# Amir Rahmati

amir.rahmati.com
rahmati@umich.edu

US Permanent Resident
Ann Arbor, MI. 413-331-9438

**Research Interests**

- Security and Privacy
- Embedded and Ubiquitous Systems
- Approximate Computing

**Education**

- **University of Michigan**, (2015-2017 (Expected)) Advisor: Prof. Atul Prakash
  - Ph.D. in Computer Science and Engineering.
- **University of Michigan**, (2013-2014) Advisor: Prof. Kevin Fu
  - M.S.E. in Computer Science and Engineering.
- **University of Massachusetts Amherst**, (2011-2012) Advisor: Prof. Kevin Fu
  Graduate Student in Computer Science Department, Transferred to the University of Michigan in Jan 2013.
- **Sharif University of Technology**, (2007-2011) Advisor: Prof. Seyed-Ghassem Miremadi
  - B.Sc. in Computer Engineering

**Work Experience**

- **Consultant, Saint Jude Medical**, (2017)
  Saint Jude Medical is one of the largest manufacturers of medical devices focused on treating cardiac, neurological and chronic pain patients. I'm working with their research & development team on the design of their next generation of medical devices and cloud platform.

**Research Experience**

- **Graduate Research Assistant** (2011-Present)
  My research focuses on improving the security of emerging technologies and resource limited devices. The projects I have been involved with have made me an expert in the design, implementation, and evaluation of computer systems. My interdisciplinary work has enabled me to work closely with distinguished faculties from different institutes and backgrounds.
  - **Internet of Things Security:** The growing trend of incorporating computer systems into everyday devices has turned mundane items in our buildings, cars, and cities into devices with sensing, computation, and communication capabilities. These capabilities enable devices to collect an unprecedented amount of information on user activities and create opportunity for attackers to breach and gain control of these systems. My research has looked at security shortcomings in current IoT systems [15], and proposed frameworks for practical fine-grained end-to-end data flow control [10,11], context-specific access-control [14,8], and privacy-adhesive data collection [16,13].
  - **Embedded Device Security:** Embedded devices are faced with unique security challenges due to their computational and energy limitations. I have tackled the problem of timekeeping in passively powered embedded devices and implemented a novel mechanism based on volatile memory decay that provided a coarse-grained sense of time to these devices [I,2,12]. The insights from this this work led me to design a new type of physical unclonable function (PUF) that provides much higher entropy compared to traditional approaches [1,5].
  - **Approximate Computing:** Approximate Computing is an emerging research area that seeks to trade-off computation accuracy for performance and power consumption. My research is the first work to explore the privacy implications of approximate memory [7], uncover several incorrect presumptions used in design of memory energy saving schemes [4], and explore the feasibility of using Flash memory as Approximate Storage [9].
  - **Medical Device Security:** Legacy systems, lack of updates, and limitations on installing security software and mechanisms have made the medical domain especially vulnerable to malware infections. To address these challenges, we developed a side-channel based malware detection system that detects anomalies in systems without the need for hardware or software modifications [II,3]. As part of a separate project, I have examined the existence of malware in the clinical domain by collecting and studying real traces from hospital networks [IV]. I have also studied the security challenges and risks that exist in the hospital networks and have provided guidelines for effective research in this space [6].
- **Undergraduate Research Assistant** in the **Dependable Systems Laboratory** (2010-2011)
  As an undergraduate research assistant, I worked closely with two graduate students on the design and implementation of a register file partitioning algorithm aimed at increasing the reliability of the system. I was also involved with a group of undergraduate students in a comparative study of real-time operating systems. In this work we developed standard environment and benchmarks to compare different performance metrics between OSes.

## Teaching Experience

- **University of Michigan** (2015-2017)
  - Primary instructor for Computer & Network Security
  - Graduate student instructor for Major Design, and Distributed Systems
- **University of Massachusetts Amherst** (2011)
  Lab instructor for Computer Literacy
- **Sharif University of Technology** (2009-2011)
  Teaching assistant for Digital System Design, Operating Systems, and Discrete Structures

## Publications

16. **Amir Rahmati**, Earlence Fernandes, Kevin Eykholt, Xinheng Chen, Atul Prakash, *"Heimdall: A Privacy-Respecting Implicit Preference Collection Framework"*, In the $15^{th}$ ACM International Conference on Mobile Systems, Applications, and Services (MobiSys'17) . Niagara Falls, NY, June 2017
15. Earlence Fernandes, **Amir Rahmati**, Jaeyeon Jung, Atul Prakash, *"The Security Implications of Permission Models of Smart Home Application Frameworks"*, In IEEE Security & Privacy, April 2017
14. Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, **Amir Rahmati**, Earlence Fernandes, Z. Morley Mao, Atul Prakash, *"ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms"*, In Proceedings of the $21^{st}$ Network and Distributed System Security Symposium (NDSS'17) . San Diego, CA, March 2017
13. Han Zhang, Kasra Edalat Nejad, **Amir Rahmati**, Harsha V. Madhyastha *"Towards Comprehensive Repositories of Opinions"*, In $15^{th}$ ACM Workshop on Hot Topics in Networks (HotNets'16). Atlanta, GA, November 2016
12. Josiah Hester, **Amir Rahmati**, Daniel Holcomb, Kevin Fu, Jacob Sorber *"Techniques for Timekeeping Without a Clock"*, In Transactions on Embedded Computing Systems (TECS'16).
11. **Amir Rahmati**, Earlence Fernandes, Atul Prakash, *"Applying the Opacified Computation Model to Enforce Information Flow Policies in IoT Applications"*, In Proceedings of the $1^{st}$ IEEE Cybersecurity Development Conference (SecDev'16) . Boston, MA, November 2016
10. Earlence Fernandes, Justin Paupore, **Amir Rahmati**, Daniel Simionato, Mauro Conti, Atul Prakash, *"FlowFence: Practical Data Protection for Emerging IoT Application Frameworks"*, In Proceedings of the $25^{th}$ USENIX Security Symposium (USENIX Sec'16). Austin, TX, August 2016
9. **Amir Rahmati**, Matthew Hicks, Atul Prakash, *"Approximate Flash Storage: A Feasibility Study"*, In the Workshop on Approximate Computing Across the System Stack (WAX'16). Atlanta, GA, April 2016
8. **Amir Rahmati**, Harsha V. Madhyastha *"Context-Specific Access Control: Conforming Permissions With User Expectations"*, In $5^{th}$ ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (CCS'SPSM). Denver, CO, October 2015
7. **Amir Rahmati**, Matthew Hicks, Daniel Holcomb, Kevin Fu *"Probable Cause: The Deanonymizing Effects of Approximate DRAM"*, In $42^{nd}$ Int. Symposium on Computer Architecture (ISCA'15). Portland, OR, June 2015
6. Sai R. Gouravajhala, **Amir Rahmati**, Peter Honeyman, and Kevin Fu, *"Malware Prognosis: How to Do Malware Research in Medical Domain"*, In USENIX Workshop on Health Information Technologies (Health Tech'14). San Diego, CA, August 2014
5. Xiaolin Xu, **Amir Rahmati**, Daniel Holcomb, Kevin Fu, Wayne Burleson *"Reliable Physical Unclonable Functions using Data Retention Voltage of SRAM Cells"*, in IEEE Transactions on CAD: Special Section on Hardware Security and Trust (TCAD).
4. **Amir Rahmati**, Matthew Hicks, Daniel Holcomb, Kevin Fu, *"Refreshing Thoughts on DRAM: Power Saving vs. Data Integrity"*, In the Workshop on Approximate Computing Across the System Stack (WACAS'14). Salt Lake City, UT, March 2014
3. Shane Clark, Benjamin Ransford, **Amir Rahmati**, Shane Guineau, Jacob Sorber, Wenyuan Xu, Kevin Fu, *"WattsUpDoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices"*, In USENIX Workshop on Health Information Technologies (Health Tech'13). Washington, D.C., August 2013
2. **Amir Rahmati**, Mastooreh Salajegheh, Daniel Holcomb, Jacob Sorber, Wayne Burleson, Kevin Fu, *"TARDIS: Time and Remanence Decay in SRAM to Implement Secure Protocols on Embedded Devices without Clocks"*, In Proceedings of the $21^{st}$ USENIX Security Symposium (USENIX Sec'12). Bellevue, WA, August 2012
1. Daniel Holcomb, **Amir Rahmati**, Mastooreh Salajegheh,Wayne Burleson, Kevin Fu, *"DRV-Fingerprinting: Using Data Retention Voltage of SRAM Cells for Chip Identification"*, In The $8^{th}$ Workshop On RFID Security And Privacy 2012 (RFIDsec'12). Nijmegen, The Netherlands, July 2012

## Selected Posters and Invited Talks

IV. **Stigmalware: Investigating the Prevalence of Malware in the Clinical Domain.**
- 35th Annual IEEE Symposium on Security and Privacy (IEEE S&P'14). April 2014

III. **Ahem: Additively Homomorphic Encryption for the Moo**
- Workshop on Cryptographic Hardware and Embedded Systems (CHES'13), August 2013

II. **Using Side Channels To Do Good**
- Workshop on Cryptographic Hardware and Embedded Systems (CHES'13), August 2013

I. **Time and Remanence Decay in SRAM**
- MIT Security Seminar series, Cambridge, MA, October 2012
- $3^{rd}$ Annual Pay-as-you-Go Workshop, Amherst, MA, July 2012
- $33^{rd}$ Annual IEEE Symposium on Security and Privacy (IEEE S&P'12), May 2012

## Honors and Awards

◇ **Student Travel Grant Recipient:** RWC'16, SecDev'16, CCS'15, ISCA'15, IEEE S&P'15, SOUPS'14, ASPLOS'14, CHES'13, IEEE S&P'13, USENIX Sec'12

◇ Ranked **1st** at the **Sharif Freshmen ACM Challenge** (2007)
Programming contest held for the freshmen entering Sharif University.

◇ Member of The **National Organization for Development of Exceptional Talents** (2000-Present)
The organization is responsible for a number of schools across Iran and trains the top students on a more advanced level on every field of study.

## Services

◇ **PC Member:** SEMS'17, SecCPS'17

◇ **Reviewer:** DSN'17, ICC'17, INFOCOM'17, CHI'17, IEEE MoST'17, NDSS'16, Micro's Top Picks'15, USENIX Sec'14, '13, '12, Canadian Journal of Electrical & Computer Engineering, Journal of Wireless Networks (WINET)

◇ **PC Meeting Secretary:** USENIX Sec'14, '13

◇ **Student Scribe:** ASPLOS'14, USENIX Sec'12

## Skills

◇ **Programming:** C, C#, C++, Java, Python, Basic, Assembly, Verilog HDL, VHDL, Prolog, MATLAB

◇ **Web:** HTML, JavaScript, PHP, MySQL

◇ **Software Tools:** Network Simulator, Packet Tracer, Wireshark

◇ **Hardware Tools:** ModelSim, Synplify, Altera Quartus, CodeVision AVR, Proteus, Xilinx ISE, HSPICE

## Activities

◇ **Manager** of University of Michigan **Systems Reading Group (SRG)** (2015-2016)

◇ **Presenter** in Security (SECRIT), Systems (SRG), and Advanced Architecture (ACAL) Reading Group, University of Michigan (2013-Present)

◇ **Elected Head** of the Computer Engineering Dept. **Student Scientific Chapter (SSC)** (2010)
SSC is the student committee concerned with directing the department extra-curriculum activities.

◇ **Computer & IT Editor and freelancer** for Sharif Daily, Sharif's official newspaper (2009-2010)
Writing has always been attractive to me and I have written several articles for the science page of Sharif Daily newspaper. I was also the editor of Computer & IT page for a three month term.

◇ **Technical Manager** - 11th ACM/ICPC - Asia Region (2009)
I directed and managed the IT team to assemble, setup, and manage over 100 PC workstations and their network for the contest, many from individual components, on a very short timeframe (5 days). It proved to be a strong technical and management challenge requiring 24x7 attention and devotion.