



**LATVIJAS
UNIVERSITĀTE**

FUZZING-BASED BLUETOOTH PROTOCOL SECURITY ASSESSMENT

REPORT 08.01.2025.

Student: Eduards Blumbergs

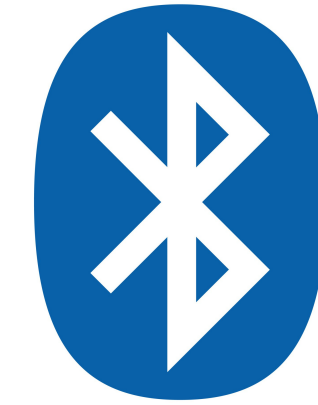
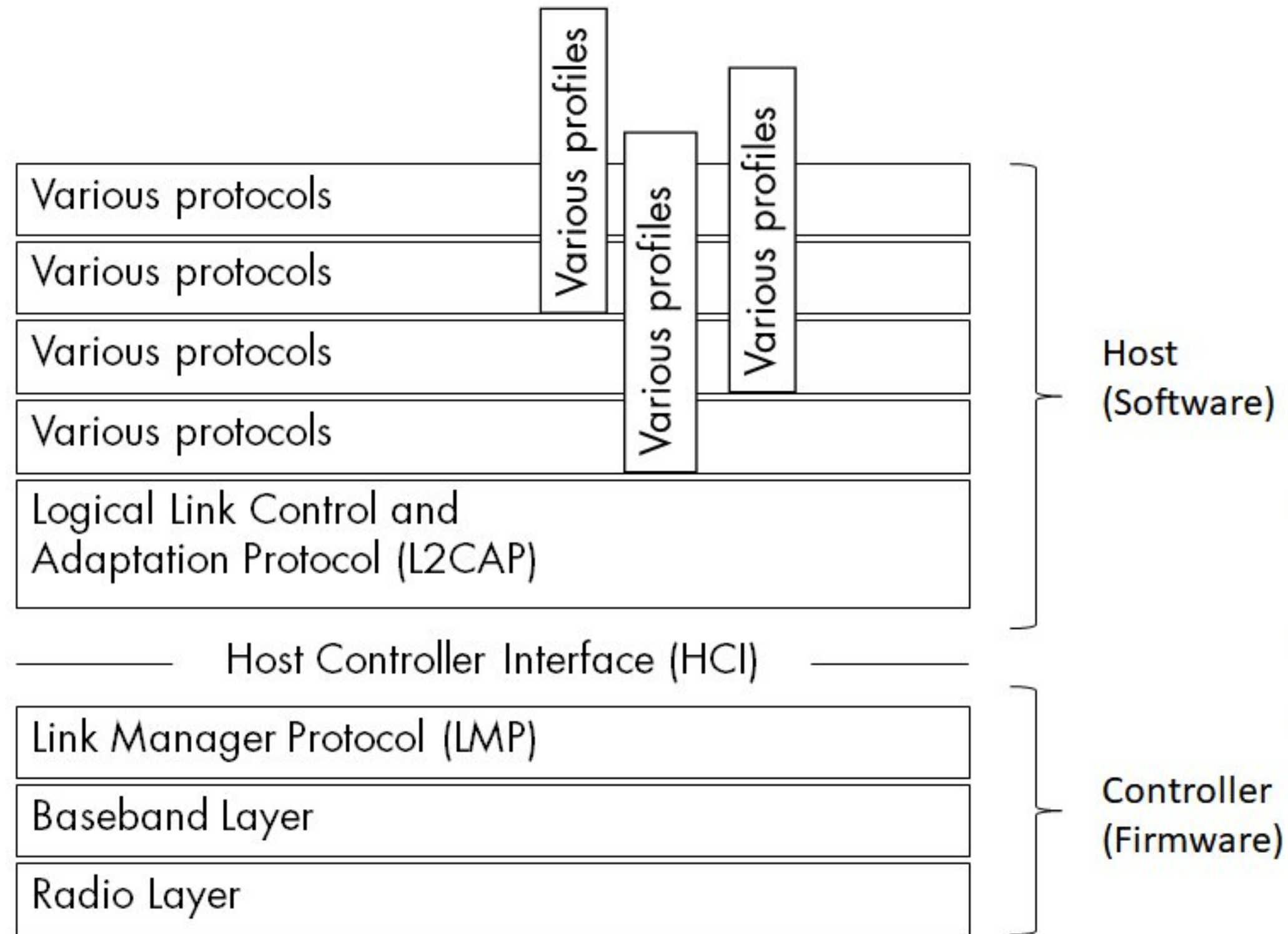
Supervisor: Asoc. Prof. Dr. Pēteris Paikens

Research Motivation

- Protocol Complexity: Legacy support introduces interoperability challenges and increases the risk of firmware vulnerabilities.
- Update Limitations: Centralized updates are often impractical or physically infeasible for many devices.
- Quality Assurance Gaps: Certification processes lack consistent enforcement of checks for malicious data processing.
- Security Risks: Vulnerable firmware can compromise OS-level protections in connected systems.

- SDP: Fingerprinting and info leaks via fuzzed requests.
- HFP/HSP: Exposes MitM and authentication flaws.
- A2DP: Reveals data leaks and buffer handling issues.
- OPP (OBEX): Exploits unauthorized access (e.g., *BlueSnarfing*).
- L2CAP: Triggers buffer overflows and protocol misuse.
- HCI: Detects command injection vulnerabilities.
- LMP: Disrupts key negotiation and causes state desynchronization.

Fuzzing Effects in Bluetooth Stack

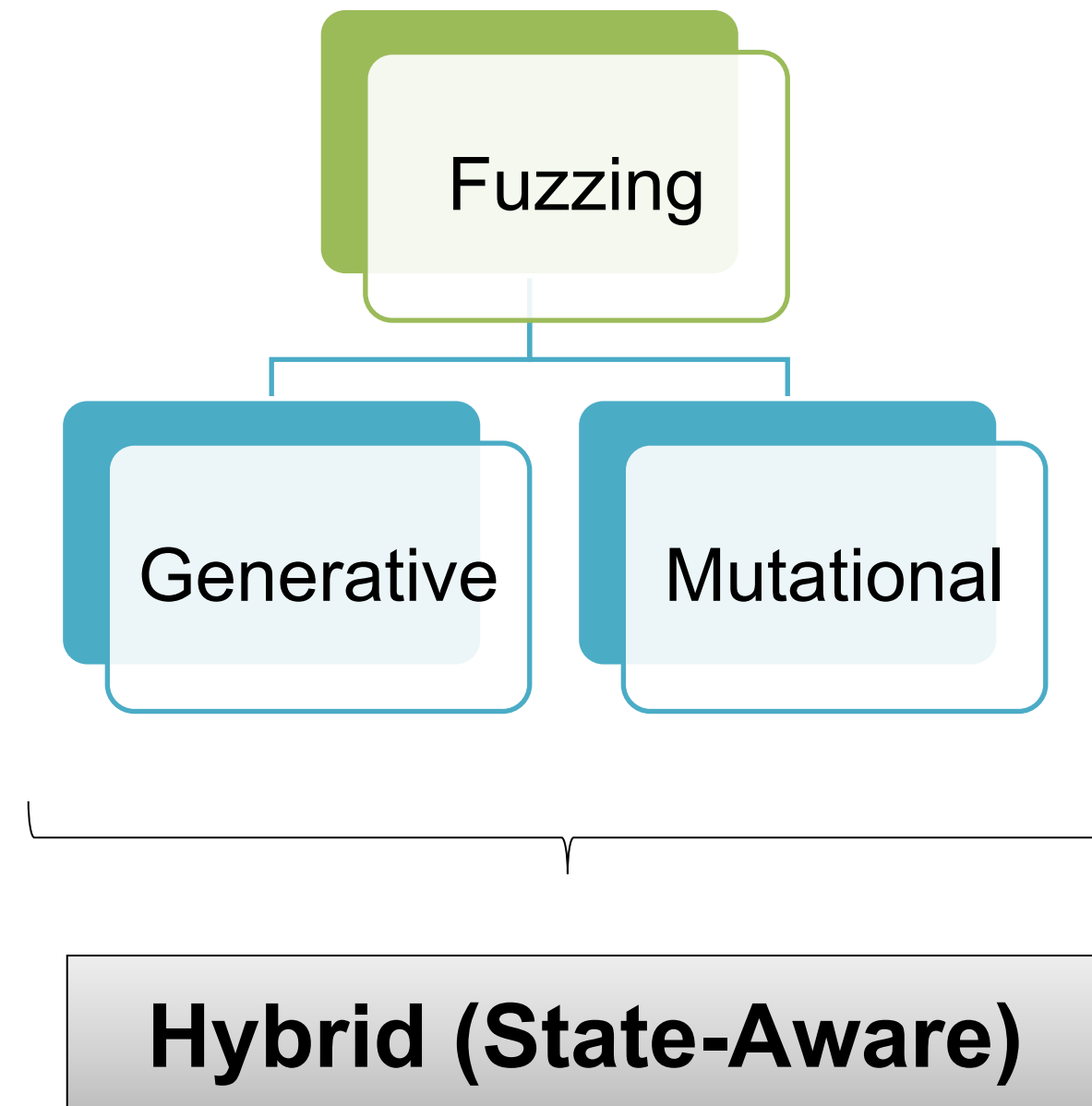


Key Fuzz Testing Approaches

Generative Approach: Creates test data from scratch using protocol specifications, system state models, or formal Bluetooth message syntax.

Mutational Approach: Modifies existing valid data by altering bits or field values.

Hybrid Approach: Combines generative and mutational methods, leveraging coverage data and AI to optimize test data and analyze results.



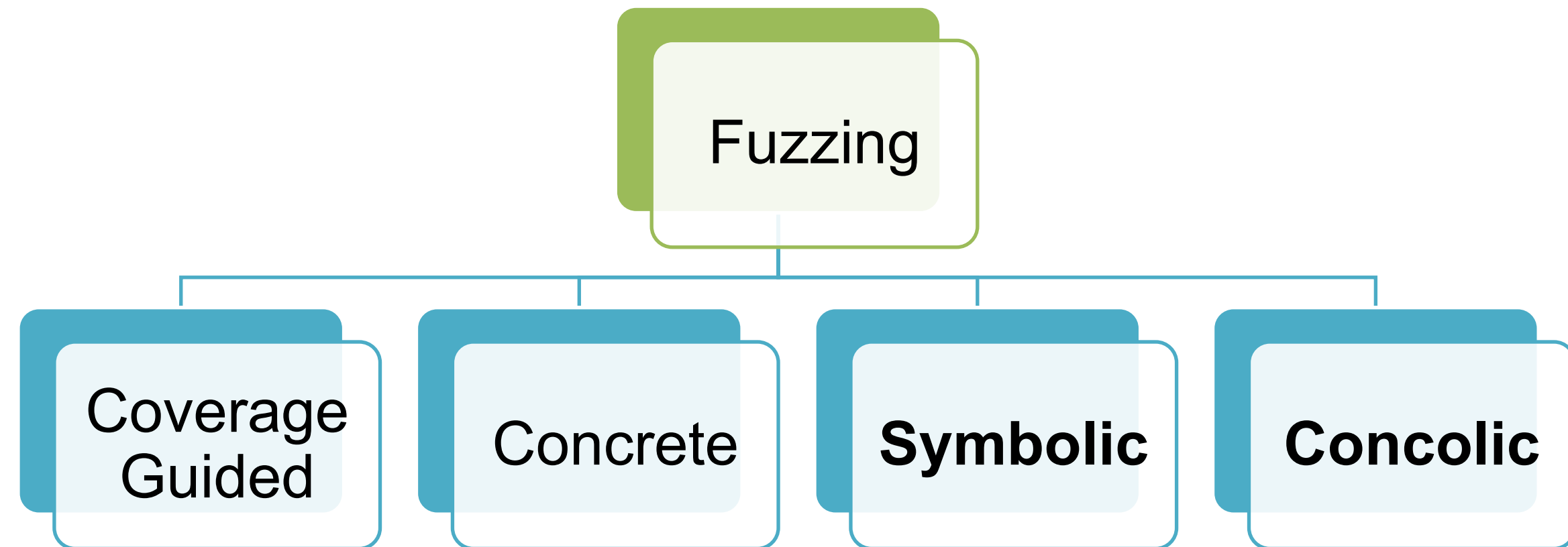
Key Types of Fuzzing Execution Procedures

Coverage-Guided Execution: Dynamically adjusts testing to maximize coverage and ensure all parts are as thoroughly tested as possible.

Concrete Execution: Uses real, specific input values for testing.

Symbolic Execution: Analyzes program execution with symbolic variable values to explore all possible execution paths in parallel.

Concolic Execution: Combines symbolic and concrete execution to more efficiently identify problematic input paths.



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**.



LATVIJAS
UNIVERSITĀTE

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 replacite 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 (IWEDI'2023).

Role: Co-authored as the 2nd author.

Paper status: Published as an online paper.

Publisher: EDI IWEDI'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

Bluetooth Classic Protocol Fuzzing Practices

Eduards BLUMBERGS¹, 0009-0005-3855-2358, Krišjānis NESENBBERGS², 0000-0002-2445-2891, Pēteris PAIKENS¹, 0000-0002-5939-5436

¹ Institute of Mathematics and Computer Science University of Latvia,
Raina blvd. 29, Riga, Latvia

² Institute of Electronics and Computer Science,
Dzerbenes str. 14, Riga, Latvia

eduards.blumbers@lu.lv, krisjanis.nesenbergs@edi.lv, peteris@ailab.lv

Abstract. As devices using the prevalent but complex Bluetooth Classic wireless protocol often contain implementation flaws which may enable security vulnerabilities, there is a need for systematic testing to identify and fix such bugs. In this paper, we explore the problems related to Bluetooth security analysis and vulnerability detection, providing a survey of the available options and best practices for remote protocol fuzzing that can be used for security testing of Bluetooth devices. The goal of this work is to lay a foundation for further practical security research testing to apply fuzzing tools and techniques to identify new vulnerabilities. We provide a literature review and explore current best practices for protocol fuzzing approaches that can be used for black-box Bluetooth hardware and firmware analysis, which is especially relevant for embedded systems that contain some sort of Bluetooth-enabled radio chip. Finally, we discuss the challenges and future research directions in this field.

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

1 Introduction

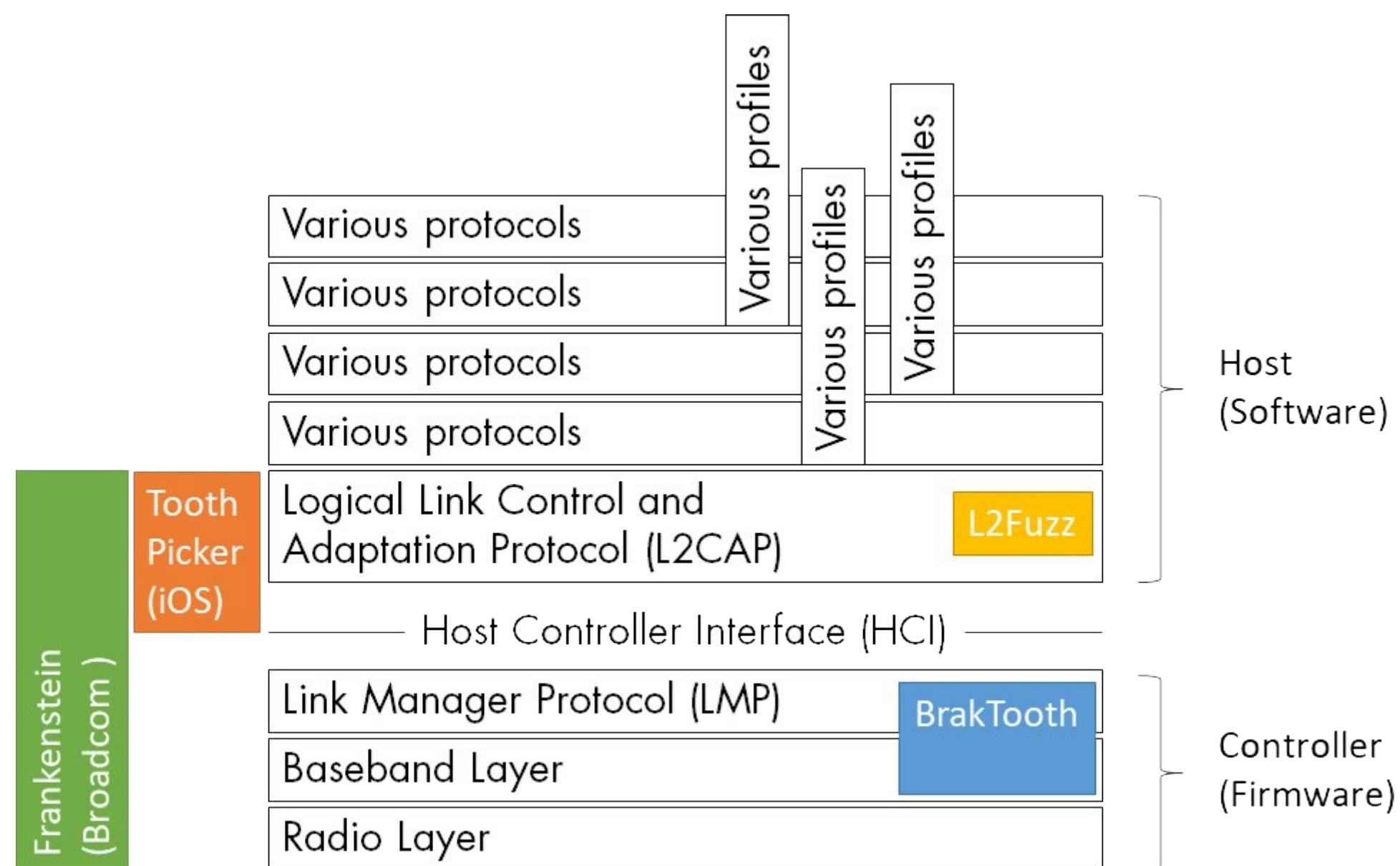


LATVIJAS
UNIVERSITĀTE

Bluetooth Classic Protocol Fuzzing Practices

Paper status: major revision in progress

Publisher: Baltic Journal of Modern Computing



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

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@ailab.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



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.



**LATVIJAS
UNIVERSITĀTE**

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 Bišas



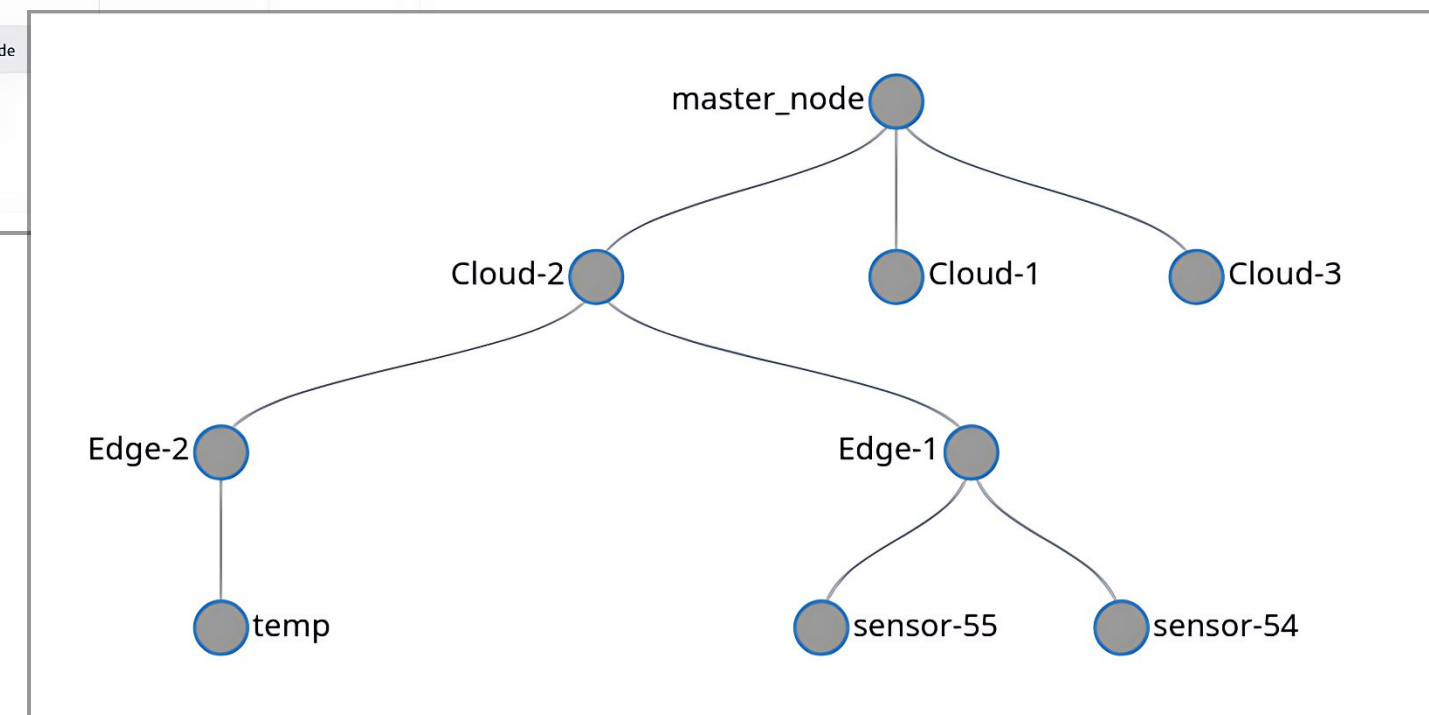
LATVIJAS
UNIVERSITĀTE

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.

Exploring Feasible Future Research Venues

As the both projects has concluded, new project opportunities are being explored to align with the thesis scope.

- ***Physics Informed Machine Learning-Based Prediction and Reversion of Impaired Fasting Glucose Management (PRAESIIDIUM)***
Proposed Future Task:
 - Develop firmware for a wearable device with **bioimpedance sensing** and **advanced signal processing**.
 - Investigate **Bluetooth functionality** and assess the **safety protocols** of the device.
- **Future Research Opportunities:**
 - Securing *CapTech* membership to identify strategic partners and secure funding for **advanced protocol fuzzing** from the European Defense Agency.
 - Submission to project calls focusing on:
 - **Automating Protocol Fuzzing Research** with **LLM and AI agent integration**.
 - Fuzzing **wireless communication protocols in UAV systems** to improve security and reliability.



**LATVIJAS
UNIVERSITĀTE**

The draft has been under development throughout the last year and currently comprises approximately 30 pages, but it 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

Next Objectives

- Exploring OTA fuzzing using the *Infineon CYW920735Q60EVB-01* development board.
- Drafting a paper on Bluetooth fuzzing with Python-based tools.
- Developing a standalone Bluetooth fuzzing test with the *Cheap Yellow Display* and *ESP32 Marauder* framework.
- Resolving *Braktooth* compatibility issues for modern systems.
- Engaging in security conferences to collaborate and share advancements with the community.
- Identifying and securing a project more closely aligned with my research focus.
- Supervise a bachelor's thesis.



LATVIJAS
UNIVERSITĀTE

Thank You!



**LATVIJAS
UNIVERSITĀTE**