

# Antonio Bianchi

Assistant Professor

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

## Research Interests

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

Specifically, my research areas are: emerging security threats in mobile platforms, automatic vulnerability detection in mobile apps, program analysis, binary analysis, reverse engineering, binary hardening, binary patching, and security of embedded devices, IoT devices, and cyber-physical systems. My research focuses on designing and developing novel automated approaches and tools to identify vulnerabilities in existing software, fix them, and prevent them.

## 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.
- 2008 – 2012 **M.Sc. in Computer Engineering**,  
Politecnico di Milano, Italy.
- 2005 – 2008 **B.Sc. in Computer Engineering**,  
Politecnico di Milano, Italy.

## Research and Professional Experience

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

---

## Publications

Names of advisees are written in **bold** font.

### At Purdue

- Aug 2024 1) **Jianliang Wu**, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, Antonio Bianchi  
“Finding Traceability Attacks in the Bluetooth Low Energy Specification and its Implementations”  
To appear in *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Aug 2024 2) Reham Mohamed, Arjun Arunasalam, Habiba Farrukh, Jason Tong, Antonio Bianchi, Z. Berkay Celik  
“ATTention Please! An Investigation of the App Tracking Transparency Permission”  
To appear in *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- May 2024 3) Muqi Zou, Arslan Khan, **Ruoyu Wu**, Han Gao, Antonio Bianchi, Dave (Jing) Tian  
“D-Helix: Improving Decompilation Accuracy via Symbolic Model Differentiation and Automatic Tuning”  
To appear in *USENIX Security Symposium (Usenix SEC)*
- May 2024 4) **Hyungsub Kim**, Rwitam Bandyopadhyay, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, Yongdae Kim, Dongyan Xu  
“A Systematic Study of Physical Sensor Attack Hardness”  
To appear in *IEEE Symposium on Security and Privacy (S&P)*
- May 2024 5) **Jianliang Wu**, **Ruoyu Wu**, Dongyan Xu, Dave (Jing) Tian, Antonio Bianchi  
“SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth”  
To appear in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*
- May 2024 6) **Doguhan Yeke**, **Muhammad Ibrahim**, Güliz Seray Tuncay, Habiba Farrukh, **Abdullah Imran**, Antonio Bianchi, Z. Berkay Celik  
“Wear’s my Data? Understanding the Cross-Device Runtime Permission Model in Wearables”  
To appear in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*
- Dec 2023 7) **Prashast Srivastava**, Flavio Toffalini, Kostyantyn Vorobyov, François Gauthier, Antonio Bianchi, Mathias Payer  
“Crystallizer: A Hybrid Path Analysis Framework To Aid in Uncovering Deserialization Vulnerabilities”  
In *Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*
- Dec 2023 8) Hammas Bin Tanveer, Mike Puchol, Rachee Singh, Antonio Bianchi, Rishab Nithyanand  
“Making Sense of Constellations: Methodologies for Understanding Starlink’s Scheduling Algorithms”  
In *Proceedings of the Conference on emerging Networking EXperiments and Technologies (CoNEXT)*
- Aug 2023 9) Kyungtae Kim, Sungwoo Kim, Kevin R. B. Butler, Antonio Bianchi, Rick Kennell, Dave (Jing) Tian  
“Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery”  
In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Aug 2023 10) Habiba Farrukh, Reham Mohamed, Aniket Nare, Antonio Bianchi, Z. Berkay Celik  
“Locln: Inferring Semantic Location from Spatial Maps in Mixed Reality”  
In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Aug 2023 11) **Siddharth Muralee**, Igibek Koishybayev, Aleksandr Nahapetyan, Greg Tystahl, Brad Reaves, Antonio Bianchi, William Enck, Alexandros Kapravelos, Aravind Machiry  
“ARGUS: A Framework for Staged Static Taint Analysis of GitHub Workflows and Actions”  
In *Proceedings of the USENIX Security Symposium (Usenix SEC)*

- Aug 2023 12) **Ruoyu Song**, Muslum Ozgur Ozmen, **Hyungsub Kim**, Raymond Muller, Z. Berkay Celik, Antonio Bianchi  
“Discovering Adversarial Driving Maneuvers against Autonomous Vehicles”  
In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Aug 2023 13) **Hyungsub Kim**, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, Dongyan Xu  
“PatchVerif: Discovering Faulty Patches in Robotic Vehicles”  
In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Jul 2023 14) Arslan Khan, Muqi Zou, Kyungtae Kim, Dongyan Xu, Antonio Bianchi, Dave Jing Tian  
“Fuzzing SGX Enclaves via Host Program Mutations”  
In *Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P)*
- Jul 2023 15) **Muhammad Ibrahim**, Andrea Continella, Antonio Bianchi  
“AoT - Attack on Things: A security analysis of IoT firmware updates”  
In *Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P)*
- May 2023 16) Priyanka Bose, Dipanjan Das, Saastha Vasani, Sebastiano Mariani, Ilya Grishchenko, Andrea Continella, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna  
“COLUMBUS: Android App Testing Through Systematic Callback Exploration”  
In *Proceedings of International Conference on Software Engineering (ICSE), 2023*
- Feb 2023 17) **Hyungsub Kim**, Muslum Ozgur Ozmen, Antonio Bianchi, Z. Berkay Celik, Dongyan Xu  
“Demo: Discovering Faulty Patches in Robotic Vehicle Control Software”  
In *Proceedings of the Symposium on Vehicle Security and Privacy (VehicleSec), colocated with NDSS*
- Feb 2023 18) Muslum Ozgur Ozmen, Habiba Farrukh, **Hyungsub Kim**, Antonio Bianchi, Z. Berkay Celik  
“Short: Rethinking Secure Pairing in Drone Swarms”  
In *Proceedings of the Symposium on Vehicles Security and Privacy (VehicleSec)*
- Dec 2022 19) **Prashast Srivastava**, Stefan Nagy, Matthew Hicks, Antonio Bianchi, Mathias Payer  
“One Fuzz Doesn’t Fit All: Optimizing Directed Fuzzing via Target-tailored Program State Restriction”  
In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*
- Aug 2022 20) **Ruoyu Wu**, Taegy Kim, Dave (Jing) Tian, Antonio Bianchi, Dongyan Xu  
“DnD: A Cross-Architecture Deep Neural Network Decompiler”  
In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Aug 2022 21) **Abdullah Imran**, Habiba Farrukh, **Muhammad Ibrahim**, Z. Berkay Celik, Antonio Bianchi  
“SARA: Secure Android Remote Authorization”  
In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- May 2022 22) Sungwoo Kim, Gisu Yeo, Taegy Kim, Junghwan “John” Rhee, Yuseok Jeon, Antonio Bianchi, Dongyan Xu, Dave (Jing) Tian  
“ShadowAuth: Backward-Compatible Automatic CAN Authentication for Legacy ECUs”  
In *Proceedings of the Asia Conference on Computer and Communications Security (AsiaCCS)*
- May 2022 23) **Hyungsub Kim**, Muslum Ozgur Ozmen, Z. Berkay Celik, Antonio Bianchi, Dongyan Xu  
“PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles”  
In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*
- May 2022 24) Kyungtae Kim, Ertza Warraich, Taegy Kim, Byoungyoung Lee, Kevin Butler, Antonio Bianchi, Dave (Jing) Tian  
“FUZZUSB: Hybrid Stateful Fuzzing of the Linux USB Gadget Stack”  
In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*
- May 2022 25) **Jianliang Wu**, **Ruoyu Wu**, Dongyan Xu, Dave (Jing) Tian, Antonio Bianchi  
“Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities”  
In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*

- Mar 2022 26) **Hyungsub Kim**, Muslum Ozgur Ozmen, [Antonio Bianchi](#), Z. Berkay Celik, Dongyan Xu  
 “Demo: Policy-based Discovery and Patching of Logic Bugs in Robotic Vehicles”  
 In *Proceedings of the Automotive and Autonomous Vehicle Security Workshop (AutoSec), collocated with NDSS*
- Oct 2021 27) Michael Reeves, Dave (Jing) Tian, [Antonio Bianchi](#), Z. Berkay Celik  
 “Towards Improving Container Security by Preventing Runtime Escapes”  
 In *Proceedings of the IEEE Secure Development Conference (SecDev)*
- Sep 2021 28) Onur Zungur, [Antonio Bianchi](#), Gianluca Stringhini, Manuel Egele  
 “APPJITSU: Investigating the Resiliency of Android Applications”  
 In *Proceedings of the European IEEE Symposium on Security and Privacy (Euro S&P)*
- Aug 2021 29) **Jianliang Wu**, **Ruoyu Wu**, Daniele Antonioli, Mathias Payer, Nils Ole Tippenhauer, Dongyan Xu, Dave (Jing) Tian, [Antonio Bianchi](#)  
 “LIGHTBLUE : Automatic Profile-Aware Debloating of Bluetooth Stacks”  
 In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Aug 2021 30) Arslan Khan, **Hyungsub Kim** Byoungyoung Lee, Dongyan Xu, [Antonio Bianchi](#), Dave (Jing) Tian  
 “M2MON: Building a MMIO-based Security Reference Monitor for Cyber-Physical Systems”  
 In *Proceedings of the USENIX Security Symposium (Usenix SEC)*
- Jun 2021 31) **Muhammad Ibrahim**, **Abdullah Imran**, [Antonio Bianchi](#)  
 “SafetyNOT: On the Usage of the SafetyNet Attestation API in Android”  
 In *Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services (MobySys)*
- May 2021 32) Nilo Redini, Andrea Continella, Aravind Machiry, Giulio De Pasquale, Dipanjan Das, [Antonio Bianchi](#), Christopher Kruegel, Giovanni Vigna  
 “Diane: Identifying Fuzzing Triggers in Apps for Effective Vulnerability Analysis of IoT Devices”  
 In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*
- Feb 2021 33) **Hyungsub Kim**, Muslum Ozgur Ozmen, [Antonio Bianchi](#), Z. Berkay Celik, Dongyan Xu  
 “PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles”  
 In *Proceedings of the Network & Distributed System Security Symposium (NDSS)*
- Feb 2021 34) **Lei Zeyu**, Yuhong Nan, Yanick Fratantonio, [Antonio Bianchi](#)  
 “On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices”  
 In *Proceedings of the Network & Distributed System Security Symposium (NDSS)*
- Aug 2020 35) **Jianliang Wu**, Yuhong Nan, Vireshwar Kumar, Dave (Jing) Tian, [Antonio Bianchi](#), Mathias Payer, Dongyan Xu  
 “BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy”  
 In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*  
**Best Paper Award**
- Sep 2019 36) Dario Nisi, [Antonio Bianchi](#), Yanick Fratantonio  
 “Exploring Syscall-Based Semantics Reconstruction of Android Applications”  
 In *Proceedings of the International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*
- [Before Purdue](#)
- Aug 2018 1) 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 2) 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 3) 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 4) 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 5) 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 6) 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 7) 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 8) 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 9) 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 10) 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 11) 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 12) 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 13) 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 14) 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 15) 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 16) [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 17) 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 18) 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 19) [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)*

---

## Peer-reviewed Accepted Talks and Presentations

- Dec 2022 DnD: Decompiling Deep Neural Network Compiled Binary  
**Ruoyu Wu**, Taegyu Kim, Dave (Jing) Tian, [Antonio Bianchi](#), Dongyan Xu  
*BlackHat Europe*, London, UK
- Aug 2022 TruEMU: An Extensible, Open-Source, Whole-System iOS Emulator  
**Trung Nguyen**, Kyungtae Kim, [Antonio Bianchi](#), Dave (Jing) Tian  
*BlackHat*, Las Vegas, NV, 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
- Dec 2015 A Dozen Years of Shellphish – From DEFCON to the Cyber Grand Challenge  
*Chaos Communication Congress*, Berlin, Germany

---

## Selected Invited Talks and Presentations

- Feb 2022 From the analysis of mobile apps to the analysis of the mobile ecosystem.  
 Keynote Speaker – *International Workshop on Security in Mobile Technologies at ACNS2022*

- Feb 2020 How not to use text messages for authentication.  
*Invited Talk – Android Security and Privacy Research (ASPIRE) Summit, Google, Mountain View, CA*
- Dec 2019 Securing Interconnected Software: from Mobile Apps to IoT Devices.  
*Invited Talk – Symantec (remote)*
- 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*

---

## Supervision Experience

### Graduated PhD Students

- Fall 2023 Hyungsub Kim, *co-advised with Berkay Celik*, Topic: Cyber-physical Systems Security  
Now postdoc at Purdue University
- Summer 2023 Jianliang Wu, *co-advised with Dongyan Xu*, Topic: Bluetooth Security  
Now faculty at Simon Fraser University
- Spring 2023 Prashast Srivastava, *co-advised with Mathias Payer*, Topic: Program Analysis  
Now PostDoc working with Prof. Suman Jana at Columbia University

### Advised Master Theses

- Nov 2022 Rowan Brock Hart, “Fuzzing Deeper Logic With Impeding Function Transformation”, Purdue University
- Dec 2019 Alessandro Brucato, “Semi-Automated Identification and Handling of Input Parsing Routines for Efficient Fuzzing and Symbolic Execution”, Politecnico di Milano

---

## University Activities

- Spring 2023 Co-advisor of the Purdue’s for the MITRE Embedded Capture the Flag (eCTF). Instructor of the related “eCTF - CS 590” class. Winner of the Best Poster Award.
- 2021, 2022, 2023 Honors Research Advisor (CS 397)
- 2019 – 2020 Graduate Admissions Committee Member
- Fall 2019 – present Started the Research meetings and the Reading Group on System Security at the PurSec Lab, attendance: about 25 students (together with Prof. Tian, Prof. Celik, and Prof. Xu)
- Fall 2019 – present Started the PurSec Lab, a System Security research group at Purdue (together with Prof. Tian, Prof. Celik, and Prof. Xu)

### PhD Thesis Defense Committees

- Jul 2023 Khaled Serag Alsharif, “Proactive Vulnerability Identification and Defense Construction – The Case for Can” – Purdue University
- Jun 2023 Habiba Farrukh, “Leveraging Multi-modal Sensing for Enhancing Security & Privacy of Mobile Systems” – Purdue University
- Jun 2023 Prashast Srivastava, “Practical Methods for Dynamic Software Analysis of Real-world Systems” – Purdue University
- May 2023 Jianliang Wu, “Securing IoT Systems via Protocol Formal Analysis and Debloating” – Purdue University
- Oct 2022 Kyungtae Kim, “Securing System and Embedded Software via Fuzzing” – Purdue University
- Sep 2021 Andrea Possemato, “A Multidimensional Analysis of The Android Security Ecosystem” – PhD student at EURECOM, France

- Jul 2021 Yicheng Cheng, "Machine Learning in the Open World" – Purdue PhD student at IUPUI campus  
[Master Thesis Committees](#)
- Apr 2023 Parvin Kumar
- Nov 2022 Rowan Brock Hart – Chair
- May 2021 Michael Reeves

---

## Engagement, Diversity, and Outreach Activities at Purdue

- 2019 – present Faculty co-Advisor of the "Purdue Capture the Flag Team (b01lers)"  
b01lers is the Purdue CTF team, playing multiple security competitions every month. Currently, b01lers has about 30 active participants (about 20 undergrads). Additionally, b01lers organizes, every year, a series of seminars on playing security competitions and b01lers CTF, an online security competition, which I contribute to by writing security challenges. Winner of Raymond James CTF in 2021 and 2023.
- 2019, 2020, 2021 Member of the organization team of the DEFCON CTF international security competition  
Organized the DEFCON CTF Quals events (more than 400 playing teams each year) and DEFCON CTF Finals event (16 in-person teams each year).
- Oct 2020 Talk at Purdue: CS 397 "Honors Seminar"
- Oct 2019 Invited Talk: "Machines Hacking Machines: Who Needs People?"  
At RoseHulman Institute of Technology (undergraduate local college)
- Sep 2019 Talk at Purdue: CS 397 "Honors Seminar"
- Aug 2019 Talk at Purdue: Graduate Student Orientation

---

## Teaching Experience

### At Purdue

- Spring 2024 **Instructor**,  
CS 527 "Software Security",  
3 credits, in-person and online, about 30 students.
- Fall 2023 **Instructor**,  
CS 490-SWS "Software Security",  
3 credits, about 10 students.
- Fall 2023 **Instructor**,  
CS 397 "Honors Seminar",  
0 credits, about 20 students.
- Spring 2023 **Instructor**,  
CS 527 "Software Security",  
3 credits, about 25 students, Graduate Teaching Award 2023 for the TA Ruoyu Song.
- Spring 2023 **Instructor**,  
CS 590 "eCTF",  
3 credits, co-instructor for the CS department, about 25 students (10 from the CS department).
- Fall 2022 **Instructor**,  
CS 490-SWS "Software Security" (*new undergrad course*),  
3 credits, about 10 students.
- Fall 2022 **Instructor**,  
CS 397 "Honors Seminar",  
0 credits, about 10 students.



- Spring 2022 **Instructor**,  
*CS 527 "Software Security"*,  
 3 credits, about 25 students.
- Fall 2021 **Instructor**,  
*CS 592-AST "Automated Security Testing" (new course, seminar-style course)*,  
 3 credits, about 10 students.
- Fall 2021 **co-Instructor**,  
*CS 397 "Honors Seminar"*,  
 0 credits, about 20 students.
- Spring 2021 **Instructor**,  
*CS 527 "Software Security" (both hybrid and online-only)*,  
 3 credits, about 30 students.
- Fall 2020 **Instructor**,  
*CERIAS Security Seminar*,  
 1 credit, about 15 students.
- Fall 2020 **Online Course Development**,  
*Designed and developed the online version of the CS 527 "Software Security" class.*
- Spring 2020 **Instructor**,  
*CS 527 "Software Security"*,  
 3 credits, about 20 students.
- Fall 2019 **Instructor**,  
*CS 590-MSS "Mobile Systems and Smartphone Security"*,  
 3 credits (**new course, valid towards the graduate degree curriculum**), about 10 students.
- [Before Purdue](#)
- Spring 2019 **Instructor**,  
*CS:4980 "Mobile Systems and Smartphone Security"*,  
 about 20 students, University of Iowa.
- Fall 2018 **Instructor**,  
*CS:3620 "Operating Systems"*,  
 about 30 students, 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.

---

## Professional Activities

### Conference Leadership/Organization

- 2024 Network & Distributed System Security Symposium (NDSS)  
*Session Chair*
- 2020 Workshop on Binary Analysis Research (BAR) at  
 Network & Distributed System Security Symposium (NDSS)  
*Program Committee Chair*
- 2019 Workshop on Binary Analysis Research (BAR) at  
 Network & Distributed System Security Symposium (NDSS)  
*Program Committee co-Chair*

### Selected Program Committee Membership

- 2024 ACM Conference on Data and Application Security and Privacy (CODASPY)
- 2024 Symposium on Vehicle Security and Privacy (VehicleSec)
- 2023 ACM Conference on Computer and Communications Security (CCS)
- 2023 European Symposium on Research in Computer Security (ESORICS)
- 2023 International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
- 2023 European Workshop on Systems Security (EuroSec)
- 2023 Network & Distributed System Security Symposium (NDSS)
- 2023 Symposium on Vehicle Security and Privacy (VehicleSec)
- 2022 Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
- 2022 Workshop on the Internet of Safe Things at  
IEEE Symposium on Security and Privacy (S&P)
- 2022 Workshop on Offensive Technologies at  
IEEE Symposium on Security and Privacy (S&P)
- 2022 Workshop on Automotive and Autonomous Vehicle Security at  
Network & Distributed System Security Symposium (NDSS)
- 2019 to 2023 Workshop on Binary Analysis Research (BAR) at  
Network & Distributed System Security Symposium (NDSS)
- 2022 IEEE Symposium on Security and Privacy (S&P)
- 2022 Network & Distributed System Security Symposium (NDSS)
- 2022 USENIX Security Symposium (Usenix SEC)
- 2021 USENIX Security Symposium (Usenix SEC)
- 2021 IEEE Symposium on Security and Privacy (S&P)
- 2021 ACM ASIA Conference on Computer and Communications Security (AsiaCCS)
- 2021 Network & Distributed System Security Symposium (NDSS)
- Jul 2020 International Workshop on Security in Mobile Technologies (SecMT)
- Jun 2020 European Symposium on Research in Computer Security (ESORICS)
- 2020 IEEE Symposium on Security and Privacy (S&P)
- 2020 ACM Conference on Computer and Communications Security (CCS)
- 2020 Network & Distributed System Security Symposium (NDSS)

### Selected Journal Reviews

- Apr 2023 ACM Computing Surveys Review (CSUR)
- Jan 2021 IEEE Transactions on Knowledge and Data Engineering (TKDE)
- Apr 2020 IEEE Transactions on Mobile Computing (TMC)
- Mar 2020 ACM Computing Surveys Review (CSUR)
- Nov 2018 IEEE Transactions on Dependable and Secure Computing (TDSC)
- Nov 2017, Dec 2017 IEEE Transactions on Information Forensics & Security (IFS)
- Sep 2017 IEEE Transactions on Mobile Computing (TMC)

---

### Grants

- Dec 2023 DARPA – Faithful Integrated Reverse-Engineering and Exploitation (FIRE),  
*FIREFLY: A Cyber-Physical Framework for Scalable CPS Modeling and Simulation*,  
co-PI, total: \$6,500,087

- Oct 2023 Lockheed Martin Corp.,  
lead PI, total: \$65,000
- Oct 2023 Apple Inc.,  
lead PI, total: \$44,388
- May 2023 DOE,  
*Enabling Secure and Resilient XFC: A Software/Hardware-security Co-design Approach*,  
co-PI, subcontractor of Virginia Tech, Purdue share: \$80,000
- 2023 Google,  
*Google ASPIRE Award*,  
co-PI, total: \$90,000 (unrestricted gift, shared with Prof. Berkay Celik)
- Jan 2023 – Dec 2025 ONR,  
*Semantic Decompilation of Deep Neural Network Binaries and Its Adversarial and Defensive Implications*,  
co-PI, my share: about \$250,000, total: \$750,655
- 2022 Google,  
*Google ASPIRE Award*,  
Voluntary Contribution, total: \$80,850 (unrestricted gift, shared with Prof. Berkay Celik)
- Jun 2022 – May 2023 ONR,  
*An Integrated Toolkit for IoT Protocol Dialecting with Formal Verification*,  
co-PI, total: \$620,000
- 2021 Google,  
*Google ASPIRE Award*,  
Voluntary Contribution, total: \$100,000 (unrestricted gift, shared with Prof. Berkay Celik)
- Aug 2020 – Aug 2024 DARPA – AMP,  
*DICER: Directed Compilation for Assured Patching*,  
lead PI (with UC Santa Barbara and EPFL as subcontractors), total: \$3,869,685
- 2020 – 2021 Google,  
*Google Security Rewards Program*,  
Voluntary Contribution, total: \$8,000 (unrestricted gift)
- Jun 2019 – Dec 2021 NSF – CRII,  
*SaTC: Vetting and Improving the Usage of Trusted Execution Environments for Authentication in Mobile Devices*,  
single PI, \$174,972
- Dec 2018 – 2022 DARPA – Computers and Humans Exploring Software Security (CHESS),  
*CHECRS: Cognitive Human Enhancements for Cyber Reasoning Systems*,  
co-PI, subcontractor of Arizona State University (ASU), my share: \$880,941
- Oct 2019 – 2022 ONR,  
*Bringing Fuzzing to the Cyber-Physical World*,  
co-PI, total: \$799,877

---

## Awards and Honors

- Feb 2024 Undergraduate Advising Award — Purdue University
- Oct 2023 Seed for Success Acorn Award, for researchers having received a sponsored grant equal to or greater than \$1 million — Grant: “DICER: Directed Compilation for Assured Patching,” lead PI
- May 2023 Best Poster Award — MITRE 2023 embedded Capture the Flag (eCTF)
- Aug 2020 Best Paper Award — USENIX Workshop on Offensive Technologies (WOOT)
- 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