Yanick Fratantonio

Senior Security Researcher
Cisco Talos

✉ *yanick@fratantonio.me*
reyammer.io
@reyammer

I work on **systems security and privacy**, and my research expertise covers a wide range of aspects, such as mobile security, reverse engineering, malware analysis, binary analysis, and web security. My research has highlighted systemic flaws in many aspects of mobile devices and developed program analysis techniques to analyze Android, Windows, and Linux malware. I have published 35+ peer-reviewed papers (3100+ citations) and I have been a speaker at top-tier industry and academic conferences, such as Black Hat USA, IEEE S&P.

Professional Experience

2020–current **Senior Security Researcher at Cisco Talos**
- Member of the Malware Research Team

2017–2020 **Assistant Professor at EURECOM**
- Co-authored 35+ peer-reviewed papers (H-index: 25, 3100+ citations), 22 of which in top-tier conferences in systems security, privacy, and software engineering
- Speaker at several top-tier academic and industry systems security conferences
- DARPA CHESS grant on human-assisted binary analysis tools (Co-PI, Eurecom portion: ∼1M EUR)
- Research Impact:
  - New phishing attacks on mobile password managers (Keeper, LastPass, etc.)
  - New systemic clickjacking attacks on all modern Android apps
  - First survey on Linux malware
- Developed MOBISEC, the first open-access course on mobile security:
  - Material: `https://mobisec.reyammer.io/`
  - APK analysis pipeline: `https://mobisec.reyammer.io/analysis`
  - Challenges on app dev, reversing, and exploitation: `https://challs.reyammer.io`
- Hackademic advisor of EURECOM's NOPS hacking group

2020 **Visiting Assistant Professor at TU Wien**
- Visited the systems security group at TU Wien for a short 6-month sabatical

2018–2021 **DEFCON CTF Organizer**
- Member of the Order Of the Overflow (OOO), the (now-retired) DEFCON CTF organizers
- I have designed and developed challenges for various categories, ranging from reverse engineering, to shellcoding, exploitation, and cryptography
- See some of my challenges at: `https://reyammer.io/tags/defcon/`

2011–2017 **Ph.D. University of California Santa Barbara**

- Earned a Ph.D. with a thesis on mobile systems security
- Research Impact: My research has highlighted systemic flaws in many aspects of mobile devices, including Graphic User Interfaces, bootloaders, hardware memory modules, cryptography, dynamic code loading, authentication, and fingerprint API
- "Distinguish Practical Paper" Award at IEEE Security and Privacy for Cloak & Dagger
- "Outstanding Student" Award in Computer Science at UC Santa Barbara
- Co-author of Andrubis, a publicly available platform to analyze malicious Android apps. The service (now discontinued) analyzed more than one million Android apps.
- Lead of four-year long DARPA APAC (Automatic Program Analysis for Cybersecurity) program, for which I was in charge of several key aspects of the program, such as writing quarterly progress reports, preparing deliverables, presenting research work at PI meetings, and leading my team's participation to several engagements
- Advised 20+ students and 10+ research projects published in top venues
- Co-organized five editions of UCSB iCTF
- Member of the Shellphish hacking team

2016 **Internship at Georgia Institute of Technology**

- Unveiled several Android UI design shortcomings (clickjacking, phishing, a11y), leading to Cloak & Dagger attacks. More info at `https://cloak-and-dagger.org`

2014 **Internship at Microsoft Research**

- Worked on a Windows crash dump analysis system based on reverse symbolic execution
- Developed a new disassembly framework for x86, implementing various IRs and APIs
- This is now used in production at Microsoft, and *it processes 1M+ crash dumps / day*

2010 **Internship at University of California, Santa Barbara**

- Designed and developed Shellzer, an analysis tool for Windows malicious shellcode
- It has been integrated in Wepawet (a now-discontinued service to analyze drive-by exploits)
- I have been in charge of the design, implementation, infrastructure, and deployment
- It has analyzed 100K+ real-world malicious shellcode over 4 years

2005–2011 **Master of Science & Bachelor of Science**

- MS in Computer Engineering at Politecnico of Milan, 110/110 with laude
- MS in Computer Science at the University of Illinois at Chicago
- BS in Computer Engineering at Politecnico of Milan, 110/110 with laude

Publications (Selection)

For a complete list see `https://reyammer.io/publications/` or my Google Scholar profile at `https://scholar.google.com/citations?user=v9-OixsAAAAJ&hl=en`

- Andrea Possemato, Simone Aonzo, Davide Balzarotti, **Yanick Fratantonio**. Trust, But Verify: A Longitudinal Analysis Of Android OEM Compliance and Customization. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2021.
- **Yanick Fratantonio**, Chenxiong Qian, Pak Chung, Wenke Lee. Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2017.
  Distinguished Practical Paper Award at IEEE Security & Privacy 2017
- Andrea Possemato, **Yanick Fratantonio**. Towards HTTPS Everywhere on Android: We Are Not There Yet. In Proceedings of the USENIX Security Symposium, 2020
- Simone Aonzo, Alessio Merlo, Giulio Tavella, **Yanick Fratantonio**. Phishing Attacks on Modern Android. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2018

- Andrea Possemato, Andrea Lanzi, Pak Chung, Wenke Lee, **Yanick Fratantonio**. ClickShield: Are You Hiding Something? Towards Eradicating Clickjacking on Android. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2018.
  CSAW Europe Applied Research Competition Finalist 2018 and First place at CLUSIT 2018 - Best Italian Computer Security Master Thesis
- Emanuele Cozzi, Mariano Graziano, **Yanick Fratantonio**, Davide Balzarotti. Understanding Linux Malware. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2018

Community Service (Selection)

For a complete list see `https://reyammer.io/service/`

- Technical Program Committee Member for USENIX Security, ACM CCS, WWW, ACSAC, RAID, USENIX WOOT, USENIX Enigma, DIMVA, WiSec, NSS, ICDCS, ESSOS, EUROSEC, MalIOT
- Associate Editor for IET Information Security Journal
- Reviewer for Agence Nationale de la Recherche (ANR), IEEE Security & Privacy

Languages

Italian (Mother tongue)

English (Full professional proficiency)

Serbian (Basic)

German (Basic)