

Amir Rahmati

Assistant Professor, Computer Science
Affiliated Professor, Electrical & Computer Engineering
Stony Brook University
August 10, 2026

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 I'm interested in improving the security and privacy of emerging technologies, such as Cyber-Physical, AR/VR, and Machine Learning systems. My work focuses on designing, building, and evaluating practical solutions that tackle security and privacy challenges in these domains. As we move toward a connected, ML-driven world, my research creates an avenue for these systems to incorporate security in their design.

Positions

- Assistant Professor, Department of Computer Science, Stony Brook University (2018-Present)
 - Affiliated Faculty, Department of Electrical & Computer Engineering (2025-Present)
- Adjunct Faculty, School of Engineering, University of Guelph (2025-Present)
- System Architect, KNOX Security, Samsung Research America (2017-2018)
- Senior System Engineer, Saint Jude Medical, (2016-2017)

Professional Memberships

- National Academy of Inventors (NAI) Senior Member
- Institute of Electrical and Electronics Engineers (IEEE) Senior Member
- Global Anti-Scam Alliance (GASA) Associate Member

Education

- **Ph.D. in Computer Science and 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

- *Stony Brook University*
 - *Graduate Courses*
 - **Computer Architecture (CSE502):** Fall'25
 - **Computer System Security (CSE509):** Fall'23
 - **Network Security (CSE508):** Fall'22,'19,'18, Spring'22
 - **Seminar in Computer Security (CSE659):** Fall'24-'18, Spring'25-'19, Summer'22
 - *Undergraduate Courses*
 - **Software Security (CSE360):** Fall'25-'21
 - **Computer Security Fundamentals (CSE331):** Fall'24,'20
 - **Senior Honors Research Project I/II (CSE495/496):** Spring'25,Fall'24
 - **WISE Honors Research Project I/II (WSE495/496):** Spring'25,Fall'24
 - **Undergraduate College Seminar (SBU 102):** Spring'25
 - **WISE: Research and Discovery in STEM (WSE380):** Fall'21, Spring'21
 - *K-12 Engagements*
 - **Simons Summer Research Program for K12 students:** Summer'26,'25
 - **CS & Informatics Research Experience for K12 students (CSIRE):** Summer'26-'22
- *Stony Brook Institute at Anhui University*
 - **Fundamentals of Computer Security (YJ40212):** Spring'25,'24
- *University of Michigan*
 - **Computer & Network Security (EECS588):** Winter'17
- *University of Massachusetts, Amherst*
 - **Computer Literacy (COMPSCI-105):** Lab instructor - Fall'11

Honors and
Awards

- **Certified Information Systems Security Professional (CISSP)**, 2026
- **Young Academic Inventor Award**, National Academy of Inventors (NAI), 2026
- **National Academy of Inventors (NAI) Senior Member**, 2025
- **CSAW Applied Research Competition Finalist**, 2024
- **Faculty Leadership Award**, Department of Computer Science, Stony Brook University, 2024
- **Best Student Presentation Award**, ACM CCS Workshop Cybersecurity in Healthcare (HealthSec), 2024
- **Best Repeatability Evaluation Award**, International Conference on Cyber-Physical Systems (ICCPS), 2024
- **Institute of Electrical and Electronics Engineers (IEEE) Senior Member**, 2024
- **Distinguished Paper Award**, Network and Distributed System Security Symposium (NDSS), 2024
- **Meta Research Award**, 2022
- **Facebook Research Award**, 2020
- **NVIDIA Grant**, 2018
- **Best Research Paper Award**, IEEE Cybersecurity Development Conference (SecDev), 2018
- **Elected Head of the Sharif University Computer Engineering Dept. Student Scientific Chapter (SSC)**, 2010
- Member of Iran's **National Organization for Development of Exceptional Talents (NODET)**, 2000

Conference
Publications

30. “*AppScopes: Fine-grained Access Control for App Collaboration on Android*”
Sanket Goutam, Kasra Kakaee, Amir Rahmati
IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS’26).
Nov. 2026
29. “*Taking a Bite Out of the Forbidden Fruit: Characterizing Third-Party Iranian App Stores*”
Amir Hossein Khanlari, Amir Rahmati
ACM Internet Measurement Conference (IMC’26). October 2026
28. “*Atlas: Enabling Cross-Vendor Authentication for IoT*”
Sanket Goutam, Omar Chowdhury, Amir Rahmati
EAI Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles (SMARTSP’26). Nov. 2026
27. “*Proteus: A Practical Framework for Privacy-Preserving Device Logs*”
Sanket Goutam, Hunter Kippen, Michael Grace, Amir Rahmati
Privacy Enhancing Technologies Symposium (PETS’26). July, 2026.
26. “*Obfusc8: LLM-Augmented PowerShell Obfuscation*”
Kwangyun Keum, Dheeraj Kumar, Bogdan Barchuk, Sai Chand Boyapati, Rohit Deopura, Amir Rahmati
IEEE Secure Development Conference (SecDev’25). October 2025.
25. “*Understanding Minimal-Time Attacks Against Reinforcement Learning Agents*”
Veena Krish, Amir Rahmati
IEEE Secure Development Conference (SecDev’25). October 2025.
24. “*On User Privacy in MNO: Machine Unlearning Techniques for Data Compliance and Security*”
Emanuel Figetakis, Ahmed Refaey Hussein, Amir Rahmati
IEEE International Conference on Communications (ICC’25). June 2025
23. “*The Poorest Man in Babylon: A Longitudinal Study of Cryptocurrency Investment Scams*”
Muhammad Muzammil, Abisheka Pitumpe, Xigao Li, Amir Rahmati, Nick Nikiforakis
The Web Conference (WWW’25). May 2025
22. “*Fast Koopman Surrogate Falsification using Linear Relaxations and Weights*”
Stanley Bak, Abdelrahman Hekal, Niklas Kochdumper, Ethan Lew, Andrew Mata and Amir Rahmati
International Symposium on Automated Technology for Verification and Analysis (ATVA’24). October 2024
21. “*Biosignal Authentication Considered Harmful Today*”
Veena Krish, Nicola Paoletti, Milad Kazemi, Scott Smolka, Amir Rahmati
USENIX Security Symposium (USENIX Sec’24). August 2024
20. “*Zero-One Attack: Degrading Closed-Loop Neural Network Control Systems using State-Time Perturbations*”
Stanley Bak, Sergiy Bogomolov, Abdelrahman Hekal, Veena Krish, Andrew Mata, Amir Rahmati
International Conference on Cyber-Physical Systems (ICCPS’24). May 2024 ★ *Best Repeatability Evaluation Award*
19. “*Falsification using Reachability of Surrogate Koopman Models*”
Stanley Bak, Sergiy Bogomolov, Abdelrahman Hekal, Niklas Kochdumper, Ethan Lew, Andrew Mata, Amir Rahmati
ACM International Conference on Hybrid Systems: Computation and Control (HSCC’24). May 2024

18. *“Like, Comment, Get Scammed: Characterizing Comment Scams on Media Platforms”*
Xigao Li, Amir Rahmati, Nick Nikiforakis
Network and Distributed System Security Symposium (NDSS’24). February 2024
★ *Distinguished Paper Award* ★ *CSAW 2025 Applied Research Competition Finalist*
17. *“Erebus: Access Control for Augmented Reality Systems”*
Sanket Goutam, Yoonsang Kim, Amir Rahmati, Arie Kaufman
USENIX Security Symposium (USENIX Sec’23). August 2023
16. *“Scan Me If You Can: Understanding and Detecting Unwanted Vulnerability Scanning”*
Xigao Li, Babak Amin Azad, Amir Rahmati, Nick Nikiforakis
The Web Conference (WWW’23). April 2023
15. *“Accelerating Certified Robustness Training via Knowledge Transfer”*
Pratik Vaishnavi, Kevin Eykholt, Amir Rahmati
Conference on Neural Information Processing Systems (NeurIPS’22). November 2022
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). April 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). April 2020
10. *“Tyche: A Risk-Based Permission Model for Smart Homes”*
Amir Rahmati, Earlene Fernandes, Kevin Eykholt, Atul Prakash
IEEE Cybersecurity Development Conference (SecDev’18). October 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, Earlene Fernandes, Bo Li, Amir Rahmati, Chaowei 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”*
Earlene 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, Earlene 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 Appified IoT Platforms”*
Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlene 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, Earlene Fernandes, Atul Prakash
IEEE Cybersecurity Development Conference (SecDev’16). November 2016
3. *“FlowFence: Practical Data Protection for Emerging IoT Application Frameworks”*
Earlene Fernandes, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti, Atul Prakash
USENIX Security Symposium (USENIX Sec’16). August 2016
2. *“Probable Cause: The Deanononymizing 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

Journal
Publications

6. “On the Security of RL-Based Artificial Pancreas Systems”
Preston Chang, Veena Krish, and Amir Rahmati
Communications in Computer and Information Science (CCIS’25). Dec 2025
5. “A Study of the Effects of Transfer Learning on Adversarial Robustness”
Pratik Vaishnavi, Kevin Eykholt, Amir Rahmati
Transactions on Machine Learning Research (TMLR’24). May 2024
4. “Provable Observation Noise Robustness for Neural Network Control Systems”
Veena Krish, Andrew Mata, Kerianne Hobbs, Stanley Bak, Amir Rahmati
Research Directions: Cyber-Physical Systems. November 2023
3. “Synthesizing Pareto-Optimal Signal-Injection Attacks on ICDs”
Veena Krish, Nicola Paoletti, Scott A. Smolka, Amir Rahmati
IEEE Access (Access’23). January 2023
2. “Persistent Clocks for Batteryless Sensing Devices”
Josiah Hester, Nicole Tobias, Amir Rahmati, Lanny Sitanayah, Daniel Holcomb, Kevin Fu, Wayne Burleson, Jacob Sorber
ACM 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

Workshop
Publications

21. “From Fake Job Offer to Full Environment Compromise: Anatomy of the Contagious Interview Campaign”
Abisheka Pitumpe, Jan Podleski, Amirhossein Khanlari, Piotr Dziubecki, Devendran Muthukumaramani, Amir Rahmati
International Workshop on Cyber Crime 2026 (IWCC’26). August 2026
20. “GitTemporalAI: Leveraging Temporal Knowledge Graphs and LLMs for Multi-Agent Repository Intelligence”
Dongsheng Luo, Raju Rangaswami, Amir Rahmati, Erez Zadok
Multi-Agent AI in the Real World Workshop at AAAI 2025 (MARV’25). March 2025
19. “Security Analysis of RL-Based Artificial Pancreas Systems”
Preston Chang, Veena Krish, Amir Rahmati
ACM CCS Workshop “Cybersecurity in Healthcare” (HealthSec’24). Oct. 2024 ★ *Best Student Presentation Award*
18. “On the Feasibility of Compressing Certifiably Robust Neural Networks”
Pratik Vaishnavi, Veena Krish, Farhan Ahmed, Kevin Eykholt, Amir Rahmati
Workshop on Trustworthy and Socially Responsible Machine Learning (TSRML’22). December 2022
17. “Ares: A System-Oriented Wargame Framework for Adversarial ML”
Farhan Ahmed, Pratik Vaishnavi, Kevin Eykholt, Amir Rahmati
IEEE Deep Learning and Security Workshop (DLS’22). May 2022
16. “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). October 2021
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, Wenyan 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
- Other Publications
12. *“Scams at Scale: Unmasking Crypto Fraud and Social Engineering on the Modern Web”*
Abisheka Pitumpe, Muhammad Muzammil, Xigao Li, Nick Nikiforakis, Amir Rahmat
XRDS: Crossroads, The ACM Magazine for Students. Summer 2025
 11. *“Taking off the Rose-Tinted Glasses: A Critical Look at Adversarial ML Through the Lens of Evasion Attacks”*
Kevin Eykholt, Farhan Ahmed, Pratik Vaishnavi, Amir Rahmati
Preprint (arXiv:2410.12076). October 2024
 10. *“Growing Energy Resiliency Through Research”*
William Anderson, Arie Kaufman, Amir Rahmati, Yoonsang Kim, Sanket Goutam, Michael Gouzman, Yacov Shamash, Alex Shevchenko, Claran J. Marti, Nicolaos Maltas, Peng Zhang, Yifan Zhou, Benjamin Hsiao, Vyacheslav Solovyov, Juan Pablo Trelles, Fanglin Che, Hsi-Wu Wong, Alessandro Sabato, Christopher Niezrecki, Douglas Van Bossuyt, Dan Nussbaum, H. Scott Coombe
Future Force. Vol. 9, No. 1. April 2023
 9. *“Decentralized cooperative communication-less multi-agent task assignment with monte-carlo tree search”*
Mohammadreza Daneshvaramoli, Mohammad Sina Kiarostami, Saleh Khalaj Monfared, Helia Karisani, Hamed Khashehchi, Dara Rahmati, Saeid Gorgin, Amir Rahmati
Preprint (arXiv:1910.12062). October 2019
 8. *“New Problems and Solutions in IoT Security and Privacy”*
Earlence Fernandes, Amir Rahmati, Nick Feamster
Preprint (arXiv:1910.03686). October 2019
 7. *“Transferable Adversarial Robustness using Adversarially Trained Autoencoders”*
Pratik Vaishnavi, Kevin Eykholt, Atul Prakash, Amir Rahmati
Preprint (arXiv:1909.05921). September 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, Earlece 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?"*
Earlece 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"*
Earlece 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 Dimensions of State Repression"*
Meredith Blank, Anita Ravishankar, Amir Rahmati
Cyber Conflict Project Report. February 2014

Patents

2. *"An Advanced Privacy Filter for System Logs on Computing Devices"* US Patent No.: 63,960,570
Sanket Goutam, Hunter Michael Kippen, Luke Deshotels, Michael Grace, Amir Rahmati. January 2026
1. *"System and method for flow-based architecture"*. U.S. Patent No. 10,868,814
Tristan Morris, Amir Rahmati. December 2020

Selected Posters

5. *"Design of privacy preservation system in augmented reality"*
Kim, Yoonsang, Saeed Boorboor, Amir Rahmati, and A. Kaufman
IEEE Symposium on Visualization for Cyber Security (VizSec). 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

10. *"Cybersecurity Maturity Model Certification"*
Panelist at MTRC Cybersecurity Workshop. September 2023
9. *"Understanding & Countering Malicious Bot Activities"*
Speaker at Naval Postgraduate School Defense Energy Seminar. August 2023
8. *"Cybersecurity Digital Education"*
Panelist at LIFC Educational Series. February 2022
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 3rd Annual Pay-as-you-Go Workshop. July 2012

Professional Service

- **Steering Committee:** CEWIT’20
- **Organizing Committee:** NeurIPS’26, SafeThings’21, USENIX Sec’20, CCS’20, WWW’20, SACMAT’20
- **PC Member:** USENIX Sec’27–’20, PETS’27, PoPETs’27, IEEE Euro S&P’27–’25, SPWID’27,’24–’22,’20, IEEE S&P SAGAI’26, AsiaCCS’26, NDSS’26,’24, WWW’26–’20, SafeThings’25–’17, CPSIoTSec’26–’22, ASPLOS’24, CCS’23,’21, ICML’22, DSN-DSML’21, SACMAT’21,’20, EWLi’19, IoTSec’19, IoT S&P’18, SEMS’17, SecCPS’17
- **Reviewer:** IEEE Transactions on Image Processing’26, HealthSec’25, Electronics’25,’21–’19, IEEE Security & Privacy’25,’23,’21, NeurIPS’26,’25,’23,’22, IEEE Internet of Things Journal’25,’20–’18, Proceedings of IEEE’24, IEEE Transactions on Cloud Computing’24, IEEE Transactions on Dependable and Secure Computing’24,’23,’18, Journal of Computer Security’24,’23,’21, IEEE Transaction on Mobile Computing’24,’23,’19, Image and Vision Computing’24, IEEE Transactions on Information Forensics & Security’23–’21, Transactions on Software Engineering’22,’21, Applied Sciences’22,’21, IEEE Transactions on Image Processing’21, IEEE Sensors’21–’19, Journal of Cybersecurity and Privacy’21, Computers’21, IEEE Internet Computing’20, Symmetry’20, Sustainability’20, Concurrency and Computation: Practice and Experience’20, IEEE Transaction on VLSI Systems’19, Future Internet’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–’12, Journal of Wireless Networks (WINET’12)
- **Panelist:** NSF Cyber-Physical Systems (CPS) Feb’26, NSF Graduate Research Fellowship Program (GRFP)’25, NSF Secure & Trustworthy Cyberspace (SaTC) Oct’24, March’22, April’17
- **Judge/Mentor:** Stony Brook Undergraduate Research & Creative Activities (URECA)’25, 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, FIT Engineering Design Workshop’19
- **Open-Source Projects:**
 - ARCH Verification Competition (2024-Present)
My group has participated in the ARCH-Comp annual competition using FReaK framework developed in our HSCC 2024 paper.
 - IBM Adversarial Robustness Toolbox (ART) (2022-2024)
My group has been collaborating closely with IBM research to expand functionalities to the ART toolbox. ([#1668](#), [#1700](#), [#1705](#), [#1968](#), [#1988](#), [#1993](#), [#2218](#))
 - Ares: a system-oriented wargame framework for adversarial ML (2021)
In collaboration with IBM, my group has created a test framework for system-level security
- **University Committees/Services:**
 - **Stony Brook University**
 - Lead and POC for National Centers of Academic Excellence in Cybersecurity (CAE-R) (2024-2026)
 - Academic Liaison - Critical Infrastructure Security Consortium (CISC) CyberLearn Project (2024-2026)
 - Member of SUNY AI Task Force, Data Privacy and Security Working Group (2023-2024)
 - **CS Department - Stony Brook University**
 - Graduate Research Day Organizer (2019-2026)
 - Diversity Committee (2019-2026)
 - Graduate Student Organization Faculty Advisor (2019-2026)
 - Graduate Curriculum Committee (2019-2026)
 - Graduate Admission Committee (2018-2026)
 - Faculty Hiring Committee (2022-2023)
 - Stipend Committee (2022)
 - Graduate Grievance and Appeals Committee (2020)
 - Academic Job Panel Organizer (2019)
 - Open House Organizer (2019)
 - Grad Orientation Security Area Presenter (2018-2019)

Consulting

- Academic Liaison, Critical Infrastructure Security Consortium (CISC) CyberLearn Project (2024-2025)
- Consultant, Wisewire, Inc. (2024)

- Cybersecurity Advisor, ApplyBoard Inc. (2022-2023)
- Reviewer, Cambridge University Press (2022)
- Subject Matter Expert, ASR International Corporation (2019)
- System Consultant, Abbott Laboratories (2017)

Broader Impact

- **Access Control in Augmented Reality System (2023):** AR systems pose unique Access Control challenges due to their continuous access to the user’s video feed and their ability to shape users’ field of vision. Our work creates a principled framework for AR devices to adhere to the principle of least privileged. Inspired by our work, Apple introduced updates to the access control system used in their Vision Pro AR product in 2024.
- **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 the 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.
- **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 Configure for Wearables*.
- **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 the 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.

Advising and Mentorship

- | Ph.D. Students: | Status |
|---|---------------------------------|
| - Kasra Kakaee (2025-Present) | Pre-Quals |
| - Amir Khanlari (2025-Present) | Ph.D. Candidate |
| - Abisheka Pitumpe (2023-Present) | Ph.D. Candidate |
| - Sanket Goutam (2021-2026) | Senior SWE, Samsung Research |
| ★ <i>Inclusive Computing Fellowship Award (2022)</i> | |
| - Veena Krish (2019-2025) | Research Scientist, Snowflake |
| ★ <i>Turner Dissertation Fellowship Award (2024)</i> | |
| ★ <i>John Marburger III Fellowship Award (2023)</i> | |
| ★ <i>WPhD President (2022-2024)</i> | |
| - Pratik Vaishnavi (2018-2024) | <i>Research Scientist, Meta</i> |
| - Xigao Li (2018-2023) [Co-advised with Nick Nikiforakis] | <i>Research Scientist, Meta</i> |

Master’s Students:

Went on to

- | | |
|-----------------------------------|---|
| - Kashish Lalwani (2025-2026) | |
| - Arnav Desai (2025-2026) | |
| - Pranav Sista (2024-2025) | |
| - Sagor Sikdar (2023-2024) | <i>Ph.D. Student at Penn State University</i> |
| - Tirth Mehta (2022-2023) | <i>Software Development Engineer at Audible</i> |
| - Archit Gajpal (2022-2023) | <i>Software Engineer at Bloomberg</i> |
| - Kalpan Tumdi (2022-2023) | <i>Software Development Engineer at Audible</i> |
| - Karan Gada (2021-2022) | <i>Ph.D. Student at Stony Brook University</i> |
| - Farhan Ahmed (2021-2022) | <i>Research Software Engineer at IBM Research</i> |
| - Ajay Sarjoo (2021-2022) | <i>Software Engineer at Bloomberg</i> |
| - Atharva Kadam (2021-2022) | <i>Software Engineer at NetApp</i> |
| - 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> |

- Harpreet S. Chawla	(2018-2020)	<i>Ph.D. Student at Texas A&M University</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	(2018-2019)	<i>Software Engineer at Twitter</i>
– Undergraduate Students:		
		Went on to
- Vincent Zheng	(2025-2026)	
- Ryan Hung	(2025-2026)	
- Lucy Liu	(2025-2026)	
- Xiaoran Xie	(2025)	
- Amal Bilal	(2025)	
- Yash Tamhane	(2025)	
- Abas Safi	(2025)	<i>Master Student at Georgia Tech</i>
- Sophie Leonhardt	(2024-2025)	<i>Data Science Analyst at JPMorgan Chase</i>
- Urvi Bhatnagar	(2024-2025)	<i>Junior Data Scientist at Capgemini</i>
- Tyler Wang	(2024-2025)	<i>Software Engineer at Apple</i>
- Preston Chang	(2023-2024)	<i>Master Student at Stony Brook University</i>
- Jack Liu	(2021-2022)	<i>Software Developer at Epic</i>
- 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>
– K-12 Students:		
		Went on to
- Alexander Park	(Cinco Ranch High School, 2025)	
- Maheen Asaf	(Herricks High School, 2024)	
- Aayush Dave	(American High School, 2024)	
- Bryan Zhu	(Bellevue High, 2024)	
- Lisa Wan	(Glen Ridge High School, 2023)	
- Natalia Pahlavan	(Jericho Senior High School, 2022)	Undergraduate Student at Stanford University
– Visiting Students:		
		Went on to
- Yuxin Sun	(Tongji University, 2019)	<i>Graduate Student at ETH Zurich</i>
– Doctoral Committees:		
		Thesis Title
- Muhammad Muzammil	(07/2026)	“Measuring and Mitigating Traditional Threats Targeting Cryptocurrency Ecosystems”
- Andrew Mata	(06/2026)	“Robustness of Deep Learning-Enabled Control Systems”
- Christos Tsoukaladelis	(05/2026)	“Silent Changes: Understanding and Mitigating Integrity Threats in Web Content and Containerized Applications”
- Sanket Goutam	(05/2026)	“Building Privacy-Preserving Infrastructures for Modern Consumer Devices”
- Xinyu Zhang	(12/2025)	“Towards Human-AI Collaborative Exploration of Empty Spaces in High-Dimensional Data and Parameter Spaces”
- Joyanta Debnath	(05/2025)	“On the Development of an X.509 Certificate Chain Validation Implementation with Formal Correctness Guarantees”
- Veena Krish	(05/2025)	“Robustness of Cyber-Physical Systems to Adversarial Observations”
- Johnny So	(04/2025)	“Protecting the Integrity of Modern Web Resources by Leveraging Patterns of Change”
- Pratik Vaishnavi	(07/2024)	“Advancing Usability in Training and Evaluation of Adversarially Robust Neural Networks”
- Xigao Li	(08/2023)	“Measuring the Role of Automation in Malicious Web Activities”
- Seyedhamed Ghavamnia	(05/2023)	“Attack Surface Reduction through System Call Filtering”
- Krithika Yethiraj	(06/2022)	“Detecting and Mitigating Hardware Security Attacks in Emerging Technologies and Applications”

- 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:		Thesis Title
- Zihan Ding	(05/2023)	“E-taxi Fleet under Short-term Power System Failure”
- Sayali Anil Alatkhar	(05/2020)	“Causal Inference in Smart Homes through Traffic Signatures”
– Undergrad Honors Thesis Supervisor:		Thesis Title
- Sophie Leonhardt	(05/2025)	“Rising Cost of ML Research”
- Urvi Bhatnagar	(05/2025)	“Rising Cost of ML Research”
- Preston Chang	(05/2024)	“Security Analysis of ML-Based Artificial Pancreas Systems”
– Research Proficiency Exam Committees:		Talk Title
- Amir Hossein Khanlari	(08/2026)	“Security Analysis of the iOS In-App Subscriptions”
- Amir Najafi Zadeh	(08/2026)	“Understanding and Optimizing KV-Cache Management for Long-Context LLM Inference”
- Narong Chaiwut	(12/2025)	“Time for Actions: A Longitudinal Study of the GitHub Actions Marketplace”
- Abisheka Pitumpe	(08/2025)	“End-to-End Analysis of Cryptocurrency Scam Ecosystems”
- Adebayo Braimah	(08/2025)	“Curriculum trained hierarchical policy for UAV navigation”
- Aishik Deb	(07/2025)	“Efficient On-Policy Reinforcement Learning via Exploration of Sparse Parameter Space”
- Muhammad Farrukh	(06/2025)	“Modernizing C Legacy Systems into Memory-Safe Languages via LLM-Assisted Transpilation”
- Tanqiu Jiang	(02/2025)	“RobustKV: Defending Large Language Models against Jailbreak Attacks via KV Eviction”
- Natheesan Ratnasegar	(02/2024)	“Survey of computer systems simulators”
- Hieu Mai	(12/2023)	“High Performance Network Processing and Offloading Techniques”
- Sanket Goutam	(12/2023)	“Privacy-preserving Infrastructures for Pervasive Computing Ecosystems”
- Doris Gutierrez	(12/2023)	“User Experience in Immersive Visual Display Systems”
- Christos Tsoukaladelis	(08/2023)	“Characterizing and Defending the Integrity of Online Web Content”
- Joyanta Debnath	(07/2023)	“Increasing Resiliency of X.509 Public Key Infrastructure with Better Implementation Guarantee”
- Yilun Wu	(12/2022)	“DEVFUZZ: Automatic Device Model-Guided Device Driver Fuzzing”
- Johnny So	(05/2022)	“Quantifying Web Integrity”
- 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”