

DAN BORGOGNO

Security Researcher & Security Engineer

@ danborgogno@gmail.com
github.com/danborgogno

+54 9 358 4384 096

Córdoba, Argentina

linkedin.com/in/danborgogno

PROFILE

Principal Security Engineer and internationally recognized security researcher with over 12 years of experience building and securing enterprise systems. Expert in offensive security, cloud architecture, and automated security platforms. Led security programs for fintech and cyber-insurance companies, architected AI-powered vulnerability assessment platforms, and discovered critical vulnerabilities in national critical infrastructure. International speaker at DEF CON (main track) and ekoparty. Specialized in Android security research, reverse engineering, and payment system security.

EXPERIENCE

Freelance Web Developer

Independent, Río Cuarto

⌚ 2010 – Oct 2014

- Dynamic website development: analysis, design, implementation, and testing of websites adapted to customer requirements
- Content management system development

Freelance Security Consultant & Researcher

Independent, Córdoba

⌚ 2013 – Present

- Delivered custom penetration testing, security audits, and exploit development services for enterprise clients across financial, government, and technology sectors
- Recognized expert in Android application security, specializing in dynamic analysis using Frida and advanced reverse engineering techniques
- Discovered critical security vulnerabilities in national critical infrastructure systems including SUBE (national transportation payment system) and DNI Digital Argentino (national digital identity), leading to security improvements
- Conducted security research on Android applications, NFC payment systems, and IoT devices using advanced reverse engineering tools (Ghidra, JADX)

Front-end Developer

Globant, Córdoba

⌚ Oct 2014 – Aug 2015

📍 Software consulting

- JavaScript developer for Southwest Airlines' main website (www.southwest.com), developing single-page applications
- Daily collaboration with U.S. stakeholders in English

Java Developer / SDL Champion

McAfee (Intel Security), Córdoba

⌚ Aug 2015 – Jul 2019

📍 Cybersecurity product division

- Developed core backend components and web UI for McAfee Active Response, a leading enterprise threat detection and response platform
- Served as Security Development Lifecycle (SDL) Champion, establishing secure coding standards and review processes across development teams

- Designed and prototyped advanced post-intrusion detection capabilities and forensic analysis features
- Led global threat-hunting engineering team as Scrum Master, mentoring engineers and driving product development initiatives

Back-end & Cloud Services Developer

MercadoLibre, Córdoba

📅 Feb 2019 – Apr 2020

📍 E-commerce and logistics platform

- Developed high-throughput backend systems (Java & Go) for package lifecycle and logistics operations serving millions of transactions
- Built scalable microservices, REST APIs, and system integrations leveraging distributed data stores (KVS, relational databases) and AWS infrastructure
- Contributed to system reliability improvements and monitoring solutions for critical logistics operations

Security Engineer (Red/Blue Team & Architecture)

NaranjaX, Córdoba

📅 Apr 2020 – Oct 15, 2022

📍 Fintech / Digital Banking

- Led penetration testing and security assessments for critical financial services infrastructure including web applications, mobile apps, and backend APIs
- Collaborated across red and blue teams to enhance threat detection capabilities, reducing mean time to detection and improving security posture
- Architected secure system designs for sensitive financial data handling and implemented defensive security controls
- Established security training programs and delivered workshops to development teams, fostering security-first culture across engineering organization
- Developed automated security tooling for vulnerability scanning, misconfiguration detection, and CI/CD pipeline security integration

Principal Security Engineer / Acting CISO

Latu Seguros, Córdoba

📅 Oct 2022 – Aug 2025

📍 Cyber-insurance startup

- Architected and led all security initiatives as sole security leader, establishing comprehensive security program from ground zero
- Built enterprise-grade AWS security (IAM, Cognito, GuardDuty, CloudWatch, Config, S3, VPC) and deployed CrowdStrike EDR with zero security incidents
- Performed security code reviews and penetration testing across all production systems
- Architected and developed AI-powered automated attack-surface assessment platform: distributed orchestration system managing multiple security tools (Nmap, Nuclei, Burp Suite), automated security assessments (attack surface discovery, vulnerability detection, web service analysis, email security), integrated Anthropic Claude LLM with custom agentic framework for iterative security analysis, and developed proprietary scoring algorithms
- Led security assessments for enterprise clients (code audits, cloud reviews, IPA validation) and executed manual penetration tests for major financial institutions, identifying critical vulnerabilities

SECURITY RESEARCH & TALKS

- **DEF CON (Main Track, 2024)** — "Invisible Transactions: Hacking Screenless Bluetooth POS Devices" (co-presented with Ileana Barrionuevo). Groundbreaking research on mobile POS vulnerabilities, significantly impacting understanding of IoT, NFC, and EMV payment system security
- **Ekoparty Security Conference, 2020** — "Hacking the Digital DNI" (Best Talk Award). Comprehensive security research on Argentina's national digital identity system, leading to security enhancements

- **Ekoparty Security Conference, 2019** — "Free rides! SUBE, REDBUS, SATBUS and others" (Best Talk Award). Pioneering research revealing critical vulnerabilities in national public transportation payment systems
- Expert in Android application security auditing using Frida, with proven track record of discovering vulnerabilities in high-security applications including national identity and payment systems
- Research expertise spans Android Security (Frida, reverse engineering), IoT Security, NFC & EMV Payments, Payment Systems, and Bluetooth Security protocols

TECHNICAL SKILLS

Offensive Security

Penetration Testing

Reverse Engineering

Cloud Security

Android Security

Web Security

Secure Architecture

Languages: Go, Java, Python, Kotlin, Ruby, C/C++, Assembly (x86/x64, ARM), JavaScript/TypeScript, Bash, SQL

Cloud & Infrastructure: AWS (IAM, Cognito, CloudWatch, GuardDuty, Config, Lambda, EC2, S3, VPC, CloudTrail), Docker, Kubernetes, Terraform, CI/CD pipelines

Offensive Security Tools: Burp Suite Professional, Nmap, Metasploit Framework, Nuclei, SQLMap, GraphQL security testing, Wireshark, Hashcat, John the Ripper, Hydra, Aircrack-ng suite

Reverse Engineering & Mobile: Frida (expert), Ghidra, IDA Pro, JADX, APKtool, Objection, MobSF, Radare2, GDB/LLDB

Payment Systems & IoT: NFC security analysis, Bluetooth/BLE protocol analysis, EMV chip card security, POS device assessment, embedded systems security

Defensive Security: CrowdStrike Falcon EDR, ELK Stack (Elasticsearch, Logstash, Kibana), AWS GuardDuty, CloudWatch, Google Workspace administration, SIEM integration

Methodologies: OSCP-level penetration testing, OWASP Top 10/Mobile/API, PTES, threat modeling (STRIDE, DREAD), secure SDLC, red/blue/purple team exercises, incident response

EDUCATION

National University of Río Cuarto, Córdoba

Computer Science / Systems Analyst

⌚ 2008 – 2014

📍 GPA 7.3/10

AWARDS & RECOGNITION

- **Best Talk Award — Ekoparty 2019:** "Free rides! SUBE, REDBUS, SATBUS and others"
- **Best Talk Award — Ekoparty 2020:** "Hacking the Digital DNI"
- **DEF CON Main Track Speaker — 2024:** Selected for premier security conference main track

LANGUAGES

Spanish (Native)

English (Advanced / Professional)