Jacopo Corbetta

jacopo.corbetta@gmail.com
jacopo.cc | jacopo | jacopocorbetta

I like defense-in-depth and programs that behave as we intend them to – and I don't disdain tricks to get there, binary or network as they may be.

Profile

- Currently part of Qualcomm's Product Security team. I was previously in the CISO R&D team of Philips.
- Former Graduate Student Researcher at the UCSB Computer Security Lab.
- Hacked with CTF team Shellphish all the way to DEF CON and the third place at the DARPA Cyber Grand Challenge (first place self-funded, and we published and open-sourced our system). Later, I helped organize *the* DEF CON CTF with the Order of the Overflow.
- Moonlighted for years as system and network administrator.

Research Work

web **Are We Using the Crypto We Want? TLS Cipher-Suite Negotiation and its Discontents**
Jacopo Corbetta, Christopher Kruegel, Giovanni Vigna; this was my master thesis
Study on how HTTPS cipher preferences are used in practice, both by security-conscious system administrators and by browsers, and how even best intentions can bring surprises (and lower security!).

binary **Driller: Augmenting Fuzzing Through Selective Symbolic Execution**
Nick Stephens, John Grosen, Christopher Salls, Andrew Dutcher, Ruoyu Wang, Jacopo Corbetta, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna; published at the 2016 Network & Distributed System Security Symposium (NDSS)
Part of our effort towards auto-exploitation for the DARPA Cyber Grand Challenge finals. Driller automatically complements fuzzing with symbolic execution, using the strengths of both, to allow deep (and fast!) exploration of binaries.

mobile **What the App is That? Deception and Countermeasures in the Android User Interface**
Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, Yanick Fratantonio, Christopher Kruegel, Giovanni Vigna; published at the 2015 IEEE Symposium on Security and Privacy (S&P)
Android opens the door to new and powerful GUI attacks on users, as demonstrated by our attack system and its performance in the user study. We implemented two defenses: market-level (static analysis), and device-level (UI information).

web **Eyes of a Human, Eyes of a Program: Leveraging different views of the web for analysis and detection**
Jacopo Corbetta, Luca Invernizzi, Christopher Kruegel, Giovanni Vigna; published at the 2014 International Symposium on Research in Attacks, Intrusions and Defense (RAID)
Fraudsters sometimes try to evade static web page analysis with obfuscation tricks: this tool catches them precisely because they do that.

binary **Transparent and Efficient Instrumentation and Debugging of 32-bit Binaries**
Joint thesis with Alessandro Pignotti; our Diploma di Licenza at Sant'Anna School of Advanced Studies
Dynamic Binary Translators (e.g., Valgrind) often suffer from bad performance due to register or memory pressure. Our prototype runs 32-bit Windows binaries into 64-bit processes, leveraging the strong similarity of the two architectures but leaving the extended space free for analysis and translation needs.

education **Ten Years of iCTF: The Good, The Bad, and The Ugly**
Giovanni Vigna, Kevin Borgolte, Jacopo Corbetta, Adam Doupé, Yanick Fratantonio, Luca Invernizzi, Dhilung Kirat, Yan Shoshitaishvili; published at the 2014 USENIX 3GSE Summit
Part of the organization of our attack-defense CTF (iCTF). Presents our solutions to the many challenges of running live security competitions, and our internal framework.

Projects

binary Worked on the AFL-based **coverage-guided fuzzer that led us to qualify for the DARPA CGC** (automated exploitation and patching with no human involvement) finals, and cooperated in the subsequent Driller project and CGC finals. Gave a **talk on this at the 32C3 Computer Chaos Club (CCC)** congress. We open-sourced our system, mechaphish, and detailed it and our experience in various conferences, on the **IEEE Security & Privacy Magazine**, and **on Phrack**.

Qualcomm At **Qualcomm**, I am working in mobile, automotive, and IoT security: fuzzing network stacks, reviewing Android components, system designs, Wi-Fi attack/defense, ... I presented my fuzzing results at the Xiaomi's Developer Summit in Beijing (MIDC 2019) and at the 2020 NDSS Binary Analysis Research workshop (invited speaker).

binary In 2019 and 2020 I served in the program committee of the Binary Analysis Research (BAR) workshop, associated to the Network and Distributed System Security Symposium (NDSS) conference.

binary Played in many security competitions (**CTFs**) with the Shellphish team, including the DEFCON CTF finals, and the related network defense and infrastructure. Developed a couple of experimental tools, like an injector of C code into statically-linked binaries. I then helped organize the DEF CON CTF in the Order of the Overflow, including maintaining the infrastructure and the playable archive using Docker, AWS, Kubernetes, Django, and custom continuous integration.

admin **System and network administrator** under many hats – even for UCSB's security lab itself – beside doing it as part-time work while an undergraduate student. At UCSB, this included managing 100+ servers in parallel, and containing possibly-malicious software via an assortment of network rules and system hardening.

Philips At **Philips**, I implemented network security measures, including new monitoring solutions, guided hardening, conducted pentesting and redteaming, and assisted in automated fuzzing. Contact privately for more information.

web When Chrome introduced extensions, coded a very popular (50,000+ users) minimalistic GMail integration.

web MeanEditor, a WYSIWIM (What You See Is What You Mean) **visual editor** for MediaWiki. It was one of the editors considered by the Wikipedia Usability initiative.

net Member of the pESApod team that participated in the European Space Agency *Lunar Robotic Challenge*, helping mainly on the network and software part for our hexapod robot.

binary Experimented with defense-in-depth within the same process ("high-interaction" program compartmentalization). The prototype split trusted and untrusted object files, and used seccomp and x86 segments for fast enforcement.

Tools of the Trade

Code *Proficient:* C, Python.
I also know: x86/x64 assembly, C++, HTML/JavaScript.
I have used: Java, Ruby, C#, Rust.

Tools Dynamic binary translation, virtualization, gdb, nasm, QEMU, AFL, IDA Pro, testing, git, bash, ...

Education

2011-2016 **Graduate Student Researcher/M.Sc. in the Computer Security Group**
Computer Science Department, University of California, Santa Barbara, USA

advisors Professor Christopher Kruegel, Professor Giovanni Vigna

2011 **M.Sc. in Computer Engineering**
Information Engineering Department, University of Pisa, Italy

thesis *Inner-Eye: Appearance-based Detection of Computer Scams*

supervisors Professor Beatrice Lazzerini, Professor Giovanni Frosini, Professor Giovanni Vigna, Professor Christopher Kruegel

Detection of typical computer scams, utilizing imaging and text-matching techniques for robustness.

2010 **Diploma di Licenza**
Information Engineering Sector, Sant'Anna School of Advanced Studies, Italy
Full Scholarship as Allievo Ordinario

thesis *Transparent and Efficient Instrumentation and Debugging of 32-bit Binaries*

supervisors Professor Giovanni Vigna, Professor Christopher Kruegel

Sant'Anna School of Advanced Studies is a government-established institution that complements university studies with additional courses and research opportunities.

2009 **B.Sc. in Computer Science**
Information Engineering Department, University of Pisa, Italy

thesis *Design and Implementation of a Neural Network Architecture Based on Receptive Fields*

supervisors Professor Beatrice Lazzerini, Professor Francesco Marcelloni

Worked on a system using conditional fuzzy clustering. Analyzed its poor performance on some datasets, identified the weakness that caused the problem, and used a simple heuristic to reduce its impact.