Earlence T. Fernandes

CONTACT INFORMATION

Department of Computer Science and Engineering
9500 Gilman Drive
La Jolla, CA 92093, USA

(734) 709-4334
efernandes@ucsd.edu
earlence.com

RESEARCH INTERESTS

Computer systems security; Adversarial machine learning from a systems perspective.

EMPLOYMENT

University of California, San Diego
Assistant Professor of Computer Science **July 2022 - present**

University of Wisconsin-Madison
Assistant Professor of Computer Science **Aug 2019 - July 2022**

University of Washington, Seattle
Research Associate with Prof. Tadayoshi Kohno **June 2017 - June 2019**

Microsoft Research, Redmond, WA
Research Intern with Jaeyeon Jung, Oriana Riva, Suman Nath **Summers 2014-2016**

Vrije Universiteit, Amsterdam, The Netherlands
Scientific Programmer with Prof. Bruno Crispo and Prof. Mauro Conti **Oct 2010 - June 2012**

Accenture, Pune, India
Senior Programmer **Aug 2009 - Aug 2010**

EDUCATION

University of Michigan, Ann Arbor

Ph.D., Computer Science and Engineering, April 2017

- Advisor: Prof. Atul Prakash
- Committee: Prof. Z. Morley Mao, Prof. J. Alex Halderman, Prof. Florian Schaub
- Thesis: Securing Personal IoT Platforms Through Systematic Analysis and Design

M.S.E., Computer Science and Engineering, May 2014

University of Pune, India

B.E. (Bachelor of Engineering, Computer Engineering), 9^{th} rank out of ~2000 students, June 2009

AWARDS

- Google Research Scholar Award for Stateful Authorization (2024).
- NSF CAREER Award for Secure Trigger-Action Systems (2022).
- Amazon Research Award for Verifiable Distributed Computation (2022).
- Facebook Research Award for Trust in AR/VR (joint with R. Chatterjee and Y. Zhao, 2021).
- IEEE SecDev 2018 Best Research Paper Award.
- IEEE S&P 2016 Distinguished Practical Paper Award.
- UMich PhD Fellowship 2012.

BROADER IMPACT

- The U.S. Stop sign used in our experiments for the CVPR 2018 paper is on display at the Science Museum in London (and is now a part of their permanent collection on self-driving car security).
- Our CVPR 2018 paper on physical adversarial machine learning was cited as one of the motivating factors for the DARPA GARD program.
- Briefed the Union Cycliste Internationale (UCI; the governing body for the sport of professional cycling such as the Tour de France) on technology and wireless fraud, following the publication of our WOOT 2024 paper on a security analysis of Shimano wireless gear shifting.

- Worked with Shimano (largest bicycle component manufacturer in the world) to address flaws in their wireless gear shifting product; led to a worldwide deployment of software fixes.
- Our work on fun-tuning attacks (IEEE S&P 2025 paper) led to mitigations in Google's LLM fine-tuning infrastructure.
- Our work on optimization-based obfuscated adversarial prompts (`https://imprompter.ai/`) led to mitigations in the mistral.ai LeChat agent.
- Our security analysis of Slack private messages (USENIX Security 2022 paper) received a bug bounty payout.
- Invited expert for a DARPA ISAT Study on AI Cyber-User-In-The-Loop attacks.
- Briefed the JASONs (DARPA/DoD) for a summer study on AI Security.
- Briefed U.S. Congressperson Pramila Jayapal on IoT security.
- Briefed the National Academies on AI Security.
- Briefed the FTC on AI Security.

Conference Papers

Google Scholar Profile: `https://scholar.google.com/citations?user=OSPeHGAAAAAJ&hl=en`

1. Fun-tuning: Characterizing the Vulnerability of Proprietary LLMs to Optimization-based Prompt Injection Attacks via the Fine-Tuning Interface.
   Andrey Labunets, Nishit Pandya, Ashish Hooda, Xiaohan Fu, **Earlence Fernandes.** *46th IEEE Symposium on Security and Privacy*, (Oakland 2025), San Francisco, CA, May 2025. Acceptance Rate 14.8%.
2. Stateful Least Privilege Authorization for the Cloud.
   Leo Cao, Luoxi Meng, Deian Stefan, **Earlence Fernandes.** *33rd USENIX Security Symposium,* (USENIX Sec 2024), Philadelphia, PA, August 2024. Acceptance Rate: 19.1%.
3. Scalable Metadata Hiding for Privacy-Preserving IoT Systems.
   Yunang Chen, David Heath, Rahul Chatterjee, **Earlence Fernandes.** *Proceedings on Privacy Enhancing Technologies Symposium,* (PoPETS 2024), Bristol, UK, July 2024. Acceptance Rate: 21%.
4. MakeShift: Security Analysis of Shimano Di2 Wireless Gear Shifting in Bicycles.
   Maryam Motallebighomi, **Earlence Fernandes**, Aanjhan Ranganathan. *USENIX WOOT Conference on Offensive Technologies,* (WOOT 2024), Philadelphia, PA, Aug 2024, Acceptance Rate: 35%.
5. Experimental Security Analysis of Sensitive Data Access by Browser Extensions.
   Rishabh Khandelwal, Asmit Nayak, **Earlence Fernandes**, Kassem Fawaz. *ACM Web Conference,* (WWW 2024), Singapore, May 2024, Acceptance Rate: 20.2%.
6. Experimental Analyses of the Physical Surveillance Risks in Client-Side Content Scanning.
   Ashish Hooda, Andrey Labunets, Tadayoshi Kohno, **Earlence Fernandes.** *28th Network and Distributed Security Symposium,* (NDSS 2024), San Diego, CA, Feb 2024, Acceptance Rate: 19.9%.
7. Architecting Trigger-Action Platforms for Security, Performance and Functionality.
   Deepak Sirone Jegan, Michael Swift, **Earlence Fernandes**. *28th Network and Distributed Security Symposium,* (NDSS 2024), San Diego, CA, Feb 2024, Acceptance Rate: 19.9%.
8. SkillFence: A Systems Approach to Practically Mitigating Voice-Based Confusion Attacks.
   Ashish Hooda, Matt Wallace, Kushal Jhunjhunwala, **Earlence Fernandes**, Kassem Fawaz. *ACM International Conference on Ubiquitous Computing*, (UbiComp/IMWUT 2022).
9. Experimental Security Analysis of the App Model in Collaboration Platforms.
   Yunang Chen, Yue Gao, Nick Ceccio, Rahul Chatterjee, Kassem Fawaz. **Earlence Fernandes**. *31st USENIX Security Symposium*, (USENIX Sec 2022), Boston, MA, Aug 2022, Acceptance Rate: 18.1%.

10. Practical Data Access Minimization in Trigger-Action Platforms.
Yunang Chen, Mohannad Alhanahnah, Andrei Sabelfeld, Rahul Chatterjee, **Earlence Fernandes**. *31st USENIX Security Symposium*, (USENIX Sec 2022), Boston, MA, Aug 2022, Acceptance Rate: 18.1%.

11. GRAPHITE: A Practical Framework for Generating Automatic Physical Adversarial Machine Learning Attacks.
Ryan Feng, Neal Mangaokar, Jiefeng Chen, **Earlence Fernandes**, Somesh Jha, Atul Prakash. *7th IEEE European Symposium on Security and Privacy* (EuroS&P 2022), Genoa, June 2022.

12. SoK: Authentication in Augmented and Virtual Reality.
Sophie Stephenson, Bijeeta Pal, Stephen Fan, **Earlence Fernandes**, Yuhang Zhao, Rahul Chatterjee. *43rd IEEE Symposium on Security and Privacy* (Oakland 2022), San Francisco, May 2022.

13. SoK: Context Sensing for Access Control in the Adversarial Home IoT.
Weijia He, Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, **Earlence Fernandes**, Josiah Hester, Blase Ur. *6th IEEE European Symposium on Security and Privacy* (EuroS&P 2021), Online Event, Sep 2021.

14. Invisible Perturbations: Physical Adversarial Examples Exploiting the Rolling Shutter Effect.
Athena Sayles, Ashish Hooda, Mohit Gupta, Rahul Chatterjee, **Earlence Fernandes**. *Computer Vision and Pattern Recognition* (CVPR 2021), Online Event, June 2021 (arXiv:2011.13375), Acceptance Rate: 23.7%.

15. Data Privacy in Trigger-Action Systems.
Yunang Chen, Amrita Roy Chowdhury, Ruizhe Wang, Andrei Sabelfeld, Rahul Chatterjee, **Earlence Fernandes.** *42nd IEEE Symposium on Security and Privacy* (Oakland 2021), Online Event, May 2021, Acceptance Rate: 12.1%.

16. Sequential Attacks on Kalman filter-based Forward Collision Warning Systems.
Yuzhe Ma, Jon Sharp, Ruizhe Wang, **Earlence Fernandes**, Xiaojin Zhu. *35th AAAI Conference on Artificial Intelligence* (AAAI 2021), Online Event, Feb 2021, Acceptance Rate: 21.4%.

17. Tyche: A Risk-Based Permission Model for Smart Homes.
Amir Rahmati, **Earlence Fernandes**, Kevin Eykholt, Atul Prakash. *3rd IEEE Cybersecurity Development Conference,* (SecDev 2018), Boston, MA, Oct 2018.
Best Research Paper Award.

18. Rethinking Authentication and Access Control for the Home Internet of Things.
Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Durmuth, **Earlence Fernandes**, Blase Ur. *27th USENIX Security Symposium,* (USENIX Sec 2018), Baltimore, MD, Aug 2018, Acceptance Rate: 19%.

19. Robust Physical-World Attacks on Deep Learning Visual Classification.
Kevin Eykholt, Ivan Evtimov, **Earlence Fernandes**, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno, Dawn Song. *Computer Vision and Pattern Recognition* (CVPR 2018), Salt Lake City, UT, June 2018 (supersedes arXiv:1707.08945), Acceptance Rate: 29.6%.

20. Is Tricking a Robot Hacking?
Ryan Calo, Ivan Evtimov, **Earlence Fernandes**, Tadayoshi Kohno, David O'Hair. *Proceedings of WeRobot*, Stanford, CA, April 2018 (This is an inter-disciplinary conference at the intersection of technology law and robotics).

21. Decentralized Action Integrity for Trigger-Action IoT Platforms.
Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash. *22nd Network and Distributed Security Symposium,* (NDSS 2018), San Diego, CA, February 2018, Acceptance Rate: 21.4%.

22. Heimdall: A Privacy-Respecting Implicit Preference Collection Framework.
Amir Rahmati, **Earlence Fernandes**, Kevin Eykholt, Xinheng Chen, Atul Prakash. *15th ACM International Conference on Mobile Systems, Applications, and Services,* (MobiSys 2017), Niagara Falls, NY, June 2017, Acceptance Rate: 18%.

23. ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms.
Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, **Earlence Fernandes**, Z. Morley Mao, Atul Prakash. *21st Network and Distributed Security Symposium,* (NDSS 2017), San Diego, CA, Feb 2017, Acceptance Rate: 16%.

24. Applying the Opacified Computation Model to Enforce Information Flow Policies in IoT Applications.
Amir Rahmati, **Earlence Fernandes**, and Atul Prakash. *1st IEEE Cybersecurity Development Conference,* (SecDev 2016), Boston, MA, Nov 2016, Acceptance Rate: 38.6%.

25. Appstract: On-The-Fly App Content Semantics With Better Privacy.
Earlence Fernandes, Oriana Riva, and Suman Nath. *22nd Annual Intl. Conf. on Mobile Computing and Networking,* (MobiCom 2016), New York, NY, Oct 2016, Acceptance Rate: 14%.

26. FlowFence: Practical Data Protection for Emerging IoT Application Frameworks.
Earlence Fernandes, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti, Atul Prakash. *25th USENIX Security Symposium,* (USENIX Sec 2016), Austin, TX, Aug 2016, Acceptance Rate: 15.4%.

27. Security Analysis of Emerging Smart Home Applications.
Earlence Fernandes, Jaeyeon Jung, Atul Prakash. *37th IEEE Symposium on Security and Privacy,* (S&P 2016), San Jose, CA, May 2016, Acceptance Rate: 13.3%.
Distinguished Practical Paper Award.

28. Android UI Deception Revisited: Attacks and Defenses.
Earlence Fernandes, Qi Chen, Justin Paupore, Georg Essl, J. Alex Halderman, Z. Morley Mao, Atul Prakash. *20th Intl. Conf. on Financial Cryptography and Data Security,* (FC 2016), Barbados, Feb 2016, Acceptance Rate: 26%.

29. Decomposable Trust for Android Applications.
Earlence Fernandes, Ajit Aluri, Alexander Crowell, Atul Prakash. *45th Annual IEEE/IFIP Intl. Conf. on Dependable Systems and Networks,* (DSN 2015), Rio de Janeiro, Brazil, June 2015, Acceptance Rate: 21.8%.

30. MOSES: Supporting Operation Modes on Smartphones.
Giovanni Russello, Mauro Conti, Bruno Crispo, **Earlence Fernandes**. *17th ACM Symposium on Access Control Models and Technologies,* (SACMAT 2012), Newark, NJ, Jun 2012, Acceptance Rate: 26%.

31. YAASE: Yet Another Android Security Extension.
Giovanni Russello, Bruno Crispo, **Earlence Fernandes**, Yury Zhauniarovich. *3rd IEEE Intl. Conf. on Privacy, Security, Risk and Trust,* (PASSAT 2011), Boston, MA, Oct 2011.

Journal Papers

1. Program Analysis of Commodity IoT Applications for Security and Privacy: Opportunities and Challenges.
Z. Berkay Celik, **Earlence Fernandes**, Eric Pauley, Gang Tan, Patrick McDaniel. ACM Computing Surveys, (CSUR 2019).

2. Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?
Earlence Fernandes, Amir Rahmati, Kevin Eykholt, Atul Prakash. *IEEE Security and Privacy: Systems Attacks and Defenses*, (S&P Magazine 2017), (arXiv:1705.08522)

3. The Security Implications of Permission Models in Smart Home Application Frameworks.
Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash. *IEEE Security and Privacy Volume 15 Issue 2,* (S&P Magazine 2017).

4. MOSES: Supporting and Enforcing Security Profiles on Smartphones.
   Yury Zhauniarovich, Giovanni Russello, Mauro Conti, Bruno Crispo, **Earlence Fernandes**. *IEEE Transactions on Dependable and Secure Computing,* (TDSC 2014).
5. FM 99.9 Radio Virus: Exploiting FM Radio Broadcasts for Malware Deployment.
   Earlence Fernandes, Bruno Crispo, Mauro Conti. *IEEE Transactions on Information Forensics and Security,* (TIFS 2013).
6. CRePE: A system for enforcing fine-grained Context-related Policies on Android.
   Mauro Conti, Bruno Crispo, **Earlence Fernandes**, Yury Zhauniarovich. *IEEE Transactions on Information Forensics and Security,* (TIFS 2012).

Workshop Papers

1. Analyzing the Interpretability Robustness of Self-Explaining Models.
   Haizhong Zheng, **Earlence Fernandes**, Atul Prakash. *Security and Privacy of Machine Learning Workshop* (co-located with ICML 2019), Long Beach, CA, June 2019.
2. Analysis of the Susceptibility of Smart Home Programming Interfaces to End User Error.
   Mitali Palekar, **Earlence Fernandes**, Franziska Roesner. *IEEE Workshop on the Internet of Safe Things,* (SafeThings 2019), San Francisco, CA, May 2019.
3. Physical Adversarial Examples for Object Detectors.
   Kevin Eykholt, Ivan Evtimov, **Earlence Fernandes**, Bo Li, Amir Rahmati, Florian Tramer, Atul Prakash, Tadayoshi Kohno, Dawn Song. 12th USENIX Workshop on Offensive Technologies (WOOT 2018), Baltimore, MD, August 2018 (supersedes arXiv:1712.08062).
4. The State of Physical Attacks on Deep Learning Systems.
   Earlence Fernandes. *2018 USENIX Summit on Hot Topics in Security,* (HotSec 2018), Baltimore, MD, August 2018.
5. Cybersecurity in the Smart City.
   Yuyi Taylor, Guy Verrier, Yuan Tian, **Earlence Fernandes**, Tadayoshi Kohno. *2018 USENIX Summit on Hot Topics in Security,* (HotSec 2018), Baltimore, MD, August 2018.
6. Securing Trigger-Action Platforms.
   Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash. *2017 USENIX Summit on Hot Topics in Security,* (HotSec 2017), Vancouver, BC, August 2017 (arXiv:1707.00405).
7. Support for Security and Safety of Programmable IoT Systems.
   Alex Gyori, **Earlence Fernandes**, Amir Rahmati, Atul Prakash, Darko Marinov. *ISSTA 2017 Workshop on Testing Embedded and Cyber-Physical Systems,* (TECPS 2017), Santa Barbara, CA, July 2017.
8. My OS ought to know me better: In-app Behavioral Analytics as an OS service.
   Earlence Fernandes, Oriana Riva, Suman Nath. *15th Workshop on Hot Topics in Operating Systems,* (HotOS XV), Kartause Ittingen, Switzerland, May 2015, Acceptance Rate: 31.8%.
9. Practical Always-On Taint Tracking on Mobile Devices.
   Justin Paupore, **Earlence Fernandes**, Sankardas Roy, Xinming Ou, Atul Prakash. *15th Workshop on Hot Topics in Operating Systems,* (HotOS XV), Kartause Ittingen, Switzerland, May 2015, Acceptance Rate: 31.8%.
10. OASIS: Operational Access Sandboxes for Information Security.
    Mauro Conti, **Earlence Fernandes**, Justin Paupore, Atul Prakash, Daniel Simionato. (alphabetical order) *4th ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices,* (SPSM 2014), Scottsdale, AZ, Nov 2014.
11. Beyond Instruction Level Taint Propagation.
    Beng Heng Ng, **Earlence Fernandes**, Ajit Aluri, David Velazquez, James Yang, Atul Prakash. *6th ACM European Workshop on Systems Security,* (EuroSec 2013), Prague, Czech Republic, Apr 2013.

Books

1. Instant Android Systems Development, **Earlence Fernandes**, *Packt Publishers, UK, 2013.*

Patents

- System and Method for Extracting and Sharing Application-Related User Data.
  Oriana Riva, Suman Nath, Doug Burger, **Earlence Fernandes**. *U.S. Patent US11169991B2*
- De-siloing Applications for Personalization and Task Completion Services.
  Oriana Riva, Suman Nath, Doug Burger, **Earlence Fernandes**. *U.S. Patent US10028116B2*
- Method and Apparatus for Improved Security in Trigger Action Platforms.
  Yunang Chen, Mohannad Alhanahnah, Andrei Sabelfeld, Rahul Chatterjee, **Earlence Fernandes**. *U.S. Patent US20220394043A1*

Miscellany

1. DEMO: Sequential Attacks on Forward Collision Warning.
   Yuzhe Ma, Jon Sharp, Ruizhe Wang, **Earlence Fernandes**, Jerry Zhu. AutoSec 2021 (co-located with NDSS), Feb 2021.

tr- IFTTT vs. Zapier: A Comparative Study of Trigger-Action Programming Frameworks.
Amir Rahmati, **Earlence Fernandes**, Jaeyeon Jung, Atul Prakash. Preprint (arXiv:1709.02788), Sep 2017.

tr- Per-App Profiles with AppFork: The Security of Two Phones with the Convenience of One.
Temitope Oluwafemi, **Earlence Fernandes**, Oriana Riva, Franziska Roesner, Suman Nath, Tadayoshi Kohno. *Microsoft Research Technical Report, MSR-TR-2014-153, December 2014.*

tr- TIVOs: Trusted Visual I/O Paths for Android.
Earlence Fernandes, Qi Alfred Chen, Justin Paupore, Georg Essl, J. Alex Halderman, Z. Morley Mao, Atul Prakash. *University of Michigan, Technical Report CSE-TR-586-14.*

invited- The confinement problem: 40 years later.
Alexander Crowell, Beng Heng Ng, **Earlence Fernandes**, Atul Prakash. *JIPS 9, 2013.*

poster- Anception: Hybrid Virtualization for Android Applications.
Earlence Fernandes, Ajit Aluri, Alexander Crowell, Atul Prakash. *USENIX Security, 2013.*

poster- Demonstrating the effectiveness of MOSES for separation of execution modes.
Giovanni Russello, Mauro Conti, Bruno Crispo, **Earlence Fernandes**, Yury Zhauniarovich. *ACM CCS, 2012.*

Invited Talks

- "AI Systems Security," July 2025, at University of Toronto (Host: Nicolas Papernot).
- "AI Systems Security," May 2025, at UC Santa Cruz (Host: Alvaro Cardenas).
- "AI Systems Security," May 2025, at UC Riverside (Host: Trent Jaeger).
- "AI Systems Security," Apr 2025, at Microsoft.
- "AI Systems Security," Feb 2025, ***Keynote*** at the GenAI Summit.
- "Least Privilege Authorization for the Internet," Nov 2024, at University of California, Irvine (Host: Gene Tsudik).
- "Least Privilege Authorization for the Internet," Sep 2024, at University of Toronto (Host: Davie Lie).
- "Least Privilege Authorization for the Internet," Aug 2024, at Stony Brook University (Host: Amir Rahmati).
- "Rethinking the role of the Cloud in IoT Services," Jul 2024, at Dagstuhl Seminar on IoT Security and Privacy, Germany (Organizers: Gene Tsudik, Wenyuan Xu, Alexandra Dimitrienko, Bruno Crispo).
- "Experimental Analyses of the Surveillance Risks in Client-side Content Scanning," Mar 2024, at University of Padova, Italy (Host: Mauro Conti) and Chalmers University of Technology, Gothenburg, Sweden (Host: Andrei Sabelfeld).
- "End to End Computer Security for Evolved Systems," Feb 2023, at IIT Bombay, India (Host: Manoj Prabhakaran).
- "End to End Computer Security for Evolved Systems," June 2022, at University of Toronto, Canada (Host: David Lie).

- "Tailored Privilege for Trigger-Action Systems via Garbled Circuits," Apr 2022, at Carnegie Mellon University, USA (Host: Bryan Parno).
- "Tailored Privilege for Trigger-Action Systems," Mar 2022, at Microsoft Research Redmond, USA (Host: Marcus Peinado).
- "Decentralized Action Integrity for Trigger-Action Platforms," Nov 2020, at the Chalmers University of Technology, Gothenburg, Sweden (Host: Andrei Sabelfeld).
- "Decentralized Action Integrity for Trigger-Action Platforms," Nov 2020, at the Ohio State University, Ohio, USA (Host: Zhiqiang Lin).
- "Physical Attacks on Object Detectors," June 2020, at the Workshop on Adversarial Machine Learning in Computer Vision co-located with CVPR, Seattle, WA, USA.
- "Decentralized Action Integrity for Trigger-Action IoT Platforms," Oct 2019, at the Triangle Area Privacy and Security Day, Duke University, NC, USA.
- I was invited to brief the JASON defense advisory group for the 2018 summer study. The JASONs are a group of elite scientists that the U.S. Department of Defense contracts with to solve challenging problems. JASON members include physicists, biologists, mathematicians, chemists, and computer scientists. Over the years, 11 Nobel prize winners have been members. See `https://en.wikipedia.org/wiki/JASON_(advisory_group)` for more details.
- "Physical Attacks on Deep Learning Systems," May 2018, at 2nd ARO/IARPA Workshop on Adversarial Learning, College Park, MD, USA.
- "Computer Security and Privacy for the Physical World," Nov 2017 ***Keynote*** at IoT Security and Privacy Workshop co-located with CCS 2017, and Sep 2017 invited talk at University of California Berkeley, USA (Host: Dawn Song).
- "Robust Physical-World Attacks on Deep Learning Models," Sep 2017, Stanford University, USA.
- "IoT Security: What, Why, and How," May 2017, IEEE Mobile Security Technologies (MoST) workshop affiliated with IEEE S&P 2017, San Jose, CA, USA.
- "Securing IoT Platforms through Systematic Analysis and Design," Nov 2016, University of Illinois at Urbana-Champaign, USA (Host: Darko Marinov).
- "Modern Cyber-Physical Systems Security: Attacks and Defenses," Aug 2016, University of Washington, Seattle, USA (Host: Yoshi Kohno).
- "FlowFence: Practical Data Protection for Emerging IoT Application Frameworks," Aug 2016, Microsoft Research, Redmond, USA.
- "Security Analysis of Emerging Smart Home Applications," May 2016, CMU Silicon Valley, USA (Host: Patrick Tague).
- "Towards a Safer IoE: Detecting and Correcting Abnormal Interactions between Things in Smart Homes," Mar 2016, University of Illinois at Urbana-Champaign, and Qualcomm Research, San Diego, USA.
- "SmartThings Security Analysis," Aug 2015, Microsoft Research, Redmond, USA.
- "Appstract: On-device behavioral analytics," Aug 2014, Microsoft Research, Redmond, USA.
- "Trusted Visual I/O Paths," Aug 2014, Microsoft Research, Redmond, USA.

Academic Service

- **Funding agency reviewing:** 2023-2024 NSF CAREER panel.
- **PC co-chair**: IEEE Workshop on Internet of Safe Things (co-located with IEEE S&P) 2021, ACM Workshop on CPS and IoT Security (co-located with CCS) 2022, IEEE Workshop on Secure Generative AI Agents (SAGAI, co-located with IEEE S&P 2025).
- **PC Member**: USENIX Security 2018-2023 and 2025, Oakland 2023-2025, CCS 2020, NDSS 2020, IoT S&P 2018 (co-located with SIGCOMM 2018), Machine Learning and Computer Security Workshop 2017 (co-located with NIPS 2017), IoT S&P 2017 (co-located with CCS 2017), SafeThings 2017 (co-located with SenSys 2017), SecureComm 2017, IEEE MoST 2017 (co-located with S&P 2017), IEEE Security and Privacy (S&P) 2017 Shadow Committee, SecCPS Workshop 2017 (co-located with IEEE HASE 2017), SEMS 2017 (co-located with Euro S&P 2017), ICISS 2014-2016.
- **External Reviewer**: UbiComp/IMWUT 2018, USENIX Security 2017, ACM WiSec 2017, IEEE Transactions on Mobile Computing 2017, CHI 2017, NDSS 2017, IEEE DSN 2016, DIMVA 2015, IEEE Transactions on Computers 2013.

- **Publicity Co-Chair**: Workshop on Security for Embedded and Mobile Systems (SEMS; co-located with EuroSP 2017).
- **Invited Panelist**: Security at University of Michigan IT (SUMIT) conference 2016.
- **Broadening Participation in Computing**: Served as a mentor for the Wisconsin Science and Computing Emerging Research Stars (WISCERS) program (2021-2022). It is a system to increase research participation of undergraduate students from historically under-represented groups by pairing them with mentors and graduate student guides. Served as a project mentor for ERSP at UCSD (2023).

Current PhD Students

- Andrey Labunets
- Luoxi Meng
- Nishit Pandya

Graduated Students and Last known position

- Xiaohan Fu (co-advised with Rajesh Gupta), PhD (2025). Research Engineer at Gray Swan AI.
- Yunang Chen (co-advised with Rahul Chatterjee), PhD (2023). Engineer at Google.
- Leo Cao, MS (2024). PhD Student at UW Madison.
- Ashish Hooda, MS (2021). PhD from UW Madison, Researcher at DeepMind.
- Jon Sharp, MS (2020). Software Engineer at Amazon.
- Tyler Gu, BS (2021). PhD student at UIUC.
- Ruizhe Wang, BS (2021). Winner of the DeWitt Scholarship and honorable mention at the CRA outstanding undergraduate researcher awards. MS/PhD student at Univ. of Waterloo.
- Luna Sayles, MS (2021).

Past Mentoring Experience (prior to tenure-track)

- Ivan Evtimov, University of Washington Ph.D. student (adversarial deep learning).
- Mitali Palekar, University of Washington B.S. student (trigger-action programming).
- Zhi Qian Seah, University of Michigan, Bachelor Thesis Technical Advisor ("Partitioning the Android System Services").

Teaching

- CSE 291 (UCSD): LLM Security.
- CSE 227 (UCSD): Graduate Computer Security.
- CSE 127 (UCSD): Introduction to Computer Security.
- CSE 291 (UCSD): Secure Systems Construction.
- CS 642 (UW Madison): Introduction to Computer Security.
- CS 839/782 (UW Madison): Advanced Computer Security and Privacy.
- CSE 590Y (UW Seattle): Graduate Seminar in Adversarial Deep Learning.
- EECS 588 (Michigan): Graduate Course in Computer and Network Security.

Press Coverage

Much of my work has been covered in the media: Wired, Schneier on Security, The Verge, Gizmodo, Ars Technica, CNET, Mashable, Detroit Free Press, ZDNet, Yahoo News.

Consulting

I have consulted on a variety of security and privacy topics for the following organizations.

- Briefed the JASONs/U.S. Department of Defense on Machine Learning Security.
- Discussed and made recommendations about IoT security in a round table with Congressperson Pramila Jayapal.
- Briefed the NASEM and FTC on physical ML security.
- Invited expert for the DARPA ISAT Study on AI Cyber-User-In-The-Loop attacks.
- Provided dataset privacy analysis to demographers at UW Madison and a health data company.