Antonio Bianchi
Curriculum Vitae

antoniob@purdue.edu
https://antoniobianchi.me
Last update: November 2024

Interests

My research interests span the domains of **Software and Systems Security**. In particular, I have been focusing on the broad area of **security of smart devices and edge devices**, such as smartphones, smartwatches, IoT devices, robotic vehicles, and embedded systems.

Education

- Ph.D., Thesis: "Identifying and Mitigating Trust Violations in the Mobile Ecosystem," Computer Science Department, UC Santa Barbara, July 2018.
  Advisors: Prof. Giovanni Vigna and Prof. Christopher Kruegel.
- M.S., Computer Science, University of Illinois at Chicago, May 2012.
- M.S., Computer Engineering, Politecnico di Milano, Italy, April 2012.
- B.Sc., Computer Engineering, Politecnico di Milano, Italy, September 2008.

Previous Positions

- ASST Professor, Department of Computer Sciences, The University of Iowa, Iowa City, IA, August 2018 – July 2019.

Present Position

- ASST Professor, Department of Computer Sciences, Purdue University, West Lafayette, IN, August 2019 – present.

Awards and Honors

- Qualified for the DARPA/ARPA-H AIxCC Final event as part of the Shellphish team (7 teams qualified out of 42 participating teams), 2024.
- Seed for Success Acorn Award for researchers having received a sponsored grant equal to or greater than $1 million, from Purdue's Office of Research. Grant: "FIREFLY: A Cyber-Physical Framework for Scalable CPS Modeling and Simulation (co-PI)," 2024.
- Undergraduate Advising Award, from Purdue CS Department, 2024.
- Seed for Success Acorn Award for researchers having received a sponsored grant equal to or greater than $1 million, from Purdue's Office of Research. Grant: "DICER: Directed Compilation for Assured Patching (PI)," 2023.
- Best Poster Award — MITRE 2023 embedded Capture the Flag (eCTF), 2023.

- Best Paper Award — USENIX Workshop on Offensive Technologies (WOOT), 2020.
- NSF Directorate for Computer and Information Science and Engineering (CISE) Research Initiation Initiative (CRII) Award, 2019.
- Distinguished Paper Award — Network & Distributed System Security Symposium (NDSS), 2016.
- Third Place (First Place Self-funded Team) at the DARPA Cyber Grand Challenge, as part of the Shellphish team, 2016.
- Regents Special Fellowship — University of California, Santa Barbara, 2012.

Publications

Note:
* indicates primary author, ^{P} denotes author who is postdoctoral researcher (or on other pre-faculty position) *at the time of writing.* Similarly, ^{U} and ^{G} indicate authors who were undergraduate and graduate students, respectively *at the time of writing.*
^{A}denotes advisees. ^{M}denotes PhD advisors.

Articles Refereed In Conference Proceedings

1. Jianliang Wu^{*A}, Patrick Traynor, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. Finding Traceability Attacks in the Bluetooth Low Energy Specification and its Implementations. In *USENIX Security Symposium (UsenixSEC)*, 2024. (18.32% acceptance rate)
2. Reham Mohamed^{*G}, Arjun Arunasalam^G, Habiba Farrukh^G, Jason Tong, Antonio Bianchi, and Z. Berkay Celik. ATTention Please! An Investigation of the App Tracking Transparency Permission. In *USENIX Security Symposium (UsenixSEC)*, 2024. (18.32% acceptance rate)
3. Muqi Zou^{*G}, Arslan Khan^G, Ruoyu Wu^{AG}, Han Gao^G, Antonio Bianchi, and Dave (Jing) Tian. D-Helix: Improving Decompilation Accuracy via Symbolic Model Differentiation and Automatic Tuning. In *USENIX Security Symposium (UsenixSEC)*, 2024. (18.32% acceptance rate)
4. Abdullah Imran^{*AG}and Antonio Bianchi. Automated detection of cryptographic inconsistencies in Android's Keymaster implementations. In *Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2024. (16.3% acceptance rate)
5. Hyungsub Kim^{*AG}, Rwitam Bandyopadhyay^G, Muslum Ozgur Ozmen^G, Z. Berkay Celik, Antonio Bianchi, Yongdae Kim, and Dongyan Xu. A Systematic Study of Physical Sensor Attack Hardness. In *IEEE Symposium on Security and Privacy (S&P)*, 2024. (17.8% acceptance rate)
6. Jianliang Wu^{*AG}, Ruoyu Wu^{AG}, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. SoK: The Long Journey of Exploiting and Defending the Legacy of King Harald Bluetooth. In *IEEE Symposium on Security and Privacy (S&P)*, 2024. (17.8% acceptance rate)
7. Doguhan Yeke^{*AG}, Muhammad Ibrahim^{AG}, Güliz Seray Tuncay, Habiba Farrukh^G, Abdullah Imran^{AG}, Antonio Bianchi, and Z. Berkay Celik. Wear's my Data? Understanding the Cross-Device Runtime Permission Model in Wearables. In *IEEE Symposium on Security and Privacy (S&P)*, 2024. (17.8% acceptance rate)
8. Prashast Srivastava^{*AG}, Flavio Toffalini, Kostyantyn Vorobyov, François Gauthier, Antonio Bianchi, and Mathias Payer. Crystallizer: A Hybrid Path Analysis Framework To Aid in Uncovering Deserialization Vulnerabilities. In *ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE)*, 2023. (21% acceptance rate)
9. Hammas Bin Tanveer^{*G}, Mike Puchol, Rachee Singh, Antonio Bianchi, and Rishab Nithyanand. Making Sense of Constellations: Methodologies for Understanding Starlinks Scheduling Algorithms. In *Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, 2023.

10. Kyungtae Kim[*G], Sungwoo Kim[G], Kevin R. B. Butler, Antonio Bianchi, Rick Kennell, and Dave (Jing) Tian. Fuzz The Power: Dual-role State Guided Black-box Fuzzing for USB Power Delivery. In *USENIX Security Symposium (UsenixSEC)*, 2023. (29.2% acceptance rate)

11. Habiba Farrukh[*G], Reham Mohamed[G], Aniket Nare, Antonio Bianchi, and Z. Berkay Celik. LocIn: Inferring Semantic Location from Spatial Maps in Mixed Reality. In *USENIX Security Symposium (UsenixSEC)*, 2023. (29.2% acceptance rate)

12. Siddharth Muralee[*AG], Igibek Koishybayev[*G], Aleksandr Nahapetyan[G], Greg Tystahl[G], Brad Reaves, Antonio Bianchi, William Enck, Alexandros Kapravelos, and Aravind Machiry. ARGUS: A Framework for Staged Static Taint Analysis of GitHub Workflows and Actions. In *USENIX Security Symposium (UsenixSEC)*, 2023. (29.2% acceptance rate)

13. Ruoyu Song[*AG], Muslum Ozgur Ozmen[G], Hyungsub Kim[AG], Raymond Muller[G], Z. Berkay Celik, and Antonio Bianchi. Discovering Adversarial Driving Maneuvers against Autonomous Vehicles. In *USENIX Security Symposium (UsenixSEC)*, 2023. (29.2% acceptance rate)

14. Hyungsub Kim[*AG], Muslum Ozgur Ozmen[G], Z. Berkay Celik, Antonio Bianchi, and Dongyan Xu. PatchVerif: Discovering Faulty Patches in Robotic Vehicles. In *USENIX Security Symposium (UsenixSEC)*, 2023. (29.2% acceptance rate)

15. Arslan Khan[*G], Muqi Zou[G], Kyungtae Kim[G], Dongyan Xu, Antonio Bianchi, and Dave Jing Tian. Fuzzing SGX Enclaves via Host Program Mutations. In *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2023. (35% acceptance rate)

16. Muhammad Ibrahim[*AG], Andrea Continella, and Antonio Bianchi. AoT - Attack on Things: A security analysis of IoT firmware updates. In *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2023. (35% acceptance rate)

17. Priyanka Bose[*G], Dipanjan Das[G], Saastha Vasan[G], Sebastiano Mariani[G], Ilya Grishchenko[P], Andrea Continella, Antonio Bianchi, Christopher Kruegel[M], and Giovanni Vigna[M]. COLUMBUS: Android App Testing Through Systematic Callback Exploration. In *International Conference on Software Engineering (ICSE), 2023*, 2023. (26% acceptance rate)

18. Hyungsub Kim[*AG], Muslum Ozgur Ozmen[G], Antonio Bianchi, Z. Berkay Celik, and Dongyan Xu. Demo: Discovering Faulty Patches in Robotic Vehicle Control Software. In *Symposium on Vehicle Security and Privacy (VehicleSec), colocated with NDSS*, 2023.

19. Muslum Ozgur Ozmen[*G], Habiba Farrukh[G], Hyungsub Kim[AG], Antonio Bianchi, and Z. Berkay Celik. Short: Rethinking Secure Pairing in Drone Swarms. In *Symposium on Vehicles Security and Privacy (VehicleSec)*, 2023.

20. Ruoyu Wu[*AG], Taegyu Kim[G], Dave (Jing) Tian, Antonio Bianchi, and Dongyan Xu. DnD: Decompiling Deep Neural Network Compiled Binary. Peer-reviewed Talk at *BlackHat Europe*, London, UK, 2022.

21. Prashast Srivastava[*AG], Stefan Nagy[G], Matthew Hicks, Antonio Bianchi, and Mathias Payer. One Fuzz Doesnt Fit All: Optimizing Directed Fuzzing via Target-tailored Program State Restriction. In *Annual Computer Security Applications Conference (ACSAC)*, 2022. (24.1% acceptance rate)

22. Ruoyu Wu[*AG], Taegyu Kim[G], Dave (Jing) Tian, Antonio Bianchi, and Dongyan Xu. DnD: A Cross-Architecture Deep Neural Network Decompiler. In *USENIX Security Symposium (UsenixSEC)*, 2022. (18.1% acceptance rate)

23. Abdullah Imran[*AG], Habiba Farrukh[G], Muhammad Ibrahim[AG], Z. Berkay Celik, and Antonio Bianchi. SARA: Secure Android Remote Authorization. In *USENIX Security Symposium (UsenixSEC)*, 2022. (18.1% acceptance rate)

24. Trung Nguyen[*U], Kyungtae Kim[G], Antonio Bianchi, and Dave (Jing) Tian. TruEMU: An Extensible, Open-Source, Whole-System iOS Emulator. Peer-reviewed Talk at *BlackHat*, Las Vegas, NV, 2022.

25. Sungwoo Kim*[G], Gisu Yeo[G], Taegyu Kim[G], Junghwan "John" Rhee[G], Yuseok Jeon, Antonio Bianchi, Dongyan Xu, and Dave (Jing) Tian. ShadowAuth: Backward-Compatible Automatic CAN Authentication for Legacy ECUs. In *Asia Conference on Computer and Communications Security (AsiaCCS)*, 2022. (18.3% acceptance rate)
26. Hyungsub Kim*[AG], Muslum Ozgur Ozmen[G], Z. Berkay Celik, Antonio Bianchi, and Dongyan Xu. PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles. In *IEEE Symposium on Security and Privacy (S&P)*, 2022. (14.5% acceptance rate)
27. Kyungtae Kim*[G], Ertza Warraich[G], Taegyu Kim[G], Byoungyoung Lee, Kevin Butler, Antonio Bianchi, and Dave (Jing) Tian. FUZZUSB: Hybrid Stateful Fuzzing of the Linux USB Gadget Stack. In *IEEE Symposium on Security and Privacy (S&P)*, 2022. (14.5% acceptance rate)
28. Jianliang Wu*[AG], Ruoyu Wu[AG], Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. Formal Model-Driven Discovery of Bluetooth Protocol Design Vulnerabilities. In *IEEE Symposium on Security and Privacy (S&P)*, 2022. (14.5% acceptance rate)
29. Hyungsub Kim*[AG], Muslum Ozgur Ozmen[G], Antonio Bianchi, Z. Berkay Celik, and Dongyan Xu. Demo: Policy-based Discovery and Patching of Logic Bugs in Robotic Vehicles. In *Automotive and Autonomous Vehicle Security Workshop (AutoSec), colocated with NDSS*, 2022.
30. Michael Reeves*[G], Dave (Jing) Tian, Antonio Bianchi, and Z. Berkay Celik. Towards Improving Container Security by Preventing Runtime Escapes. In *IEEE Secure Development Conference (SecDev)*, 2021.
31. Onur Zungur*[G], Antonio Bianchi, Gianluca Stringhini, and Manuel Egele. APPJITSU: Investigating the Resiliency of Android Applications. In *European IEEE Symposium on Security and Privacy (EuroS&P)*, 2021. (32% acceptance rate)
32. Jianliang Wu*[AG], Ruoyu Wu*[AG], Daniele Antonioli, Mathias Payer, Nils Ole Tippenhauer, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. LIGHTBLUE: Automatic Profile-Aware Debloating of Bluetooth Stacks. In *USENIX Security Symposium (UsenixSEC)*, 2021. (18.7% acceptance rate)
33. Arslan Khan*[G], Hyungsub Kim[AG], Byoungyoung Lee, Dongyan Xu, Antonio Bianchi, and Dave (Jing) Tian. M2MON: Building a MMIO-based Security Reference Monitor for Cyber-Physical Systems. In *USENIX Security Symposium (UsenixSEC)*, 2021. (18.7% acceptance rate)
34. Muhammad Ibrahim*[AG], Abdullah Imran[AG], and Antonio Bianchi. SafetyNOT: On the Usage of the SafetyNet Attestation API in Android. In *ACM International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2021. (21.7% acceptance rate)
35. Nilo Redini*[G], Andrea Continella, Aravind Machiry, Giulio De Pasquale[G], Dipanjan Das[G], Antonio Bianchi, Christopher Kruegel[M], and Giovanni Vigna[M]. Diane: Identifying Fuzzing Triggers in Apps for Effective Vulnerability Analysis of IoT Devices. In *IEEE Symposium on Security and Privacy (S&P)*, 2021. (12.1% acceptance rate)
36. Hyungsub Kim*[AG], Muslum Ozgur Ozmen[G], Antonio Bianchi, Z. Berkay Celik, and Dongyan Xu. PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles. In *Network & Distributed System Security Symposium (NDSS)*, 2021. (15.2% acceptance rate)
37. Lei Zeyu*[AG], Yuhong Nan[P], Yanick Fratantonio, and Antonio Bianchi. On the Insecurity of SMS One-Time Password Messages against Local Attackers in Modern Mobile Devices. In *Network & Distributed System Security Symposium (NDSS)*, 2021. (15.2% acceptance rate)
38. Jianliang Wu*[AG], Yuhong Nan[P], Vireshwar Kumar[P], Dave (Jing) Tian, Antonio Bianchi, Mathias Payer, and Dongyan Xu. BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy. In *USENIX Workshop on Offensive Technologies (WOOT)*, 2020.
    Best Paper Award.
39. Dario Nisi*[G], Antonio Bianchi, and Yanick Fratantonio. Exploring Syscall-Based Semantics Reconstruction of Android Applications. In *International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, 2019. (22% acceptance rate)

40. Moritz Eckert^{*G}, Antonio Bianchi, Ruoyu Wang^{G}, Yan Shoshitaishvili^{G}, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. HeapHopper: Bringing Bounded Model Checking to Heap Implementation Security. In *USENIX Security Symposium (UsenixSEC)*, 2018. (19.1% acceptance rate)

41. Antonio Bianchi*, Yanick Fratantonio^{G}, Aravind Machiry, Christopher Kruegel^{M}, Giovanni Vigna^{M}, Simon Pak Ho Chung, and Wenke Lee. Broken Fingers: On the Usage of the Fingerprint API in Android. In *Network & Distributed System Security Symposium (NDSS)*, 2018. (21.5% acceptance rate)

42. Antonio Bianchi*, Eric Gustafson^{G}, Yanick Fratantonio^{G}, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. Exploitation and Mitigation of Authentication Schemes Based on Device-Public Information. In *Annual Computer Security Applications Conference (ACSAC)*, 2017. (19.7% acceptance rate)

43. Nilo Redini^{*G}, Aravind Machiry, Dipanjan Das^{G}, Yanick Fratantonio^{G}, Antonio Bianchi, Eric Gustafson^{G}, Yan Shoshitaishvili^{G}, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. BootStomp: On the Security of Bootloaders in Mobile Devices. In *USENIX Security Symposium (UsenixSEC)*, 2017. (16.3% acceptance rate)

44. Aravind Machiry*, Eric Gustafson^{G}, Chad Spensky^{G}, Chris Salls^{G}, Nick Stephens^{U}, Ruoyu Wang^{G}, Antonio Bianchi, Yung Ryn Choe, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. BOOMERANG: Exploiting the Semantic Gap in Trusted Execution Environments. In *Network & Distributed System Security Symposium (NDSS)*, 2017. (16% acceptance rate)

45. Ruoyu Wang^{*G}, Yan Shoshitaishvili^{G}, Antonio Bianchi, Aravind Machiry, John Grosen^{U}, Paul Grosen^{U}, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. Ramblr: Making Reassembly Great Again. In *Network & Distributed System Security Symposium (NDSS)*, 2017. (16% acceptance rate)
    Distinguished Paper Award.

46. Yanick Fratantonio^{*G}, Antonio Bianchi, William Robertson, Engin Kirda, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. TriggerScope: Towards Detecting Logic Bombs in Android Apps. In *IEEE Symposium on Security and Privacy (S&P)*, 2016. (13.3% acceptance rate)

47. Vitor Afonso^{*G}, Antonio Bianchi, Yanick Fratantonio^{G}, Adam Doupé^{G}, Mario Polino^{G}, Paulo de Geus, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. Going Native: Using a Large-Scale Analysis of Android Apps to Create a Practical Native-Code Sandboxing Policy. In *Network & Distributed System Security Symposium (NDSS)*, 2016. (15.4% acceptance rate)

48. Simone Mutti^{*G}, Yanick Fratantonio^{G}, Antonio Bianchi, Luca Invernizzi^{G}, Jacopo Corbetta^{G}, Dhilung Kirat^{G}, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. BareDroid: Large-Scale Analysis of Android Apps on Real Devices. In *Annual Computer Security Applications Conference (ACSAC)*, 2015. (24.4% acceptance rate)

49. Antonio Bianchi*, Yanick Fratantonio^{G}, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. NJAS: Sandboxing Unmodified Applications in non-rooted Devices Running Stock Android. In *ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2015.

50. Yanick Fratantonio^{*G}, Aravind Machiry, Antonio Bianchi, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. CLAPP: Characterizing Loops in Android Applications. In *Symposium on the Foundations of Software Engineering (FSE)*, 2015. (25.4% acceptance rate)

51. Yanick Fratantonio^{*G}, Aravind Machiry, Antonio Bianchi, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. CLAPP: Characterizing Loops in Android Applications. In *International Workshop on Software Development Lifecycle for Mobile (DeMobile)*, 2015.

52. Yanick Fratantonio^{*G}, Antonio Bianchi, William Robertson, Manuel Egele, Christopher Kruegel^{M}, Engin Kirda, and Giovanni Vigna^{M}. On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users. In *Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 2015. (22.7% acceptance rate)

53. Antonio Bianchi*, Jacopo Corbetta^{G}, Luca Invernizzi^{G}, Yanick Fratantonio^{G}, Christopher Kruegel^{M}, and Giovanni Vigna^{M}. What the App is That? Deception and Countermeasures in the Android User Interface. In *IEEE Symposium on Security and Privacy (S&P)*, 2015. (13.5% acceptance rate)

54. Yinzhi Cao[*G], Yanick Fratantonio[G], Antonio Bianchi, Manuel Egele, Christopher Kruegel[M], Giovanni Vigna[M], and Yan Chen. EdgeMiner: Automatically Detecting Implicit Control Flow Transitions through the Android Framework. In *Network & Distributed System Security Symposium (NDSS)*, 2015. (16.9% acceptance rate)
55. Sebastian Poeplau[*U], Yanick Fratantonio[G], Antonio Bianchi, Christopher Kruegel[M], and Giovanni Vigna[M]. Execute This! Analyzing Unsafe and Malicious Dynamic Code Loading in Android Applications. In *Network & Distributed System Security Symposium (NDSS)*, 2014. (18.6% acceptance rate)
56. Antonio Bianchi[*], Yan Shoshitaishvili[G], Christopher Kruegel[M], and Giovanni Vigna[M]. Blacksheep: Detecting Compromised Hosts in Homogeneous Crowds. In *ACM Conference on Computer and Communications Security (CCS)*, 2012. (18.9% acceptance rate)

In Press

1. Ruoyu Wu[*AG], Muqi Zou[G], Arlsan Khan[G], Taegyu Kim, Dongyan Xu, Dave (Jing) Tian, and Antonio Bianchi. NeuroScope: Reverse Engineering Deep Neural Network on Edge Devices using Dynamic Analysis. To appear in *USENIX Security Symposium (UsenixSEC)*, 2025. (TBD acceptance rate)
2. Hongwei Wu[*AG], Ruoyu Wu[AG], Jianling Wu[A], Ayushi Sharma[G], Aravind Machiry, and Antonio Bianchi. VeriBin: Adaptive Verification of Patches at the Binary Level. To appear in *Network & Distributed System Security Symposium (NDSS)*, 2025. (TBD acceptance rate)
3. Zeyu Lei[*AG], Güliz Seray Tuncay, Beatrice Carissa Williem[U], Z. Berkay Celik, and Antonio Bianchi. ScopeVerif: Analyzing the Security of Android's Scoped Storage via Differential Analysis. To appear in *Network & Distributed System Security Symposium (NDSS)*, 2025. (TBD acceptance rate)

Books, Book Chapters, Technical Reports, Theses

1. Yan Shoshitaishvili[*G], Antonio Bianchi[G], Kevin Borgolte[G], Amat Cama[G], Jacopo Corbetta[G], Francesco Disperati[G], Audrey Dutcher[G], John Grosen[U], Paul Grosen[U], Aravind Machiry, Chris Salls[G], Nick Stephens[U], Ruoyu Wang[G], and Giovanni Vigna[M]. Mechanical Phish: Resilient Autonomous Hacking. In *IEEE Security & Privacy Magazine – SPSI: Hacking without Humans*, 2018.
2. Antonio Bianchi[G], Kevin Borgolte[G], Jacopo Corbetta[G], Francesco Disperati[G], Andrew Dutcher[G], John Grosen[U], Paul Grosen[U], Aravind Machiry, Christopher Salls[G], Yan Shoshitaishvili[G], Nick Stephens[U], Giovanni Vigna[M], and Ruoyu Wang[G]. Cyber Grand Shellphish. In *Phrack Magazine*, 2017.

Invited Lectures

National and International Meetings

1. "Fuzzing SGX Enclaves via Host Program Mutations," Invited Talk – Intel, Apr 2024.
2. "Security Analysis of Three Emerging Pieces of Android OS," Invited Talk – Google, Oct 2022.
3. "From the analysis of mobile apps to the analysis of the mobile ecosystem," Keynote Speaker – International Workshop on Security in Mobile Technologies at ACNS, Feb 2022.
4. "How not to use text messages for authentication," Invited Talk – Android Security and PrIvacy Research (ASPIRE) Summit, Google, Mountain View, CA, Feb 2020.
5. "Securing Interconnected Software: from Mobile Apps to IoT Devices," Invited Talk – Symantec, Dec 2019.
6. "Cyber Grand Shellphish: Shellphish and the DARPA CGC," Peer-reviewed Talk - DEF CON, Las Vegas, NV, USA, Aug 2016.

7. “A Dozen Years of Shellphish – From DEFCON to the Cyber Grand Challenge,” Invited Talk - Nuit Du Hack, Paris, France, Jul 2016.
8. “A Dozen Years of Shellphish – From DEFCON to the Cyber Grand Challenge,” Peer-reviewed Talk - Chaos Communication Congress (CCC), Berlin, Germany, Dec 2015.
9. “A Dozen Years of Shellphish – From DEFCON to the Cyber Grand Challenge,” Invited Talk - HITCON Enterprise, Taipei, Taiwan, Aug 2015.

Universities and Other Institutions

1. “Research at PurSec Lab.” Invited Talk – Rose-Hulman Institute of Technology, Terre Haute, IN, Nov 2023.
2. “Machines Hacking Machines: Who Needs People?” Invited Talk – Rose-Hulman Institute of Technology, Terre Haute, IN, Oct 2019.
3. “Detecting Vulnerable Code: from Mobile Apps to IoT Devices.” Invited Talk – Grinnell College, Grinnell, IA, Sep 2018.

Other Professional Activities

1. **Organization of Security Competitions (CTFs).** Throughout my career, I have been involved in the organization of numerous security competitions, typically called Capture the Flag Competitions (CTFs, in short).
   (a) ACSAC CTF, 2024.
   (b) DEF CON CTF (in 2019, 2020, 2021, and 2024): The largest CTF competition in the world with more than 500 teams participating online each year in the Qualification Event and 16 teams participating in-person to the Final Event.
   (c) UCSB iCTF (in 2024): Organized by the ACTION NSF AI Institute, the Shellphish CTF team, and the UCSB Women in Computer Science group. This competition focused on high-school and undergraduate participants.
   (d) b01lers CTF (in 2022 and 2023): The Capture the Flag competitions organized by b01lers, the Purdue CTF team.
2. **Qualified to the Final Event of the DARPA/ARPA-H AI Cyber Challenge (AIxCC).**

Funding

1. Agency/Title of Grant:	United States Military Academy West Point: Investigating Private Data Collection on Edge Devices and Its Impact on the Military Population
2. Duration of Funding:	09/01/2024 - 08/31/2025
3. Total Amount of Award:	$117,532
4. Your Role:	PI; award made to Purdue
1. Agency/Title of Grant:	Lockheed Martin Corp.: An End-to-end Pipeline for Lifting and Patching DNN Binaries for Adversarial and Defensive Applications
2. Duration of Funding:	04/1/2024 - 12/15/2024
3. Total Amount of Award:	$121,000
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	DARPA – Artificial Intelligence Cyber Challenge (AIxCC): Gift
2. Duration of Funding:	03/15/2024 - open ended
3. Total Amount of Award:	$50,000
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	DARPA – Faithful Integrated Reverse-Engineering and Exploitation (FIRE): FIREFLY: A Cyber-Physical Framework for Scalable CPS Modeling and Simulation
2. Duration of Funding:	11/30/2023 - 05/29/2027
3. Total Amount of Award:	$6,500,087
4. Your Role:	CO-PI; award made to Purdue

1. Agency/Title of Grant:	Lockheed Martin Corp.: Towards an End-to-end Pipeline for Lifting and Patching DNN Binaries for Adversarial and Defensive Applications
2. Duration of Funding:	10/01/2023 - 12/22/2023
3. Total Amount of Award:	$65,000
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	DOE: Enabling Secure and Resilient XFC: A Software/Hardware-security Co-design Approach
2. Duration of Funding:	06/01/2023 - 12/31/2023
3. Total Amount of Award:	$80,000
4. Your Role:	CO-PI; subcontract from Virginia Tech

1. Agency/Title of Grant:	Google: Gift: Android Security and PrIvacy REsearch (ASPIRE) Award, Exploring the Implementation and Usage of Android Storage APIs
2. Duration of Funding:	10/15/2023 - open ended
3. Total Amount of Award:	$90,000
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	ONR: Semantic Decompilation of Deep Neural Network Binaries and Its Adversarial and Defensive Implications
2. Duration of Funding:	01/01/2023 - 12/31/2025
3. Total Amount of Award:	$750,655
4. Your Role:	CO-PI; award made to Purdue

1. Agency/Title of Grant:	Google: Gift: Android Security and PrIvacy REsearch (ASPIRE) Award, Improving the Security and Usability of the Wear OS Permission Model
2. Duration of Funding:	10/15/2022 - open ended
3. Total Amount of Award:	$80,850
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	ONR: An Integrated Toolkit for IoT Protocol Dialecting with Formal Verification
2. Duration of Funding:	08/01/2022 - 07/31/2023
3. Total Amount of Award:	$620,000
4. Your Role:	CO-PI; award made to Purdue

1. Agency/Title of Grant:	Google: Gift: Android Security and PrIvacy REsearch (ASPIRE) Award, Improving the Usability of Android APIs for Conformity of Standard Security Practices
2. Duration of Funding:	10/15/2021 - open ended
3. Total Amount of Award:	$100,000
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	DARPA – Assured Micropatching (AMP): DICER: Directed Compilation for Assured Patching
2. Duration of Funding:	08/05/2020 - 08/04/2024
3. Total Amount of Award:	$3,869,685
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	Google: Gift: Google Security Rewards Program
2. Duration of Funding:	04/15/2020 - open ended
3. Total Amount of Award:	$8,000
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	ONR: Bringing Fuzzing to the Cyber-Physical World
2. Duration of Funding:	01/15/2020 - 01/14/2023
3. Total Amount of Award:	$799,877
4. Your Role:	CO-PI; award made to Purdue

1. Agency/Title of Grant:	DARPA – Computers and Humans Exploring Software Security (CHESS): CHECRS: Cognitive Human Enhancements for Cyber Reasoning Systems
2. Duration of Funding:	09/01/2019 - 03/31/2023
3. Total Amount of Award:	$705,103
4. Your Role:	CO-PI; subcontract from Arizona State University

1. Agency/Title of Grant:	NSF: CRII Award: SaTC: Vetting and Improving the Usage of Trusted Execution Environments for Authentication in Mobile Devices
2. Duration of Funding:	06/01/2019 - 05/31/2021
3. Total Amount of Award:	$174,972
4. Your Role:	PI; award made to Purdue

1. Agency/Title of Grant:	DARPA – Computers and Humans Exploring Software Security (CHESS): CHECRS: Cognitive Human Enhancements for Cyber Reasoning Systems
2. Duration of Funding:	11/29/2018 - 08/31/2019
3. Total Amount of Award:	$175,838
4. Your Role:	CO-PI; subcontract from Arizona State University

Graduated MS and PhD Students

1. Muhammad Ibrahim, PhD requirements completed in September 2024.
   PhD Thesis Title: Analyzing Secure and Attested Communication in Mobile Devices
2. Ruoyu Wu, PhD Graduated Summer 2024 (co-advised with Prof. Dongyan Xu).
   PhD Thesis Title: Towards Reverse Engineering Deep Neural Networks on Edge Devices
   Current Position: Google (Software Engineer)
3. Hyungsub Kim, PhD Graduated Fall 2023 (co-advised with Prof. Dongyan Xu).
   PhD Thesis Title: Defeating Cyber and Physical Attacks in Robotic Vehicles
   Current Position: Tenure-track Assistant Professor at IU Bloomington
4. Jianliang Wu, PhD Graduated Summer 2023 (co-advised with Prof. Dongyan Xu).
   PhD Thesis Title: Securing IoT Systems via Protocol Formal Analysis and Debloating
   Current Position:Tenure-track Assistant Professor at Simon Fraser University
5. Prashast Srivastava, PhD Graduated Spring 2023 (co-advised with Prof. Mathias Payer).
   PhD Thesis Title: Practical Methods for Dynamic Software Analysis of Real-world Systems
   Current Position: PostDoc working with Prof. Suman Jana at Columbia University
6. Rowan Brock Hart, MS Graduated Fall 2022.
   MS. Thesis Title: Fuzzing Deeper Logic with Impeding Function Transformation
   Current Position: Intel (Security Engineer)

Teaching

Semester & Year	Course Number	Title of Course	Number of Students	Student Classification
At Purdue:				
Fall 2024	CS39700	Honors Seminar	55	Undergraduate
Fall 2024	CS42600	Computer Security	61	Undergraduate
Spring 2024	CS52700	Software Security	29	Graduate
Fall 2023	CS39700	Honors Seminar	31	Undergraduate
Fall 2023	CS49000-SWS	Software Security	10	Undergraduate
Spring 2023	CS52700	Software Security	29	Graduate
Fall 2022	CS39700	Honors Seminar	19	Undergraduate
Fall 2022	CS49000-SWS	Software Security	13	Undergraduate
Spring 2022	CS52700	Software Security	32	Graduate
Fall 2021	CS39700	Honors Seminar	33	Undergraduate
Fall 2021	CS59200-AST	Automated Security Testing	14	Graduate
Spring 2021	CS52700	Software Security	29	Graduate
Fall 2020	CS59100-SEC	CERIAS Security Seminar	15	Graduate
Spring 2020	CS52700	Software Security	21	Graduate
Fall 2019	CS59000-MSS	Mobile Systems and Smartphone Security	10	Graduate
At the University of Iowa:				
Spring 2019	CS4980	Mobile Systems and Smartphone Security	21	Graduate
Fall 2018	CS3620	Operating Systems	53	Undergraduate

Table 1: Teaching assignments.
CS39700 is a zero-credit course, CS59100-SEC is a 1 credit course, all other courses are 3 credit hours.

Service

1 University

- Faculty Advisor of "B01lers" (Purdue Capture the Flag Student Organization), 2019 – present.
- Instructor responsible for CS591-SEC "CERIAS Security Seminar", 2020.

2 Professional

- NSF SAtC Panelist: 2024.
- Program Committee Chair: Workshop on Binary Analysis Research (BAR) at the Network & Distributed System Security Symposium (NDSS), 2020.
- Program Committee Co-Chair: Workshop on Binary Analysis Research (BAR) at the Network & Distributed System Security Symposium (NDSS), 2019.
- Session Chair: NDSS 2024, VehicleSec 2024.
- Program Committee for IEEE Symposium on Security and Privacy (S&P): 2020, 2021, 2022, 2024, 2025.
- Program Committee for USENIX Security Symposium (UsenixSEC): 2020, 2021, 2024, 2025.
- Program Committee for Network & Distributed System Security Symposium (NDSS): 2020, 2021, 2023.
- Program Committee for ACM Conference on Computer and Communications Security (CCS): 2020, 2023.
- Program Committee for the Annual Computer Security Applications Conference (ACSAC): 2024.
- Program Committee for International Symposium on Research in Attacks, Intrusions and Defenses (RAID): 2023, 2024.
- Program Committee for ACM ASIA Conference on Computer and Communications Security (AsiaCCS): 2021.
- Program Committee for European Symposium on Research in Computer Security (ESORICS): 2020, 2023.
- Program Committee for ACM Conference on Data and Application Security and Privacy (CODASPY): 2024.
- Program Committee for Symposium on Vehicle Security and Privacy (VehicleSec): 2023, 2024.
- Program Committee for European Workshop on Systems Security (EuroSec): 2023, 2024.
- Program Committee for Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA): 2022.
- Program Committee for Workshop on Offensive Technologies (WOOT): 2022, 2024.
- Program Committee for Workshop on the Internet of Safe Things: 2022.
- Program Committee for International Workshop on Security in Mobile Technologies (SecMT): 2020.
- Program Committee for Workshop on Binary Analysis Research (BAR) at NDSS: 2019, 2020, 2021, 2022, 2023.
- Paper Shepherding: ACSAC 2024, RAID 2024, ACSAC 2023, RAID 2023, USENIX 2022, NDSS 2022, S&P 2019.
- Journal Reviewer for Computer & Security: 2024.
- Journal Reviewer for ACM Computing Surveys Review (CSUR): 2020, 2023.

- Journal Reviewer for IEEE Transactions on Knowledge and Data Engineering (TKDE): 2021.
- Journal Reviewer for IEEE Transactions on Mobile Computing (TMC): 2020.
- Journal Reviewer for IEEE Transactions on Dependable and Secure Computing (TDSC): 2018.