Matheus Eduardo Garbelini

PhD Student · Electronic Engineer
Single, 24 years
2 Jln Tiga Ratus #03-05, 488067 - 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);
- Embedded Systems and Software/Hardware engineering.

Education

- PhD Student. Singapore University of Technology and Design (SUTD), expected graduation in September 2023. Cumulative 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 - Advanced speaking, writing and reading.
- Spanish - Basic speaking, basic writing and reading.
- Brazilian Portuguese - Native.

Publications

- Garbelini, Matheus E., Chundong Wang, Sudipta Chattopadhyay, Sun Sumei, and Ernest Kurniawan. "Sweyn-Tooth: Unleashing Mayhem over Bluetooth Low Energy". 2020 USENIX Annual Technical Conference (USENIX-ATC 20). 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

2019 - Ongoing

PhD student - Research on wireless security related projects with the goal to design new technologies to improve the current state of Internet of Things network security and Ultimately enable automated low-level wireless security testing to be viable.

Lactec - Electronic Department

Prado Velho, Curitiba, Paraná

2017 - 2018

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.

Zulgg Tecnologias S/A

Águas Belas, São José dos Pinhais, Paraná

2016 - 2017

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.

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.
- Familiar with Wi-Fi and Bluetooth Low Energy (BLE) 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 runtime and supervisory systems. Experience with OpenPLC project.

Contributions

- Contributed to Open Source projects such as Scapy and OpenPLC.
- Disclosed Bluetooth Low Energy (BLE) exploits, testing scripts & platform for BLE Link-Layer experimentation (118 stars): `https://github.com/Matheus-Garbelini/sweyntooth_bluetooth_low_energy_attacks`
- Disclosed ESP32/ESP8266 Wi-Fi Proof of concept & testing tool (675 stars): `https://github.com/Matheus-Garbelini/esp32_esp8266_attacks`