Yanick Fratantonio

PhD Candidate

Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA, USA
93106-5110
✉ *yanick [AT] cs.ucsb.edu*
http://cs.ucsb.edu/~yanick

Research Interests

My research interests span the areas of systems and software security, specifically focusing on *mobile systems security and privacy*. My research aims at developing novel program analysis techniques to characterize and identify evasive hard-to-detect malicious code, detecting and preventing high-impact security vulnerabilities, and performing large-scale studies to assess the practicality of novel security mechanisms when deployed in real-world scenarios.

Education

2011-now **Ph.D. Student in the Computer Security Lab**,
Computer Science Department, University of California, Santa Barbara, USA.
Current GPA: 4.00 out of 4.00

supervisors Professor Christopher Kruegel, Professor Giovanni Vigna

2008-2011 **M.Sc. in Computer Engineering**,
Department of Electronics and Information, Polytechnic of Milan, Italy.
Final grade: 110 *cum laude* out of 110

2009-2011 **M.Sc. in Computer Science**,
University of Illinois at Chicago, USA.

2005-2008 **B.Sc. in Computer Engineering**,
Department of Electronics and Information, Polytechnic of Milan, Italy.
Final grade: 110 *cum laude* out of 110

Research Experience

06/2016 - 09/2016 **Research Intern**, *Georgia Tech*, Atlanta, GA.

06/2014 - 09/2014 **Research Intern**, *Microsoft Research*, Redmond, WA.

09/2011 - present **Research Assistant**, *UC Santa Barbara*, Santa Barbara, CA.

07/2010 - 10/2010 **Visiting Researcher**, *UC Santa Barbara*, Santa Barbara, CA.

Publications

[1] Nilo Redini, Aravind Machiry, Dipanjan Das, **Yanick Fratantonio**, Antonio Bianchi, Eric Gustafson, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna. BootStomp: On the Security of Bootloaders in Mobile Devices. In Proceedings of the USENIX Security Symposium (SEC), 2017

[2] **Yanick Fratantonio**, Chenxiong Qian, Pak Chung, Wenke Lee. Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop. In Black Hat USA, 2017

[3] **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.

[4] Vasilios Mavroudis, Shuang Hao, **Yanick Fratantonio**, Federico Maggi, Giovanni Vigna, Christopher Kruegel. On the Privacy and Security of the Ultrasound Ecosystem. In Proceedings of the Privacy Enhancing Technologies Symposium (PETS), 2017

[5] Andrea Continella, **Yanick Fratantonio**, Martina Lindorfer, Alessandro Puccetti, Ali Zand, Christopher Kruegel, Giovanni Vigna. Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis. In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), 2017

[6] Vasilios Mavroudis, Shuang Hao, **Yanick Fratantonio**, Federico Maggi, Giovanni Vigna, Christopher Kruegel. Talking Behind Your Back: Attacks and Countermeasures of Ultrasonic Cross-device Tracking. In Black Hat Europe, 2016

[7] Victor van der Veen, **Yanick Fratantonio**, Martina Lindorfer, Daniel Gruss, Clementine Maurice, Giovanni Vigna, Herbert Bos, Kaveh Razavi, Cristiano Giuffrida. Drammer: Deterministic Rowhammer Attacks on Mobile Platforms. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2016

[8] **Yanick Fratantonio**, Antonio Bianchi, William Robertson, Engin Kirda, Christopher Kruegel, Giovanni Vigna. TriggerScope: Towards Detecting Logic Bombs in Android Apps. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2016

[9] Weidong Cui, Marcus Peinado, Sang Kil Cha, **Yanick Fratantonio**, Vasileios Kemerlis. RETracer: Triaging Crashes by Reverse Execution from Partial Memory Dumps. In Proceedings of the International Conference on Software Engineering (ICSE), 2016

[10] Vitor Afonso, Antonio Bianchi, **Yanick Fratantonio**, Adam Doupe, Mario Polino, Paulo de Geus, Christopher Kruegel, Giovanni Vigna. Going Native: Using a Large-Scale Analysis of Android Apps to Create a Practical Native-Code Sandboxing Policy. In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), 2016

[11] Luca Falsina, **Yanick Fratantonio**, Stefano Zanero, Christopher Kruegel, Giovanni Vigna, Federico Maggi. Grab'n Run: Secure and Practical Dynamic Code Loading for Android Applications. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2015

[12] Simone Mutti, **Yanick Fratantonio**, Antonio Bianchi, Luca Invernizzi, Jacopo Corbetta, Dhilung Kirat, Christopher Kruegel, Giovanni Vigna. BareDroid: Large-Scale Analysis of Android Apps on Real Devices. In Proceedings of the Annual Computer Security Applications Conference (ACSAC), 2015

[13] Antonio Bianchi, **Yanick Fratantonio**, Christopher Kruegel, Giovanni Vigna. NJAS: Sandboxing Unmodified Applications in non-rooted Devices Running Stock Android. In Proceedings of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), 2015

[14] **Yanick Fratantonio**, Aravind Machiry, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna. CLAPP: Characterizing Loops in Android Applications. In Proceedings of the ACM Symposium on the Foundations of Software Engineering (FSE), 2015. **Best Paper Award at the UCSB Graduate Student Workshop on Computing 2016**.

[15] **Yanick Fratantonio**, Aravind Machiry, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna. CLAPP: Characterizing Loops in Android Applications (Invited Talk). In Proceedings of International Workshop on Software Development Lifecycle for Mobile (DeMobile), 2015

[16] **Yanick Fratantonio**, Antonio Bianchi, William Robertson, Manuel Egele, Christopher Kruegel, Engin Kirda, Giovanni Vigna. On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users. In Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2015

[17] Antonio Bianchi, Jacopo Corbetta, Luca Invernizzi, **Yanick Fratantonio**, Christopher Kruegel, Giovanni Vigna. What the App is That? Deception and Countermeasures in the Android User Interface. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2015

[18] Yinzhi Cao, **Yanick Fratantonio**, Antonio Bianchi, Manuel Egele, Christopher Kruegel, Giovanni Vigna, Yan Chen. EdgeMiner: Automatically Detecting Implicit Control Flow Transitions through the Android Framework. In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), 2015

[19] Martina Lindorfer, Matthias Neugschwandtner, Lukas Weichselbaum, **Yanick Fratantonio**, Victor van der Veen, Christian Platzer. Andrubis - 1,000,000 Apps Later: A View on Current Android Malware Behaviors. In Proceedings of the International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2014

[20] Giovanni Vigna, Kevin Borgolte, Jacopo Corbetta, Adam Doupe, **Yanick Fratantonio**, Luca Invernizzi, Dhilung Kirat, Yan Shoshitaishvili. Ten Years of iCTF: The Good, The Bad, and The Ugly. In Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE), 2014

[21] Lukas Weichselbaum, Matthias Neugschwandtner, Martina Lindorfer, **Yanick Fratantonio**, Victor van der Veen, Christian Platzer. Andrubis: Android Malware Under The Magnifying Glass. In Technical Report TR-ISECLAB-0414-001, 2014

[22] Sebastian Poeplau, **Yanick Fratantonio**, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna. Execute This! Analyzing Unsafe and Malicious Dynamic Code Loading in Android Applications. In Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), 2014

[23] Manuel Egele, David Brumley, **Yanick Fratantonio**, Christopher Kruegel. An Empirical Study of Cryptographic Misuse in Android Applications. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2013

[24] **Yanick Fratantonio**, Christopher Kruegel, Giovanni Vigna. Shellzer: A Tool for the Dynamic Analysis of Malicious Shellcode. In Proceedings of the Symposium on Recent Advances in Intrusion Detection (RAID), 2011

Awards

- Distinguished Practical Paper Award, IEEE Security & Privacy, 2017
- Best Paper Award at the Graduate Student Workshop on Computing, UC Santa Barbara, 2016

- Outstanding Student Award in Computer Science, UC Santa Barbara, 2015
- Best Reviewer Award for the Graduate Student Workshop on Computing (GSWC) 2013
- Best Reviewer Award for the Graduate Student Workshop on Computing (GSWC) 2012
- Student Travel Grant for USENIX Security 2013, IEEE S&P 2013, CCS 2015

University Service

2015 **Organizer of the first CS Student Research Colloquium**, *UC Santa Barbara*.

2013 **Judge for assigning the UCSB Senior Captsone $1000 Best Presentation Award**, *UC Santa Barbara*.

2013-2014 **Graduate Student Representative**, *Computer Science Department, UC Santa Barbara*.

2012-2015 **Program Committee Member of the Graduate Student Workshop on Computing (GSWC)**, *UC Santa Barbara*.

Professional Activities

Program Committee Member, *USENIX Enigma, 2017*.

Program Committee Member, *ACM Workshop on Malicious Software and Hardware in Internet of Things (MALIOT), 2017*.

Program Committee Member, *Tyrrhenian International Workshop on Digital Communications (TIWDC), 2017*.

Reviewer, *IEEE Security & Privacy Journal*.

Reviewer, *Computers & Security (COSE)*.

Reviewer, *ACM Transactions on Privacy and Security (TOPS)*.

Reviewer, *IEEE Transactions on Dependable and Secure Computing (TDSC)*.

Reviewer, *Journal of Information Security and Applications (JISA)*.

Reviewer, *IET Information Security Journal*.

Reviewer, *Future Generation Computer Systems Journal (FGCS)*.

External Reviewer, *Symposium on Network and Distributed System Security (NDSS), 2015, 2016*.

External Reviewer, *ACM Conference on Computer and Communications Security (CCS), 2014*.

Program Committee Member, *USENIX Security Symposium Shadow PC, 2014*.

External Reviewer, *USENIX Security Symposium, 2014, 2015, 2016, 2017*.

External Reviewer, *IEEE Symposium on Security and Privacy (S&P), 2013*.

Program Committee Member, *The Graduate Student Workshop on Computing (GSWC), 2013, 2014, 2015*.

External Reviewer, *The Graduate Student Workshop on Computing (GSWC), 2012*.

Teaching Experience

2015 **Guest Lecture on "Android Hacking" at CS279 Advanced Topics in Computer Security**, *UC Santa Barbara*, Santa Barbara, CA.

2015 **Guest Lecture at CS595 seminar titled "Introduction to Graduate School in Computer Science"**, *UC Santa Barbara*, Santa Barbara, CA.

2011-2015 **International Capture the Flag (iCTF) — Organizer**, *UC Santa Barbara*, Santa Barbara, CA.
Participated in the organization of one of the world's largest educational hacking competition

Talks

06/2017 **Research Seminar: Securing Mobile Devices from Evasive Malware**, *USI Lugano*, Lugano, Switzerland.

05/2017 **Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop**, *IEEE Symposium on Security & Privacy (S&P)*, San Jose, CA.

04/2017 **Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop**, *Georgia Tech Cybersecurity Series*, Atlanta, GA.

05/2016 **TriggerScope: Towards Detecting Logic Bombs in Android Apps**, *IEEE Symposium on Security & Privacy (S&P)*, San Jose, CA.

03/2016 **CLAPP: Characterizing Loops in Android Applications**, *UCSB Graduate Student Workshop on Computing (GSWC)*, Santa Barbara, CA.

09/2015 **CLAPP: Characterizing Loops in Android Applications**, *ACM Symposium on the Foundations of Software Engineering (FSE)*, Bergamo, Italy.

08/2015 **CLAPP: Characterizing Loops in Android Applications (Invited Talk)**, *International Workshop on Software Development Lifecycle for Mobile (DeMobile)*, Bergamo, Italy.

07/2015 **On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users**, *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*, Milan, Italy.

09/2014 **End-of-Internship Talk**, *Microsoft Research*, Redmond, WA.

05/2014 **Security Threats on Mobile: What You & App Developers Can Do About It (Invited Talk)**, *Mobile Santa Barbara Meetup*, Santa Barbara, CA.

01/2014 **EdgeMiner: Automatically Detecting Implicit Control Flow Transitions through the Android Framework**, *DARPA APAC PI Meeting*, San Diego, CA.

07/2013 **ShellNoob: a shellcode writing toolkit**, *Black Hat USA Arsenal 2013*, Las Vegas, NV.

10/2012 **Shellzer: a tool for the dynamic analysis of malicious shellcode**, *UCSB Graduate Student Workshop on Computing (GSWC)*, Santa Barbara, CA.

09/2011 **Shellzer: a tool for the dynamic analysis of malicious shellcode**, *Symposium on Recent Advances in Intrusion Detection (RAID)*, Menlo Park, CA.

Research Tools and Open Source Contributions

Andrubis A publicly-available sandbox to statically and dynamically analyze benign and malicious Android applications.

Shellzer A shellcode analyzer that I developed for my Master thesis. From November 2011, *Shellzer* is the shellcode analyzer used by *Wepawet*, a well known publicly available service for detecting and analyzing web-based threats.

ShellNoob — A toolkit to write shellcode. This tool has been well-accepted by the community, it was recently included in the security-focused Kali Linux distribution. URL: `https://github.com/reyammer/shellnoob`

BareDroid — A system that allows the scalable analysis of Android applications on bare-metal devices. URL: `https://github.com/ucsb-seclab/baredroid`

iCTF Framework — A framework to host attack-defense Capture the Flag competitions. URL: `https://github.com/ucsb-seclab/ictf-framework`

Grab'n Run — A library to make dynamic code loading secure *by design*. URL: `https://github.com/lukeFalsina/Grab-n-Run`

Languages

Mother tongue — Italian

Other languages — English (Full professional proficiency)

Media Coverage

- TechCrunch: Cloak & Dagger is a newly-discovered Android exploit that lets hackers hide malicious activity
- Mashable: A new Android attack with a cool name can wreak havoc on your phone
- The Hacker News: All Android Phones Vulnerable to Extremely Dangerous Full Device Takeover Attack
- WIRED: How to Block the Ultrasonic Signals You Didn't Know Were Tracking You
- Fortune: Inaudible Soundwaves Expose a Spooky New Pathway for Hackers
- SlashDot: Serious Hacks Possible Through Inaudible Ultrasound
- Schneier on Security: Hardware Bit-Flipping Attacks in Practice
- Ars Technica: Using Rowhammer bitflips to root Android phones is now a thing
- WIRED: Elegant Physics (and Some Down and Dirty Linux Tricks) Threaten Android Phones
- SlashDot: Rowhammer Attack Can Now Root Android Devices

Tests

Oct 2010 — GRE Test: 800/800 (Math section)

Hacking Competitions

- Member of the organization team of the iCTF 2011, 2012, 2013, 2014, and 2015
- Member of the Shellphish hacking group (one of the top-ten hacking teams worldwide)
- Finished in 8th position at the DEFCON CTF Quals 2016
- Finished in 9th position at the DEFCON CTF Finals 2015
- Finished in 12th position at the DEFCON CTF Quals 2015
- Finished in 10th position at the DEFCON CTF Quals 2014
- Finished in 7th position at the DEFCON CTF Finals 2013
- Finished in 7th position at the DEFCON CTF Quals 2013
- Leader of the m0j0j0j0 team that finished in 12th position at the iCTF 2011

Artistic Skills

- I have played the piano for eight years
- I have been playing the guitar for ten years

References

Giovanni Vigna
Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106
✉ vigna@cs.ucsb.edu

Christopher Kruegel
Department of Computer Science
University of California, Santa Barbara
Santa Barbara, CA 93106
✉ chris@cs.ucsb.edu

Wenke Lee
Georgia Tech
Atlanta, GA 30332
✉ wenke.lee@gmail.com

Weidong Cui
Microsoft Research
Redmond, WA 98052
✉ wdcui@microsoft.com

Engin Kirda
College of Computer and Information Science
Northeastern University - CCIS
Boston, MA 02115
✉ ek@ccs.neu.edu

William Robertson
College of Computer and Information Science
Northeastern University - CCIS
Boston, MA 02115
✉ wkr@ccs.neu.edu

Updated

July, 2017