Matheus Eduardo Garbelini

Research Fellow · PhD · Electronic Engineer
Single, 27 years
SUTD, 8 Somapah Rd, Singapore, 487372 - Singapore
+65 9392-1654 | matheus_garbelini@mymail.sutd.edu.sg | matheus-garbelini.github.io/home/ | matheus_garbelini

Research Interests

Focuses in research fields related to software/hardware security in wireless Internet of Things (IoT) and Cyber-Physical systems.

- Wireless Security;
- Fuzzing and other Software testing techniques applied to vulnerability discovery;
- Cyber-physical Systems and Industrial Internet of Things (IIoTs).

Education

- Doctor of Philosophy (PhD) in Computer Science. Singapore University of Technology and Design (SUTD), completed in September 2023. GPA: 4.5/5.0;
- Electronic Engineer. Pontifical Catholic University of Paraná (PUCPR), completed in 2018;
- Electronic Technician. National Service of Industrial Learning (SENAI), completed in 2014.

Idioms

- English - Fluent speaking, writing and reading;
- Spanish - Basic speaking, basic writing and reading;
- Brazilian Portuguese - Native.

Publications

- M. E. Garbelini, Z. Shang, S. Chattopadhyay, S. Sun and E. Kurniawan, “5GHOUL: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing”. Under Submission (2023).
- M. E. Garbelini, Z. Shang, S. Chattopadhyay, S. Sun and E. Kurniawan, “Towards Automated Fuzzing of 4G/5G Protocol Implementations Over the Air”. 2022 IEEE Global Communications Conference (2022).
- Garbelini, M. E., Bedi, V., Chattopadhyay, S., Sun, S., and Kurniawan, E. “BrakTooth: Causing Havoc on Bluetooth Link Manager via Directed Fuzzing”. 31st USENIX Security Symposium (2022).
- Garbelini, Matheus E., Chundong Wang, Sudipta Chattopadhyay, Sun Sumei, and Ernest Kurniawan. “SweynTooth: Unleashing Mayhem over Bluetooth Low Energy”. 2020 USENIX Annual Technical Conference (2020).
- Garbelini, Matheus E., Chundong Wang, and Sudipta Chattopadhyay. “GREYHOUND: Directed Greybox Wi-Fi Fuzzing.” IEEE Transactions on Dependable and Secure Computing (2020).
- Garbelini, Matheus, and Gilberto Reynoso-Meza. “Multi-Objective Evolutionary Optimization Pid Tuning for Longitudinal Movement of an Aircraft”. XIII Simpósio Brasileiro de Automação Inteligente (2017).
- Garbelini, Matheus E. et al. “Yaw and Pitch Control Tuning using Multiobjective Optimisation Techniques”. XII Simpósio Brasileiro de Automação Inteligente (2015).

Participation in Workshops

- Presenter at Singapore Cybersecurity R&D Workshop 2020: "Deep Dive into IoT Security and IoT Protocol Vulnerabilities". https://sgcsc.sg/cybersecurity-rd-workshop-2020/. 09 Oct 2020.

Experience

SUTD - ASSET Research group — *Singapore*

Research Fellow - Research on 5G and Open RAN security, with focus on topics such as automated vulnerability detection, new attack surfaces and countermeasures. — *2023 - Ongoing*

SUTD - ASSET Research group — *Singapore*

PhD student - Research on wireless security related with the goal to design new technologies that enables automated low-level wireless security testing and vulnerability detection. — *2019 - 2023*

Lactec - Electronic Department — *Prado Velho, Curitiba, Paraná*

Intern - Worked in the development of a hardware platform for electronic automotive injection simulation; Responsible for software architecture on linux platform and development of back-end and front-end for local server in a power quality analyzer project; Development of hardware and software for pyrometer wireless communication system. — *2017 - 2018*

Zulgg Tecnologias S/A — *Águas Belas, São José dos Pinhais, Paraná*

Intern - Development of embedded software, hardware and web services in applications for 3D printer, Industry 4.0 (PLC, remotes, supervisory systems and related hardware) using ARM, ESP8266, ESP32 microcontrollers and embedded Linux platforms; Development of mobile and desktop applications using C# and Web technologies such as NodeJs, Cordova and NwJs. — *2016 - 2017*

Fellowships and Awards

- Discoverer of several wireless vulnerabilities in popular Wi-Fi and Bluetooth Low Energy IoT Chipsets. A total of 23 Common Vulnerabilities and Exposures (CVEs) were issued as of October 2020 for a range of IoT semiconductor vendors such as Texas Instruments, Espressif Systems, Cypress, NXP, Microchip, Dialog Semi., STMicroelectronics, ON Semi. and Telink Semi.: http://asset-group.github.io/disclosures/sweyntooth/, https://github.com/Matheus-Garbelini/esp32_esp8266_attacks.
- SweynTooth research received attention from regulatory government agencies such as CSA Singapore, Health Science Authority (HSA) Singapore, Department of Homeland Security (DHS) USA and Food and Drug Administrations (FDA) which published instructions to affected wireless product vendors & critical infrastructure.
- Research featured in Wired, Science Magazine and many other news articles. Furthermore, Cyber Security Agency of Singapore (CSA) congratulated research outcome in honourable post: https://www.linkedin.com/feed/update/urn:li:activity:6689492842139783168/.
- Acknowledged by Medtronic as outstanding research contributor: https://global.medtronic.com/xg-en/product-security/outstanding-research-contributors.html
- Upcoming 5G security research founding granted by National Cybersecurity R&D (NCR) Programme.
- Awarded by Espressif Systems with a 2200$ Bug Bounty for discovering a critical Wi-Fi vulnerability in their wireless System-on-chips (ESP32, ESP8266) named Zero PMK Installation (CVE-2019-12587).
- 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.

- PUCPR Research scholarship: Hardware and software development of content-centric wireless nodes using LoRa and Xbee radio modules.
- CnPq Research scholarship with 2 published short papers at Brazilian Symposium on Intelligent Automation (2015 and 2017) in the field of evolutionary multi-objective optimization.
- PUCPR Mobile Robotics Team Fellowship: Leading electronic designer (2016 - 2018) in development of Hardware and firmware of motor control boards for demanding DC motors used in combat robots; Participated in robot competitions and related events.

Additional Skills

- Main programming languages: Python, C/C++, C#, Assembly, Matlab.
- Proficient with Wi-Fi and Bluetooth platforms security and development.
- Familiar with development of Desktop, Web and Mobile (HTML, CSS, Javascript, PHP, NodeJs, Cordova and Xamarin) applications applied to embedded systems and Internet of Things.
- Good knowledge in software development for embedded systems based on AVR, ARM, ESP and Linux platforms.
- Familiarity with PLCs and supervisory systems. Experience with OpenPLC project.

Contributions

- Disclosed Bluetooth Classic (BT) exploits, testing scripts & platform for BT Baseband experimentation: `https://github.com/Matheus-Garbelini/braktooth_esp32_bluetooth_classic_attacks`
- Disclosed Bluetooth Low Energy (BLE) exploits, testing scripts & platform for BLE Link-Layer experimentation: `https://github.com/Matheus-Garbelini/sweyntooth_bluetooth_low_energy_attacks`
- Disclosed ESP32/ESP8266 Wi-Fi Proof of concept & testing tool: `https://github.com/Matheus-Garbelini/esp32_esp8266_attacks`
- Contributed to Open Source projects such as Scapy and OpenPLC.