

Andrea Mambretti

IBM Research Europe
Systems Security

Phone USA: +1 (617)-372-7293

Phone CH: +41 77 926 32 67

Address:

Säumerstrasse 4, 8803
Rüschlikon, Switzerland



Work Email: amb@zurich.ibm.com

Personal Email: 55aa@mbr.sh

URL: <https://mbr.sh>

Twitter: [@m4mbr3](https://twitter.com/m4mbr3)

GitHub: [m4mbr3@github](https://github.com/m4mbr3)

Linkedin: [m4mbr3@linkedin](https://www.linkedin.com/in/m4mbr3)

Born: November 7, 1989—Como, Italy

Nationality: Italian

Synopsis

I am a systems security researcher at IBM Research Europe, in the [Zurich Laboratory](#). I hold a PhD in Cybersecurity from [Northeastern University](#) in Boston where I worked in the [SecLab](#) under the supervision of [Engin Kirda](#).

Previously, I worked and studied at [Politecnico di Milano](#) where I got my Bachelor and Master degrees in Computer Engineering. During this period, I spent most of my time in the [NECST research laboratory](#) with professors [Stefano Zanero](#), [Federico Maggi](#) and [Marco Domenico Santambrogio](#).

My main research interests are in systems and hardware security with special focus on kernel exploitation and transient execution attacks.

In the past years, I took part in many CTF competitions (such as ruCTF, ICTF and DEFCON) as member of both “Tower of Hanoi” and “[Shellphish](#)” hacking teams.

Education

2015-2022 **Ph.D.** in Cybersecurity, [Northeastern University](#)

THESIS: *Execution Security in the Spectre Era*

ADVISOR: [Prof. Engin Kirda](#)

COMMITTEE MEMBERS:

[Prof. Guevara Noubir](#), [Northeastern University](#)

[Prof. Aanjhan Ranganathan](#), [Northeastern University](#)

[Dr. Alessandro Sorniotti](#), [IBM Research Europe - Zurich](#)

[Dr. Anil Kurmus](#), [IBM Research Europe - Zurich](#)

[Prof. Vasileios P. Kemerlis](#), [Brown University](#)

2015-2018 **MASTER OF SCIENCE** in Cybersecurity, [Northeastern University](#)

2011-2014 **MASTER OF SCIENCE** in Computer Science Engineering, [Politecnico di Milano](#)

GRADE: 101/110

THESIS: *PRIVMUL: PRIVilege separation for Multi-User Logic applications*

ADVISOR: [Prof. Federico Maggi](#)
CO-ADVISOR: [Prof. William Robertson, Northeastern University](#)
CO-ADVISOR: [Prof. Stefano Zanero](#)

2008-2011 **BACHELOR** in Computer Science Engineering, [Politecnico di Milano](#)

2003-2008 **DIPLOMA** in Computer Science, [ITIS Badoni](#)

Areas of specialization

Systems Security - Operating Systems - Distributed Systems - Compilers

Programming Languages

C/C++, Assembly (x86 32/64bit), Python, Rust, Bash, Java, Erlang.

Languages

Italian	Mother tongue
English	TOEFL 2015 - 96/120
Greek	Basic

Work Experience

Apr 2021-
now **IBM RESEARCH - ZURICH**
Research Staff Member in Security and Privacy Department

May 2019-
Apr 2020 **IBM RESEARCH - ZURICH**
Security Researcher Intern in Security and Privacy Department

Feb-Jun 2018 **IBM RESEARCH - ZURICH**
Security Researcher Intern in Cloud and Computing Infrastructure Department

Feb 2014 **SECURE NETWORK S.R.L.**
Security Consultant

Publications & talks

CONFERENCE PUBLICATIONS

Cross-Cache Attacks for the Linux Kernel via PCP Messaging

C. Migliorelli, A. Mambretti, A. Sorniotti, V. Zaccaria, A. Kurmus

In Proceedings of the Network and Distributed System Security (NDSS) Symposium, San Diego, California, USA, February 2026

SoK: Automating Kernel Vulnerability Discovery and Exploit Generation

A. Kurmus, A. Mambretti, A. Sorniotti, V. Lenders, D. Pfammatter, B. Tellenbach

In Proceedings of the 19th USENIX WOOT Conference on Offensive Technologies, Seattle, WA,

USA, August 2025

GhostRace: Exploiting and Mitigating Speculative Race Conditions

H. Ragab, A. Mambretti, A. Kurmus, C. Giuffrida

In Proceedings of the 33rd Usenix Security Symposium (Usenix Security), Philadelphia, Pennsylvania, USA, August 2024

Bypassing memory safety mechanisms through speculative control flow hijacks

A. Mambretti, A. Sandulescu, A. Sorniotti, W. Robertson, E. Kirda, A. Kurmus

In Proceedings of the 6th IEEE European Symposium on Security and Privacy (IEEE EuroSP), Vienna, Austria, September 2021

GhostBuster: understanding and overcoming the pitfalls of transient execution vulnerability checkers

A. Mambretti, P. Convertini, A. Sorniotti, A. Sandulescu, E. Kirda, A. Kurmus

In Proceedings of the 28th IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), Honolulu, Hawaii, USA, March 2021

HotFuzz: Discovering Algorithmic Denial-of-Service Vulnerabilities Through Guided Micro-Fuzzing

W. Blair, A. Mambretti, S. Arshad, M. Weissbacher, W. Robertson, E. Kirda, M. Egele

In Proceedings of the Network and Distributed System Security (NDSS) Symposium, San Diego, California, USA, February 2020

Speculator: A Tool to Analyze Speculative Execution Attacks and Mitigations

A. Mambretti, M. Neugschwandtner, A. Sorniotti, E. Kirda, W. Robertson, A. Kurmus

In Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC), San Juan, Puerto Rico, December 2019

Education Game Design: An Empirical Study of the Effects of Narrative.

C. Jemmali, S. Bunian, A. Mambretti, M. Seif El-Nasr

In Proceedings of the 13th International Conference on the Foundations of Digital Games (FDG). Malmo, Sweden, August 2018

Trellis: Privilege Separation for Multi-User Applications Made Easy.

A. Mambretti, K. Onarlioglu, C. Mulliner, W. Robertson, E. Kirda, F. Maggi, S. Zanero

In Proceedings of the International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), Paris, France, September 2016

LAVA: Large-scale Automated Vulnerability Addition.

B. Dolan-Gavitt, P. Hulin, E. Kirda, T. Leek, A. Mambretti, W. Robertson, F. Ulrich, R. Whelan

In Proceedings of the IEEE Symposium on Security and Privacy (Oakland). San Jose, California, USA, May 2016

WORKSHOP PUBLICATIONS

Two methods for exploiting speculative control flow hijacks

A. Mambretti, A. Sandulescu, M. Neugschwandtner, A. Sorniotti, A. Kurmus

In Proceedings of the 13th USENIX Workshop on Offensive Technologies (WOOT). Santa Clara, California, USA, August 2019

DISSERTATIONS

PRIVMUL: PRIVilege separation for Multi-user Logic applications

Master Thesis, Politecnico di Milano, Milano, Italy, December 2014

Execution Security in the Spectre era

PhD Thesis, Northeastern University, Boston (MA), USA, January 2022

REFeree SERVICE

2027	The Network and Distributed System Security Symposium (NDSS)
2026	23rd Annual International Conference on Privacy, Security and Trust (PST)
2026	Annual Computer Security Applications Conference (ACSAC)
2026	29th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID)
2026	Conference on Detection of Intrusions and Malware & Assessment (DIMVA)
2026	19th European Workshop on Systems Security (EUROSEC)
2026	The ACM Conference on Computer and Communications Security (CSS)
2026	The Network and Distributed System Security Symposium (NDSS)
2025	Annual Computer Security Applications Conference (ACSAC)
2025	28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
2025	Conference on Detection of Intrusions and Malware & Assessment (DIMVA)
2025	18th European Workshop on Systems Security (EUROSEC)
2024	27th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
2024	Annual Computer Security Applications Conference (ACSAC)
2024	17th European Workshop on Systems Security (EUROSEC)
2024	Conference on Detection of Intrusions and Malware & Assessment (DIMVA)
2023	Conference on Computer and Communications Security (CCS)
2023	Annual Computer Security Applications Conference (ACSAC)
2023	16th European Workshop on Systems Security (EUROSEC)
2022	IEEE Workshop on Offensive Technologies (WOOT)
2019	IEEE Transaction on Computers
2019	ACM Transactions on Privacy and Security
2018	IEEE Transactions on Computers

SEMINARS & TALKS

2025	Zisc Lunch Seminar , ETH Zurich, “Ghostrace: Exploiting and Mitigating Speculative Race Conditions”
2023	Offensive and Defensive Cybersecurity Course , Politecnico di Milano, “Execution Security in the Spectre Era”
2022	Offensive and Defensive Cybersecurity Course , Politecnico di Milano, “Execution Security in the Spectre Era”
2021	ACSAC , Virtual, “A tutorial on using Speculator for studying and prototyping speculative execution attacks”
2021	Offensive and Defensive Cybersecurity Course , Politecnico di Milano, “Execution Security in the Spectre Era”
2021	PacSec , Virtual, “Defeating stack canaries and memory safety with speculative execution”
2021	Black Hat , Las Vegas, USA, “The dark age of memory corruption mitigation in the spectre era”
2019	PacSec , Tokyo, Japan, “Exploiting speculative control flow hijacks”
2019	Microarchitectural Security Reading Group , EPFL, “Speculator: A Tool to Analyze Speculative Execution Attacks and Mitigations”
2019	Zisc Lunch Seminar , ETH Zurich, “Speculator: Towards speculative execution debugging”
2019	Cybersecurity and Privacy Institute , Northeastern University, “Let’s Not Speculate: Discovering and Analyzing Speculative Execution Attacks”
2016	Security Seminar , Boston University, “Trellis: Privilege Separation for Multi-user Application Made Easy”
2013	MIT Meeting , Massachusetts Institute of Technology, “AndROMeda, Analyzer of Android (custom) ROM in the wild”
2013	Computer Security Course , Politecnico di Milano, “Introduction to assembly & exploiting”
2013	Poul Workshop , Politecnico di Milano, “Reverse engineering applied to Malware Analysis”
2012	NecstSummerWorkShop 1st edition , Goglio di Baceno, “Reverse engineering for fun and profit”

Summer Schools

2013 [SysSec "Reverse Engineering" Summer School, Amsterdam](#)

Grants, honors & awards

2025 Promoted to Staff Research Scientist
2022 IBM A-level accomplishment on Transient Execution Research
2021 IBM Open Source Significant Contributor - Speculator
2019 Black Hat Europe 2019 Student Free Pass
2019 ACSAC Student Conferenship (1000\$)
2018 BlackHat USA 2017 Student Free Pass
2016 USENIX OSDI Student Travel Grant (1145\$)
2016 IEEE Security and Privacy (Oakland) Student Travel Grant (1400\$)

Last updated: May 13, 2026