



**LATVIJAS
UNIVERSITĀTE**

FUZZING-BASED BLUETOOTH PROTOCOL SECURITY ASSESSMENT

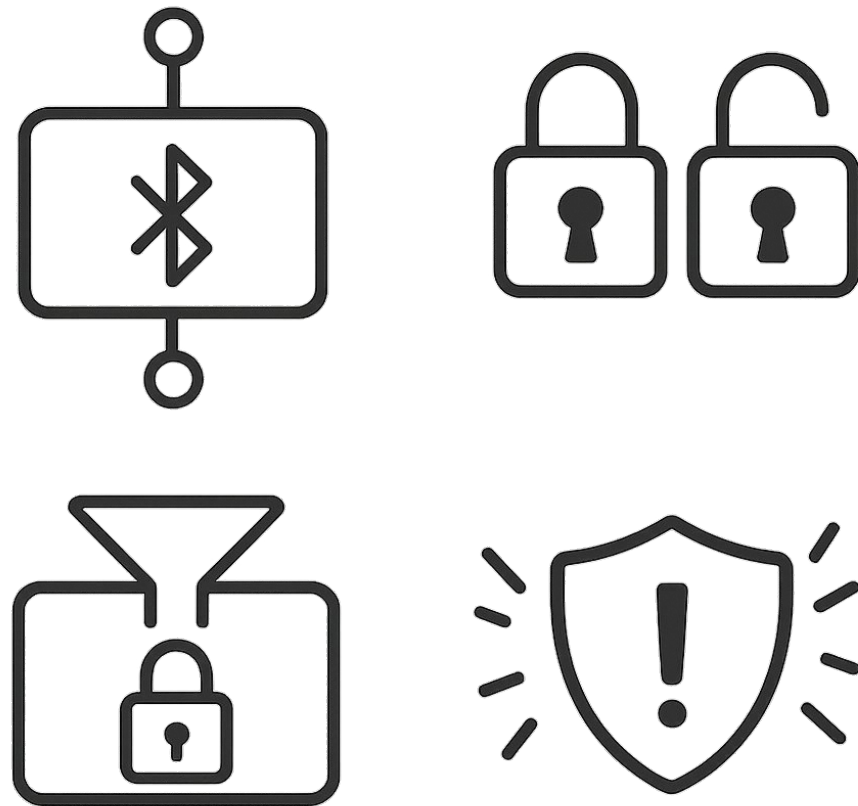
REPORT 08.10.2025.

Student: Eduards Blumbergs

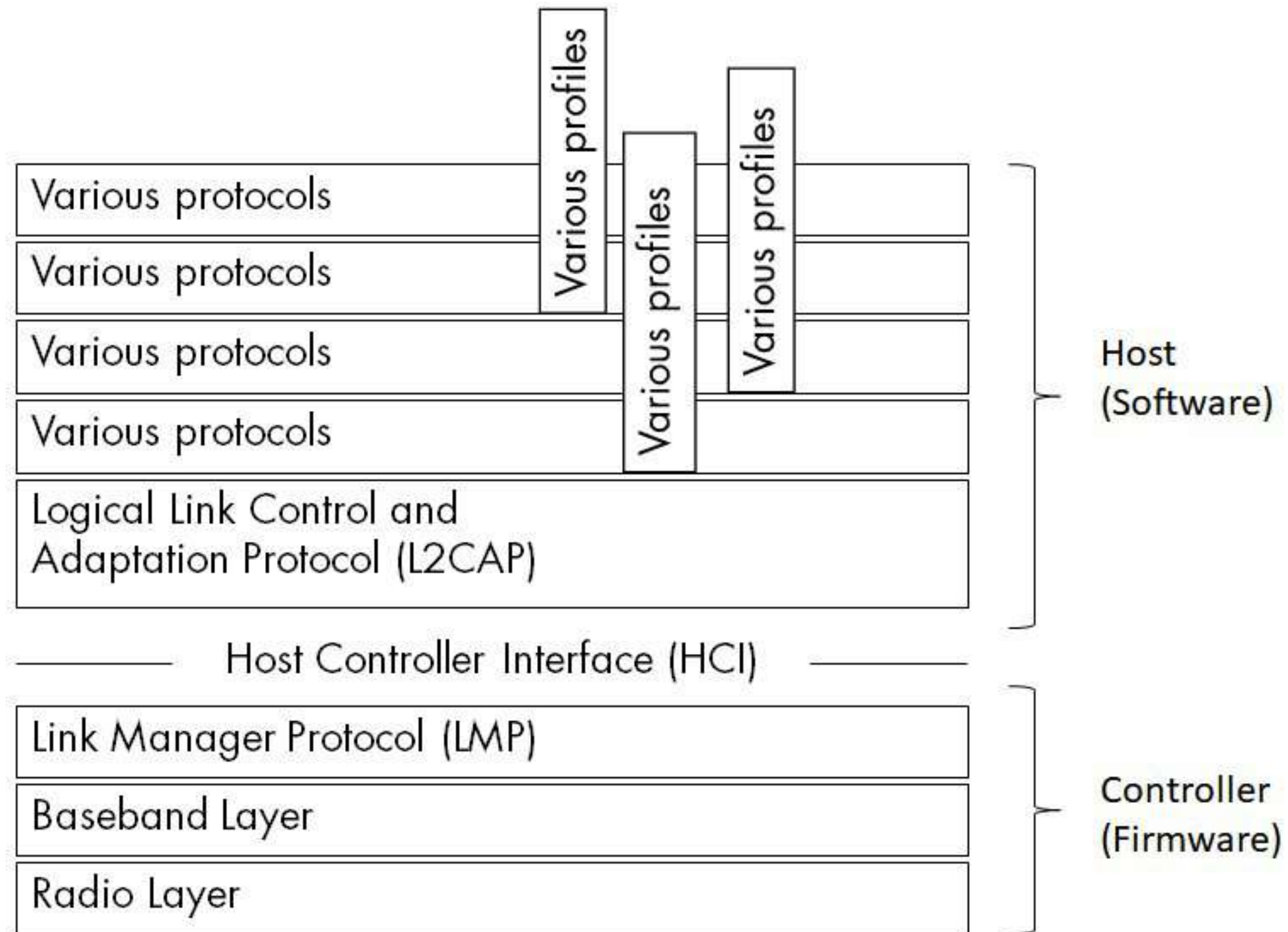
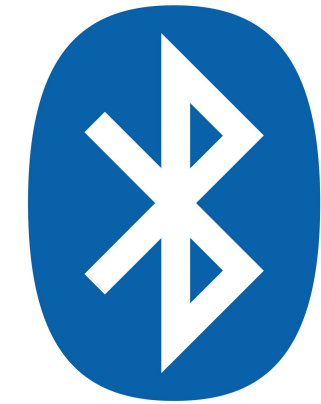
Supervisor: Asoc. Prof. Dr. Pēteris Paikens

Research Motivation

- Complexity: Bluetooth is stateful, timing-sensitive, no single testing method addresses all its layers and nuances.
- Limited ground truth: Hard to define logic bug oracles without access to internal specifications.
- Compatibility: Bluetooth Classic (aka. BR/EDR) security shouldn't be overlooked. While Bluetooth Low Energy (BLE) is advancing, BR/EDR is still the *de facto* standard protocol for short-range wireless audio.
- Limitations: Delivering centralized firmware updates can be impractical or physically difficult, leaving unpatched security gaps.
- Low Quality Assurance: The certification process overlooks poor safeguards against malicious data processing.
- OS Security Risks: Firmware vulnerabilities can compromise the connected systems.



Fuzzing Effects in Bluetooth Stack Layers

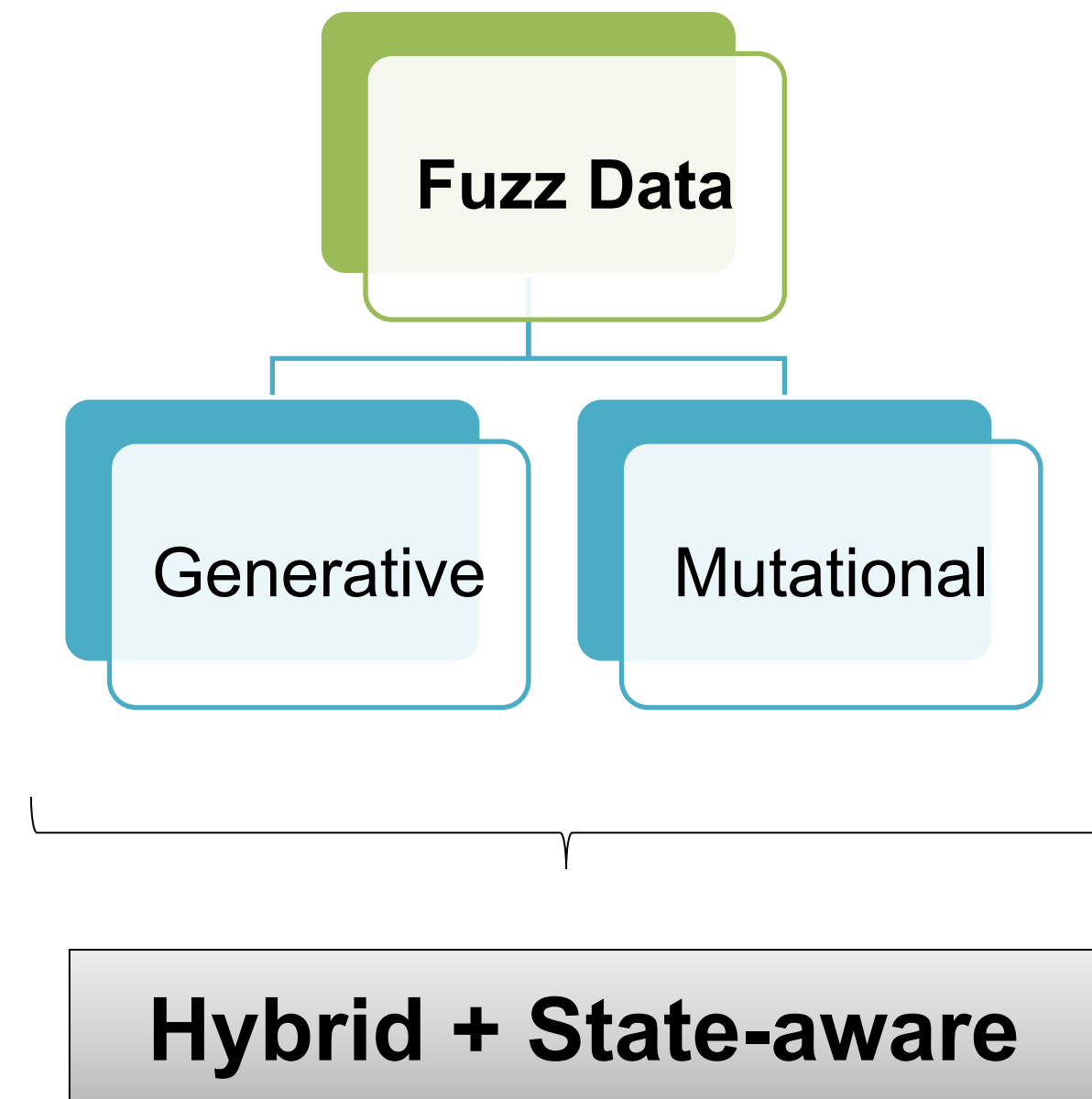


Key Fuzz Data Approaches

Generative approach: creating test from protocol specifications (top-down) rev-engineering traffic (bottom-up), using state models, or formal Bluetooth message grammars, producing *state-valid* sequences for injection .

Mutational approach: starting from valid PDUs and modify bytes, lengths, or TLV fields to expose parser and boundary bugs.

Hybrid + State-aware: Combine generative sequences and mutations, use feedback (coverage, heuristics, ML etc.) to guide transformations, state transitions and uncover deep protocol logic.



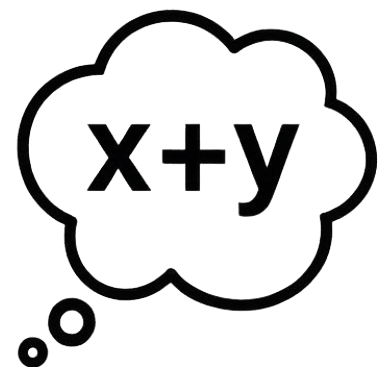
Key Fuzzing Execution Procedures



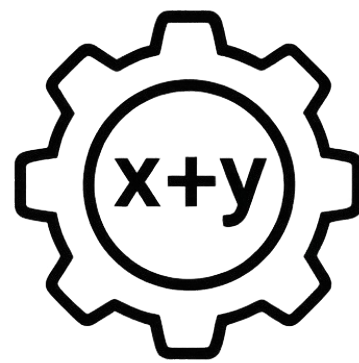
Coverage-guided



Concrete



Symbolic



Concolic

Coverage-guided: dynamically evolves inputs using feedback, best suited for instrumentable host stacks (not for closed-source or embedded).

Concrete: run tests with real, specific input values (normal fuzzing).

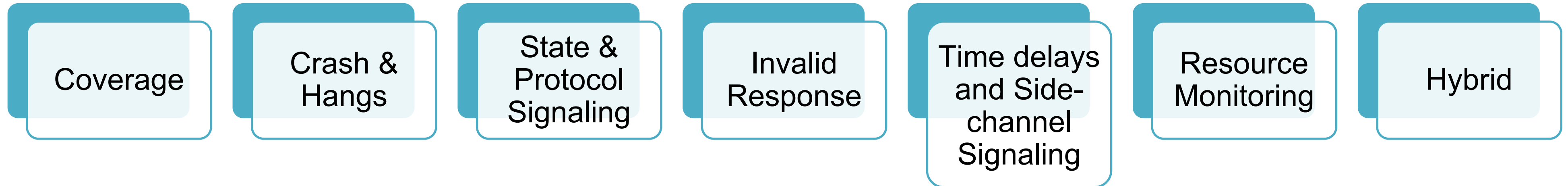
Symbolic: analyzes program execution with symbolic variable values to explore all possible execution paths simultaneously.

Concolic: combines symbolic reasoning with concrete runs to narrow down and reach problematic paths more efficiently.



LATVIJAS
UNIVERSITĀTE

Feedback for Direction and Automation



Coverage Feedback: New code paths (block / edge traces).

Crash & Hang Detection: Reproducible failures (crashes, timeouts, hangs).

State & Protocol Signaling: Inputs advancing valid Bluetooth states (e.g., pairing).

Invalid Response Semantics: Unexpected or incorrect protocol replies.

Time Delays & Side-channel Signaling: Latency, retries, power and CPU anomalies.

Resource Monitoring: Leaks & exhaustion of resources.

Hybrid: Combined multiple feedback for prioritization.

Bluetooth Security Research in the *WearSec* (Through April 2024)

Highlights

- Exploring the most promising and effective tools, methodologies, and vulnerabilities, with a focus on the physical layer and advanced protocol fuzzing techniques.
- Contribution to the **fuzzing methodologies** for wearable devices.

Outcome

- Designed and engineered a protocol fuzzing workflow using advanced tools and custom scripts.

Outreach and Dissemination

- Validated foundational tools and frameworks for wireless protocol **fuzzing research**.
- Co-authored the research papers and contributed to the development of a knowledge base influencing both academic and industry practices in **wearable device security**.



Wearable Device RF Fingerprinting: An Experimental Study

Wearable Device RF Fingerprinting: an Experimental Study Using COTS Hardware

Artis Rušins^{1*}, Eduards Blumbergs², Deniss Tiščenko¹,
Kirils Solovjovs¹ and Pēteris Paikens²

¹Institute of Electronics and Computer Science, 14 Dzerbenes st., Riga, Latvia

²Institute of Mathematics and Computer Science, University of Latvia, Raina blvd. 29, Riga, Latvia

*Contact: artis.rusins@edi.lv

I. INTRODUCTION

In the past 7 years there has been sharp increase in number of connected wearable devices worldwide from 325 million in 2016 to 1105 million in 2022 [1]. This has led to growing concerns about privacy of the data collected by these devices. Wearable devices are becoming more sophisticated and can collect a wide range of data about the user and it is usually sent over using Bluetooth or Bluetooth Low Energy (BLE) standards which we are investigating. RF fingerprinting is one of the emerging techniques that can identify specific device by analyzing radio waveforms generated by target device and extracting unique features from it. However, wearable device RF fingerprinting is relatively unexplored research topic and thus it is important to investigate its effectiveness before offering countermeasures. In this paper we try to replicate results of previous RF fingerprinting attempts for Bluetooth devices.

In this paper we:

- Gather wearable device radio data in isolated environment for automated data capture
- Extract carrier frequency offset (CFO) and amplitude scaling factor fingerprints from the data

to detect presence of device by its unique RF fingerprints [2]. CFO is the difference between the frequency at which radio transmission is supposed to happen and the frequency at which it actually happens. The "scaling factor" is amplitude variations within a packet and is used to normalize amplitude to roughly $[-1;1]$ before demodulation. Both CFO and amplitude scaling is usually done by Bluetooth chipset, and these values are not available to user, so we extract them manually.

III. EXPERIMENTAL SETUP

One of key challenges in extracting RF fingerprints is determining which radio packets are from our DUT and which come from nearby devices. To address this, we do all radio recording inside a radio frequency anechoic chamber. Our recording devices of choice are Ettus Research USRP B210 and B200 software defined radios, due to availability and good software support. They can both record at sampling rate up to 56 MHz. To capture all Bluetooth channels, we use 2 SDRs, with one of them recording lower end of the Bluetooth spectrum and the other one higher end.

Radio frequency anechoic chamber Data capture host

Prepared for: International Workshop on Embedded Digital Intelligence (IWoEDI'2023).

Role: Co-authored as the 2nd author.

Paper status: Published as an online paper.

Publisher: EDI IWoEDI'2023 conference website.



**LATVIJAS
UNIVERSITĀTE**

Research funded by the Latvian Council of Science, project "Automated wireless security analysis of wearable devices" (WearSec), project No. Izp-2020/1-0395

Evaluating Bluetooth BR/EDR Communication Resilience: Methods and Fuzzing Tools

Paper status: major revision in progress

Article

Evaluating Bluetooth BR/EDR Communication Resilience: Methods and Fuzzing Tools

Eduards Blumbergs^{1,2}, Krišjānis Nesenbergs² and Pēteris Paikens¹

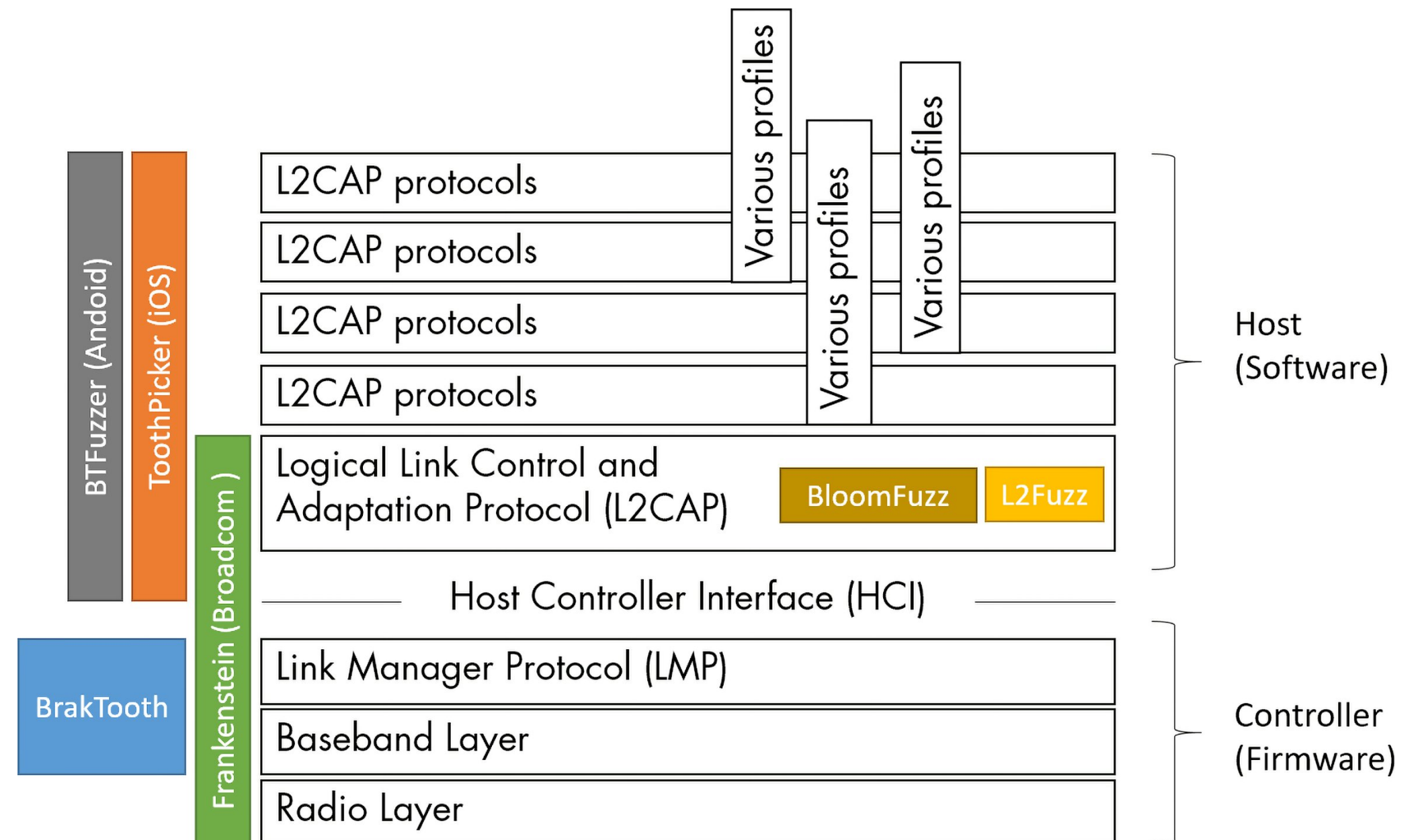
¹ Institute of Mathematics and Computer Science University of Latvia, Raina blvd. 29, Riga, Latvia, imcs@lumil.lv

² Institute of Electronics and Computer Science, Dzerbenes str. 14, Riga, Latvia, info@edi.lv

* Correspondence: eduards.blumbergs@edi.lv, krisjanis.nesenbergs@edi.lv, peteris@ailab.lv

Abstract: Bluetooth Classic (BR/EDR) remains a core wireless technology for billions of devices, yet it has faced several security issues. Recent high-profile studies have renewed focus and highlighted significant vulnerabilities in the implementation of the BR/EDR protocol that allow denial of service (DoS) or remote code execution (RCE). These vulnerabilities underscore the necessity for thorough testing of this widely used protocol, with fuzz testing being an effective method to reveal challenging implementation flaws [1]. We examine key BR/EDR protocol fuzzing frameworks from academia and industry, focusing on challenges in stateful protocol fuzzing and evaluating essential techniques across all layers of the stack, including fuzzers targeting firmware (*Frankenstein* [2] and *BrakTooth* [3]), L2CAP-layer (*L2Fuzz* [4], *BloomFuzz* [5]) and application-layer (*ToothPicker* for iOS [6] and *BTfuzzer* for Android (*BTfuzzer* [7])). This paper aims to bridge the existing gap in comprehensive analyses of contemporary BR/EDR protocol fuzzing tools by systematically evaluating their methodologies, scope, prerequisites, and effectiveness through a comparative study. We provide guidance for practitioners, developers, and researchers, emphasizing the difficulties associated with stateful protocols, hardware instrumentation, and multidimensional timing and concurrency issues. Drawing from a recent fuzzing survey [1], we propose future avenues for research.

Keywords: Bluetooth; Fuzzing; Vulnerability Assessment; Security Testing; Hardware Security; Firmware Vulnerabilities; Protocol Analysis



Research funded by the Latvian Council of Science, project “Automated wireless security analysis of wearable devices” (WearSec), project No. Izp-2020/1-0395



LATVIJAS
UNIVERSITĀTE

Wearable Device Bluetooth/BLE Physical Layer Dataset

Artis Rusins ^{1,†}, Deniss Tiscenko ^{1,†}, Eriks Dobelis ^{2,†}, Eduards Blumbergs ^{1,†}, Krisjanis Nesenbergs ^{1,*,†} and Peteris Paikens ^{2,†}

- ¹ Institute of Electronics and Computer Science, 14 Dzerbenes St., LV-1006 Riga, Latvia; artis.rusins@edi.lv (A.R.); e.blumbergs@gmail.com (E.B.)
² Institute of Mathematics and Computer Science, University of Latvia, Raina blvd. 29, LV-1006 Riga, Latvia; peteris@aialab.lv (P.P.)
* Correspondence: krisjanis.nesenbergs@edi.lv
† These authors contributed equally to this work.

Abstract: Wearable devices, such as headsets and activity trackers, rely heavily on the Bluetooth and/or the Bluetooth Low Energy wireless communication standard to exchange data with smartphones or other peripherals. Since these devices collect personal health and activity data, ensuring the privacy and security of the transmitted data is crucial. Therefore, we present a dataset that captures complete Bluetooth communications—including advertising, connection, data exchange, and disconnection—in an RF isolated environment using software-defined radio. We were able to successfully decode the captured Bluetooth packets using existing tools. This dataset provides researchers with the ability to fully analyze Bluetooth traffic and gain insight into communication patterns and potential security vulnerabilities.

Dataset: <https://pubfaii.edi.lv/wearsecdata>

Dataset License: CC-BY-SA

Keywords: RF; PHY layer; SDR; wireless; Bluetooth; BLE; wearable devices



Citation: Rusins, A.; Tiscenko, D.; Dobelis, E.; Blumbergs, E.; Nesenbergs, K.; Paikens, P. Wearable Device Bluetooth/BLE Physical Layer Dataset. *Data* 2024, 9, 53. <https://doi.org/10.3390/data9040053>

1. Summary

Bluetooth is a very popular communication standard that is used to exchange data between devices over short range. It is mostly used by various types of wearable devices, smartphones, and computer peripherals. There are many existing studies that outline both the privacy and security risks with this standard, most notably the possibility to fingerprint the devices' radio frequency (RF) waveform, thus breaking Bluetooth's integrated



Wearable Device Bluetooth/BLE Physical Layer Dataset

Paper status: published (doi.org/10.3390/data9040053)

Publisher: MDPI Data

Table 1. Devices in the dataset.

Folder Name	Class	Bluetooth Version	Chipset
Amazfit_Band_5	Activity Tracker	5.0	not disclosed
Apple_AirPods_(3rd_generation)	Headset	5.0	Apple H1
Apple_AirPods_Pro_(2nd_generation)	Headset	5.3	Apple H2
Apple_Watch_SE_(2nd_Gen)	Activity Tracker	5.3	Apple S5
Apple_Watch_Series_8	Activity Tracker	5.3	Apple S8
Beats_Solo3_Wireless	Headset	4.0	Apple W1
Bose_QuietComfort_Earbuds_II	Headset	5.3	Qualcomm QCC5171
eSense	Headset	-	not disclosed
Fitbit_Charge_5	Activity Tracker	5.1	not disclosed
Fitbit_Versa_4	Activity Tracker	5.2	not disclosed
Garmin_Instinct_Crossover	Activity Tracker	5.0	not disclosed
Garmin_Venu_SQ	Activity Tracker	5.0	Nordic Semiconductor nRF52810
Garmin_Vivoactive_4	Activity Tracker	5.0	not disclosed
Google_Pixel_Buds_Pro	Headset	5.3	Broadcom BCM43015A0WKUBG
Google_Pixel_Watch	Activity Tracker	5.2	Exynos 9110+Cortex M33
Huawei_Band_3e	Activity Tracker	4.2	Ambiq Micro Apollo3 Blue
I7-TWS	Headset	-	not disclosed
JBL_TUNE510BT	Headset	5.0	Realtek RTL8763B
Unknown_BT_headphones_black	Headset	-	not disclosed
Mangoman	Headset	-	not disclosed
noise	-	-	-
Raycon_The_Everyday_Earbuds	Headset	5.0	Airoha AB1562M
Redmi_Buds_3	Headset	5.0	not disclosed
Samsung_Galaxy_Buds2_Pro	Headset	5.3	BES BES2700YP
Samsung_Galaxy_S20_FE	Smartphone	5.0	not disclosed
Samsung_Galaxy_Watch5	Activity Tracker	5.2	Exynos W920
Smart_Bracelet_LP715(G)	Activity Tracker	4.0	not disclosed
Smart_Bracelet_XMSH07HM	Activity Tracker	4.0	not disclosed
Sony_WF-1000XM4	Headset	5.2	MediaTek MT2822SA
Sony_WH-1000XM5	Headset	5.2	MediaTek MT2822AA
Xiaomi_Smart_Band_7	Activity Tracker	5.2	Dialog DA14706
ZABOW_Scorpion	Headset	-	not disclosed

Research funded by the Latvian Council of Science, project “Automated wireless security analysis of wearable devices” (WearSec), project No. Izp-2020/1-0395

11 Cyber-Physical Systems

Securing Latvia's Future

*Krišjānis Nesenbergs, Eduards Blumbergs
and Pēteris Paikens*

Introduction: Cyber-Physical Systems at the Crossroads of Emerging Security Issues

In the contemporary era, driven by technological innovation, a multitude of sophisticated systems have emerged that combine the domains of physical operations and computational intelligence, including smart transportation, urban infrastructure, advanced biomedical wearables, consumer devices, and resilient military technologies. These systems, collectively known as cyber-physical systems (CPS), represent a significant advancement in the integration of computational algorithms and the physical world. CPSs play a key role in enabling advanced defense mechanisms, increased situational awareness, and optimized logistic and support systems, focusing on increased automation, precision, reliability, and operational efficiency through the integration of sensors, actuators, and embedded systems that interact directly with the operational environment.



**LATVIJAS
UNIVERSITĀTE**

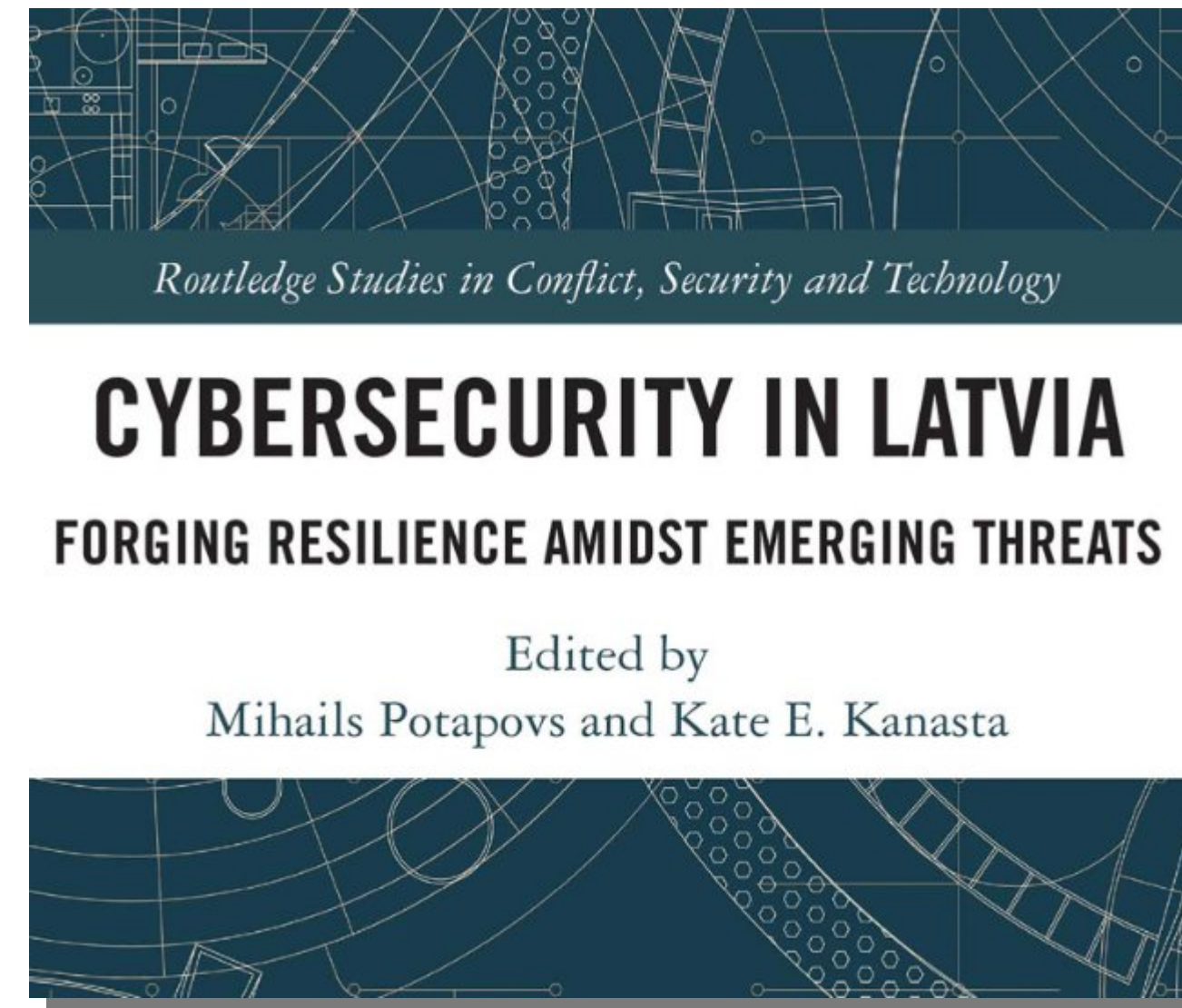
Cyber-Physical Systems: Securing Latvia's Future

Cybersecurity in Latvia (Book)

Publisher: Routledge

DOI: 10.4324/9781003638858-11

ISBN: 9781003638858



Shifting Research Focus: February to November 2024

Post-*WearSec* Engagement

- Latvian Council of Science-funded project *Smart Materials, Photonics, Technologies, and Engineering Ecosystem* (VPP-EM-FOTONIKA-2022/1-0001)

Project Task Involvement Highlights

- Developing tools to **enable future IoT-Edge-Cloud environment research.**
- Creating **foundational features and interfaces.**

Outreach and Dissemination

- Created and presented a poster at conferences.
- Produced and created a promotional video for the task.
- Contributed to and co-authored the paper.



ELEKTRONIKAS UN
DATORZINĀTŅU
INSTITŪTS



INSTITUTE OF
ELECTRONICS AND
COMPUTER SCIENCE

Article

A Set of Tools and Data Management Framework for the IoT-Edge-Cloud Continuum

Janis Judvaitis ^{*}, Eduards Blumbergs, Audris Arzovs, Andris Ivars Mackus, Rihards Balass and Leo Selavo

Institute of Electronics and Computer Science, Dzerbenes Street 14, LV-1006 Riga, Latvia; eduards.blumbergs@edi.lv (E.B.); rihards.balass@edi.lv (R.B.); leo.selavo@edi.lv (L.S.)
^{*} Correspondence: janis.judvaitis@edi.lv

Abstract: Developing and managing complex IoT-Edge-Cloud Continuum (IECC) systems are challenging due to the system complexity and diversity. Internet of Things (IoT), Edge, and Cloud components combined with artificial intelligence (AI) in data processing systems must ensure strong security and privacy for data sources. The approach of the IECC Data Management Framework (DMF) introduces a novel combination of multiple easy-to-configure plugin environments using data visualization features. These contributions collectively address the critical challenges inherent in heterogeneous environments such as scalability, data privacy, and configuration management by standardizing data flow configurations and increasing stakeholder trust in sensitive applications, particularly in critical infrastructure monitoring.

Keywords: IoT; edge; cloud; IoT-Edge-Cloud Continuum; software framework; differential privacy; management tool

1. Introduction

Developing, managing, and validating IoT-Edge-Cloud Continuum (IECC) systems present significant challenges due to their complex, multilayered structures, and heterogeneous components. Integrating Internet of Things (IoT), Edge, Cloud computing, and artificial intelligence (AI) requires not only technical sophistication but also strict data privacy and security measures.

These challenges, if left unresolved, can significantly obstruct the scalability, security, and privacy of IECC systems. The integration of IoT, Edge, and Cloud systems is essential for driving innovation in domains like healthcare, smart cities, and industrial IoT. However, the lack of unified standards, complex architectures, and fragmented expertise limits their effective deployment and creates vulnerabilities that compromise trust and reliability.



Citation: Judvaitis, J.; Blumbergs, E.; Arzovs, A.; Mackus, A.I.; Balass, R.; Selavo, L. A Set of Tools and Data Management Framework for the IoT-Edge-Cloud Continuum. *Appl. Syst. Innov.* **2024**, *7*, 130. <https://doi.org/10.3390/asi7060130>

Academic Editor: Andrius Bika



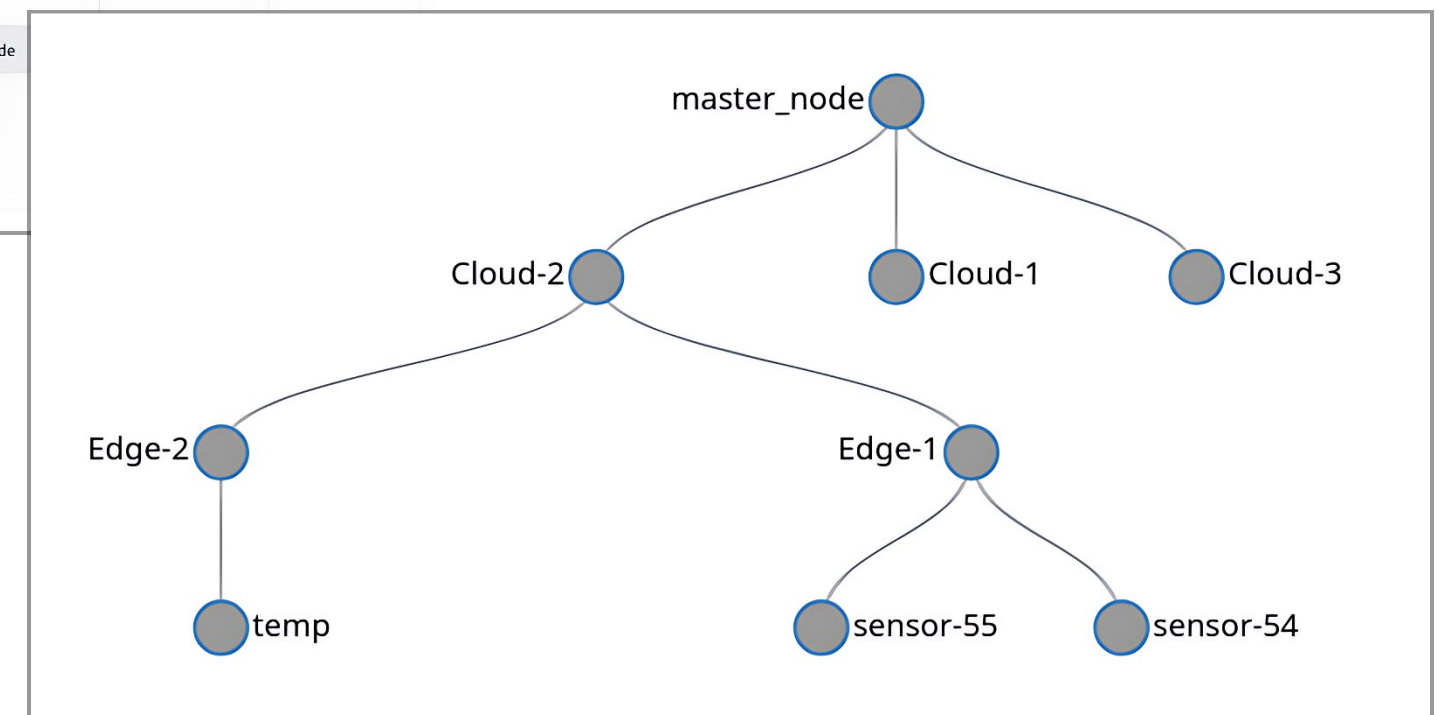
LATVIJAS
UNIVERSITĀTE

A Set of Tools and Data Management Framework for the IoT-Edge-Cloud Continuum

Paper status: published (doi.org/10.3390/asi7060130)

Publisher: MDPI Applied System Innovation

Name	Actions	Plugins	Parent	Label	Address:Port
Cloud-1	<input type="text" value="New Name"/> <input type="button" value="Rename"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input checked="" type="checkbox"/> energy-status <input checked="" type="checkbox"/> example-plugin <input checked="" type="checkbox"/> visualizer <input checked="" type="checkbox"/> differential-privacy <input checked="" type="checkbox"/> configurator <input type="button" value="Update"/>	<input type="text" value="master_node"/> <input type="button" value="Update"/>	<input type="text" value="Cloud"/> <input type="button" value="Update"/>	127.0.0.1:8000
Cloud-2	<input type="text" value="New Name"/> <input type="button" value="Rename"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	<input checked="" type="checkbox"/> energy-status <input checked="" type="checkbox"/> example-plugin <input type="checkbox"/> visualizer <input type="checkbox"/> differential-privacy <input type="checkbox"/> configurator <input type="button" value="Update"/>	<input type="text" value="master_node"/> <input type="button" value="Update"/>		



Research funded by the Latvian Council of Science, project "Smart Materials, Photonics, Technologies and Engineering Ecosystem" project No VPP-EM-FOTONIKA-2022/1-0001.

Shifting Research Focus Again: Through December 2025

Upon concluding previous projects, efforts were directed towards exploring new projects that would be consistent with the thesis objectives.

- ***Physics-Informed Machine Learning-Based Prediction and Reversion of Impaired Fasting Glucose Management (PRAESIIDIUM)***
Main task – Development of bioimpedance sensing wearable firmware and sensor driver (*Zephyr*);
Relation to Bluetooth security – Investigation of Bluetooth functionality and protocol safety (e.g. deadlocking, *BlueSnarfing* prevention).
- **Progress and Efforts in Identifying Future Research Opportunities:**
 - Searching opportunities on AI Protocol Fuzzing Automation and Fuzzing Wireless Communication.
 - Participation in pitching sessions abroad.
 - Looking for future funding from the European Defense Agency and strategic partnerships through Capability Technology group.



The draft has been under development, still requires significant additional work.

UNIVERSITY OF LATVIA
FACULTY OF SCIENCE AND TECHNOLOGY
DOCTORAL PROGRAMME IN COMPUTER SCIENCE AND
MATHEMATICS

**FUZZING-BASED BLUETOOTH PROTOCOL
SECURITY ASSESSMENT**

DOCTORAL THESIS DRAFT



Objectives 2025/2026

Top priorities:

- **Writing the draft (most important):**

Status: In progress - *Next:* finish the core chapters and results, then - an internal review.

- **Reworking a paper “Evaluating Bluetooth BR/EDR Communication Resilience: Methods and Fuzzing Tools” (equally important):**

Status: In progress - *Next:* restructure and update, then - prepare the submission.

- **Drafting a paper on Bluetooth fuzzing (important):**

Status: In progress - *Next:* complete the methods, figures, submit to the workshop.

- **Engaging in security conferences (also important):**

Status: In progress - *Next:* submit abstracts, schedule talks/posters, and set collaboration targets.

- **Identifying and securing an aligned research project.**

Status: In progress - *Next:* prepare tailored proposals for collaboration/funding.

Primary development (active engineering and experiments):

- **Standalone fuzzing test.**

Status: In progress - *Next:* integrate fuzzer module, validate on the target hardware.

- **OTA fuzzing on the development board.**

Status: In progress - *Next:* map OTA update flow, instrument bootloader, and design fuzz corpus.

Stability and compatibility (re-evaluation):

- **Bluetooth compatibility issues (lower priority).**

Status: Partly done - *Next:* re-run tests on up-to-date kernels, and list failing assumptions.

Completed objective: Supervised Bachelor's Thesis

- "Semantic vs. Non-Semantic CSS: Quantifying CSS Impact On Web Performance".

Thank You!



**LATVIJAS
UNIVERSITĀTE**