MARCUS FELIPE BOTACIN

https://scholar.google.com/citations?user=Y8JHVbcAAAAJ
mfbotacin@gmail.com - https://marcusbotacin.github.io/
https://twitter.com/marcusbotacin - https://github.com/marcusbotacin

EMPLOYMENT

Assistant Professor *9/2024 - TBD*
Texas A&M University (TAMU), USA
Visiting Assistant Professor *10/2022 - 8/2024*
Texas A&M University (TAMU), USA
Lecturer *2021/2*
Federal University of Paraná (UFPR), Brazil

OTHER PROFESSIONAL ACTIVITIES

Scientific Board Advisor *3/2023 - 8/2024*
CYMDALL -https://www.cymdall.com/**, Israel**
Security Startup developing hardware-assisted detection mechanisms.

Scientific Board Advisor *8/2024 - 8/2024*
AppThreat -https://appthreat.com/**, UK**
Security company developing open-source tools.

EDUCATION

Ph.D. in Computer Science *2017 - 2021*
Federal University of Paraná (UFPR), Brazil
Thesis Title: "*On the Malware Detection Problem: Challenges and New Approaches*"
Advisor: Prof. Dr. André Ricardo Abed Grégio (UFPR)
CoAdvisor: Prof. Dr. Paulo Lício de Geus (UNICAMP)
Thesis Committee: Ph.D. Leigh Metcalf (CERT, Carnegie Mellon University), Ph.D. Leyla Bilge (Norton LifeLock), Prof. Dr. Daniel Oliveira (UFPR)
M.Sc. in Computer Science *2015 - 2017*
University of Campinas (UNICAMP), Brazil
Dissertation Title: "*Hardware-Assisted Malware Analysis*"
Advisor: Prof. Dr. Paulo Lício de Geus (UNICAMP)
CoAdvisor: Prof. Dr. André Ricardo Abed Grégio (UFPR)
Dissertation Committee: Prof. Dr. Carlos Maziero (UFPR), Prof. Dr. Sandro Rigo (UNICAMP)
B.Sc. in Computer Engineering *2010 - 2015*
University of Campinas (UNICAMP), Brazil
Final Project Title: "*Malware detection via syscall patterns identification*"
Advisor: Prof. Dr. Paulo Lício de Geus (UNICAMP)

INTERNATIONAL RESEARCH EXPERIENCE

University of Florida **NSF US-Brazil Collaboration**
Visiting Researcher hosted by Prof. Ph.D. Daniela Oliveira (UF, Gainesville, USA) August/2018 and May/2019

Friedrich-Alexander-Universität Erlangen-Nürnberg **DAAD Germany-Brazil Collaboration**
Visiting Researcher hosted by: Prof. Ph.D. Tilo Muller (FAU, Erlangen, GER) November/2018

RESEARCH INTERESTS

Malware Analysis, Evasion, and Detection	**Hardware-Assisted Security Solutions**
Sandbox Development and Antivirus Operation	**Reverse Engineering**

RESEARCH GRANTS

NSF SaTC: CORE: Small: An evaluation framework and methodology to streamline Hardware Performance Counters as the next-generation malware detection system - PI - 2024=2026 - $ 523.415,00 - `https://www.nsf.gov/awardsearch/showAward?AWD_ID=2327427&HistoricalAwards=false`

CURRENTLY ADVISED STUDENTS (AT TAMU): 15

Seyyed Ali Ayati - PhD (2023/10-TBD)
Soumyajyoti Dutta - PhD (2024/Spring-TBD) - Prev: MSc - Project-Based (2023/5-2023/12)
Eden Garze - PhD (2024/Fall-TBD)
Mabon Ninan - PhD (2024/Fall-TBD)
Uros Stanic - PhD (2024/Fall-TBD) - Prev: Undergrad -Faculty of Technical Sciences of Novi Sad (Serbia) - Computer Science Student Advancement Program (CSSAP) Summer Internship
Giorgia di Pietro - PhD visitor - Sapienza University of Rome - Spring/25
Akshat Punjabi - MSc - Project-Based (2023/8-In Progress)
Yash Phatak - MSc - Project-Based (2024/8-In Progress)
Bhavan Dondapati - MSc - Project-Based (2023/8-In Progress)
Tushar Premanand - Alumni Project (2024/Fall -In Progress)
Ayushri Jain - Alumni Project (2024/Fall -In Progress) - Prev: Directed Studies (2024/Fall)
Sushmita Pattanaik - Alumni Project (2024/Fall -In Progress)
Zach Smith - undergrad - Research Course - (Spring/25 - In Progress)
Fady Seha - undergrad - Research Course - (Spring/25 - In Progress)
mason - directed
John Ammon - Undergrad - Directed Studies (2025/Spring - In Progress) - Prev: NSF REU (2024) - Prev: Project-based (2023/5-2023/12)

GRADUATED STUDENTS (AT TAMU): 1

Nhat Nguyen, Msc - Spring/2025 - "AutoPYara: A Python/Java Framework for automatic YARA rule generation using semi-supervised clustering"

PREVIOUSLY ADVISED STUDENTS (AT TAMU): 14

Nhat Nguyen - MSc Thesis - (2024/Summer - 2025/Spring)
Anushka Garg - Directed Studies (2024/1)
Pranav Taukari - Directed Studies (2024/1) - MSc - Project-Based (2023/4-2023/6)
Snehith Bikumandla - MSc - Project-Based (2023-Aug/2023)
Parul Damahe - MSc - Project-Based (2023-Aug/2023) (2023/Summer)
Sidharth Anil - MSc - Project-Based (2023/5-2024/6)
Manoj Reddy Gurram - MSc - Project-Based (2023/8-2025/SPring)
Sahil Salunkhe - MSc - Project-Based (2023/8-In Progress)
Mohina Ahmadi - MSc - Volunteer Summer Internship (2024/Summer - 2024/Fall)
George Demetriou - Summer Internship - Halliburton Program - (2024/Summer)
Shrey Joshi - Summer Internship - Halliburton Program - (2024/Summer)
Jayesh Tripathi - Alumni Project (2024/Fall)
Rohan Dalvi - Alumni Project (2024/Fall)
Sai Akash Uppala - Alumni Project (2024/Fall)

(CO)ADVISED UNDERGRADUATE STUDENTS (IN BRAZIL): 5

Lucas Baganha Galante (UNICAMP, 2017-2019) - Linux Malware and ML-based malware detection.
Giovanni Bertão (UNICAMP, 2017-2019) - Large-scale malware repositories and application crawling.
Vitor Falcão da Rocha (UNICAMP, 2016-2017) - Anti-forensics and malware anti-analysis.
Raphael Machinicki (UFPR, 2019-2020) - Analysis of Android apps' operations.
Felipe Duarte Domingues (UFPR/UNICAMP, 2019-2021) - Antivirus' operations.

GRADUATION COMMITTEES (AT TAMU): 2

Chair: Nhat Nguyen, CSE MSc - Spring/2025
Member: Atharva Girish Agashe - ECE MSc - Spring/2025

ACADEMIC AWARDS

Top-3 Best PhD Thesis in Security - Brazilian Computer Society - 2022
Best PhD Thesis - Department of Informatics/UFPR - 2022
Best Master Dissertation in Security - 1st place - Brazilian Computer Society - 2018
Best Master Dissertation - Institute of Computing/UNICAMP - 2018
Best Undergraduate Security Research Paper (co-author)- 1st place - Brazilian Computer Society - 2018
Travel Grant - Student Diversity Grant - USENIX ENIGMA - 2019

CONTESTS PRIZES

Participation in the Machine Learning-based malware evasion challenge (`mlsec.io`**).**

Defenders 2021: 1st place
Defenders 2020: 2nd place

Attackers 2021: 1st place
Attackers 2019: 2nd place

Attackers 2020: 1st place

DEVELOPMENT PROJECTS

Corvus: Public, Online Malware Analysis Sandbox - `https://corvus.inf.ufpr.br/`

FEATURED TALKS

"*Near-memory In-Memory Detection of Fileless Malware*" **- Keynote at the Brazilian security symposium (SBSEG) 2023 -** `https://sbseg2023.ufjf.br/programacao/palestrantes/`
"*Why Is Our Security Research Failing? Five Practices to Change!*" **- USENIX ENIGMA 2023 -** `https://www.youtube.com/watch?v=7XUKwSExJG0&t=4s&pp=ugMICgJwdBABGAE%3D`
"*Does Your Threat Model Consider Country and Culture? A Case Study of Brazilian Financial Malware to show that it Should!*" **- USENIX ENIGMA 2021 -** `https://www.youtube.com/watch?v=5mrEJ83rBDY`
"*All You Always Wanted to Know About Antiviruses* " **- HackInTheBox 2023 -** `https://conference.hitb.org/hitbsecconf2023ams/session/commsec-all-you-always-wanted-to-know-about-antiviruses/` **-** `https://www.youtube.com/watch?v=fnexx1Ek168`

MEDIA COVERAGE

NSF SaTC HPC grant award on TAMU website: `https://engineering.tamu.edu/news/2023/08/innovative-approach-detecting-malware-through-hardware-integrated-protection.html`

OTHER EVENTS

US participant in the NSF-FAPESP Workshop on Cybersecurity and Privacy (2025): `https://fapesp.br/nfwsecurity`

ACADEMIC COMMUNITY SERVICES

National Science Foundation (NSF) Panelist (+ad-hoc reviewer).
Guest Editor for ACM DTRAP Special Issue on Non-conventional Malware (2023).
PC member for USENIX Security 2025, 2024, 2023, 2022
PC member for ACM Conference on Computer and Communications Security (CCS) 2025, 2024, 2023
PC member for Network and Distributed System Security (NDSS) Symposium 2025, 2024
PC member for ACM Annual Computer Security Applications Conference (ACSAC) 2024, 2023
PC member for International Symposium on Research in Attacks, Intrusions and Defenses (RAID) 2024, 2023
PC member for ACM Asia Conference on Computer and Communications Security (AsiaCCS) 2024
PC member for IEEE/ACM International Symposium on Microarchitecture (MICRO) 2024
PC member for International Conference on Applied Cryptography and Network Security (ACNS 2025)
PC member for Workshop on Rethinking Malware Analysis (WoRMA) - 2025, 2024
PC member for International Workshop on Re-design Industrial Control Systems with Security (RICSS) 2024, 2023
Artifact Evaluation Committee for the Journal of Systems Research (JSys).
Artifact Evaluation Committee for USENIX Security 2020 and USENIX WOOT 2020.
Artifact Evaluation Committee for Journal of Systems Research (JSys)
External reviewer for the Brazilian Security Symposium (SBSeg) - 2015 to 2022.

Ad-hoc reviewer for 57 different journals:

- **ACM Computing Surveys (CSUR)**
- **ACM Digital Threats: Research and Practice (DTRAP)**
- **ACM Transactions on Embedded Computing Systems (TECS)**
- **ACM Transactions on Privacy and Security (TOPS)**
- **Cell: Patterns**
- **Elsevier/ACTA Psychologica (Psy. of security)**
- **Elsevier Computers and Electrical Engineering (COMPELECENG)**
- **Elsevier Computers & Security**
- **Elsevier Computers in Human Behavior**
- **Elsevier e-Prime - Advances in Electrical Engineering, Electronics and Energy Announcement**
- **Elsevier Forensic Science International: Digital Investigation (Digital Investigation)**
- **Elsevier Internet of Things and Cyber-Physical Systems (IOTCPS)**
- **Elsevier Journal of Information Security and Applications (JISA)**
- **Elsevier Journal of Systems Software (JSS)**
- **Elsevier Machine Learning With Applications (MLWA)**
- **Elsevier Microprocessors and Microsystems**
- **EURASIP Journal on Wireless Communications and Networking**
- **IEEE Communications**
- **IEEE Consumer Electronics Magazine (CEMag)**
- **IEEE Internet Computing (IC)**
- **IEEE Internet of Things Journal**
- **IEEE Journal of Radio Frequency Identification (JRFID)**
- **IEEE Open Journal of the Computer Society (OJCS)**
- **IEEE Security and Privacy Magazine**
- **IEEE Transactions on Artificial Intelligence (TAI)**
- **IEEE Transactions on Consumer Electronics (TCE)**
- **IEEE Transacations on Computational Social Systems (TCSS)**
- **IEEE Transactions on Cybernetics (CYB)**
- **IEEE Transactions on Dependable and Secure Computing (TDSC)**
- **IEEE Transactions on Emerging Topics in Computing (TETC)**
- **IEEE Transactions on Information Forensics and Security (TIFS)**
- **IEEE Transactions on Machine Learning in Communications and Networking (TMLCN)**
- **IEEE Transactions on Mobile Computing (TMC)**
- **IEEE Transactions on Network Science and Engineering (TNSE)**
- **IEEE Transactions on Network and Service Management (TNSM)**
- **IEEE Transactions on Reliability (TR)**
- **IEEE Transactions on Service Computing (TSC)**
- **IEEE Transactions on Software Engineering (TSE)**
- **IOS Press Journal of Intelligent & Fuzzy Systems (IFS)**
- **PLOS One (PONE).**
- **Springer Artificial Intelligence Review**
- **Springer Cluster Computing**
- **Springer Computing**
- **Springer International Journal of Information Security**
- **Springer Journal of Computer Virology and Hacking Techniques (JCVHT)**
- **Springer Journal of Intelligent Information Systems (JIIS).**
- **Springer Knowledge and Information Systems**
- **Springer Scientific Reports**
- **Springer The Journal of SuperComputing**
- **Springer World Wide Web**
- **Taylor and Francis' Network: Computation in Neural Systems (TNET)**
- **Taylor and Francis' Deviant Behavior (UDBH)**
- **Wiley Concurrency and Computation: Practice and Experience**
- **Wiley Expert Systems**
- **Wiley Journal of Software: Evolution and Process**
- **Wiley Journal of Software: Practice and Experience**
- **Wiley Security and Privacy (SPY)**

ACADEMIC COMMUNITY SERVICES AWARDS

Distinguished reviewer for NDSS 2024
Noteworthy reviewer for RAID 2023
Top Reviewer for ACSAC 2023

PUBLICATION SUMMARY

- **17 papers published in international journals**
  - **Springer Journal in Computer Virology: 4**
  - **ACM Transactions on Privacy and Security (TOPS): 3**
  - **Elsevier Computers and Security: 4**
  - **ACM Digital Threats: Research and Practice (DTRAP): 2**
  - **Elsevier Expert Systems With Applications (ESWA): 2**
  - **ACM Computing Surveys (CSUR): 1**
  - **IEEE Transactions on Dependable and Secure Computing (TDSC): 1**
  - **Elsevier Digital Investigation: 1**
- **16 papers in International conferences**
  - **ACM Reversing and Offensive-oriented Trends Symposium (ROOTS): 3**
  - **Springer Information Security Conference (ISC): 3**
  - **ACM International Symposium on Research in Attacks, Intrusions and Defenses (RAID): 2**
  - **Springer Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA): 1**
  - **ACM Availability, Reliability and Security (ARES): 1**
  - **ACM Conference on Code Generation and Optimization (CGO): 1**
  - **ACM Memory Systems (MEMSYS): 1**
  - **IEEE Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC): 1**
  - **USENIX Security: 1**
  - **The International Conference on Security and Cryptography (SECRYPT): 1**
  - **Workshop on Offensive Technologies (WOOT): 1**
- **12 papers in Brazilian conferences (SBSeg).**
- **2 book chapters (in Portuguese).**

SELECTED PUBLICATIONS

Research on Brazilian Malware

"*One Size Does Not Fit All: A Longitudinal Analysis of Brazilian Financial Malware*" - ACM TOPS 2021 - `https://dl.acm.org/doi/10.1145/3429741`

· **"*The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study*" - ACM ARES 2019 -** `https://dl.acm.org/doi/10.1145/3339252.3340103`

Research on Malware Research Methods

"*Why do we need a theory of maliciousness*" - Springer Information Security Conference (ISC) 2022 - `https://link.springer.com/chapter/10.1007/978-3-031-22390-7_22`

"*Challenges and pitfalls in malware research*" - **ELSEVIER Computers & Security 2021 -** https://www.sciencedirect.com/science/article/pii/S0167404821001115

"*We need to talk about antiviruses: challenges & pitfalls of AV evaluations*" - **ELSEVIER Computers & Security 2020 -** https://www.sciencedirect.com/science/article/pii/S0167404820301310

"*Understanding uses and misuses of similarity hashing functions for malware detection and family clustering in actual scenarios*" - **ELSEVIER Digital Investigation 2021 -** https://www.sciencedirect.com/science/article/abs/pii/S266628172100

Research on Sandbox Development

"*The other guys: automated analysis of marginalized malware*", **Springer Journal of Computer Virology and Hacking Techniques 2018 -** https://link.springer.com/article/10.1007/s11416-017-0292-8

"*Enhancing Branch Monitoring for Security Purposes: From Control Flow Integrity to Malware Analysis and Debugging*" - **ACM Transactions on Privacy and Security 2018 -** https://dl.acm.org/doi/10.1145/3152162

Research on Hardware-Assisted Security

"*Who Watches the Watchmen: A Security-focused Review on Current State-of-the-art Techniques, Tools, and Methods for Systems and Binary Analysis on Modern Platforms*". **ACM Computing Surveys (2018)**

"*Near-Memory In-Memory Detection of Fileless Malware*" - **ACM MEMSYS 2020 -** https://dl.acm.org/doi/10.1145/3422575.3422775

Research on Applied Security

"*Dissecting Applications Uninstallers and Removers: Are They Effective?*" **- Springer Information Security Conference (ISC) 2022 -** https://link.springer.com/chapter/10.1007/978-3-031-22390-7_20

"*On the Security of Application Installers and Online Software Repositories*" - **DIMVA 2020 -** https://link.springer.com/chapter/10.1007/978-3-030-52683-2_10

Research on Antivirus Internals

"*AntiViruses under the microscope: A hands-on perspective*" - **Elsevier Computers & Security 2021 -** https://www.sciencedirect.com/science/article/pii/S0167404821003242

Research on Code Obfuscation

"*A Game-Based Framework to Compare Program Classifiers and Evaders*" - **ACM CGO 2023 -** https://dl.acm.org/doi/10.1145/3579990.3580012