

# Amir Rahmati

Assistant Professor  
Department of Computer Science  
Stony Brook University  
February 22, 2022

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 and privacy of emerging technologies and resource-limited devices, such as embedded and Internet of Things (IoT) devices, AR systems, and Machine Learning systems. My work involves designing, building, and evaluating systems that tackle security challenges in these domains. As we move toward a connected, ML-driven world where many resource and energy limited devices have access to our data and activities, my research creates an avenue for these systems to incorporate security and privacy in their design.
- Positions**
- **Assistant Professor, Department of Computer Science, Stony Brook University (2018-Present)**
  - **System Architect, KNOX Security, Samsung Research America (2017-2018)**
- 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**
- *Stony Brook University*
    - **WISE: Research and Discovery in STEM (WSE380):** Spring'21, Fall'21
    - **Software Security (CSE360):** Fall'21
    - **Computer Security Fundamentals (CSE331):** Fall'20
    - **Network Security (CSE508):** Spring'22, Fall'19,'18
    - **Seminar in Computer Security (CSE659):** Spring'21,'20,'19, Fall'21,'20,'19,'18
  - *University of Michigan*
    - **Computer & Network Security (EECS588):** Winter'17
- Conference Publications**
14. *“Transferring Adversarial Robustness Through Robust Representation Matching”*  
Pratik Vaishnavi, Kevin Eykholt, Amir Rahmati  
USENIX Security Symposium (USENIX Sec'22). August 2022
  13. *“Good Bot, Bad Bot: Characterizing Automated Browsing Activity”*  
Xigao Li, Babak Amin Azad, Amir Rahmati, Nick Nikiforakis  
IEEE Symposium on Security and Privacy (S&P'21). May 2021      ★ *Best Film Editing Award*
  12. *“Valve: Securing Function Workflows on Serverless Computing Platforms”*  
Pubali Datta, Prabuddha Kumar, Tristan Morris, Michael Grace, Amir Rahmati, Adam Bates  
The Web Conference (WWW'20). Apr 2020
  11. *“An Intent-Based Automation Framework for Securing Dynamic Consumer IoT Infrastructures”*  
Vasudevan Nagendra, Arani Bhattacharya, Vinod Yegneswaran, Amir Rahmati, Samir Das  
The Web Conference (WWW'20). Apr 2020
  10. *“Tyche: A Risk-Based Permission Model for Smart Homes”*  
Amir Rahmati, Earlence Fernandes, Kevin Eykholt, Atul Prakash  
IEEE Cybersecurity Development Conference (SecDev'18). Oct 2018      ★ *Best Research Paper Award*
  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, Bo Li, Amir Rahmati, Chaiwei Xiao, Atul Prakash, Tadayoshi Kohno, 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. *“ContextIoT: Towards Providing Contextual Integrity to Apified 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 Deanonimizing 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

15. *“Can Attention Masks Improve Adversarial Robustness?”*  
Pratik Vaishnavi, Tianji Cong, Kevin Eykholt, Atul Prakash, Amir Rahmati  
AAAI Workshop on Engineering Dependable and Secure Machine Learning Systems (EDSMLS’20). February 2020
14. *“Protecting Visual Information in Augmented Reality from Malicious Application Developers”*  
Jinhan Hu, JK Jensen, Amir Rahmati, Robert LiKamWa  
ACM Workshop on Wearable Systems and Applications (WearSys’19). June 2019
13. *“The State of Physical Attacks on Deep Learning Systems”*  
Earlence Fernandes, Ivan Evtimov, Kevin Eykholt, Chaowei Xiao, Amir Rahmati, Florian Tramer, Bo Li, Atul Prakash, Tadayoshi Kohno, Dawn Song  
USENIX Summit on Hot Topics in Security (HotSec’18). August 2018
12. *“Physical Adversarial Examples for Object Detectors”*  
Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Florian Tramer, Atul Prakash, Tadayoshi Kohno, Dawn Song  
USENIX Workshop on Offensive Technologies (WOOT’18). August 2018
11. *“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  
Workshop on the Bright and Dark Sides of Computer Vision (CV-COPS’18). June 2018
10. *“Caterpillar: Iterative Concolic Execution for Stateful Programs”*  
Laurent Simon, Shuying Liang, Amir Rahmati, Mike Grace  
International KLEE Workshop on Symbolic Execution (KLEE’18). April 2018
9. *“Securing Trigger-Action Platforms”*  
Earlence Fernandes, Amir Rahmati, Jaeyeon Jung, Atul Prakash  
USENIX Summit on Hot Topics in Security (HotSec’17). August 2017
8. *“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
7. *“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
6. *“Approximate Flash Storage: A Feasibility Study”*  
Amir Rahmati, Matthew Hicks, Atul Prakash  
Workshop on Approximate Computing Across the System Stack (WAX’16). April 2016
5. *“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

4. *“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
3. *“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
2. *“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
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 (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

*Other  
Publications*

8. *“New Problems and Solutions in IoT Security and Privacy”*  
Earlence Fernandes, Amir Rahmati, Nick Feamster  
Preprint (arXiv:1910.03686). Oct 2019
7. *“Transferable Adversarial Robustness using Adversarially Trained Autoencoders”*  
Pratik Vaishnavi, Kevin Eykholt, Atul Prakash, Amir Rahmati  
Preprint (arXiv:1909.05921). Sep 2019
6. *“Robust Classification using Robust Feature Augmentation”*  
Kevin Eykholt, Swati Gupta, Atul Prakash, Amir Rahmati, Pratik Vaishnavi, Haizhong Zheng  
Preprint (arXiv:1905.10904). May 2019
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 (S&P Magazine), Special Issue on Systems Attacks and Defenses. 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 (S&P Magazine) Volume 15, Issue 2. 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

*Patents*

1. *“US20190334906A1: System and method for flow-based architecture”*

*Selected Posters*

5. *“Design of Privacy Preservation System in Augmented Reality”*  
Yoonsang Kim, Saeed Boorboor, Amir Rahmati, Arie Kaufman  
IEEE Symposium on Visualization for Cyber Security (VizSec’21). Oct 2021
4. *“Automatic Detection of Confused-Deputy Attacks on ARM TrustZone Environments”*  
Darius Suci, Stephen McLaughlin, Hayawardh Vijayakumar, Lee Harrison, Michael Grace, Amir Rahmati  
IEEE Cybersecurity Development Conference (SecDev’18). Oct 2018
3. *“Toward Secure and Serverless Trigger-Action Platforms”*  
Pubali Datta, Tristan Morris, Hayawardh Vijayakumar, Michael Grace, Adam Bates, Amir Rahmati  
IEEE Cybersecurity Development Conference (SecDev’18). Oct 2018

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*

8. *“What is Cybersecurity?”*  
Panelist at LIFC November Educational Series. November 2021
7. *“Smart Infrastructure”*  
Panelist at CEWIT 2021 Conference (CEWIT’21). November 2021
6. *“Verifying Sensor-Noise Robustness of Reinforcement Learning”*  
Invited talk at Trusted AI at Scale. July 2021
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<sup>rd</sup> Annual Pay-as-you-Go Workshop. July 2012

*Professional Service*

- **Steering Committee:** CEWIT’20
- **Organizing Committee:** SafeThings’21, USENIX Sec’20, CCS’20, WWW’20, SACMAT’20
- **PC Member:** ICML’22, USENIX Sec’22,’21,’20, WWW’22,’21,’20, SafeThings’22,’21,’20,’19,’18,’17, CCS’21, DSN-DSML’21, SACMAT’21,’20, SPWID’20, EWiLi’19, IoTSec’19, IoT S&P’18, SEMS’17, SecCPS’17
- **Reviewer:** Journal of Computer Security’21, IEEE Security & Privacy’21, IEEE Transactions on Information Forensics & Security’21, Transactions on Software Engineering’21, IEEE Transactions on Image Processing’21, IEEE Sensors’21,’20,’19, Applied Sciences’21, Electronics’21,’20,’19, Journal of Cybersecurity and Privacy’21, Computers’21, IEEE Internet of Things Journal’20,’19,’18, IEEE Internet Computing’20, Symmetry’20, Sustainability’20, Concurrency and Computation: Practice and Experience’20, IEEE Transaction on VLSI Systems’19, IEEE Transaction on Mobile Computing’19, Future Internet’18, IEEE Transactions on Dependable and Secure Computing’18, IEEE Transactions on Information Forensics & Security’18, CCS’18, USENIX ATC’18, CHI’18,’17, DSN’17, ICC’17, INFOCOM’17, IEEE MoST’17, NDSS’16, Micro’s Top Picks’15, Canadian Journal of Electrical & Computer Engineering’15, USENIX Sec’14,’13,’12, Journal of Wireless Networks (WINET’12)
- **Panelist:** NSF Secure & Trustworthy Cyberspace (SaTC) March’22, April’17
- **Organizer:** Stony Brook CS Graduate Research Day’21,’19, SBU Graduating Student List, SBU CS Academic Job Panel’19, SBU CS Open House’19, CS Grad Orientation Security Area’19,’18
- **Judge:** WAC Lighting Foundation Invitational Science Fair’22, AFRL SFFP’21, DoD SMART Scholarship’22,’21,’20, Catacosinos Fellowship’19, NDSEG Fellowship’20,’19, SBU 3-Minute Thesis Competition’19, SBUHacks Hackathon’19,’18
- **Mentor:** FIT Engineering Design Workshop’19
- **Departmental Committees:**
  - SBU CS Graduate Grievance and Appeals Committee (’20)
  - SBU CS Diversity Committee (’19-Present)
  - SBU CS Graduate Curriculum Committee (’19-Present)
  - SBU CS Graduate Admission Committee (’18-Present)

*Consulting*

- Subject Matter Expert, ASR International Corporation (2019)
- System Consultant, Abbott Laboratories (2017)

*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. Some of the artifacts of this project are displayed at the London Science Museum and German Hygiene Museum. IEEE Spectrum, Yahoo News, Wired, Engadget, Telegraph, Car and Driver, CNET, Digital Trends, SCMagazine, Schneier on Security, Ars Technica, and Fortune were among the outlets that covered these findings.

- **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.
- **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.

*Honors and Awards*

- **Best Research Paper Award:** IEEE Cybersecurity Development Conference, 2018
- Member of Iran’s **National Organization for Development of Exceptional Talents** (2000-Present)

*Advising and Mentorship*

– **Ph.D. Students:**

|                    |   | <b>Status</b>   |
|--------------------|---|-----------------|
| - Sanket Goutam    | (2021-Present)                                    | Pre-Quals       |
| - Veena Krish      | (2019-Present)                                    | Ph.D. Candidate |
| - Xigao Li         | (2018-Present) [Co-advised with Nick Nikiforakis] | Ph.D. Candidate |
| - Pratik Vaishnavi | (2018-Present)                                    | Ph.D. Candidate |

– **Master Students:**

|                       |                | <b>Went on to</b>   |
|-----------------------|----------------|---|
| - Kalpan Tumdi        | (2022-Present) |   |
| - Tirth Mehta         | (2022-Present) |   |
| - Archit Gajpal       | (2022-Present) |   |
| - Farhan Ahmed        | (2021-Present) |   |
| - Karan Gada          | (2021-Present) |   |
| - Ajay Sarjoo         | (2021-Present) |   |
| - Atharva Kadam       | (2021-Present) |   |
| - Gaurav Verma        | (2019-2020)    | <i>Research Aide at Argonne National Laboratory</i>         |
| - Debapriya Mukherjee | (2019-2020)    | <i>Software Engineering Analyst at BlackRock</i>            |
| - Ravinder Singh      | (2019-2020)    | <i>Software Development Engineer at Amazon</i>              |
| - Raunak Laddha       | (2019-2020)    | <i>Technical Staff at Oracle</i>                            |
| - Gaurang Khanwalkar  | (2019-2020)    | <i>Software Development Engineer at Amazon Web Services</i> |
| - Shivam Singh        | (2019-2020)    | <i>Software Development Engineer at Amazon</i>              |
| - Niranjana Agnihotri | (2019-2020)    | <i>Software Engineer at Microsoft Azure Storage</i>         |
| - Harsh Chandnani     | (2019-2020)    | <i>Software Development Engineer at Amazon</i>              |
| - Diksha Saini        | (2019-2020)    | <i>Software Development Engineer at Amazon</i>              |
| - Prabuddha Kumar     | (2018-2020)    | <i>Software Development Engineer at Amazon</i>              |
| - Vivek Sah           | (2018-2019)    | <i>Software Development Engineer at Audible</i>             |
| - Govindrao Kulkarni  | (2018-2019)    | <i>Software Engineer at Oracle</i>                          |
| - Hardik Singh Negi   | (2018-2019)    | <i>Software Engineer at VMWare</i>                          |
| - Michael Anderson    | (2018-2019)    | <i>Data Scientist at LMI Government Consulting</i>          |
| - Aditya Godambe      | (2018-2019)    | <i>Software Engineer at Amazon</i>                          |
| - Vinod Loganathan    | (2019-2019)    | <i>Software Engineer at Twitter</i>                         |

– **Undergraduate Students:**

|                 |                | <b>Went on to</b>                               |
|-----------------|----------------|---|
| - Jack Liu      | (2021-Present) |   |
| - Farhan Ahmed  | (2019-2021)    | <i>Master Student at Stony Brook University</i> |
| - Ajay Sarjoo   | (2019-2020)    | <i>Master Student at Stony Brook University</i> |
| - Atharva Kadam | (2019-2020)    | <i>Master Student at Stony Brook University</i> |
| - Tejaswi Gorde | (2019-2020)    | <i>Tech Analyst at Bank of America</i>          |
| - Gaurav Gandhi | (2019-2020)    | <i>Software Engineer at Amazon Web Services</i> |
| - Shilong Li    | (2019-2020)    | <i>Master Student at Stony Brook University</i> |
| - Avik Kadakia  | (2019-2020)    | <i>Software Engineer at Epic</i>                |

– **Visiting Students:**

**Went on to**

- Yuxin Sun (Tongji University, 2019) *Graduate Student at ETH Zurich*

– **Doctoral Committees:**

- Thang Bui (02/2021) “Mining Relationship-Based Access Control Policies”
- Aria Rezaei (12/2020) “On Challenges in Privacy Protection for Social and Correlated Data”
- Vasudevan Nagendra (12/2019) “Towards Achieving Performance, Scalability and Security in Emerging Network Infrastructures”
- Abbas Razzaghpanah (10/2019) “Lumen: Studying Mobile Apps Using Crowd-Sourced Data in User Space”

– **Masters Committees:**

- Sayali Anil Alatar (05/2020) “Causal Inference in Smart Homes through Traffic Signatures”

– **Research Proficiency Committees:**

- Zavosh Mottahedeh (12/2021) “A Survey of Techniques for Improvement of DNN Accelerators”
- Veena Krish (12/2021) “Robustness of Cyber-Physical Systems under Adversarial Observation Uncertainty”
- Farid Samandi (02/2021) “Leveraging FPGA Layout to Minimize Jitter in Statistical Time-to-Digital Converters”
- Pratik Vaishnavi (10/2020) “Model-agnostic Approaches for Improving Adversarial Robustness of Visual Recognition Models”
- Xigao Li (08/2020) “Characterizing Automated Browsing Activity over the Internet”
- Sanaz Sheikhi (01/2020) “Attack Detection and Forensic Reconstruction of Cyber Attack Campaigns”
- Raveendra Soori (12/2019) “NUCAlloc: Fine-Grained Block Placement in Hashed Last-Level NUCA Caches”
- Hamed Ghavamnia (07/2019) “Attack Surface Reduction for Software in Container Environments”
- Darius-Andrei Suciu (08/2017) “How TrustZone can help improve mobile device security”