

## CURRENT POSITION

### University of Wisconsin, Madison, WI

Assistant Professor at the Electrical and Computer Engineering Department.

Affiliate faculty member in the Department of Computer Sciences.

Aug. 2017 – present

April. 2018 – present

## EDUCATION

### University of Michigan, Ann Arbor, MI

Ph.D. in Computer Science and Engineering

- Dissertation Title: Location Privacy Protection in the Mobile Era and Beyond
- Advisor: Prof. Kang G. Shin

Sep. 2011 – August 2017

### American University of Beirut, Beirut, Lebanon

M.S. in Electrical and Computer Engineering

Sep. 2009 – Feb. 2011

B.E. in Computer and Communications Engineering

Sep. 2005 – Jun. 2009

## WORK EXPERIENCE

### University of Michigan, Ann Arbor, MI

Graduate Student Research Assistant in the Real-Time Computing Lab

Sep. 2011 – May 2017

### HP Labs, Palo Alto, CA

Research Associate

May 2014 – April 2016

### Qualcomm Research Silicon Valley, Santa Clara, CA

Engineering Intern

May 2013 – Aug. 2013

### American University of Beirut, Beirut, Lebanon

Research Assistant

Sep. 2006 – Aug. 2011

### Institute of Communications and Navigation, German Aerospace Center (DLR), Germany

Summer Intern

Jul. 2008 – Sep. 2008

## PUBLICATIONS

### Conference and Workshop Papers

1. V. Chandrasekaran, C. Gao, B. Tang, K. Fawaz, S. Jha, and S. Banerjee, "Face-Off: Adversarial Face Obfuscation," in *Privacy Enhancing Technologies Symposium (PETS '21)*, Accepted.
2. R. Khandelwal, T. Linden, H. Harkous, and K. Fawaz, "PriSEC: A Privacy Settings Enforcement Controller," in *30th USENIX Security Symposium (USENIX Security 2021)*, Accepted.
3. J. Li, A. R. Chowdhury, Y. Kim, and K. Fawaz, "Kaleido: Real-Time Privacy Control for Eye-Tracking Interactive Systems," in *30th USENIX Security Symposium (USENIX Security 2021)*, Accepted.
4. S. Ahmed, A. R. Chowdhury, K. Fawaz, and P. Ramanathan, "Preech: A System for Privacy-Preserving Speech Transcription," in *29th USENIX Security Symposium (USENIX Security 2020)*, August 2020.
5. T. Linden, R. Khandelwal, H. Harkous, and K. Fawaz, "The Privacy Policy Landscape After the GDPR," in *Privacy Enhancing Technologies Symposium (PETS '20)*, July 2020.

6. J. Li, K. Fawaz, and Y. Kim, "Velody: Nonlinear Vibration Challenge-Response for Resilient User Authentication," in *26th ACM Conference on Computer and Communications Security (CCS '19)*, London, United Kingdom, November 2019.
7. C. Gao, K. Fawaz, S. Sur, and S. Banerjee, "Practical Privacy Protection for Audio Sensing Against Multi-Microphone Adversaries," in *Privacy Enhancing Technologies Symposium (PETS '19)*, Stockholm, Sweden, July 2019.
8. H. Harkous, K. Fawaz, R. Lebert, F. Schaub, K.G. Shin and K. Aberer, "Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning," *27th USENIX Security Symposium (USENIX Security 2018)*, Baltimore, MD, USA, August 2018.
9. C. Gao, V. Chandrasekaran, K. Fawaz and S. Banerjee, "Traversing the Quagmire that is Privacy in your Smart Home," *the 2018 Workshop on IoT Security and Privacy (IoT S&P 18)*, Budapest, Hungary, August 2018.
10. H. Feng\*, K. Fawaz\* and K.G. Shin (\* co-primary authors), "Continuous Authentication for Voice Assistants," *23rd Annual International Conference on Mobile Computing and Networking (ACM MobiCom 2017)*, Snowbird, UT, USA, October 2017.
11. K.C. Garikipati, K. Fawaz, and K.G. Shin, "RT-OPEX: Flexible Scheduling for Cloud-RAN processing," *12th International Conference on emerging Networking EXperiments and Technologies (ACM CoNext 2016)*, Irvine, CA, USA, December 2016.
12. K. Fawaz, K.H. Kim, and K.G. Shin, "Protecting Privacy of BLE Device Users," *25th USENIX Security Symposium (USENIX Security 2016)*, Austin, TX, USA, August 2016.
13. K. Fawaz, K.H. Kim, and K.G. Shin, "Privacy vs. Reward in Indoor Location-Based Services," *16th Privacy Enhancing Technologies Symposium (PETS 2016)*, Dramstadt, Germany, July 2016.
14. H. Harkous, K. Fawaz, K.G. Shin, and K. Aberer "PriBots: Conversational Privacy with Chatbots," *SOUPS 2016 Workshop on the Future of Privacy Indicators*, Denver, CO, USA, June 2016.
15. K. Fawaz, H. Feng and K.G. Shin, "Anatomization and User-Level Prevention of Mobile Apps' Location Privacy Threats," in *24th USENIX Security Symposium (USENIX Security 2015)*, Washington D.C., USA, August 2015.
16. H. Feng, K. Fawaz and K.G. Shin, "LinkDroid: Reducing Unregulated Aggregation of App Usage Behaviors," in *24th USENIX Security Symposium (USENIX Security 2015)*, Washington D.C., USA, August 2015.
17. K. Fawaz and K.G. Shin, "Location Privacy for Smartphone Users," in *21st ACM Conference on Computer and Communications Security (CCS '14)*, Arizona, USA, November 2014.
18. K. Fawaz and H. Artail, "A Two-layer Cache Replication Scheme for Dense Mobile Ad hoc Networks," in *IEEE Globecom 2012*, California, USA, December 2012.
19. K. Fawaz, N. Abbani, and H. Artail, "A Privacy-Preserving Cache Management System for MANETs," in *19th International Conference on Telecommunications (ICT 2012)*, Jounieh, Lebanon, April 2012.
20. M. Dabbagh, A. Ghandour, K. Fawaz, W. El Hajj, and H. Hajj, "Slow Port Scanning Detection," in *7th International Conference on Information Assurance and Security (IAS 2011)*, Melaka, Malaysia, December 2011.
21. A. Ghandour, K. Fawaz, and H. Artail, "Fuzzy Cognitive Vehicular Ad hoc Networks," in *IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2011)*, Shanghai, China, October 2011.
22. A. Ghandour, K. Fawaz, H. Artail, and R. Hamadeh, "Extending the DSRC's Control Channel using Cognitive Networking Concepts and Fuzzy Logic," in *22nd IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2011)*, Toronto, Canada, September 2011.
23. A. Ghandour, K. Fawaz, and H. Artail, "Data Delivery Guarantees in Congested Vehicular Ad hoc Networks Using Cognitive Networks," in *The 7th International Wireless Communications and Mobile Computing Conference (IWCMC 2011)*, Istanbul, Turkey, July 2011.
24. K. Fawaz, A. Ghandour, M. Olliek, and H. Artail, "Improving Reliability of Safety Applications in Vehicle Ad hoc Networks through the Implementation of a Cognitive Network," in *IEEE 17th International Conference on Telecommunications (ICT 2010)*, Doha, Qatar, April 2010.
25. A. Ghandour, K. Fawaz, A. Chehab and A. Kayssi, "Wavelet Transform-Based Transient Current Analysis for Detection of Gate-oxide Shorts in CMOS," in *4th IEEE International Design and Test Workshop (IDT 2009)*, Riyadh, Saudi Arabia, Nov. 2009.

26. W. Wang, T. Jost, C. Mensing, A. Dammann, and K. Fawaz, "Indoor Propagation Effects on ToA Error for Joint GNSS and Terrestrial Radio Based Localization," in *69th IEEE Vehicular Technology Conference (VTC 2009 - Spring)*, Barcelona, Spain, April 2009.
27. H. Artail, M. Safieddine, T. Safar, M. El-Khatib, T. Ibrahim, and K. Fawaz, "Dynamic Simulations of VANET Scenarios," in *International Conference on Wireless Access in Vehicular Environments (WAVE 2008)*, Dearborn, MI., December 2008.
28. H. Artail, J. El-Hage, R. Aouad, K. Fawaz, "ASKME: Adaptive and Self-evolving Knowledge-base for Mobile Environments," in *6th International Conference on Informatics and Systems*, Cairo, Egypt, March 2008.

### Journal and Magazine Papers

1. K. Fawaz, K.G. Shin, "Security and Privacy in Internet of Things," *IEEE Computer Magazine*, vol. 52, issue 4, pp. 40-49, May 2019.
2. H. Feng, K. Fawaz, K.G. Shin, "Wearable Technology Brings Security Alexa and Siri," *GetMobile: Mobile Computing and Communications*, vol. 21, issue 1, pp. 35-38, May 2018.
3. R. Naja, N. Mouawad, A. Ghandour, and K. Fawaz, "Speed Trap Optimal Patrolling: STOP Playing Stackelberg Security Games," *Springer Wireless Personal Communications*, Springer Wireless Personal Communications, vol. 98, issue 4, pp. 3563-3582, February 2018.
4. K. Fawaz, A. Artail, R. Al-Khansa, H. Artail, and H. Safa, "Replication Enabled Distributed Cache Invalidation Method," *Wireless Communications and Mobile Computing*, vol. 15, issue 13, pp. 1711-1728, September 2015.
5. K. Fawaz, F. Zaraket, W. Masri, and H. Harkous, "PBCOV: A Property Based Coverage Criterion," *Software Quality Journal*, vol. 23, issue 1, pp. 171-202, March 2015.
6. A. Ghandour, K. Fawaz, H. Artail, M. Di Felice and L. Bononi, "Improving Vehicular Safety Message Delivery through the Implementation of a Cognitive Vehicular Network," *Elsevier Ad Hoc Networks*, vol. 11, no. 8, pp. 2408-2422, November 2013.
7. K. Fawaz, and H. Artail, "DCIM: Distributed Cache Invalidation Method for Maintaining Cache Consistency in Wireless Mobile Networks," in *IEEE Transactions on Mobile Computing*, vol. 12, no. 4, pp. 680-693, April 2013.
8. H. Artail, K. Fawaz, and A. Ghandour, "A Proxy-Based Architecture for Dynamic Discovery and Invocation of Web Services from Mobile Devices," in *IEEE Transactions on Service Computing*, vol. 5, no. 1, pp. 99-115, March 2012.
9. H. Artail, R. Antoun, and K. Fawaz, "CRUST: Implementation of Clustering and Routing Functions for Mobile Ad hoc Networks Using Reactive Tuple Spaces," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1064 - 1081, August 2009.
10. H. Artail, and K. Fawaz, "A Fast HTML Web Page Change Detection Approach Based on Hashing and Reducing the Number of Similarity Computations," *Data and Knowledge Engineering*, vol. 66, no. 2, pp. 326-337, August 2008.

### PATENTS

#### Granted

1. US Patent 9686023, "Methods and systems of dynamically generating and using device-specific and device-state-specific classifier models for the efficient classification of mobile device behaviors", V. Sridhara, R. Gupta, K. Fawaz, Jun. 20, 2017.
2. US Patent 9684870, "Methods and Systems of Using Boosted Decision Stumps and Joint Feature Selection and Culling Algorithms for the Efficient Classification of Mobile Device Behaviors", K. Fawaz, V. Sridhara, R. Gupta, Jun. 20, 2017.
3. US Patent 9323929, "Pre-identifying Probable Malicious Rootkit Behavior Using Behavioral Contracts", D. Fiala, M. Christodorescu, V. Sridhara, R. Gupta, K. Fawaz, Apr. 26, 2016.
4. US Patent 9147072, "Method and System for Performing Behavioral Analysis Operations in a Mobile Device based on Application State", K. Fawaz, V. Sridhara, R. Gupta, M. Christodorescu, Sep. 29, 2015.

#### Pending (public)

1. US Patent App US20180068671A1, "System and method for authenticating voice commands for a voice assistant", K. Fawaz, H. Feng, K.G. Shin, March. 8, 2018.
2. WO Patent App WO2017146727A1, "Device privacy protection", K. Fawaz, K. Kim, Aug. 31, 2017.
3. WO Patent App WO2016122499A1, "Controlling the release of personal information", K. Fawaz, K. Kim, Aug. 4, 2016.
4. US Patent App 14/826,430, "Using Normalized Confidence Values For Classifying Mobile Device Behaviors", K. Fawaz, V. Sridhara, R. Gupta, Y. Chen, Aug. 14, 2015.

#### INVITED TALKS

- AI and the changing landscape of privacy notice and choice, Ohio State University, October 2018.
- AI and the changing landscape of privacy notice and choice, University of South Carolina, October 2020.
- Polisis: Automated Analysis and Presentation of Privacy Policies Using Deep Learning, The Federal Trade Commission, Washington, D.C., June 2019.
- AI and the changing landscape of privacy notice and choice, COMSNETS 2019, Bengaluru, India, January 2019.
- AI and the changing landscape of privacy notice and choice, Global Cyber Security Initiative (GCSI), Chicago, November 2018.
- Location Privacy of Smartphone Users, Google (Mountain View), August 2014.

#### TEACHING EXPERIENCE

**University of Wisconsin, Madison, WI**

**Aug. 2017 – present**

- Mobile Computing Laboratory (ECE 454), Fall 2020.
- Digital System Fundamentals (ECE 352), Spring 2019.
- Mobile Computing Laboratory (ECE 454), Fall 2019.
- Mobile Computing Laboratory (ECE 454), Spring 2019.
- Mobile and Wireless Networks (ECE 707), Fall 2018.
- Security and Privacy of Computers and Networks (ECE 901), Spring 2018.
- Mobile Computing Laboratory (ECE 454), Fall 2017.

#### SERVICE

- Member of the Technical Program Committee of IEEE S&P 2021, USENIX Security 2021, PETS 2021, ESCORICS 2020, ACM MobiCom 2020, ACM MobiCom 2019, ACM CCS 2019, USENIX Security 2018.
- Serving on the Awards and Distinguished Lecture Series Committees of the ECE department in the University of Wisconsin.
- Served on the Graduate Curriculum and the Graduate Recruiting, Admissions and Fellowships Committees of the ECE department in the University of Wisconsin.
- Member of the Institute of Electric and Electronic Engineers (IEEE), IEEE Computer Society, IEEE Communications Society, USENIX Association, and the ACM.

#### CURRENT SUPPORT

- Kassem Fawaz (PI). AI-Powered Diagnostics and Generation of Android Permission Rationales. Google, 2021. Amount to be determined.
- Suman Banerjee (PI), Kassem Fawaz, Kangwook Lee, Mohit Gupta. MLWiNS: Supporting Distributed Machine Learning Applications for the Nomadic Edge. National Science Foundation, 2021. \$890,000.00.
- Kassem Fawaz (PI). CAREER: Presentation and Mitigation of Privacy Risks for Online Users. National Science Foundation, 2021. \$508,343.00.
- Somesh Jha (PI), Kassem Fawaz, Atul Prakash, and Nicolas Papernot. Enhancing ML Robustness Using Physical-World Constraints. Defense Advanced Research Projects Agency, 2020. \$2,700,000.00.
- Kassem Fawaz (PI), Soyoun Ahn, David Noyce, and Parmesh Ramanathan. Harnessing Mobile Ad Hoc Networks to Improve Vulnerable Road User Safety. Federal Highway Administration, 2018. \$924,000.

- Remzi Arpaci-Dusseau (PI), Aditya Akella, Suman Banerjee, Kassem Fawaz, and Shiv Venkataraman. ECDI: Computation, Communication, and Storage Infrastructure For The Roaming Edge. NSF/VMware Research Grant, 2018. \$3,000,000.00.

#### HONORS AND AWARDS

- NSF CAREER Award 2020.
- The Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies, 2019.
- ACM CoNEXT 2016 student travel grant.
- PETS 2016 student travel grant.
- Honorable mention at the 2015 CSE Honors Competition at the University of Michigan.
- USENIX Security 2015 student travel grant.
- CCS 2014 student travel grant.
- Rackham travel grant 2014, 2015, 2016.
- Full departmental fellowship, University of Michigan, 2011.
- Abdul Hadi Debs Endowment award for academic excellence, American University of Beirut, June 2011.
- Distinguished graduate award for the class of 2009, American University of Beirut, June 2009.
- Placement on the dean's honor list, American University of Beirut, Sep. 2005 – June 2009.

#### LANGUAGES

Excellent speaking and writing skills in English and Arabic