

Matheus Eduardo Garbelini, Ph.D

✉ matheus_garbelini@sutd.edu.sg

🐦 @MatheusGarbelin

🌐 LinkedIn

🌐 <https://matheus-garbelini.github.io/home/>



Employment History

- Oct 2023 – Ongoing **Post-doctoral Research Fellow.** Singapore University of Technology and Design (SUTD), Integrant of ASSET Research Group.
- Jan 2019 – Sep 2019 **Research Assistant.** Singapore University of Technology and Design (SUTD), Integrant of ASSET Research Group.
- Dec 2017 – Dec 2018 **R&D Engineering Intern.** Lactec. Curitiba, Brazil.
- Jan 2016 – Dec 2017 **R&D Engineering Intern.** Zulgg Tecnologias. São José dos Pinhais, Brazil.

Education

- Sep 2019 – Sep 2023 **Ph.D., Singapore University of Technology and Design,** Computer Science. Thesis title: *Directed Stateful Fuzzing of Wireless Protocols.* * Received Outstanding Thesis Award.
- Feb 2014 – Dec 2018 **B.E. Electronic Engineering, Pontifical Catholic University of Paraná (PUCPR),** Curitiba, Brazil. * Received Best Student Award.

Key Research Contributions

- 2024 **IoT Defense.** Proposed, designed and evaluated technology for defending Bluetooth Low Energy (BLE) devices against over-the-air attacks (paper in ACSAC 2024).
- 2019-2024 **IoT/Wireless Software Testing via Fuzzing.** Proposed, designed and evaluated some of the pioneering technologies for Wireless Protocol Fuzzing for 5G NR, Bluetooth BR/EDR, Bluetooth Low Energy (BLE), Zigbee etc (papers in USENIX ATC 2020, USENIX Security 2022, IEEE TDSC 2020, ICST 2024 etc.).

Awards and Honours

- 2024 **2024 Outstanding Thesis Award** from Singapore University of Technology and Design for PhD thesis "Directed Stateful Fuzzing of Wireless Protocols".
- 2023 **36,000 USD award** from [Qualcomm Inc.](#) and [MediaTek Inc.](#) for finding a total of 12 security flaws (7 with **High severity**) in 5G baseband modems.
- 2022 **6,000 USD award** from [Intel](#) for discovering two Intel AX200 attacks under the BrakTooth family of security vulnerabilities.
- 2020 **Recognized by Medtronic Inc.** as an outstanding research contributor for discovering Sweyn-Tooth family of vulnerabilities.
- 2018 Awarded with PUCPR Marcelino Champagnat award for best student in Electronic Engineering class of 2018 and PUCPR Deans's list of 2017 for remarkable academic performance.

Broader Research Impact

- 2019-2024 Works on Wireless Fuzzing have discovered over [70 security vulnerabilities](#) across Wi-Fi, Bluetooth Low Energy, Bluetooth BR/EDR, CoAP, Zigbee and 5G NR implementations.

Broader Research Impact (continued)

- 2020-2024 📌 Research has been featured in [WIRED](#), [HackerNews](#), [ThreatPost](#), [PC Magazine](#), [Security-Week](#) along with **100+ news articles** worldwide. Such research has also raised alerts from regulatory agencies like [CSA \(Singapore\)](#), [HSA \(Singapore\)](#), [IMDA \(Singapore\)](#), [CISA \(Department of Homeland Security\)](#), [FDA \(USA\)](#) etc.
- 2019-2023 📌 Research on Wireless fuzzing (Wi-Fi, Bluetooth BR/EDR and Bluetooth Low Energy) has been translated by Keysight Technologies in their [IoT Security Assessment Software](#).
- 2023 📌 Discovery of 5G security vulnerabilities (5Ghoul) [featured by Channel News Asia](#).
- 2020-2022 📌 [Recognized by Cyber Security Agency \(CSA\) Singapore](#) for discovering SweynTooth and BrakTooth family of security vulnerabilities.

Notable Open-source Contribution

- 2024 📌 [U-Fuzz](#): Over-the-air IoT protocol Fuzzing tool. Experimented to find 11 new vulnerabilities across CoAP, Zigbee and 5G NR implementations. **GitHub ★: 70+**.
- 2023 📌 [5Ghoul](#): Over-the-air 5G SA exploits and 5G NR fuzzing tool. Independently used by industry (pen testing companies) to find 5G SA vulnerabilities. **GitHub ★: 500+**.
- 2022 📌 [BrakTooth](#): Over-the-air Bluetooth BR/EDR exploits. Independently used by industry (e.g., Samsung and MediaTek) to find Bluetooth BR/EDR vulnerabilities. **GitHub ★: 430+**.
- 📌 [Bluetooth BR/EDR Sniffer](#): Reverse engineered Bluetooth BR/EDR sniffer. **GitHub ★: 490+**.
- 2020 📌 [SweynTooth](#): A set of Bluetooth Low Energy (BLE) exploits. Independently used by industry (e.g., EM Semiconductor, Microchip) and government agencies (e.g., regulatory agencies) to find BLE security vulnerabilities. **GitHub ★: 260+**.

Selected Key Publications

1. *VaktBLE: A Benevolent Man-in-the-Middle Bridge to Guard against Malevolent BLE Connections*. Geovani Benita and Leonardo Sestrem and [Matheus E. Garbelini](#) and Sudipta Chattopadhyay and Sumei Sun and Ernest Kurniawan. 40th Annual Computer Security Applications Conference (ACSAC) 2024.
2. *U-Fuzz: Stateful Fuzzing of IoT Protocols on COTS Devices*. Zewen Shang, [Matheus E. Garbelini](#), and Sudipta Chattopadhyay. 17th IEEE International Conference on Software Testing, Verification and Validation (ICST) 2024.
3. *BrakTooth: Causing Havoc on Bluetooth Link Manager via Directed Fuzzing*. [Matheus E. Garbelini](#), Vaibhav Bedi, Sudipta Chattopadhyay, Sumei Sun, and Ernest Kurniawan. USENIX Security Symposium 2022.
4. *SweynTooth: Unleashing Mayhem over Bluetooth Low Energy*. [Matheus E. Garbelini](#), Chundong Wang, Sudipta Chattopadhyay, Sumei Sun, and Ernest Kurniawan. USENIX Annual Technical Conference (USENIX ATC) 2020.

Research Publications

Google Scholar: https://scholar.google.com/citations?user=_PXBxu0AAAAJ&hl=en

Maintained List: <https://matheus-garbelini.github.io/home/publication/>

Bibliography

- 1 [Matheus E. Garbelini](#), Z. Shang, S. Chattopadhyay, S. Sun, and E. Kurniawan, “5Ghoul: unleashing chaos on 5g edge devices via stateful multi-layer fuzzing,” **IEEE Transactions on Dependable and Secure Computing (TDSC)**, **Under Minor Review**, 2025.

- 2 G. Benita, L. Sestrem, [Matheus E. Garbelini](#), S. Chattopadhyay, S. Sun, and E. Kurniawan, "VaktBLE: a benevolent man-in-the-middle bridge to guard against malevolent BLE connections," **40th Annual Computer Security Applications Conference (ACSAC)**, 2024.
- 3 G. Hua, [Matheus E. Garbelini](#), and S. Chattopadhyay, "AirBugCatcher: automated wireless reproduction of IoT bugs," **40th Annual Computer Security Applications Conference (ACSAC)**, 2024.
- 4 Z. Shang, [Matheus E. Garbelini](#), and S. Chattopadhyay, "U-fuzz: Stateful fuzzing of IoT protocols on cots devices," **17th IEEE International Conference on Software Testing, Verification and Validation (ICST)**, 2024. [🔗 URL: https://asset-group.github.io/papers/U-Fuzz.pdf](https://asset-group.github.io/papers/U-Fuzz.pdf).
- 5 A. K. T. Yeo, [Matheus E. Garbelini](#), S. Chattopadhyay, and J. Zhou, "Vitrobench: Manipulating in-vehicle networks and cots ecus on your bench," **Vehicular Communications, Journal First**, 2023. [🔗 URL: https://asset-group.github.io/papers/VitroBench.pdf](https://asset-group.github.io/papers/VitroBench.pdf).
- 6 [Matheus E. Garbelini](#), V. Bedi, S. Chattopadhyay, S. Sun, and E. Kurniawan, "Braktooth: Causing havoc on bluetooth link manager via directed fuzzing," **USENIX Security Symposium**, 2022. [🔗 URL: https://asset-group.github.io/papers/BrakTooth.pdf](https://asset-group.github.io/papers/BrakTooth.pdf).
- 7 [Matheus E. Garbelini](#), Z. Shang, S. Chattopadhyay, S. Sun, and E. Kurniawan, "Towards automated fuzzing of 4g/5g protocol implementations over the air," **IEEE Global Communications Conference (GLOBECOM)**, 2022. [🔗 URL: https://asset-group.github.io/papers/AutoFuzz4G5G.pdf](https://asset-group.github.io/papers/AutoFuzz4G5G.pdf).
- 8 [Matheus E. Garbelini](#), C. Wang, and S. Chattopadhyay, "Greyhound: Directed greybox wi-fi fuzzing," **IEEE Transactions on Dependable and Secure Computing (TDSC), Journal First**, 2020. [🔗 URL: https://asset-group.github.io/papers/Greyhound.pdf](https://asset-group.github.io/papers/Greyhound.pdf).
- 9 [Matheus E. Garbelini](#), C. Wang, S. Chattopadhyay, S. Sun, and E. Kurniawan, "Sweyntooth: Unleashing mayhem over bluetooth low energy," in **USENIX Annual Technical Conference (USENIX ATC)**, 2020. [🔗 URL: https://asset-group.github.io/papers/SweynTooth.pdf](https://asset-group.github.io/papers/SweynTooth.pdf).

Patents

- 2022 [📖](#) [Method and System for Detecting Anomalies of Server and Client](#), US Patent no. US11349963B1. Inventor: Sudipta Chattopadhyay (SUTD), [Matheus Eduardo Garbelini \(SUTD\)](#), Francis-Bs Ngian (Keysight Technologies) and Cyril Tan (Keysight Technologies).




Research Grants I Helped to Write

- 2023-2026 [📖](#) **MOE Tier 2 Award**, Towards Automated Fuzzing and Debugging of Closed Communication Protocol Stacks (550K SGD).
- 2022-2025 [📖](#) **Future Communications Program (FCP)**, Towards Differential Fuzzing of 5G and beyond 5G Communications (967K SGD).
- 2020-2023 [📖](#) **NRF National Satellite of Excellence in Trustworthy Systems and Software**, Over-the-air Security Testing of Wireless Protocol Implementations (548K SGD).
- 2021-2023 [📖](#) **NRF National Satellite of Excellence in Trustworthy Systems and Software**, Towards a Universal IoT Protocol Testing Infrastructure (398K SGD).



Invited Presentations, Talks & Sessions

- Oct 2024 [📖](#) [Panel: Secured Communication Networks](#), World Telecommunication Standardization Assembly, New Delhi.
- August 2024 [📖](#) [5Ghoul Framework - 5G NR Attacks & 5G OTA Fuzzing](#), DEFCON32, Las Vegas.

Invited Presentations, Talks & Sessions (continued)

- May 2024  [IoT and 5G Security: Discovering Wireless Protocol Vulnerability through Fuzzing](#), Singapore *ISC²* Chapter.
- Jan 2024  [Small group QA Session Facilitator](#), Singapore Global Young Scientists Summit (GYSS).
- October 2020  [Invited Tutorial on IoT Security](#), Singapore International Cyber Week, 2020.

Teaching Assistance

- 2024  **Software Testing and Verification**, Class size = 35
- 2020  **Systems Security**, Class size = 45

Advised Students (As a Postdoc.)

Current PhD Students




- Sept 2023-Present  **Shijie Luo**. *A Practical Approach to Inject Attacks into 5G NR*. *Ongoing work*.
-  **Zewen Shang**. *Towards Universal IoT Protocol Testing Infrastructure*. First Author paper in [IEEE International Conference on Software Testing, Verification and Validation \(ICST\) 2024](#).
-  **Guoqiang Hua**. *Automated Exploit Generation and Debugging for Over-the-air Attacks*. First Author paper in [Annual Computer Security Applications Conference \(ACSAC\) 2024](#).
-  **Geovani Benita**. *Efficient Link-layer Attacks and Defence for Wireless Network*. First Author paper in [Annual Computer Security Applications Conference \(ACSAC\) 2024](#).
-  **Anthony Yeo**. *Vehicular Communication Security: From Testbed to Attacks and Defence*. First Author paper in [Vehicular Communications, Impact Factor: 6.7](#).

Professional Service

Journal Review

- 2025  [ACM Computing Surveys](#)

Technical Program Committee

-  [DATE 2025](#), [ACM CPSS 2025](#).
- 2024  [ICCD 2024](#).
- 2023  [SOLI 2023](#).