Ahmed M. Fawaz

CONTACT INFORMATION

University of Illinois at Urbana-Champaign
Coordinated Science Laboratory
1308 W. Main St.
Urbana, IL, 61801-2307

Mobile: 1-217-974-0348
E-mail: afawaz2@illinois.edu
Website: http://ahmedfawaz.me

NATIONALITY

United States of America

EDUCATION

Ph.D. in Electrical and Computer Engineering

University of Illinois at Urbana-Champaign **August 2017**

- Dissertation Title: *Achieving Cyber Resiliency Against Lateral Movement Through Detection and Response*
- Advisor: William H. Sanders

M.S. in Electrical and Computer Engineering

University of Illinois at Urbana-Champaign **May 2013**

- Thesis Title:*A Response Taxonomy and Cost Model for Advanced Metering Infrastructures*
- Advisor: William H. Sanders

B.E. in Electrical and Computer Engineering, with Distinction

American University of Beirut, Lebanon **July 2011**

RESEARCH INTERESTS

- Cyber security and resiliency
- Critical infrastructure and cyber-physical systems
- Distributed computing and distributed systems

PROFESSIONAL EXPERIENCE

University of Illinois at Urbana-Champaign

Research Assistant with Professor William H. Sanders **August 2011 – present**

- Developed a game-theoretic method to respond to lateral attacker movement in a network by blocking hosts predicatively. Currently developing an adaptive controller that controls the topology and healing rates of machines to stop lateral movement.
- Developed PowerAlert, a trusted out-of-box verifier, that uses power measurements as a trust base and exploits diversity and randomness to prevent adaptation. Developed Tireless, a novel continuous-time game employed by PowerAlert, to find the optimal strategy for an attacker evading detection.
- Developed a distributed monitoring fusion framework that detects lateral attacker movement. The method uses host-level information to correlate network flows and then chains the correlated flows to learn chains of lateral movement.
- Designed a method to detect anomalous behavior in application programs. The anomaly detection method uses a behavior model learned by fusing low-level application behavior. The data collection and fusion method were implemented as part of a Windows kernel-level monitor called Kobra.
- Developed a response cost model in smart meter networks that fuses the cyber network and physical state of the distribution grid. Presented the cost model as part of an intrusion response mechanism to the Department of Energy (DOE) as part of a test AMI deployment. The test deployment consisted of 25 meters connected with an RF network through 4 cells relays.
- Tested FirstEnergy's AMI for compliance with DOE's security requirements. As part of this work, I reverse-engineered a proprietary wireless communication protocol for smart meters using NI-USRP.

Schweitzer Engineering Laboratories (SEL)

Engineering Intern **May 2013 – August 2013**

Evaluated the use of software-define networking (SDN) in substations to ensure fault tolerance when a switch fails. Then used watchdog, SEL's SDN switch, to implement intrusion response actions that forward packets to an IDS with known unpatched attack signatures. The actions block the packets and redirects to a logging server for forensics.

DigitCom LLC

Subject Matter Expert **December 2012 – May 2015**

- Reviewed the cyber security state of a small power utility.
- Developed teaching material for internal hands-on security training. The material reviewed basic security concepts related to phishing attacks and password hygiene, then moved to more advanced topics in application and network security.
- Produced white papers about challenges to SCADA security due to BYOD schemes, malware delivery in air-gapped systems, and consequences of intrusions to cyber-physical industrial control systems.

École Polytechnique Fédérale de Lausanne (EPFL)

Summer Internship with Professor Jean-Pierre Hubaux **July 2010 – September 2010**

Evaluated the location privacy properties of the Nokia Instant Community (NIC) by implementing Mobivacy (mobivacy.sf.net), a modular simulation framework for evaluating location privacy-preserving mechanisms.

American University of Beirut

Research Assistant and Projects **September 2008 – July 2011**

- Conducted research in the area of testing of fault models for CMOS adder circuits for different technologies.
- Designed a privacy-preserving advertising system that delivers targeted mobile advertisements. The method uses collaborative aggregation of messages to hide the source against an advertisement server.
- Designed and evaluated a cooperative collision avoidance protocol for vehicular ad hoc networks (VANETs) in sudden braking scenarios.

Teaching Experience

University of Illinois at Urbana-Champaign

Teaching Assistant

Computer Systems and Programming (ECE 220) **Aug 2016 – present**

- Designed a curriculum for James Scholar honor students that introduces cyber security, algorithm design and analysis, and critical reading of academic papers. The students were encouraged to discover the concepts through class discussions and assignments. Also organized a student programming competition as part of this course.
- Led a regular lab discussion session during which I introduced and discussed course material, introduced machine problems (MPs), and explained lab problems and helped students solve them. I also created new exam problems and machine problems and assisted in correcting exams and MPs.

Computer System Analysis (ECE 541) **Sept 2014 – Dec 2014**

Led problem-solving sessions during office hours to assist students in solving homework assignments and projects. Presented lectures on stochastic activity networks (SANs) and pseudo- random number generation methods.

Advanced Seminar (CS 591) **July 2012 – May 2013**

- Co-designed, led, and taught an advanced seminar course for computer science and power system researchers on the cyber-physical aspects of the power grid. The goal of the seminar is to bridge the knowledge gap between the students in the two disciplines and enable them to communicate and collaborate effectively.

- Presented our teaching approach, findings, and lessons learned at the National Initiatives for Cybersecurity Education 2016 (NICE'16).

American University of Beirut

Teaching Assistant

Mobile Ad-hoc and Sensor Networks (EECE 656)
Computer Networks (EECE 450) **Sept. 2009 – July 2010**

Corrected projects and graded presentations and assignments. I assisted students in picking projects during office hours.

AWARDS

- Mavis Future Faculty Fellow 2016
- AUB Alumni Association in Dubai and Northern Emirates Scholarship (all semesters attended)
- AUB's Faculty of Engineering Dean's Honor List (all semesters attended)

PUBLICATIONS

1. Fawaz, A., Noureddine, M., Ujcich, B. E., and Sanders, W. H., "TIRELESS: A Continuous-Time Game for Optimally Checking System State Integrity," submitted for publication.
2. Fawaz, A., Noureddine, M., and Sanders, W. H., "PowerAlert: An Integrity Checker using Power Measurement," submitted for publication.
3. A. M. Fawaz and W. H. Sanders, "Learning Process Behavioral Baselines for Anomaly Detection," Proceedings of the *22nd IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2017)*, Christchurch, New Zealand, January 22-25, 2017, to appear.
4. A. Fawaz, A. Bohara, C. Cheh, and W. H. Sanders, "Lateral Movement Detection Using Distributed Data Fusion," Proceedings of the *35th Symposium on Reliable Distributed Systems (SRDS)*, Budapest, Hungary, Sept. 26-29, 2016, to appear.
5. Fawaz, A., and Sanders, W. H, "Poster: Learning Process Behavioral Baselines for Anomaly Detection," *RAID 2016*, [Poster]
6. M. A. Noureddine, A. Fawaz, W. H. Sanders, and T. Baar, "A Game-Theoretic Approach to Respond to Attacker Lateral Movement," Proceedings of the *7th Conference on Decision and Game Theory for Security (GameSec 2016)*, New York, New York, November 2-4, 2016, Lecture Notes in Computer Science vol. 9996, Springer, 2016, pp. 294-313.
7. Fawaz, A., Berthier, R., and Sanders, W. H., "A Response Cost Model for Advanced Metering Infrastructures," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, March 2016, pp. 543-553.
8. Stephen McLaughlin, Brett Holbert, Ahmed Fawaz, Robin Berthier and Saman Zonouz, "A Multi-Sensor Intrusion and Energy Theft Detection Framework for Advanced Metering Infrastructures," *IEEE JSAC Smart Grid Communications Series*, vol. 31, no. 7, pp. 1319-1330, July 2013.
9. Fawaz, A., Berthier, R., and Sanders, W. H.,"Cost Modeling of Response Actions for Automated Response and Recovery in AMI," In *Proceedings of the Third IEEE International Conference on Smart Grid Communication (SmartGridComm 2012)*, Tainan City, Taiwan, Nov. 5-8, 2012, pp. 348-353.
10. Fawaz, A., Berthier, R., Sanders, W. H., and Pal., P., "Understanding the Role of Automated Response Actions in Improving AMI Resiliency," In *Proceedings of the NIST Cybersecurity for Cyber-Physical Systems Workshop*, Gaithersburg, Maryland, Apr. 23-24, 2012.
11. Fawaz, A., Jabber, A., Kassem, A., Chehab, A., and Kayssi, A., "Assessing Testing Techniques for Resistive-Open Defects in Nanometer CMOS Adders," In *Proceedings of the IEEE International Conference on Electronics, Circuits, and Systems (ICECS 2011)*, Beirut, Lebanon, Dec. 11-14, 2011, pp. 165-168.
12. Fawaz, A., Hojaij, A., Kobeissi, H., and Artail, H., "An On-Demand Mobile Advertising System that Protects Source Privacy using Interest Aggregation," In *Proceedings of the IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2011)*, Shanghai, P.R. China, Oct. 10-12, 2011, pp. 127-134.

13. Fawaz, A., Hojaij, A., Kobeissi, H., and Artail, H., “Using Cooperation among Peers and Interest Mixing to Protect Privacy in Targeted Mobile Advertisement,” In *Proceedings of the 11th International Conference on Telecommunications for Intelligent Transport Systems (ITST 2011)*, Saint Petersburg, Russia, Aug. 23-25, 2011, pp. 474-479.
14. Fawaz, A., and Artail, H. , “Enhanced Cooperative Collision Avoidance in Sudden Vehicle Braking Scenarios,” In *Proceedings of the IEEE 17th International Conference on Telecommunications (ICT 2010)*, Doha, Qatar, April 4-7, 2010, pp. 806-813.

Activities and Service

- Served on Engineering Graduate Student Advisory Committee (EGSAC) 2015-2016.
- Participated in Mentoring Undergraduates in Science & Engineering (MUSE) 2016-2017, 2015-2016.
- Participated in the Promoting Undergraduate Research in Engineering (PURE) program Fall 2015, Fall 2014.
- Supervised several undergraduate interns during Summer 2014.
- Served on the organizing committee for the Coordinated Science Laboratory Symposium on Emerging Topics in Control and Modeling 2012, University of Illinois, Urbana, IL.
- Student member of the Institute of Electrical and Electronics Engineers (IEEE).
- Reviewed papers for HotSoS’16, IEEE TSG, ICCPS 2013, DSN 2012, INFOCOM 2011 and PICOM’09.

Skills

Mathematical Skills	Linear Systems, Stochastic Analysis, Control Theory, Game Theory, Graph Theory, Complexity Theory, Hybrid Automata, Stochastic Activity Networks (SAN).
Programming Languages	C, C++, Java, Python, MATLAB, R, SQL, x86, LabVIEW.
Tools	Windows Driver SDK, Android, NI USRP
Databases	MySQL
Networks Simulators	Mobius, ns2
Languages	English, Arabic