SEBASTIÁN R. CASTRO

INFORMATION SECURITY & AI RESEARCHER

+1 (831) 266 5495

California, USA

srcastrot@gmail.com

in https://www.linkedin.com/in/srcastrot/

https://r4wsec.com/

PROFILE

Ph. D. CS Candidate in Information Security and AI with work experience in vulnerability research, malware analysis and autonomous cyber operations. Published author at top academic and industry conferences. Awarded by U.S. NSA and CYBERCOM direction.

EDUCATION

Ph.D. in Computer Science, University of California, Santa Cruz

September 2021 – Present

Honors: OpenAI Cybergrant, BSOE Dean Fellowship, Regents Fellowship

Master of Science (M.S) in Computer Science, University of California, Santa Cruz

March 2025

(OSEP) Certified Experienced Penetration Tester, Offensive Security

March 2021

B.E. in Systems and Computing, National University of Colombia April 2014

Honors: Full Scholarship - "PAES: Mejores Bachilleres del País"

EXPERIENCE

Graduate Researcher (Ph.D.), University of California

September 2021 – Present. Santa Cruz, CA. USA

- · Introducing Autonomous Cyber Defense research through LLM and DRL multi-agent models for enterprise threat response
- · Pioneering autonomous security research by designing a multi-agent LLM framework for binary analysis/vulnerability detection
- · Extending laboratory's academic production by investigating nation-state malware attacking industrial networks (WinDBG, IDA Pro)

Security Engineer Co-op, Amazon Web Services (AWS)

June 2025 – September 2025. Seattle, WA. USA

- · Secured ~80% AWS global network devices (2.1M+) by developing a configuration validation service (Athena, S3, Lambda, Kinesis)
- · Strengthen AWS's security posture by discovering and mitigating 70+ security issues in production network devices (NetFlow, Syslog)
- · Shaped long-term defenses with 6 clustering-based network security baselines, influencing roadmap decisions at scale

Product Security Office R&D Co-op, AMD Inc.

June 2023 – September 2023. San Diego, CA. USA June 2022 – September 2022. San Diego, CA. USA

- · Prototyped a ransomware protection solution by designing/developing a hardware-based threat detection ML agent (PMCs, C++)
- · Improved SoC security by evaluating 2 *0day* side-channel attacks (KASLR, Spectre-Retbleed JMP2RET) and 1 fault injection (Tesla)
- · Enhanced automated vulnerability research process for *PSP* Firmware by integrating internal fuzzing suite to 3+ chipsets (*Python*)

Senior Security Researcher, Sonatype Inc.

February 2020 – August 2021. Fulton, MD. USA (Rem.)

- · Protected customers' software supply chain by auditing 300+ vulnerabilities in OSS artifacts (Java, JavaScript, Python, .NET, C/C++)
- · Safeguarded users from massive threat campaigns (e.g., CursedGrabber) with the analysis and detection of their malware IOCs
- · Boosted team's research process automation by coding tools and scripts for AWS Cloud data manipulation (Java, Kotlin, Bash)

Technical & Research Lead, CSL Latin America Ltda.

May 2015 – December 2019. Bogotá, Colombia

- · Elevated the security standards of 30+ customer institutions by leading 50+ projects of penetration testing and security assessments
- · Developed tailored exploits for 80+ security flaws found in web applications/services and binary packages (PE, ELF, Android APK)
- · Amplified company's research production by developing 7 innovative security tools for post-exploitation attack vectors (Python)

Information Security Analyst, iQ Outsourcing S.A.S.

July 2013 - February 2015. Bogotá, Colombia

LEADERSHIP AND AWARDS

- · Won Commander's Award for security research contributions. Awarded by NSA/CYBERCOM Director Gen. Nakasone (April 2023)
- · Won 1st place out of 30+ teams at the Cybersecurity & Infrastructure Security Agency (CISA) ICS Competition (March 2022)
- · Won 2nd place out of 100+ teams at the National U.S. Department of Energy Cyberforce Competition CTF (November 2021)
- · Tutor & Advisor of UQBAR: Information Security Research Group (January 2018 Present)
- · Principal Tenor Voice Singer at the most important opera chorus in Colombia: Opera of Colombia Chorus (May 2015 August 2021)

PUBLICATIONS AND CONFERENCES

Author: Castro, S. et al. "Large Language Models are Autonomous Cyber Defenders"

IEEE CAI: Conference on Artificial Intelligence - Adaptive Cyber Defense. Santa Clara, CA. USA.

*Awarded Author: Castro, S. et al. "MaLO: A Multi-agent LLM Framework for Offensive Security" Cyber Recon 25, U.S. Cyber Command. West Point, NY. USA (Hunter Award)

Author: Castro, S. et al. "Ghost in the SAM: Stealthy, Robust, and Privileged Persistence through Invisible Accounts" ACM CCS CheckMATE. Salt Lake City, UT. USA.

Author: Castro, S. et al. "Meta-IDS: Towards Resilient Autonomous Cyber Defense" Cyber Recon 24, U.S. Cyber Command. *Baltimore, MD. USA*.

*Co-author: Salazar, L., Castro, S., et al. "A Tale of Two Industroyers: It was the Season of Darkness" IEEE S&P: Security and Privacy. San Francisco, CA. USA.

- 2023 *Awarded Author: A Sandbox for Understanding Nation-State Malware Attacking the Power Grid Cyber Recon 23, U.S. Cyber Command. *Baltimore*, MD. USA. (Commander's Award, Guardian Award)
- 2022 *Presenter: Suborner: A Windows Bribery for Invisible Persistence

Black Hat USA. Las Vegas, NV. USA

Hack In The Box HITB. Singapore City, Singapore

GrrCon. Grand Rapids, MI. USA

- Trainer: Malware Development & Evasion Techniques with C# and Windows APIs UOBAR. National University of Colombia. Bogotá, Colombia
- 2020 **Book co-author: Castro, S.,** Gonzalez, P., "Empire: Advanced Hacking for the Red Team" Zeroxword. *Madrid, Spain*

Presenter: Windows Tactical Ownage

C0r0n4con. *Madrid, Spain* FluCon. *Madrid, Spain*

- 2019 **Trainer:** Exploit Development for Hackers: Leveraging *x86-64* User-Mode Memory Corruption JCUN. National University of Colombia. *Bogotá, Colombia*
- 2018 *Presenter: RID Hijacking: Maintaining Access on Windows Machines

Black Hat USA. Las Vegas, NV. USA

SEC-T. Stockholm, Sweden Romhack. Rome, Italy

Derbycon 8.0. Louisville, KY. USA

2016 **Presenter & Trainer:** Passwords Auditing with *OSS frameworks* and *Markov Chains* BSides CO. *Bogotá, Colombia*

(ISC)2 Chapter. Bogotá, Colombia

CONTRIBUTIONS

Research - Windows RID Hijacking & Suborner: Publicly released two original attacks (*Black Hat USA*) reliable on all *Windows NT versions*. Reverse-engineered *Windows OS* internals. Developed modules for the *OSS* projects *Metasploit Framework*, *Empire*, *NetExec*.

Book - Empire: Advanced Hacking for the Red Team. 0xword: Published a co-authored book with the most important information security publisher in Spanish. Based on *MITRE ATT&CK* and the *Empire* framework, the text includes state-of-the-art tactics, techniques, and procedures (*TTPs*) for red team/adversary simulation exercises against *Windows/Linux* enterprise environments.

Extra contributions: Developed public exploits for CVE-2017-12635, CVE-2018-7573 for Exploit-DB and Metasploit Framework.