# Matthew Hicks

Associate Professor | Virginia Tech

mdhicks@gmail.com (217) 766-4294
ImpedimentToProgress.com GitHub: impedimentToProgress

## Research Interests

I perform research, teach, and train students to perform research at the intersection of Computer Architecture, Computer Security, and Embedded Systems. My research portfolio spans hardware and embedded system security, intermittent computation on energy harvesting devices, and micro-architecture-level security.

## Academic and Research Appointments

**Virginia Tech** — Associate Professor June 2022–present
**Virginia Tech** — Assistant Professor Sept. 2017–May 2022
**MIT Lincoln Laboratory** — Technical Staff Sept. 2016–Sept. 2017
**University of Michigan** — Lecturer Sept. 2015–Aug. 2016
**University of Michigan** — Postdoctoral Research Fellow May 2013–2015
**University of Illinois Urbana-Champaign** — Graduate Researcher May 2006–2013

## Education

**Ph.D., Computer Science** May 2013
University of Illinois Urbana-Champaign
Hybrid approaches for overcoming processor imperfections

**M.S., Computer Science** Aug. 2008
University of Illinois Urbana-Champaign
Real-time Systems

**B.S., Computer Science** May 2006
University of Central Florida
Mathematics minor; Honors College graduate

## Research at a Glance

**Funding:** $14,726,802 total project funding; $5,095,876 personal share.
**Publication summary:** 12 papers in Oakland, USENIX Security, and CCS; 17 in ISCA, ASPLOS, and MICRO; 2 in OSDI and ATC.

## Honors and Recognition

| | |
|---|---|
| 2025 | Communications of the ACM, Research Highlights |
| 2024 | Virginia Tech College of Engineering Faculty Fellow |
| 2023–2028 | CACI Faculty Fellow in Cyber Security |
| 2024 | ACM ENSsys Best Paper Award |
| 2023 | Paper selected for ISCA 50 Retrospective |
| 2022 | Top Picks in Hardware and Embedded Security |
| 2022 | ACSAC Best Poster Award |
| 2021 | NSF CAREER Award |
| 2021 | DARPA Director's Fellowship |
| 2021 | Virginia Tech College of Engineering Outstanding New Assistant Professor Award |
| 2020 | R&D 100 Award |
| 2019 | DARPA Young Faculty Award |
| 2018 | DARPA Riser |
| 2017 | Communications of the ACM, Research Highlights |
| 2016 | IEEE Symposium on Security and Privacy Distinguished Paper Award |
| 2016 | Pwnie Awards Most Innovative Research Award finalist |
| 2006–2008 | Analog Devices Fellowship |

## Research Funding

**ElasticFuzz: Flexible Distributed Fuzzing Infrastructure**
Virginia Commonwealth Cyber Initiative (CCI), SWVA Node May 1, 2026–Aug. 31, 2026
**Team:** Matthew Hicks (sole-PI)
**Total:** $15,000 **Department share:** $15,000 **Personal share:** $15,000

**Enhancing VMF: Source-agnostic Techniques for Code Coverage, Crash Triage, and Harnessing**
DoD Test Resource Management Center (TRMC) Jan. 1, 2025–Dec. 31, 2027
**Team:** Jack Davidson (UVa, PI), Matthew Hicks (co-PI), and Stefan Nagy (Univ. of Utah, co-PI)
**Total:** $4,410,000 **Department share:** $1,102,500 **Personal share:** $1,102,500

**SHF: Small: Circuit Support for Maintaining the Continuous-power Abstraction in Energy Harvesting Systems**
NSF Sept. 1, 2023–Aug. 31, 2026
**Team:** Matthew Hicks (sole-PI)
**Total:** $450,000 **Department share:** $450,000 **Personal share:** $450,000

**CAREER: Designing and Defending Novel Ultra-stealthy and Controllable Design-time Analog-domain Hardware Trojans**
NSF May 1, 2021–Apr. 30, 2026
**Team:** Matthew Hicks (sole-PI)
**Total:** $547,672 **Department share:** $547,672 **Personal share:** $547,672

**EPIC SWaPD: Energy-Preserving IoT Cryptography for Small Weight and Power Devices**
DARPA I2O Oct. 1, 2020–Sept. 30, 2024
**Team:** Angelos Stavrou (PI, Kryptowire), Matthew Hicks (co-PI), Khaled N. Khasawneh (co-PI, GMU), Brian L. Mark (co-PI, GMU), Sai Manoj Pudukotai Dinakarrao (co-PI, GMU), and Kai Zeng (co-PI, GMU)
**Total:** $7,533,591 **Department share:** $1,890,165 **Personal share:** $1,890,165

**Security Analysis of Hardware Security Primitives Employed by IoT and Cyber-physical Systems**
Virginia Commonwealth Cyber Initiative (CCI), SWVA Node June 1, 2020–Nov. 30, 2020
**Team:** Matthew Hicks (sole-PI)
**Total:** $20,000 **Department share:** $20,000 **Personal share:** $20,000

**Digital Techniques for Exposing and Eliminating Information Hidden in SRAM's Analog Domain**
DARPA I2O July 1, 2019–June 30, 2022
**Team:** Matthew Hicks (sole-PI)
**Total:** $900,539 **Department share:** $900,539 **Personal share:** $900,539

**CPI Protection Through Software Anti-Tamper (Phase 2)**
Office of the Secretary of Defense (OSD) Aug. 1, 2018–Feb. 28, 2020
**Team:** Charles Clancy III (PI, Hume), Thidapat Chantem (Co-PI, Hume), Eli Tilevich (Co-PI), and Matthew Hicks (Co-PI)
**Total:** $850,000 **Department share:** $340,000 **Personal share:** $170,000

## Publications

Underlined authors are students and postdoctoral researchers mentored by Matthew Hicks.

### Conference Publications

#### 2027

C1 **Leveraging Software Analysis for Better Bespoke Processor Generation**
Timothy Scholtz and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2027.*
**Sponsor:** National Science Foundation under Grant No. 2240744.

#### 2026

C2 **UlSWaP Bench: A Benchmark Suite for Ultra-Low Size, Weight and Power Devices**
Daniel Chiba, Harrison Williams, Rohit Sathye, and **Matthew Hicks**.
*International Conference on Embedded Wireless Systems and Networks (**EWSN**). September 2026.*
**Sponsor:** National Science Foundation under Grants No. 2046589 and No. 2240744.

C3 **$\mu$RNG: A Framework for Assessing Randomness in Intermittent Computing Devices**
Prakhar Sah and **Matthew Hicks**.
*International Symposium on Computer Architecture (**ISCA**). June 2026.*
**Sponsor:** National Science Foundation under Grant No. 2240744.

C4 **Sheriff: Arresting the Confused Deputy Undermining Ultra-low SWaP Device Trusted Execution Environments**
Prakhar Sah and **Matthew Hicks**.
*ASIA Conference on Computer and Communications Security (**AsiaCCS**). June 2026.*
**Sponsor:** National Science Foundation under Grant No. 2240744

C5 **Signal Breaker: Fuzzing Digital Signal Processors**
Cameron Santiago Garcia and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2026.*
**Sponsor:** TRMC, DARPA, and National Science Foundation under Grant No. 2240744.

**2025**

C6 **Retain The Date: Detecting Recycled Chips in the Supply Chain through SRAM's Data Retention Behavior**
Jubayer Mahmod and **Matthew Hicks**.
*Annual Computer Security Applications Conference (**ACSAC**). December 2025.*
**Sponsor:** DARPA YFA and National Science Foundation under Grant No. 2046589.

C7 **PhasePrint: Exposing Cloud FPGA Fingerprints by Inducing Timing Faults at Runtime**
Jubayer Mahmod and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2025.*
**Sponsor:** DARPA YFA and National Science Foundation under Grant No. 2046589.

C8 **ClosureX: Compiler Support for Correct Persistent Fuzzing**
Rishi Ranjan, Ian Paterson, and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2025.*
**Sponsor:** National Science Foundation under Grant No. 2046589.

C9 **A Software Caching Runtime for Embedded NVRAM Systems**
Harrison Williams and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2025.*
**Sponsor:** DARPA OPS-5G and National Science Foundation under Grant No. 2240744.

**2024**

C10 **RIPencapsulation: Defeating IP Encapsulation on TI MSP Devices**
Prakhar Sah and **Matthew Hicks**.
*USENIX WOOT Conference on Offensive Technologies (**WOOT**). August 2024.*
**Sponsor:** DARPA OPS-5G and National Science Foundation under Grant No. 2240744.

C11 **A Difference World: High-performance, NVM-invariant, Software-only Intermittent Computation**
Harrison Williams, Saim Ahmad, and **Matthew Hicks**.
*USENIX Annual Technical Conference (**ATC**). July 2024.*
**Sponsor:** DARPA OPS-5G and National Science Foundation under Grant No. 2240744.

C12 **SRAM Imprinting for System Protection and Differentiation**
Jubayer Mahmod and **Matthew Hicks**.
*ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**). July 2024.*
**Sponsor:** DARPA YFA.

C13 **UnTrustZone: Systematic Accelerated Aging to Expose On-chip Secrets**
Jubayer Mahmod and **Matthew Hicks**.
*IEEE Symposium on Security and Privacy (**Oakland**). May 2024.*
**Arm response:** Arm security response **Sponsor:** DARPA YFA.

C14 **Energy-adaptive Buffering for Efficient, Responsive, and Persistent Batteryless Systems**
Harrison Williams and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2024.*
**Sponsor:** National Science Foundation under Grant No. 2240744.

**2023**

C15 **No Linux, No Problem: Fast and Correct Windows Binary Fuzzing via Target-embedded Snapshotting**
Leo Stone, Rishi Ranjan, Stefan Nagy, and **Matthew Hicks**.
*USENIX Security Symposium (**USENIX**). August 2023.*
**Sponsor:** National Science Foundation under Grant No. 2046589.

C16 **Not All Data are Created Equal: Data and Pointer Prioritization for Scalable Protection Against Data-Oriented Attacks**
Salman Ahmed, Hans Liljestrand, Hani Jamjoom, **Matthew Hicks**, N. Asokan, and Daphne Yao.
*USENIX Security Symposium (**USENIX**). August 2023.*
**Sponsor:** Office of Naval Research under Grant N00014-22-1-2057, Virginia Commonwealth Cyber Initiative, the Natural Sciences and Engineering Research Council of Canada under RGPIN-2020-04744, and Intel Labs via the Private-AI consortium.

C17 **T-TER: Defeating A2 Trojans with Targeted Tamper-Evident Routing**
Timothy Trippel, Kang G. Shin, Kevin B. Bush, and **Matthew Hicks**.
*ACM ASIA Conference on Computer and Communications Security (**AsiaCCS**). July 2023.*

C18 **Practical Considerations of Energy Harvesting Source in Minimization of Age of Information with Updating Erasures**
Fariborz Lohrabi Pour, Harrison Williams, **Matthew Hicks**, and Dong Sam Ha.
*IEEE International Symposium on Circuits and Systems (**ISCAS**). May 2023.*
**Sponsor:** DARPA OPS-5G.

C19 **RF Energy Harvesting in Minimization of Age of Information with Updating Erasures**
Fariborz Lohrabi Pour, Harrison Williams, **Matthew Hicks**, and Dong Sam Ha.
*IEEE International Symposium on Circuits and Systems (**ISCAS**). May 2023.*
**Sponsor:** DARPA OPS-5G.

**2022**

C20 **One Fuzz Doesn't Fit All: Optimizing Directed Fuzzing via Target-tailored Program State Restriction**
Prashast Srivastava, Stefan Nagy, **Matthew Hicks**, Antonio Bianchi, and Mathias Payer.
*Annual Computer Security Applications Conference (**ACSAC**). December 2022.*
**Best poster award**. **Sponsor:** European Research Council, DARPA, AFRL, and SNSF.

C21 **Self-Reinforcing Memoization for Cryptography Calculations In Secure Memory Systems**
Xin Wang, Daulet Talapkaliyev, **Matthew Hicks**, and Xun Jian.
*International Symposium on Microarchitecture (**MICRO**). October 2022.*
**Sponsor:** National Science Foundation under Grant No. 1850025.

C22 **Fuzzing Hardware Like Software**
Timothy Trippel, Kang G. Shin, Alex Chernyakhovsky, Garret Kelly, Dominic Rizzo, and **Matthew Hicks**.
*USENIX Security Symposium (**USENIX**). August 2022.*

C23 **Invisible Bits: Hiding Secret Messages in SRAM's Analog Domain**
Jubayer Mahmod and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2022.*
**Sponsor:** DARPA YFA.

C24 **SRAM Has No Chill: Exploiting Power Domain Separation to Steal On-chip Secrets**
Jubayer Mahmod and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2022.*
**Sponsor:** DARPA YFA. **Communications of the ACM Research Highlights 2025**.

**2021**

C25 **RingRAM: A Unified Hardware Security Primitive for IoT Devices that Gets Better with Age**
Michael Moukarzel and **Matthew Hicks**.
*Annual Computer Security Applications Conference (**ACSAC**). December 2021.*
**Sponsor:** DARPA YFA.

C26 **Same Coverage, Less Bloat: Accelerating Binary-only Fuzzing with Coverage-preserving Coverage-guided Tracing**
Stefan Nagy, Anh Nguyen-Tuong, Jason Hiser, Jack Davidson, and **Matthew Hicks**.
*ACM Conference on Computer and Communications Security (**CCS**). November 2021.*
**Sponsor:** DARPA and National Science Foundation under Grant No. 1650540.

C27 **Failure Sentinels: Ubiquitous Just-in-time Intermittent Computation via hardware support for continuous, low-cost, fine-grain voltage monitoring**
Harrison Williams, Michael Moukarzel, and **Matthew Hicks**.
*International Symposium on Computer Architecture (**ISCA**). June 2021.*
**Sponsor:** DARPA OPS-5G.

C28 **Breaking Through Binaries: Compiler-quality Instrumentation for Better Binary-only Fuzzing**
Stefan Nagy, Anh Nguyen-Tuong, Jason Hiser, Jack Davidson, and **Matthew Hicks**.
*USENIX Security Symposium (**USENIX**). August 2021.*
**Sponsor:** DARPA and National Science Foundation under Grant No. 1650540.

C29 **Bomberman: Defining and Defeating Hardware Ticking Timebombs at Design-time**
Timothy Trippel, Kang G. Shin, Kevin B. Bush, and **Matthew Hicks**.
*IEEE Symposium on Security and Privacy (**Oakland**). May 2021.*
**Sponsor:** National Science Foundation under Grant No. 1646130 and the Graduate Research Fellowship Program, as well as the US Army Research Office.

**2020**

C30 **ICAS: an Extensible Framework for Estimating the Susceptibility of IC Layouts to Additive Trojans**
Timothy Trippel, Kang G. Shin, Kevin B. Bush, and **Matthew Hicks**.
*IEEE Symposium on Security and Privacy (**Oakland**). May 2020.*
**Sponsor:** National Science Foundation under the Graduate Research Fellowship Program.

C31 **Forget Failure: Exploiting SRAM Data Remanence for Low-overhead Intermittent Computation**
Harrison Williams, Xun Jian, and **Matthew Hicks**.
*International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2020.*
**Sponsor:** DARPA OPS-5G and DARPA YFA.

**2019**

C32 **Full-speed Fuzzing: Reducing Fuzzing Overhead through Coverage-guided Tracing**
Stefan Nagy and **Matthew Hicks**.
*IEEE Symposium on Security and Privacy (**Oakland**). May 2019.*
**Sponsor:** National Science Foundation under Grant No. 1650540.

**2017**

C33 **Clank: Architectural Support for Intermittent Computation**
**Matthew Hicks**.
*International Symposium on Computer Architecture (**ISCA**). June 2017.*

**2016**

C34 **Intermittent Computation without Hardware Support or Programmer Intervention**
Joel Van Der Woude and **Matthew Hicks**.
*USENIX Symposium on Operating Systems Design and Implementation (**OSDI**). November 2016.*

C35 **A2: Analog Malicious Hardware**
Kaiyuan Yang, **Matthew Hicks**, Qing Dong, Todd Austin, and Dennis Sylvester.
*IEEE Symposium on Security and Privacy (**Oakland**). May 2016.*
**Distinguished Paper award**. **Pwnie Most Innovative Research Award finalist**. **Communications of the ACM Research Highlights 2017**. **Top Picks in Hardware and Embedded Security 2022**.

C36 **ANVIL: Software-Based Protection Against Next-Generation Rowhammer Attacks**
Zelalem Birhanu Aweke, Salessawi Ferede Yitbarek, Rui Qiao, Reetuparna Das, **Matthew Hicks**, Yossi Oren, and Todd Austin.
*Symposium on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2016.*

**2015**

C37 **Probable Cause: The Deanonymizing Effects of Approximate DRAM**
Amir Rahmati, **Matthew Hicks**, Daniel E. Holcomb, and Kevin Fu.
*International Symposium on Computer Architecture (**ISCA**). June 2015.*

C38 **SPECS: A lightweight runtime mechanism for protecting software from security-critical processor bugs**
**Matthew Hicks**, Cynthia Sturton, Samuel T. King, and Jonathan M. Smith.
*Symposium on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2015.*

**2011**

C39 **Defeating UCI: Building Stealthy and Malicious Hardware**
Cynthia Sturton, **Matthew Hicks**, David Wagner, and Samuel T. King.
*IEEE Symposium on Security and Privacy (**Oakland**). May 2011.*

**2010**

C40 **Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically**
**Matthew Hicks**, Murph Finnicum, Samuel T. King, Milo M. K. Martin, and Jonathan M. Smith.
*IEEE Symposium on Security and Privacy (**Oakland**). May 2010.*

**2009**

C41 **Capo: a Software-Hardware Interface for Practical Deterministic Multiprocessor Replay**
Pablo Montesinos, **Matthew Hicks**, Samuel T. King, and Josep Torrellas.
*Symposium on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**). March 2009.*

### Journal Articles and Research Highlights

**2026**

J1 **Revisiting the Machine Unlearning Ecosystem in Vision: From Afterthought to a Lifecycle Perspective**
Emanuela Marasco, **Matthew Hicks**, Bart Slowik, Thirimachos Bourlai, and Arun Ross.
*Image and Vision Computing. June 2026.*

**2025**

J2 **SRAM has no chill: Exploiting power domain separation to steal on-chip secrets**
Jubayer Mahmod and **Matthew Hicks**.
*Communications of the ACM, 68(8):82–90. August 2025.*

**2019**

J3 **FinalFilter: Asserting Security Properties of a Processor at Runtime**
Cynthia Sturton, **Matthew Hicks**, Samuel T. King, and Jonathan M. Smith.
*Invited. IEEE Micro. Vol. 39. Num. 4. July 2019.*

**2017**

J4 **Exploiting the analog properties of digital circuits for malicious hardware**
Kaiyuan Yang, **Matthew Hicks**, Qing Dong, Todd Austin, and Dennis Sylvester.
*Communications of the ACM, 60(9):83–91. September 2017.*

### 2010

J5 **Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically**
**Matthew Hicks**, Murph Finnicum, Samuel T. King, Milo M. K. Martin, and Jonathan M. Smith.
*USENIX ;login. December 2010, 31–41.*

## Workshop Publications

### 2024

W1 **A Survey of Prototyping Platforms for Intermittent Computing Research**
Harrison Williams and **Matthew Hicks**.
*International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems. November 2024.*
**Best Paper award**. **Sponsor:** DARPA OPS-5G and National Science Foundation under Grant No. 2240744.

### 2023

W2 **Hitchhiker's Guide to Secure Checkpointing on Energy-Harvesting Systems**
Prakhar Sah and **Matthew Hicks**.
*International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems. November 2023.*
**Sponsor:** DARPA OPS-5G.

### 2017

W3 **Reap What You Store: Side-channel Resilient Computing Through Energy Harvesting**
Michael Moukarzel and **Matthew Hicks**.
*International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems. November 2017.*

W4 **SNIFFER: A High-Accuracy Malware Detector for Enterprise-based Systems**
Evan Chavis, Harrison Davis, Yijun Hou, **Matthew Hicks**, Salessawi Ferede Yitbarek, Todd Austin, and Valeria Bertacco.
*International Verification and Security Workshop. July 2017.*

### 2016

W5 **Approximate Flash Storage: A Feasibility Study**
Amir Rahmati, **Matthew Hicks**, and Atul Prakash.
*Workshop on Approximate Computing Across the System Stack. March 2016.*

### 2014

W6 **Refreshing Thoughts on DRAM: Power Saving vs. Data Integrity**
Amir Rahmati, **Matthew Hicks**, Daniel E. Holcomb, and Kevin Fu.
*Workshop on Approximate Computing Across the System Stack. March 2014.*

### 2009

W7 **Lessons Learned During the Development of the CapoOne Deterministic Multiprocessor Replay System**
Pablo Montesinos, **Matthew Hicks**, Wonsun Ahn, Samuel T. King, and Josep Torrellas.
*Workshop on the Interaction Between Operating Systems and Computer Architecture. June 2009.*

### Theses

#### 2013

T1 **Practical systems for overcoming processor imperfections**
**Matthew Hicks**.
*University of Illinois Urbana-Champaign, PhD Dissertation. May 2013.*

#### 2008

T2 **Reflex: A Real-World TB* Implementation**
**Matthew Hicks**.
*University of Illinois at Urbana-Champaign, Masters Thesis. August 2008.*

## Patents

Voltage monitoring system and method for harvesting energy in a computational environment. Harrison Williams, Matthew Hicks, Angelos Stavrou, and Michael Moukarzel. US Patent 12,540,957. 2026.

Defensive routing and related techniques. KB Bush, MD Hicks, TD Trippel. US Patent 11,347,902. 2022.

Integrated circuit (IC) portholes and related techniques. KB Bush, MD Hicks, TD Trippel. US Patent 10,839,109. 2020.

## Invited Talks

| | |
|---|---|
| **Joint Fuzzing Working Group**. Software Fuzzing Talk | June 2024 |
| **Hardwear.io security conference**. Hardware Security Lecture | June 2024 |
| **Penn State**. Software Fuzzing Seminar | November 2023 |
| **Michigan**. Intermittent Computation Seminar | October 2023 |
| **LSU**. Software Fuzzing Seminar | April 2023 |
| **UIUC**. Hardware Security Seminar | November 2022 |
| **AMD Security**. Hardware Security Seminar | December 2021 |
| **WPI**. Hardware Security Seminar | April 2021 |
| **DARPA D60**. Hardware Security Talk | September 2018 |
| **NSF Workshop on Foundations of Secure and Trusted Hardware**. | October 2017 |

## Advising and Mentoring

Faculty Mentor - 2018 – 2026 MITRE Collegiate eCTF competition

- **First place overall**
- Most flags captured
- Best defensive system

### Postdoctoral Fellows

- Harrison Williams (2024–2025)
- Michael Moukarzel (2019–2022)

### Graduate Students: Chair or Co-chair

- Daniel Chiba (PhD)
- Prakhar Sah (PhD)
- Patrick Flynn (PhD)
- Andrew Benson (PhD)
- Timothy Scholtz (PhD)
- Sam Katerov (PhD)
- Miles Zoellner (MS)
- Harrison Williams (PhD 2024, First Job: Efficient Computer)
- Jubayer Mahmod (PhD 2024, First Job: Amazon)
- Stefan Nagy (PhD 2022, First Job: Asst. Prof. Utah)
- Timothy Trippel (PhD 2021, Michigan, Co-chair with Kang Shin, First Job: Google)
- Michael Moukarzel (PhD 2019, WPI, Co-chair with Berk Sunar)
- Sam Katerov (MS 2026, First Job: continuing PhD)
- Wesley Black (MS 2026, First Job: Cryptic Vector)
- Cameron Garcia (MS 2025, First Job: Draper)
- Sydney Earp (MS 2025, First Job: PhD at CMU)
- Erin Freck (MS 2025, First Job: STR)
- Tejas Raju (MS 2025, First Job: Qualcomm)
- Rishi Ranjan (MS 2024, First Job: Apple)
- Shambhavi Anil Kuthe (MS 2024, First Job: Ichor Systems)
- Rohit Sathye (MS 2024, First Job: UT Dallas)
- Leo Stone (MS 2023, First Job: Oregon State University)
- Zeezoo Ryu (MS 2023, First Job: PhD at Ga. Tech)
- Nandita Singh (MS 2023, First Job: NXP Semiconductors)
- Jaskaran Kaur (MS 2023, First Job: HP)
- Ian Paterson (MS 2022, First Job: Brightspot)
- Che-Hsien Liao (MS 2022, First Job: Meta)
- David Gleason (MS 2022, First Job: State of Il.)
- Saim Ahmad (MS 2021, First Job: Amazon)
- KC Cowan (MS 2020, First Job: DoD)
- Fahad Ibrar (MS 2020, First Job: Oracle)
- Somyaa Rastogi (MEng 2023, First Job: Amazon)
- Sai Sanath Krishnappagari (MEng 2023, First Job: Pearson)

### Graduate Student Committees: Member

- Aravind Cheruvu (PhD 2026, Chair: Daphne Yao)
- Alok Singh (PhD 2025, Chair: Ryan Gerdes)
- Muhammad Laghari (PhD 2025, Chair: Steve Jian)
- Xin Wang (PhD 2025, Chair: Steve Jian)
- Abdullah Zubair Mohammed (PhD 2024, ECE, Chair: Ryan Gerdes)
- Ying Zhang (PhD 2023, Chair: Na Meng)
- Vito Kortbeek (PhD 2023, TU Delft, Chair: Przemyslaw Pawelczak)

- Da Zhang (PhD 2023, Chair: Steve Jian)
- Mincheol Sung (PhD 2023, ECE, Chair: Binoy Ravindran)
- Ya Xiao (PhD 2022, Chair: Daphne Yao)
- Md Salman Ahmed (PhD 2021, Chair: Daphne Yao)
- Archanaa S. Krishnan (PhD 2021, ECE, Chair: Patrick Schaumont)
- Yuan Yao (PhD 2021, Chair: Patrick Schaumont)
- Jason McGinthy (PhD 2019, ECE, Chair: Alan Michaels)
- Xiaodong Yu (PhD 2019, Chair: Daphne Yao)
- Chinecherem Dimobi (MS 2025, Chair: Dan Williams)
- Lalit Prasad Peri (MS 2025, ECE, Chair: Wenjie Xiong)
- Jacob Haltiwanger (MS 2024, Chair: Thang Hoang)
- Kiara Chambers (MEng 2024, ECE, Chair: Ryan Gerdes)
- Yuqing Liu (MS 2023, Chair: Steve Jian)
- Connor Shugg (MS 2022, Chair: Godmar Back)
- Hanwen Liu (MS 2021, Chair: Na Meng)
- Emma Meno (MS 2021, Chair: Daphne Yao)
- Hassan Nadeem (MS 2020, ECE, Chair: Binoy Ravindran)
- Akhil Ahmed Rafeeq (MS 2020, ECE, Chair: Cameron Patterson)
- John Lee (PhD, ECE, Chair: Wenjie Xiong)
- Hexuan Yu (PhD, Chair: Wenjing Lou)
- Changqi Sun (PhD, Chair: Thang Hoang)
- Muhammad Zeeshan Karamat (PhD, Chair: Christiana Garcia)

### Undergraduate Researchers

- Sean Rothenberger (2026)
- Sean Henderson (2024)
- Adam Nguyen (2024)
- Sabrina Witham (2024)
- Rishi Ranjan (2020–2022, IIT Roorkee)
- Leo Stone (2020–2021)
- Kishan Parikh (2017–2020)
- Alex Lind (2017–2020)
- Harrison Williams (2017–2019)
- Cristhian Benitez (2018–2019)
- Spencer Mullinix (2018)
- Blake Eriks (2018)
- Christina Lin (2017)
- Ryan Parker (2017)

## Courses Taught

| | | |
|---|---|---|
| Spring 2026 | **CS 4094** | Senior Capstone: Hardware & Software Fuzzing |
| Spring 2026 | **CS 6204** | System Security Seminar: Hardware & Software Fuzzing |
| Fall 2025 | **CS 4264** | Principles of Computer Security |
| Spring 2025 | **CS 4994** | Senior Capstone: physical side channels |
| Spring 2025 | **CS/ECE 5590** | System and Application Security |
| Fall 2024 | **CS 4264** | Principles of Computer Security |
| Spring 2024 | **CS 6204** | System Security Seminar: Energy Harvesting & Intermittent Computation |
| Fall 2023 | **CS 4264** | Principles of Computer Security |
| Spring 2023 | **CS/ECE 5590** | System and Application Security |
| Fall 2022 | **CS 4264** | Principles of Computer Security |
| Spring 2022 | **CS 6204** | System Security Seminar: Fuzzing |
| Fall 2021 | **CS 4264** | Principles of Computer Security |
| Spring 2021 | **CS/ECE 5590** | System and Application Security |
| Fall 2020 | **CS 3214** | Computer Systems |
| Spring 2020 | **CS 6204** | System Security Seminar: Hardware Security |
| Fall 2019 | **CS 4264** | Principles of Computer Security |
| Spring 2019 | **CS/ECE 5590** | System and Application Security |
| Fall 2018 | **CS 4264** | Principles of Computer Security |
| Spring 2018 | **CS 6204** | System security Seminar: System Security |
| Fall 2017 | **CS 4264** | Principles of Computer Security |

## Professional Service

### Program Committees

- 2017–2026 International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems (ENSsys)
- 2023–2024 ACM International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**)
- 2021–2022 USENIX Security Symposium (**Security**)
- 2017–2019, 2021 IEEE Symposium on Security and Privacy (**Oakland**)
- 2020 ACM SIGPLAN/SIGBED International Conference on Languages, Compilers, and Tools for Embedded Systems (LCTES)
- 2017–2018, 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)
- 2020 Design Automation Conference (**DAC**)
- 2018 IEEE/ACM International Symposium on Microarchitecture (**MICRO**) - ERC
- 2018 ACM International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS**) - ERC
- 2018 IEEE International Symposium on High-Performance Computer Architecture (**HPCA**) - ERC
- 2017 ACM Conference on Computer and Communications Security (**CCS**)

### Journal Reviewing

- 2026 IEEE Security and Privacy (**S&P**)
- 2024, 2026 Computers & Security (**COSE**)
- 2018, 2026 IEEE Transactions on Dependable and Secure Computing (**TDSC**)
- 2021, 2025, 2026 ACM Transactions on Privacy and Security (**TOPS**)
- 2025 IEEE Internet of Things Journal (**IoT-J**)
- 2023, 2024 Transactions on Embedded Computing Systems (**TECS**)
- 2022, 2024 IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**)
- 2024 IEEE Networking Letters
- 2024 Journal of Systems Architecture (**JSA**)
- 2019, 2023 IEEE Transactions on Very Large Scale Integration Systems (**TVLSI**)
- 2021, 2023 Transactions on Software Engineering and Methodology (**TOSEM**)
- 2023 Transactions on Software Engineering (**TSE**)
- 2018, 2022, 2023 ACM Transactions on Architecture and Code Optimization (**TACO**)
- 2021 IEEE Transactions on Circuits and Systems (**TCAS**)
- 2021 Electronics Letters
- 2020, 2021 ACM Transactions on Computer Systems (**TOCS**)
- 2018, 2021 ACM Transactions on Design Automation of Electronic Systems (**TODAES**)
- 2018, 2020 IEEE Computer Architecture Letters (**CAL**)
- 2019 ACM Transactions on Sensor Networks (**TOSN**)
- 2017, 2018 Journal of Hardware and Systems Security (**HAAS**)
- 2018 IEEE Micro (**Micro**)

## Department Service

- 2025–2026 Research Incentive Committee
- 2025–2026 Publicity Committee
- 2023–2026 IT Liaison
- 2023–2024 Department Head Search Committee
- 2022–2023 Promotion and Tenure Committee
- 2020–2021 Faculty Search Committee
- 2019–2022 Graduate Program Committee
- 2018–2020 Systems PhD Qualifier Committee
  - 2019–2020 Chair
- 2018–2019 Faculty Search Committee

## Research Software and Artifacts

Repository names link to the source code. Recorded on October 20, 2026: 37 public repositories, 119 forks, and 411 stars. Counts are retained from the original CV; entries without counts were not publicly accessible at that check.

**UlSWaP-Bench**: benchmark suite for ultra-low size, weight, and power devices.
Related publication: [C2]. 4 forks, 11 stars.

**Sheriff**: research artifacts.
Related publication: [C4]. 0 forks, 0 stars.

**SBFuzz**: fuzzer for digital signal processors.
Related publication: [C5]. 0 forks, 3 stars.

**Recycled_SoC_Detection**: data-retention-voltage-based detection of recycled counterfeit devices.
Related publication: [C6].

**NSF_CAREER**: summary of research results supported by the NSF CAREER award.
Related publication: [C7]. 0 forks, 0 stars.

**cloud_fpga_timing_signature**: AWS system for large-scale cloud FPGA signature generation.
Related publication: [C7].

**ClosureX**: compiler passes that reset program state for correct persistent fuzzing.
Related publication: [C8]. 0 forks, 3 stars.

**EnergyHarvestingDeviceTestbed**: embedded-device testbed with LED/UART examples and board setup instructions.
Related publication: [W1]. 0 forks, 2 stars.

**RIPencapsulation**: attacks that defeat TI's IP Encapsulation.
Related publication: [C10]. 0 forks, 0 stars.

**Camel**: programmer-guided continuous checkpointing using in-place SRAM state retention across short power interruptions.
Related publication: [C11]. 0 forks, 0 stars.

**ArmTrust-Zone**: Arm TrustZone setup for Xplained Pro, LPC55S69, and SAML11 devices.
Related publication: [C13].

**UnTrustZone**: project page describing the attack, approach, and vendor disclosure.
Related publication: [C13]. 0 forks, 5 stars.

**REACT-PCB**: PCB for REACT's dynamic capacitor system.
Related publication: [C14]. 0 forks, 0 stars.

**REACT**: software, benchmarks, and RF power traces for a dynamic energy-management platform for batteryless systems. 1 fork, 2 stars.
Related publication: [C14].

**EnergyReplay**: hardware for recording and replaying energy-harvesting traces.
0 forks, 0 stars.

**WinFuzz**: fast Windows binary fuzzing via target-embedded snapshotting.
Related publication: [C15]. 4 forks, 25 stars.

**SieveFuzz**: directed fuzzer that restricts exploration to program states that can reach the target.
Related publication: [C20]. 6 forks, 31 stars.

**SRAMColdBoot**: cold boot and Volt Boot attacks on the SRAM of Raspberry Pi 3 and Raspberry Pi 4 devices.
Related publication: [C24].

**SramSteganography**: converts an image into a program that imprints that image on the SRAM of MSP432, Raspberry Pi 3, and Raspberry Pi 4 devices.
Related publication: [C23].

**TDC2**: Vivado FPGA design for a time-to-digital converter (TDC) with ring-oscillator and RISC-V activity generators.
0 forks, 2 stars.

**RingRAM**: unified PUF and TRNG hardware security primitive for IoT devices.
Related publication: [C25]. 0 forks, 5 stars.

**ZUnTracer-AFL**: UnTracer-AFL ported to the Zipr binary rewriter via the ZAFL platform.
Related publication: [C26]. 0 forks, 0 stars.

**HeXcite**: binary fuzzer accelerated by coverage-preserving coverage-guided tracing, built on AFL 2.52b and ZAFL.
Related publication: [C26]. 2 forks, 25 stars.

**EmbeddedCrypto**: embedded cryptographic implementations and performance/energy evaluation for ultra-low-SWaP devices. 0 forks, 1 star.

**ZAFL**: binary fuzzing instrumentation and transformation platform.
Related publication: [C28]. 2 forks, 3 stars.

**FailureSentinels**: research artifacts.
Related publication: [C27]. 0 forks, 0 stars.

**Bomberman**: design-time detection of hardware ticking timebombs. 0 forks, 1 star.
Related publication: [C29].

**GDS2-Score**: quantifies an IC layout's fabrication-time hardware Trojan attack surface.
Related publication: [C30]. 2 forks, 10 stars.

**Nemo**: identifies security-critical signals in a hardware design. 1 fork, 7 stars.
Related publication: [C30].

**TotalRecall**: research artifacts. 1 fork, 5 stars.
Related publication: [C31].

**UnTracer-AFL**: AFL with UnTracer coverage-guided tracing.
Related publication: [C32]. 27 forks, 125 stars.

**afl-fid**: AFL modifications for fixed-input-dataset experiments.
Related publication: [C32]. 7 forks, 14 stars.

**FoRTE-FuzzBench**: fuzzing benchmarks.
Related publication: [C32]. 14 forks, 56 stars.

**Clank**: research artifacts. 1 fork, 0 stars.
Related publication: [C33].

**Ratchet**: compiler-only support for intermittent computation.
Related publication: [C34]. 4 forks, 9 stars.

**MiBench2**: the MiBench benchmark suite ported to IoT devices.
17 forks, 19 stars.

**Thumbulator**: cycle-accurate ARMv6-M instruction set simulator.
9 forks, 16 stars.

**A2**: OR1200 processor design files and simulation setup for the A2 analog hardware Trojan.
Related publication: [C35]. 5 forks, 14 stars.

**ProbableCause**: research artifacts. 1 fork, 0 stars.
Related publication: [C37].

**SPECS**: hardware and software implementations and processor errata data.
Related publication: [C38]. 4 forks, 7 stars.

**ProcessVCD**: Java package for processing value change dump (VCD) files from hardware simulations.
4 forks, 10 stars.

**UCI-BlueChip**: unused circuit identification (UCI) analysis, BlueChip run-time monitors, and three malicious hardware attacks on the Leon3 processor.
Related publication: [C40]. 3 forks, 0 stars.

**IntermittentCrypto**: intermittent-tolerant cryptographic libraries and corresponding demo.

**mspdebug**: MSP430 simulator with CPUX patches and other bug fixes.

## Media and Public Engagement

- My A2 paper (Oakland '16) was featured in computer science's preeminent trade journal, *Communications of the ACM* (September 2017): Communications of the ACM
- The embedded Capture the Flag team that I advise won first place in a national competition (6/5/18): Virginia Tech News
- I am a subject matter expert concerning reports that China compromised our nation's electronics supply chain (10/17/18): Virginia Tech News
  - This article has been read by key supply chain security decision makers in the Department of Defense.
- I appeared on a mobile device security segment on "WFXR's Living Local" (6/4/19): WFXR Living Local
- Interview with NPR: Huawei and microelectronic supply chain integrity security segment on WVTF, the local NPR station (6/18/19): WVTF / NPR
- I gave an interview with Vanity Fair's Nick Bilton on 5G network security and the impact of foreign companies (i.e., Huawei).
- Google Project Zero based its fuzzer for Apple's closed-source ImageIO image-parsing framework on our Full-speed Fuzzing approach [C32]; the fuzzer found multiple vulnerabilities reachable through popular messaging apps, which were reported and fixed (April 2020):
  - Project Zero announcement
  - Google Project Zero
- International article about my hardware fuzzing work (2/24/21): New Scientist
- A local Fox news station interviewed me about the computer chip shortage. The result is a video package that appeared on the nightly news (9/13/21): WFXR News
- There was a VT News article covering my NSF CAREER award (10/29/21): Virginia Tech News
- Semiconductor Engineering highlighted our hardware fuzzing paper [C22] (December 2022): Semiconductor Engineering
- Semiconductor Engineering's "SRAM Security Concerns Grow" featured our Volt Boot attack [C24] (May 2024): Semiconductor Engineering
- "Curious Conversations" podcast: Matthew Hicks talks about computer security in the new year (1/27/25): Curious Conversations podcast
- VT News airport Wi-Fi security tips, "Don't leave all your airport security to TSA" (3/5/25): Virginia Tech News
- WSLS interview on Wi-Fi security (3/10/25): WSLS
- WTOP interview on airport Wi-Fi security (3/17/25): WTOP
- Fox 5 DC live interview on airport Wi-Fi security (3/17/25): Fox 5 DC interview

- CBS News streaming interview on airport Wi-Fi security (3/21/25): CBS News video
- CBS weekend morning show interview on airport Wi-Fi security (3/23/25): CBS morning interview
- Travel + Leisure interview (June 2025): Travel + Leisure
- Forbes (June 2025): Forbes
- International (Russian-language) coverage of our Volt Boot attack [C24], [J2] (August 2025):
  - SecurityLab.ru (8/5/25): SecurityLab.ru
  - Habr (8/13/25): Habr

## Research and Teaching Experience

### Virginia Tech

**Associate Professor** June 2022–present

**Assistant Professor** Sept. 2017–May 2022

Lead a research group focused on security, architecture, and embedded systems. Teach undergraduate and graduate courses. Perform departmental service.

### MIT Lincoln Laboratory

**Technical Staff** Sept. 2016–Sept. 2017

Lead research on a range of low-level security topics.

### University of Michigan

**Lecturer** Sept. 2015–Aug. 2016

**EECS 388** W16
Introduction to computer security.

**EECS 183** F15
Introduction to programming (C++ and Python) for non-engineering majors.

**Postdoctoral Research Fellow** May 2013–2015

**Energy-dictated Computing** Sept. 2013–Aug. 2015
Batteries prevent the realization of the dream of computational dust. As computation moves to smaller cores, batteries account for a greater portion of the size, cost, and maintenance of embedded systems. Energy harvesting removes the need for a battery, but creates a new problem of an unpredictable power source. My work in this area seeks to build automatic program transformations and new architectures so that programs run correctly and efficiently (i.e., minimize the number of power cycles to complete a task) across power cycles. I am building systems using LLVM, miBench, and an ARM Cortex-M0+ core running on a Xilinx Virtex-5 FPGA.

**Approximate Computing** Sept. 2013–Aug. 2015

Many classes of applications accept a wide range of outputs as correct. This means that it is possible to allow errors in program outputs while still producing outputs that the application deems acceptable. Reducing guard bands to allow for some errors can reduce power consumption or increase performance. In this area, I am building an approximate experimentation platform that consists of both approximate DRAM and an approximate processor. For these projects, I am using a Xilinx Virtex-5 FPGA, an OpenRISC OR1200 processor, and an MSP430 development board.

**Malicious hardware** Sept. 2013–Aug. 2015

This research focuses on both the attack and defense directions of malicious hardware. The attack portion attempts to find and implement interesting and novel attacks in a SoC environment. The defense portion of this research focuses on developing practical and automatic techniques and tools for detecting and removing malicious circuits from HDL code.

### University of Illinois, Urbana-Champaign

**Graduate Researcher** May 2006–2013

**Imperfect hardware** Jan. 2011–Aug. 2013

Hardware is not perfect, whether it be design-time bugs created by HDL authors or run-time faults created by an attacker. My research in this area strives to protect unsuspecting software from the implications of imperfect hardware.

**Malicious hardware** May 2007–Aug. 2013

This research focuses on both the attack and defense directions of malicious hardware. The attack portion attempts to find and implement interesting and novel attacks in a SoC environment. The defense portion of this research focuses on developing practical and automatic techniques and tools for detecting and removing malicious circuits from HDL code.

**Deterministic replay on multiprocessors** Summer 2008

The goal of this research project is to combine hardware and software together in a deterministic replay system for multiprocessors that has the performance advantages of hardware-only replay, but also has the small log size and ability to record a subset of processes provided by software-only replay.

**Hardware support for real-time systems** Aug 2007–May 2008

This research focuses on the FPGA implementation of a real-time scheduling algorithm that, while theoretically optimal, is impractical on today's processors. We construct a SoC using the FPGA's built-in processor, running a lightly modified RTOS with the scheduling and other RTOS services offloaded to hardware.

**FPGA+DSP communications supercomputer** May 2006–Jan 2008

The goal of this work was to build, from the ground up, a supercomputer for multi-channel environments like packet processing or call processing. The supercomputer relies on FPGAs for packet routing and DSPs for calculation and up and down butterfly networks for deadlock free routing. The supercomputer is node-based and channels are added by attaching more nodes. I was tasked with PCB design and all FPGA development, except the crossbar switch.