Amir Rahmati

Assistant Professor
Department of Computer Science
Stony Brook University
March 11, 2018

Department of Computer Science
Stony Brook University
Stony Brook, NY 11794-2424
+1 413-331-9438
amir@rahmati.com
https://amir.rahmati.com

Research Overview

My research focuses on improving the security of emerging technologies, such as Internet of Things (IoT) devices and Cyber-Physical systems. My work involves designing, building, and evaluating systems that tackle security challenges in these domains. As we move towards a world where many resource- and energy-limited devices have access to our data & activities, my research creates an avenue for these devices to incorporate security in their design.

Positions

- **Assistant Professor, Department of Computer Science, Stony Brook University (2018-Present)**
- **System Architect, KNOX Security, Samsung Research America (2017-2018)**
- **System Consultant, Abbott Laboratories (2017)**

Education

- **Ph.D. in Computer Science & Engineering, University of Michigan (2015-2017)**
  Advisor: Prof. Atul Prakash *Committee:* J. Alex Halderman, Peter Honeyman, Vineet R. Kamat
  Thesis Title: Attacking and Defending Emerging Computer Systems Using the Memory Remanence Effect
- **M.S.E. in Computer Science and Engineering, University of Michigan (2011-2014)**
  Advisor: Prof. Kevin Fu
- **B.Sc. in Computer Engineering, Sharif University of Technology (2007-2011)**
  Advisor: Prof. Seyed-Ghassem Miremadi

Teaching Experience

- **Network Security (CSE508), Stony Brook University:** Fall'18
- **Computer & Network Security (EECS-588), University of Michigan:** Winter'17

Conference Publications

10. *"Tyche: A Risk-Based Permission Model for Smart Homes"*
    Amir Rahmati, Earlence Fernandes, Kevin Eykholt, Atul Prakash
    IEEE Cybersecurity Development Conference (SecDev'18). Sep 2018
9. *"ATtention Spanned: Comprehensive Vulnerability Analysis of AT Commands Within the Android Ecosystem"*
    Dave Tian, Grant Hernandez, Joseph Choi, Vanessa Frost, Christie Raules, Kevin Butler, Patrick Traynor, Hayawardh Vijayakumar, Lee Harrison, **Amir Rahmati**, Mike Grace
    USENIX Security Symposium (USENIX Sec'18). August 2018
8. *"Robust Physical-World Attacks on Deep Learning Visual Classification"*
    Ivan Evtimov, Kevin Eykholt, Earlence Fernandes, Tadayoshi Kohno, Bo Li, Atul Prakash, **Amir Rahmati**, Dawn Song,
    Conference on Computer Vision and Pattern Recognition (CVPR'18). June 2018 (Supersedes arXiv:1707.08945)
7. *"Decentralized Action Integrity for Trigger-Action IoT Platforms"*
    Earlence Fernandes, **Amir Rahmati**, Jaeyeon Jung, Atul Prakash
    Network and Distributed System Security Symposium (NDSS'18). February 2018 (Supersedes arXiv:1707.00405)
6. *"Heimdall: A Privacy-Respecting Implicit Preference Collection Framework"*
    Amir Rahmati, Earlence Fernandes, Kevin Eykholt, Xinheng Chen, Atul Prakash
    ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'17). June 2017
5. *"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
    Network and Distributed System Security Symposium (NDSS'17). March 2017
4. *"Applying the Opacified Computation Model to Enforce Information Flow Policies in IoT Applications"*
    Amir Rahmati, Earlence Fernandes, Atul Prakash
    IEEE Cybersecurity Development Conference (SecDev'16). November 2016
3. *"FlowFence: Practical Data Protection for Emerging IoT Application Frameworks"*
    Earlence Fernandes, Justin Paupore, **Amir Rahmati**, Daniel Simionato, Mauro Conti, Atul Prakash
    USENIX Security Symposium (USENIX Sec'16). August 2016
2. *"Probable Cause: The Deanonymizing Effects of Approximate DRAM"*
    Amir Rahmati, Matthew Hicks, Daniel Holcomb, Kevin Fu
    International Symposium on Computer Architecture (ISCA'15). June 2015
1. *"TARDIS: Time & Remanence Decay in SRAM to Implement Secure Protocols on Embedded Devices without Clocks"*
    Amir Rahmati, Mastooreh Salajegheh, Daniel Holcomb, Jacob Sorber, Wayne Burleson, Kevin Fu
    USENIX Security Symposium (USENIX Sec'12). August 2012

Workshop Publications

12. *"Robust Physical-World Attacks on Deep Learning Visual Classification"*
Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, **Amir Rahmati**, Chaiowei Xiao, Atul Prakash, Tadayoshi Kohno, Dawn Song
Workshop on the Bright and Dark Sides of Computer Vision (CV-COPS'18). June 2018
11. *"Caterpillar: Iterative Concolic Execution for Stateful Programs"*
Laurent Simon, Shuying Liang, **Amir Rahmati**
International KLEE Workshop on Symbolic Execution (KLEE'18). April 2018
10. *"Securing Trigger-Action Platforms"*
Earlence Fernandes, **Amir Rahmati**, Jaeyeon Jung, Atul Prakash
USENIX Summit on Hot Topics in Security (HotSec'17). August 2017
9. *"Support for Security and Safety of Programmable IoT Systems"*
Alex Gyori, Earlence Fernandes, **Amir Rahmati**, Atul Prakash and Darko Marinov
Workshop on Testing Embedded and Cyber-Physical Systems (TECPS'17). July 2017
8. *"Towards Comprehensive Repositories of Opinions"*
Han Zhang, Kasra Edalat Nejad, **Amir Rahmati**, Harsha V. Madhyastha
ACM Workshop on Hot Topics in Networks (HotNets'16). November 2016
7. *"Approximate Flash Storage: A Feasibility Study"*
Amir Rahmati, Matthew Hicks, Atul Prakash
Workshop on Approximate Computing Across the System Stack (WAX'16). April 2016
6. *"Context-Specific Access Control: Conforming Permissions With User Expectations"*
Amir Rahmati, Harsha V. Madhyastha
ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (CCS'SPSM'15). October 2015
5. *"Malware Prognosis: How to Do Malware Research in Medical Domain"*
Sai R. Gouravajhala, **Amir Rahmati**, Peter Honeyman, and Kevin Fu
USENIX Workshop on Health Information Technologies (Health Tech'14). August 2014
4. *"Refreshing Thoughts on DRAM: Power Saving vs. Data Integrity"*
Amir Rahmati, Matthew Hicks, Daniel Holcomb, Kevin Fu
Workshop on Approximate Computing Across the System Stack (WACAS'14). March 2014
3. *"WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices"*
Shane Clark, Benjamin Ransford, **Amir Rahmati**, Shane Guineau, Jacob Sorber, Wenyuan Xu, Kevin Fu
USENIX Workshop on Health Information Technologies (Health Tech'13). August 2013
2. *"Internet Censorship in Iran: A First Look"*
Amir Rahmati (Simorgh Aryan), Homa Aryan, J. Alex Halderman, Pseudonymous publication
USENIX Workshop on Free and Open Communications on the Internet (FOCI'13). August 2013
1. *"DRV-Fingerprinting: Using Data Retention Voltage of SRAM Cells for Chip Identification"*
Daniel Holcomb, **Amir Rahmati**, Mastooreh Salajegheh,Wayne Burleson, Kevin Fu
Workshop On RFID Security And Privacy 2012 (RFIDsec'12). July 2012

Journal Publications

2. *"Techniques for Timekeeping Without a Clock"*
Josiah Hester, **Amir Rahmati**, Daniel Holcomb, Kevin Fu, Jacob Sorber
IEEE Transactions on Embedded Computing Systems, Vol. 15, No. 4 (TECS'16). August 2016
1. *"Reliable Physical Unclonable Functions using Data Retention Voltage of SRAM Cells"*
Xiaolin Xu, **Amir Rahmati**, Daniel Holcomb, Kevin Fu, Wayne Burleson
IEEE Transactions on Computer-Aided Design of Integrated Circuits & Systems: Special Section on Hardware Security and Trust, Vol. 34, No. 6 (TCAD'15). June 2015

Selected Other Publications

5. *"IFTTT vs. Zapier: A Comparative Study of Trigger-Action Programming Frameworks"*
Amir Rahmati, Earlence Fernandes, Jaeyeon Jung, Atul Prakash
Preprint (arXiv:1709.02788). September 2017
4. *"Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?"*
Earlence Fernandes, **Amir Rahmati**, Kevin Eykholt, Atul Prakash
IEEE Security & Privacy. July 2017
3. *"The Security Implications of Permission Models of Smart Home Application Frameworks"*
Earlence Fernandes, **Amir Rahmati**, Jaeyeon Jung, Atul Prakash
IEEE Security & Privacy. April 2017
2. *"Under What Circumstances Are Insider Leaks Justified?"*
Ben Lusher, Kathryn Reeves, **Amir Rahmati**
Cyber Conflict Project Report, April 2014
1. *"Cyber Dimentions of State Repression"*
Meredith Blank, Anita Ravishankar, **Amir Rahmati**
Cyber Conflict Project Report. February 2014

Selected Posters

2. *"Stigmalware: Investigating the Prevalence of Malware in the Clinical Domain"*
   Sai R. Gouravajhala, **Amir Rahmati**, Evan Chavis, Denis Foo Kune, Peter Honeyman, Michael Bailey, Kevin Fu
   IEEE Symposium on Security and Privacy (IEEE S&P'14). April 2014
1. *"Time and Remanence Decay in SRAM"*
   Amir Rahmati, Mastooreh Salajegheh, Daniel Holcomb, Jacob Sorber, Wayne Burleson, Kevin Fu
   IEEE Symposium on Security and Privacy (IEEE S&P'12), May 2012

Panels, Invited Talks, Keynotes

5. *"Heimdall: A Privacy-Respecting Implicit Preference Collection Framework"*
   Invited talk at National Security Institute Security & Privacy Day. October 2017
4. *"IoT Security and Privacy: An Academic Perspective"*
   Panelist at IEEE Conference on Communications and Network Security (CNS'17). October 2017
3. *"Ahem: Additively Homomorphic Encryption for the Moo"*
   Short Talk at Workshop on Cryptographic Hardware and Embedded Systems (CHES'13). August 2013
2. *"Using Side Channels To Do Good"*
   Short Talk at Workshop on Cryptographic Hardware and Embedded Systems (CHES'13). August 2013
1. *"Time and Remanence Decay in SRAM"*
   Invited Talk at MIT Security Seminar series. October 2012
   Invited Talk at 3^{rd} Annual Pay-as-you-Go Workshop. July 2012

Services

- **Panelist:** NSF Secure & Trustworthy Cyberspace (SaTC) April'17
- **PC Member:** IoT S&P'18, SEMS'17, SecCPS'17, SafeThings'17
- **Reviewer:** USENIX ATC'18, IEEE Internet of Things Journal'18, CHI'18, '17, DSN'17, ICC'17, INFOCOM'17, IEEE MoST'17, NDSS'16, Micro's Top Picks'15, USENIX Sec'14, '13, '12, Canadian Journal of Electrical & Computer Engineering'15, Journal of Wireless Networks (WINET'12)
- **PC Meeting Secretary:** USENIX Sec'14, '13
- **Student Volunteer:** MobiSys'17, ASPLOS'14, USENIX Sec'12

Broader Impact of Selected Project:

- **Physical-World Attacks on Deep Learning Models (2018):** Attacks on machine learning models have generally targeted their inputs. This work for the first time showed that manipulation of physical objects can induce misclassification, creating a paradigm shift in adversarial machine learning research and spanning a new sub-field. IEEE Spectrum, Yahoo News, Wired, Engagdet, Telegraph, Car and Driver, CNET, Digital Trends, SCMagazine, Schneier on Security, Ars Technica, and Fortune were among the outlets that covered these findings.
- **Trigger-Action Platform Security (2017):** Overhauled the design of trigger-action platforms to add security as a core property. This design has been adopted by Samsung in their *Knox Wearable Services*.
- **Security of Approximate Computing Systems (2015):** Approximate computing explores the trade-off between performance and accuracy in computing systems. "Probable Cause" for the first time introduced security as a third variable in this equation and drew attention to potential security implications of emerging technologies.
- **Analysis of Internet Censorship in Iran (2013):** Performed the first systematic study of Internet censorship in Iran, one of the leading oppressors of Internet freedom. This works examined the Iranian governments censorship around the 2013 presidential election and for the first time observed whitelisting as a method used by the censors. Multiple media outputs including the Washington Post covered these findings.
- **Using Memory Remanence for Timekeeping (2012):** Developed the "TARDIS" timekeeping technique which allows for energy-free timekeeping in computing systems. This work provided a fresh perspective into the memory remanence effect and was covered by media outlets including the IEEE Spectrum.

Activities

- **Manager** of University of Michigan **Systems Reading Group (SRG)** (2015-2016)
- **Elected Head** of the Computer Engineering Dept. **Student Scientific Chapter (SSC)** (2010)
- **Computer & IT Editor and freelancer** for Sharif Daily, Sharif University's official newspaper (2009-2010)
- **Technical Manager** - 11th ACM/ICPC - Asia Region (2009)