting from the classical Master/Slave paradigm of Bluetooth, we build two new layers based on BLE stack that allow the final user to set-up, in a fast way, the desired network topology while hiding the complexity and low-level details of the BLE stack. We also prototype, as a proof of concept, an open source Android library that implements our communication paradigm and an Android application that allows the exchange of text messages across the mesh network. Last, we demonstrate how BE-Mesh enables Internet access sharing with the whole mesh from a single Internet-connected device.

Presented at IEEE INFOCOM 2019

2019

Exploiting edge computing for adaptive data update in internet of things networks

We presented a mechanism for data synchronization that considers Octodiff, a well known tool for data compression combined with an adaptive algorithm specifically tailored to limited, variable, IoT traffic volumes. By investigating the performance of the proposed architecture, we showed how the traffic amount generated by IoT cloud-services and its related cost can be conveniently reduced.

2021

Hijacking Downlink Path Selection in LoRaWAN

With the rise of the IoT, many protocols have been developed in order to fulfill the need for a wireless connectivity that assures energy efficiency and low-data rates. LoRaWAN is certainly one of the most widely used protocols. The LoRaWAN 1.1 specification aims to fix some serious security vulnerabilities in the 1.0 specification, however there still exist critical points to address. In this paper, we identify an attack that can affect LoRaWAN 1.0 and 1.1 networks, which hijacks the downlink path from the Network Server to an End Device. The attack exploits the deduplication procedure and the gateway selection during a downlink scheduling by the Network Server, which is in general implementation-dependent. The attack scheme has been proven to be easy to implement, not requiring physical layer-specific operations such as signal jamming, and could target many LoRaWAN devices at once. We discuss the implications of this attack and identify the possible mitigations that could be adopted by network providers to address this vulnerability.

Presented at IEEE GLOBECOM 2021

2022

Ruling Out IoT Devices in LoRaWAN

LoRaWAN is certainly one of the most widely used LPWAN protocol. The LoRaWAN 1.1 specification aims at fixing some serious security vulnerabilities in the 1.0 specification, however there still exist critical points that may affect the IoT security. In this demo, we show an attack that can affect LoRaWAN 1.0 and 1.1 networks, which hijacks the downlink path from the Network Server to an End Device, ruling out the target device from the network. The attack exploits the deduplication procedure and the gateway selection during a downlink scheduling by the Network Server, which is in general implementation-dependent. The attack scheme has been proven to be easy to implement, not requiring physical layer-specific operations such as signal jamming, and could target many LoRaWAN devices at once. We

demonstrate this attack and its effects by blocking a device under our control by receiving any downlink communication.

Presented at IEEE Infocom 2022

2022

BLENDER - Bluetooth Low Energy discovery and fingerprinting in IoT

Bluetooth Low Energy (BLE) is a pervasive wireless technology all around us today. It is included in most com- mercial consumer electronic devices manufactured in last years, and billions of BLE-enabled devices are produced every year, including wearable or portable ones like smartphones, smart- watches and smartbands. The success of BLE as a cornerstone in IoT and consumer electronics is both an advantage, giving wireless communication potential in the short range at low cost and consumption, and a disadvantage, from a security and privacy standpoint. BLE exposes packets that enable a potential attacker to detect, enquire and fingerprint actual devices despite manufacturers attempts to avoid detection and tracking. MAC address randomization was introduced in the BLE standard to solve some of these issues. In this paper we discuss how to detect and fingerprint BLE devices, basing our analysis and data collection on GAP (Generic Access Profile) and GATT (Generic Attribute Profile) protocols and data that can be recovered from devices by interactions allowed by the standard. In our study we focus on the possibility of enumerating and creating fingerprints of discovered devices, for crowd monitoring and recognition purposes, associating BLE randomized MAC addresses to actual devices using computed fingerprints when GATT is exploitable. We describe how large scale data collection can be obtained using automatic scanning devices with long range communication hardware, to uplink collected data in cloud-based applications and to a data store.

Presented at MEDCOMNET 2022

2023

Device discovery and tracing in the Bluetooth Low Energy domain

Bluetooth Low Energy (BLE) is a pervasive wireless technology all around us today. It is included in most commercial consumer electronic devices manufactured in the last years, and billions of BLE-enabled devices are produced every year, mostly wearable or portable ones like smartphones, smartwatches, and smartbands. The success of BLE as a cornerstone in the Internet of Things (IoT) and consumer electronics is both an advantage, enabling short range, low cost, and low power consumption wireless communications, and a disadvantage, from a security and privacy standpoint. BLE exposes packets that enable a potential attacker to detect, enquire and fingerprint actual devices despite manufacturers' attempts to avoid detection and tracking. Medium Access Control (MAC) address randomization was introduced in the BLE standard to solve some of these issues. In this paper we discuss how to detect and fingerprint BLE devices, basing our analysis and data collection on interactions allowed by the standard. In our study, we propose the Bluetooth Low Energy Nodes Detect, Enquire, (and) Recognition (BLENDER) framework for enumerating and fingerprinting BLE devices for crowd monitoring and recognition purposes, based on four different strategies used to analyze BLE-enabled devices. We will show that it is possible to associate BLE randomized MAC addresses to actual devices. We will then describe a proof of concept for large-scale data collection. In addition, to determine the spots where the stations could be optimally positioned, we created a synthetic dataset based on mobility models and then we emulated the BLENDER approach. The latter allowed training Machine Learning models to predict the expected number of devices appearing at any particular position, day, and hour.

Computer Communications, Volume 202, 42-56

2023

Friendship Security Analysis in Bluetooth Low Energy Networks

Bluetooth Low Energy (BLE) is one of the most promising low-power, short-range wireless technologies, providing a standardized technology for creating mesh networks and enabling devices to communicate with each other with limited impact on the battery. BLE Mesh networks support a variety of features, including broadcast, unicast, and multicast messaging, allowing devices to communicate in a distributed and scalable manner. These networks enable a wide range of applications, from smart homes to industrial automation and asset tracking. In recent years, the BLE standard has introduced a new feature called ”Friendship” that allows nodes with limited battery power to pair with other Bluetooth devices that are responsible for caching their messages while they sleep. In this way, the BLE Friendship allows devices to share data without the need for a continuous connection, preserving the energy-saving capabilities of the network. However, recent literature has shown that this feature can be easily exploited by malicious agents in the network to either deny friendship or establish a permanent link between the attacker and the low-power node. In this paper, we review the current status of the security of the BLE Friendship, discussing what are the most dangerous threats, and analyzing their impact on the battery of low-power nodes. Therefore, we implement one of these threats, namely, the Clear Attack, over a smart sensor scenario to show its potential in affecting the battery life of the devices. Finally, we propose and implement a set of countermeasures and mitigations that can be integrated into the BLE standard to reduce the impact of such an attack and we prove their effectiveness in preserving the energy of low-power devices.

Presented at IEEE MedComNet 2023

2024

DeLoRaN: Decentralize LoRaWAN Network Server Through Blockchain

LoRaWAN networks have become popular for enabling long-range, low-power connectivity in Internet of Things (IoT) applications. Traditional LoRa Wannetworks typically rely on a centralized architecture, which may pose limitations regarding scalability, reliability, and adaptability. In contrast, decentralized LoRaWAN networks offer a compelling alternative with several distinct features. This study explores the advantages of decentralized LoRaWAN networks over their centralized counterparts and presents DeLoRaN, a completely decentralized and fully compatible LoRaWAN network. Firstly, a decentralized network architecture enhances the availability of services by leveraging multiple copies of a LoRaWAN Network Server (NS), here called Network Controller, thereby eliminating the single points of failure. Secondly, the decentralized nature of the network improves data availability and integrity by utilizing shared and decentralized ledgers, such as blockchain technology. This ensures that data remains accessible and tamper-proof even in the presence of malicious actors or network failures. Thirdly, a decentralized network strengthens resilience by tolerating faulty or malicious nodes through the consensus mechanisms employed by the Network Controller. To prove our point, we present an implementation of our distributed approach and test it in different scenarios, to appreciate performance and scalability of DeLoRaN when compared to a centralized approach.

Presented at IEEE WCNC 2024

2023

Internet of things security issues in lorawan and bluetooth low energy

The Internet of Things (IoT) technologies are attracting the interest of scientific and industrial communities given the huge number of applications that can be designed with energy-limited devices connected to the Internet. LoRaWAN (Long Range Wide Area Network), a data-link layer with long range, low power, and low bit rate, appeared as a promising solution for IoT in which, end-devices communicate with gateways through a single hop at long distances. On the other side, the short-range IoT can leverage the potentialities of Bluetooth Low Energy (BLE) in its mesh network setting to interconnect, in proximity, multiple devices. Both technologies are already hitting a large market, but there are still several issues dealing with their security. This chapter is dedicated to the analysis of selected security issues affecting IoT networks and specifically low-power wireless systems such as LoRaWAN and BLE.

Published on CNIT Technical Report-11