

Antonio Bianchi

Assistant Professor

*Department of Computer Science
Purdue University
✉ antoniob@purdue.edu
@anton00b*

Research Interests

My research interest covers the fields of software and system security.

Specifically, my main focus is to study emerging security treats on mobile platforms and develop novel automatic systems to detect and mitigate them. In parallel, I am also doing research in the area of binary program analysis, reverse engineering, binary hardening, and security of embedded and IoT devices.

As a member of the Shellphish and OOO teams, I organized and played countless security-related competitions and won the third place at the DARPA Cyber Grand Challenge.

Research and Professional Experience

- Aug 2019 – now **Assistant Professor**,
Computer Science Department,
Purdue University.
- Aug 2018 – July 2019 **Assistant Professor**,
Computer Science Department,
The University of Iowa.
- Sep 2012 – Jul 2018 **Research Assistant**,
Security Lab — Computer Science Department,
University of California, Santa Barbara.
- Feb 2017 – Jun 2017 **Research Intern**,
Institute for Information Security & Privacy,
Georgia Institute of Technology.
- Aug 2011 – Nov 2011 **Visiting Researcher**,
Security Lab — Computer Science Department,
University of California, Santa Barbara.

Education

- 2012 – 2018 **Ph.D. in Computer Science**,
Security Lab — Computer Science Department,
University of California, Santa Barbara.
GPA: 4.0 out of 4.0
- 2009 – 2012 **M.Sc. in Computer Science**,
University of Illinois at Chicago.
GPA: 3.71 out of 4.0
- 2008 – 2012 **M.Sc. in Computer Engineering**,
Politecnico di Milano, Italy.
Final grade: 110 cum laude out of 110

Research Funding

- Jun 2019 – May 2021 NSF – CRII,
SaTC: Vetting and Improving the Usage of Trusted Execution Environments for Authentication in Mobile Devices,
sole PI, \$174,972
- Dec 2018 – 2022 DARPA – Computers and Humans Exploring Software Security (CHES),
CHECRS: Cognitive Human Enhancements for Cyber Reasoning Systems,
co-PI, share \$880,941

Publications

- Aug 2018 Moritz Eckert, **Antonio Bianchi**, Ruoyu Wang, Yan Shoshitaishvil, Christopher Kruegel, Giovanni Vigna
“HeapHopper: Bringing Bounded Model Checking to Heap Implementation Security”
In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Mar 2018 Yan Shoshitaishvili, **Antonio Bianchi**, Kevin Borgolte, Amat Cama, Jacopo Corbetta, Francesco Disperati, Audrey Dutcher, John Grosen, Paul Grosen, Aravind Machiry, Chris Salls, Nick Stephens, Ruoyu Wang, Giovanni Vigna
“Mechanical Phish: Resilient Autonomous Hacking”
In *IEEE Security & Privacy Magazine – SPSI: Hacking without Humans*
- Feb 2018 **Antonio Bianchi**, Yanick Fratantonio, Aravind Machiry, Christopher Kruegel, Giovanni Vigna, Simon Pak Ho Chung, Wenke Lee
“Broken Fingers: On the Usage of the Fingerprint API in Android”
In *Proceedings of the Network & Distributed System Security Symposium (NDSS)*
- Dec 2017 **Antonio Bianchi**, Eric Gustafson, Yanick Fratantonio, Christopher Kruegel, Giovanni Vigna
“Exploitation and Mitigation of Authentication Schemes Based on Device-Public Information”
In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*
- Aug 2017 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 (Usenix SEC)*
- Feb 2017 Aravind Machiry, Eric Gustafson, Chad Spensky, Chris Salls, Nick Stephens, Ruoyu Wang, **Antonio Bianchi**, Yung Ryn Choe, Christopher Kruegel, Giovanni Vigna
“BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments”
In *Proceedings of the Network & Distributed System Security Symposium (NDSS)*
- Feb 2017 Ruoyu Wang, Yan Shoshitaishvili, **Antonio Bianchi**, Aravind Machiry, John Grosen, Paul Grosen, Christopher Kruegel, Giovanni Vigna
“Ramblr: Making Reassembly Great Again”
In *Proceedings of the Network & Distributed System Security Symposium (NDSS)*
Distinguished Paper Award
- Jan 2017 **Antonio Bianchi**, Kevin Borgolte, Jacopo Corbetta, Francesco Disperati, Andrew Dutcher, John Grosen, Paul Grosen, Aravind Machiry, Christopher Salls, Yan Shoshitaishvili, Nick Stephens, Giovanni Vigna, Ruoyu Wang (Authors listed alphabetically)
“Cyber Grand Shellphish”
In *Phrack Magazine*
- May 2016 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)*

- Feb 2016 Vitor Afonso, **Antonio Bianchi**, Yanick Fratantonio, Adam Doupé, 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 Network & Distributed System Security Symposium (NDSS)*
- Dec 2015 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)*
- Oct 2015 **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)*
- Sep 2015 Yanick Fratantonio, Aravind Machiry, **Antonio Bianchi**, Christopher Kruegel, Giovanni Vigna
“CLAPP: Characterizing Loops in Android Applications”
In *Proceedings of the Symposium on the Foundations of Software Engineering (FSE)*
- Aug 2015 Yanick Fratantonio, Aravind Machiry, **Antonio Bianchi**, Christopher Kruegel, Giovanni Vigna
“CLAPP: Characterizing Loops in Android Applications”
In *Proceedings of International Workshop on Software Development Lifecycle for Mobile (DeMobile)*
- Jul 2015 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 & Vulnerability Assessment (DIMVA)*
- May 2015 **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)*
- Feb 2015 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 Network & Distributed System Security Symposium (NDSS)*
- Feb 2014 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 Network & Distributed System Security Symposium (NDSS)*
- Oct 2012 **Antonio Bianchi**, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna
“Blacksheep: Detecting Compromised Hosts in Homogeneous Crowds”
In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*

Invited Talks and Presentations

- Oct 2018 Detecting Vulnerable Code: from Mobile Apps to IoT Devices.
CS Colloquium Invited Talk – Purdue University
- Sep 2018 Detecting Vulnerable Code: from Mobile Apps to IoT Devices.
Invited Talk – Grinnell College
- Feb 2018 Broken Fingers: On the Usage of the Fingerprint API in Android
Network & Distributed System Security Symposium (NDSS), San Diego, California, USA
- Dec 2017 Exploitation and Mitigation of Authentication Schemes Based on Device-Public Information
Annual Computer Security Applications Conference (ACSAC), Orlando, Florida, USA
- Dec 2016 Automatic Binary Exploitation and Patching using Mechanical [Shell]Phish
HITCON Pacific, Taipei, Taiwan
- Aug 2016 Cyber Grand Shellphish: Shellphish and the DARPA CGC
DEFCON, Las Vegas, NV, USA
- Jul 2016 A Dozen Years of Shellphish – From DEFCON to the Cyber Grand Challenge
Nuit du Hack, Paris, France
- Dec 2015 A Dozen Years of Shellphish – From DEFCON to the Cyber Grand Challenge
Chaos Communication Congress, Berlin, Germany
- Aug 2015 A Dozen Years of Shellphish – From DEFCON to the Cyber Grand Challenge
HITCON Enterprise, Taipei, Taiwan
- Oct 2015 NJAS: Sandboxing Unmodified Applications in non-rooted Devices Running Stock Android
ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM), Denver, Colorado, USA
- May 2015 What the App is That? Deception and Countermeasures in the Android User Interface
IEEE Symposium on Security and Privacy (S&P), San Jose, California, USA
- Oct 2012 Blacksheep: Detecting Compromised Hosts in Homogeneous Crowds
ACM Conference on Computer and Communications Security (CCS), Raleigh, NC, USA

Teaching and Mentoring Experience

- Spring 2019 **Instructor**,
*CS:4980 “Mobile Systems and Smartphone Security”,
University of Iowa.*
- Fall 2018 **Instructor**,
*CS:3620 “Operating Systems”,
University of Iowa.*
- Nov 2015, Nov 2017 **Guest Lecture on “Mobile Security”**,
*CS279 “Advanced Topics in Computer Security”,
University of California, Santa Barbara.*
- Jan 2016 – Apr 2016 **Teaching Assistant**,
*CS160 “Translation of Programming Languages”,
University of California, Santa Barbara.*

Community Service

- 2019 Network & Distributed System Security Symposium (NDSS)
Reviewer
- Dec 2018 Workshop on Binary Analysis Research (BAR) at
Network & Distributed System Security Symposium (NDSS)
Program Committee co-Chair
- Nov 2018 IEEE Transactions on Dependable and Secure Computing (TDSC)
Journal Reviewer
- Oct 2018 Journal of Information Security and Applications (JISA)
Journal Reviewer
- Dec 2017 Workshop on Binary Analysis Research (BAR) at
Network & Distributed System Security Symposium (NDSS)
Program Committee Member
- Nov 2017, Dec 2017 IEEE Transactions on Information Forensics & Security (IFS)
Journal Reviewer
- Sep 2017 IEEE Transactions on Mobile Computing (TMC)
Journal Reviewer
- Aug 2017 USENIX Security Symposium (Usenix SEC)
External Reviewer
- Mar 2016 IEEE European Symposium on Security and Privacy (EuroS&P)
External Reviewer
- Aug 2016 USENIX Security Symposium (Usenix SEC)
Subreviewer
- May 2015 USENIX Security Symposium (Usenix SEC)
Shadow Program Committee Member
- Feb 2015 Network & Distributed System Security Symposium (NDSS)
Subreviewer
- Aug 2014 USENIX Security Symposium (Usenix SEC)
Subreviewer
- May 2013 IEEE Symposium on Security and Privacy (S&P)
Subreviewer

Media Coverage

- Sep 2017 Boffins hijack bootloaders for fun and games on Android
The Register
- Sep 2017 Mobile Bootloaders From Top Manufacturers Found Vulnerable to Persistent Threats
The Hacker News
- Sep 2017 Android security: Multiple bootloader bugs found in major chipset vendors' code
ZDNet
- Aug 2016 Mechanical Phish auto-exploit auto-patch kit lands on GitHub
The Register
- Aug 2016 Will Humans or Bots Rule Cybersecurity? The Answer Is Yes
Wired
- Mar 2016 These engineers are developing artificially intelligent hackers
The Guardian

Awards

- Feb 2017 Distinguished Paper Award — Network & Distributed System Security Symposium (NDSS)
- Aug 2016 Third Place (First Place Self-funded Team) — DARPA Cyber Grand Challenge
- Mar 2012 Regents Special Fellowship — University of California, Santa Barbara

Security Competitions

- 2018 – now Member of the organization team of the DEFCON CTF security competition
- 2012 – 2018 Member of the organization team of the UCSB iCTF security competition
- 2012 – now Member of the Shellphish security team
- 2016 DARPA Cyber Grand Challenge – 3rd Place (1st Place Self-funded Team)
- 2013 – 2018 Qualified to the DEFCON CTF Final

Research Tools and Open Source Contributions

- angr – Java engine Symbolic execution engine used by angr for Java/Dalvik bytecode
github.com/angr/angr
- PySoot A lifter from JAR/APK files to a Soot-like Python IR
github.com/angr/pysoot
- Mechanical Phish Shellphish's Cyber Reasoning System used during the DARPA Cyber Grand Challenge
github.com/mechaphish
- Patcherex Binary patcher tool used by the Shellphish's Cyber Reasoning System
github.com/shellphish/patcherex
- How2Heap An educational project for learning various heap exploitation techniques.
github.com/shellphish/how2heap
- Android UI modifications Source code of the Android UI modifications proposed in our paper: "What the App is That? Deception and Countermeasures in the Android User Interface"
github.com/ucsb-seclab/android_ui_deception

References

- **Giovanni Vigna**
Professor at University of California, Santa Barbara
vigna@cs.ucsb.edu
- **Christopher Kruegel**
Professor at University of California, Santa Barbara
chris@cs.ucsb.edu
- **Wenke Lee**
Professor at Georgia Institute of Technology
wenke.lee@gmail.com