Earlence T. Fernandes

CONTACT INFORMATION

CSE 358 Paul Allen Center
185 E Stevens Way NE
Seattle, WA 98109, USA

(734) 709-4334
earlence@cs.washington.edu
`earlence.com`

RESEARCH INTERESTS

Cyber-Physical Systems/IoT Security (Smart Homes), Adversarial Machine Learning, Operating Systems Security (Mobile Systems), Entity Extraction Algorithms.

EDUCATION

University of Michigan, Ann Arbor, MI

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

RESEARCH EXPERIENCE

University of Washington, Seattle, WA
Research Associate with Prof. Tadayoshi Kohno **June 2017 - present**
IoT/CPS security research.

University of Michigan, Ann Arbor, MI
Graduate Student with Prof. Atul Prakash **Aug 2012 - May 2017**
Security analysis and design of IoT programming frameworks, API design for constructing privacy-respecting IoT apps, Mobile systems security.

Microsoft Research, Redmond, WA
Research Intern with Jaeyeon Jung **May 2015 - Aug 2015, May 2016 - Aug 2016**
Security analyses of IoT programming frameworks.

Research Intern with Oriana Riva and Suman Nath **May 2014 - Aug 2014**
Behavioral Analytics for Android and Windows Phone apps.

Vrije Universiteit, Amsterdam, The Netherlands
Scientific Programmer with Prof. Bruno Crispo and Prof. Mauro Conti **Oct 2010 - June 2012**
Member of the S-Mobile project on Android security – Contextual access control, Lightweight virtualization to support Bring-Your-Own-Device use cases.

CONFERENCE & WORKSHOP PAPERS

1. 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.
2. 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%.
3. 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).

4. 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).

5. 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%.

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. 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%.

9. 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%.

10. 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%.

11. 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%.

12. 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%.

13. 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.

14. 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, February 2016, Acceptance Rate: 26%.

15. 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%.

16. 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%.
17. 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%.
18. 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.
19. 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.
20. 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%.
21. 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.

Journals/Columns /Preprints

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

Books

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

Patents

- A Framework For Privacy-Respecting Implicit Data Collection.
  Atul Prakash, Amir Rahmati, **Earlence Fernandes**, Kevin Eykholt. *U.S. Patent Filing Reel 043410/0797*
- System and Method for Extracting and Sharing Application-Related User Data.
  Oriana Riva, Suman Nath, Doug Burger, **Earlence Fernandes**. *U.S. Patent 14/734,991*
- De-siloing Applications for Personalization and Task Completion Services.
  Oriana Riva, Suman Nath, Doug Burger, **Earlence Fernandes**. *U.S. Patent 14/618,854*

Miscellany

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.*

Honors and Awards

- Nominee, UW Postdoc Mentoring Award.
- IEEE S&P 2016 Distinguished Practical Paper Award.
- U.S. Qualcomm Innovation Fellowship Finalist (with Alex Gyori of UIUC).
- UMich PhD Fellowship 2012.

Invited Talks

- "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: Prof. 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: Prof. Darko Marinov).
- "Modern Cyber-Physical Systems Security: Attacks and Defenses," Aug 2016, University of Washington, Seattle, USA (Host: Prof. 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: Prof. 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

- PC Member for: IoT S&P 2018 (co-located with SIGCOMM 2018), USENIX Security 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 for: 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).
- Panelist: Security at University of Michigan IT (SUMIT) conference 2016.

Mentoring Experience

- Jeremy Workman, Purdue University (Fort Wayne Campus), Bachelor Thesis Technical Advisor ("Implementation of Mobile VoIP using Wireless Broadband," Main Advisors: Paul Lin and Gary Steffen).
- Zhi Qian Seah, University of Michigan, Bachelor Thesis Technical Advisor ("Partitioning the Android System Services," Main Advisor: Atul Prakash).
- Ivan Evtimov, University of Washington Ph.D. student (adversarial deep learning).
- Mitali Palekar, University of Washington B.S. student (trigger-action programming).

Teaching Experience

- Primary Instructor for EECS 588 (at Michigan): Graduate Course in Computer and Network Security.
- Primary Instructor for CSE 590Y (at UW): Graduate Seminar in Adversarial Deep Learning.

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, Reddit, Popular Mechanics, and the International Business Times. For more details, please visit: `https://iotsecurity.eecs.umich.edu`