# Marcos Bajo - h3xduck

(+34) 689 90 99 64 h3xduck.github.io linkedin.com/in/h3xduck/
marcossbajo@gmail.com github.com/h3xduck

## Summary

PhD student at CISPA Helmholtz Center for Information Security (3rd year) under Prof. Christian Rossow. I research offensive low-level software exploitation attack techniques and mitigation bypasses on Linux and Windows. I publish and present my work in top-tier security venues such as USENIX Security (Honorable Mention Award), IEEE S&P and Black Hat USA. I maintain high-impact open-source projects like TripleCross ( 2k GitHub stars).

## Education

**PhD in Cybersecurity** **September 2023 – Present**
*CISPA Helmholtz Center for Information Security* *Dortmund, Germany*
- Systems Security Group, supervised by Prof. Dr. Christian Rossow.
- Research on offensive low-level software exploitation techniques, including Control Flow Integrity bypasses.

**MSc in Cybersecurity** **September 2022 – July 2023**
*University Carlos III of Madrid - Average grade: 8.81, Thesis grade: 10, Honours Award* *Madrid, Spain*
- English program, 90% of subjects taught in English.
- Honours awardee for my master's thesis about a novel malware analysis tool for protocol reverse engineering.

**BSc in Computer Science and Engineering** **September 2018 – July 2022**
*University Carlos III of Madrid - Average grade: 8.42, Thesis grade: 10, Honours Award* *Madrid, Spain*
- Full English program, every subject taught in English.
- 7 times Honours awardee, including on my bachelor's thesis about a novel type of malware using eBPF in Linux systems.

## Experience

**Researcher, Teaching Assistant** **September 2023 – Present**
*Technical University of Dortmund* *Dortmund, Germany*
- Systems/software security researcher, focused on attack techniques for exploiting vulnerabilities that bypass state-of-the-art defenses. Teaching assistant for the MSc-level Software Security course at TU Dortmund.

**Cybersecurity researcher** **September 2022 – May 2023**
*University Carlos III of Madrid — Computer Security Lab (COSEC)* *Madrid, Spain*
- Research and implementation of advanced malware analysis techniques: taint analysis, binary instrumentation with Intel Pin, other reversing techniques. Study of anti-debugging systems and binary obfuscation.

## Publications

**Crashing Through Defenses: Exploiting Segfaults and Chaining around Intel CET** **May 2026**
*Marcos Bajo, Ritvik Goyal, Apostolos Chatzianagnostou, Christian Rossow* *IEEE S&P 2026*
- Novel software exploitation attack (Segmentation Fault-Oriented Programming) that bypasses state-of-the-art defenses like Intel CET, affects every Linux system. Discovery of novel weaknesses in the Linux kernel handling of signals.

**PLATYPUS: Restricting Cross-Module Transitions to Mitigate Code-Reuse Attacks** **May 2026**
*Apostolos Chatzianagnostou, Marcos Bajo, Christian Rossow* *IEEE S&P 2026*
- Novel software exploitation defense that thwarts code reuse attacks by enforcing execution jails.

**Await() a Second: Evading Control Flow Integrity by Hijacking C++ Coroutines** **August 2025**
*Marcos Bajo, Christian Rossow* *USENIX Security 2025*
- Honorary Mention Award (Top 6% between the accepted papers).
- Novel software exploitation attack technique (Coroutine-Frame Oriented Programming) to bypass Control Flow Integrity (CFI) defenses by abusing C++20 coroutines in Linux and Windows. Attackers can execute arbitrary code despite state-of-the-art CFI protections such as Intel CET, LLVM CFI or Microsoft Control Flow Guard (CFG).

## Talks and Conferences

**RootedCON Madrid 2026** | *Binary Exploitation in the Control Flow Integrity Era* **March 2026**
- Spain's largest cybersecurity congress, in front of around 1000 people. *Madrid, Spain*

**Black Hat USA 2025** | *Breaking Control Flow Integrity by Abusing Modern C++* **August 2025**
- One of world's most prestigious cybersecurity conferences, with more than 20,000 attendees. *Las Vegas, NV, USA*

**RootedCON Madrid 2023** | *TripleCross: A Linux eBPF rootkit* **March 2023**
- Spain's largest cybersecurity congress, in front of around 1000 people. *Madrid, Spain*

**eBPF Summit 2022** | *Analysis of offensive capabilities of eBPF* **September 2022**
- Largest online annual conference about the eBPF technology. *Online*

## Security Disclosures

**Coroutine-Frame Oriented Programming attack** **January 2025**

*Microsoft Security Response Center* *Publicly Acknowledged*

- I collaborated with the MSRC team to fix the vulnerabilities in the MSVC-compiled C++ coroutine implementation and mitigate my published Coroutine-Frame Oriented Programming attack. Acknowledgement public.

**Segmentation-Fault Oriented Programming attack** **January 2026**

*Linux Kernel Security Team*

- I reported the novel vulnerabilities involving our SFOP research, affecting the Linux kernel. Currently being addressed.

## Notable Projects

**Offensive eBPF – *TripleCross* rootkit** | *C, eBPF, Assembly, Linux Kernel* **October 2021 – June 2022**

*Bachelor's Thesis (1900+ Stars, 240+ Forks on GitHub)* *https://github.com/h3xduck/TripleCross*

- Research about the offensive capabilities of the eBPF technology in Linux systems. Development of a malicious eBPF rootkit featuring novel techniques such as library injection and execution hijacking. Creation of a network backdoor that allows for remote control by an attacker, including obfuscation techniques to avoid detection by firewalls. Incorporation of privilege escalation mechanisms, in addition to persistence and malware stealth techniques.

**Kernel Rootkit for Linux – *Umbra* rootkit** | *C, Linux Kernel, POSIX Sockets* **April 2021 – September 2021**

*Personal Project (130+ Stars on GitHub)* *https://github.com/h3xduck/Umbra*

- Development on my own initiative of a loadable kernel module (LKM) for Linux which opens a network backdoor and allows for complete and remote control (C2) to a malicious party after receiving commands from the network.
- Low-level programming using the kernel API, usage of ftrace and netfilter hooks for privilege escalation, and deep inspection of the network traffic. Development of malware-like user space modules.

**Raw Sockets library - *RawTCP_Lib*** | *C, POSIX Sockets, Valgrind, CMake* **March 2021 – May 2022**

*Personal Project (70+ Stars on GitHub)* *https://github.com/h3xduck/RawTCP_Lib*

- Development on my own initiative of a static low-level library for creating and operating TCP/IP packets, in addition to sending and receiving packets through raw sockets. Creation of a specialized application for network attacks, including spoofing techniques. Prevention of memory leaks using Valgrind.

## Languages

**Spanish**: Native level.
**English**: Fluent. C1 Certificate by Cambridge. Working language for PhD research and teaching.
**German**: B1 level. Currently studying B2 at TU Dortmund while living in Germany.

## Honours & Awards

**USENIX Security Honorary Mention Award**: Top 6% between Accepted Papers at USENIX Security 2025.
**Master Thesis Honours**: Awarded Honours as distinction between MSc theses already graded maximum points.
**Bachelor Thesis Honours**: Awarded Honours as distinction between BSc theses already graded maximum points.

## Courses and Activities

**Independent Research**: Binary exploitation techniques and metamorphic malware. Writer at my cybersecurity blog.
**Public Speaking**: My talks and university lectures are generally very well-regarded. I have attended several workshops at CISPA to improve my public speaking skills.
**Practical Ethical Hacking - TCM Security (25 CEU hours)**: Enumeration, Vulnerability Scanning, Exploitation of common vulnerabilities, Buffer Overflows, Active Directory pentesting, OWASP Top 10, post-exploitation techniques.
**CTF Player**: Ex-member of a CTF team, Top 50 in the world. Favourite personal category: PWN (binary exploitation).

## Technical Skills

**Skills**: Reverse engineering, binary exploitation, vulnerability research, malware analysis, taint analysis
**Tools and technologies I use every day**: GDB, eBPF, Intel PIN, Ghidra, LaTeX, GCC, LLVM
**Languages (proficient)**: C, x86 Assembly, C++
**Other languages with experience**: Python, Java, SQL, JavaScript, C#
**Operating systems**: Linux, Windows, Android