Matthew Hicks

mdhicks@gmail.com
www.ImpedimentToProgress.com
github.com/impedimentToProgress
(217) 766-4294

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.

Education

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

Master of Science, Computer Science **August 2008**
University of Illinois Urbana-Champaign
Real-time Systems

Bachelor of Science, Computer Science **May 2006**
University of Central Florida
Mathematics Minor
Honors College Graduate

Publication Summary

12x(**Oakland, USENIX, CCS**), 10x(**ISCA, ASPLOS, MICRO**), 1x(**OSDI**)

Funding Summary

Total: $10,205,384 **My share:** $3,881,958

Recognition

2022 Top Picks in Hardware and Embedded Security

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

2016 IEEE Symposium on Security and Privacy Distinguished Paper Award

2016 Pwnie Awards Most Innovative Research Award finalist

2006–2008 Analog Devices Fellowship

FUNDING

SHF: Small: Circuit Support for Maintaining the Continuous-power Abstraction in Energy Harvesting Systems

- Sponsor: NSF
- Project timeframe: 09-1-23 to 08-31-26
- Team: Matthew Hicks (sole-PI)
- Total: $450,000
- Department share: $450,000
- My share: $450,000

CAREER: Designing and Defending Novel Ultra-stealthy and Controllable Design-time Analog-domain Hardware Trojans

- Sponsor: NSF
- Project timeframe: 05-1-21 to 04-30-26
- Team: Matthew Hicks (sole-PI)
- Total: $547,672
- Department share: $547,672
- My share: $547,672

EPIC SWaPD: Energy-Preserving IoT Cryptography for Small Weight and Power Devices

- Sponsor: DARPA I2O
- Project timeframe: 10-1-20 to 09-30-24
- Team: Angelos Stavrou (PI, Krpytowire), 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: $7,437,173
- Department share: $1,793,747.11
- My share: $1,793,747.11

Security Analysis of Hardware Security Primitives Employed by IoT and Cyber-physical Systems

- Sponsor: Virginia Commonwealth Cyber Initiative (CCI), SWVA Node
- Project timeframe: 06-1-20 to 11-30-20
- Team: Matthew Hicks (sole-PI)
- Total: $20,000
- Department share: $20,000
- My share: $20,000

Digital Techniques for Exposing and Eliminating Information Hidden in SRAM's Analog Domain

- Sponsor: DARPA I2O
- Project timeframe: 7-1-19 to 6-30-22
- Team: Matthew Hicks (sole-PI)
- Total: $900,539
- Department share: $900,539
- My share: $900,539

CPI Protection Through Software Anti-Tamper (Phase 2)

- Sponsor: Office of the Secretary of Defense (OSD)
- Project timeframe: 8-1-18 to 2-28-20
- 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
- My share: $170,000

Conference Publications

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: `https://developer.arm.com/documentation/109291/latest`

No Linux, No Problem: Fast and Stateful Windows Binary Fuzzing via Target-embedded Snapshotting. Leo Stone, Rishi Ranjan, Stefan Nagy, and Matthew Hicks. USENIX Security Symposium (**USENIX**). August 2023.

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.

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.

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.

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.

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.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

Full-speed Fuzzing: Reducing Fuzzing Overhead through Coverage-guided Tracing. Stefan Nagy and Matthew Hicks. IEEE Symposium on Security and Privacy (**Oakland**). May 2019.

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

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.

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.
Top Picks in Hardware and Embedded Security 2022.

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.

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.

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.

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.

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.

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.

OTHER PUBLICATIONS

FinalFilter: Asserting Security Properties of a Processor at Runtime. Cynthia Sturton, Matthew Hicks, Samuel T. King, and Jonathan M. Smith. Invited. IEEE Micro. Vol. 34. Num. 4. July 2019.

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.

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.

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

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.

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

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.

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.

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

PROFESSIONAL SERVICE

Program Committee:

- 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**)
- 2017–2023 International Workshop on Energy Harvesting & Energy-Neutral Sensing Systems (ENSsys)
- 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 Reviewer:

- 2019, 2023 IEEE Transactions on Very Large Scale Integration Systems (**TVLSI**)
- 2021, 2023 Transactions on Software Engineering and Methodology (**TOSEM**)
- 2023 Transactions on Embedded Computing Systems (**TECS**)
- 2023 Transactions on Software Engineering (**TSE**)
- 2022 IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (**TCAD**)
- 2021 IEEE Transactions on Circuits and Systems (**TCAS**)
- 2021 Electronics Letters
- 2021 ACM Transactions on Privacy and Security (**TOPS**)
- 2018, 2020 IEEE Computer Architecture Letters (**CAL**)
- 2020, 2021 ACM Transactions on Computer Systems (**TOCS**)
- 2019 ACM Transactions on Sensor Networks (**TOSN**)
- 2018 IEEE Transactions on Dependable and Secure Computing (**TDSC**)

- 2017, 2018 Journal of Hardware and Systems Security (**HAAS**)
- 2018, 2022, 2023 ACM Transactions on Architecture and Code Optimization (**TACO**)
- 2018 IEEE Micro (**Micro**)
- 2018, 2021 ACM Transactions on Design Automation of Electronic Systems (**TODAES**)

Department Service

- 2018–2019 Faculty Search Committee
- 2018–2020 Systems PhD Qualifier Committee
  - 2019–2020 Chair
- 2019–2022 Graduate Program Committee
- 2020–2021 Faculty Search Committee
- 2022–2023 Promotion and Tenure Committee

Advising

Faculty Mentor - 2018 – 2023 MITRE Collegiate eCTF competition

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

Postdoctoral Fellows:

- Michael Moukarzel (2019–2022)

Student Committees:

- Chair
  - Harrison Williams (PhD)
  - Jubayer Mahmod (PhD)
  - Daniel Chiba (PhD)
  - Prakhar Sah (PhD)
  - Rishi Ranjan (MS)
  - Cameron Garcia (MS)
  - Sydney Earp (MS)
  - Paisley Code (MS)
  - Erin Freck (MS)
  - Rohit Sathye (MS)
  - 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)
  - Leo Stone (MS 2023, First Job:)
  - 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)
  - 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)
  - Sai Sanath Krishnappagari (MEng 2023)
- Member
  - 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)
  - 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)
  - Gregory Martin (PhD, Chair: Ryan Gerdes)
  - Niti Sharma (MS, Chair: Steve Jian)
  - Jongouk Choi (PhD, Chair: Changhee Jung)
  - Muhammad Laghari (PhD, Chair: Steve Jian)
  - Alok Singh (PhD, Chair: Ryan Gerdes)
  - Abdullah Zubair Mohammed (PhD, ECE, Chair: Ryan Gerdes)
  - Pantea Kiaei (PhD, Chair: Patrick Schaumont)
  - Xin Wang (PhD, Chair: Steve Jian)
  - Ying Zhang (PhD, Chair: Na Meng)
  - John Lee (PhD, ECE, Chair: Wenjie Xiong)
  - Jacob Haltiwanger (MS, Chair: Thang Hoang)
  - Ahmad Humayun (PhD, Chair: Muhammad Ali Gulzar)

Undergraduates:

- 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

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

Work Experience

Virginia Tech
Associate Professor **June 2022 to present**
Assistant Professor **September 2017 to 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 **September 2016 to September 2017**

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

University of Michigan
Lecturer **September 2015 to August 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 to 2015**

- **Energy-dictated Computing** **September 2013 to Present**
  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 a ARM Cortex-M0+ core running on a Xilinx Virtex-5 FPGA.

- **Approximate Computing** **September 2013 to Present**
  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, a OpenRISC OR1200 processor, and an MSP430 development board.

- **Malicious hardware** **May 2007 to Present**
  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 to 2013**

- **Imperfect hardware** **January 2011 to Present**
  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 to Present**
  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 to 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 to 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.