

Timothy Trippel

University of Michigan
Department of Computer Science & Engineering
2260 Hayward St, Ann Arbor, MI 48109

Phone: (574) 807-2771
Email: trippel@umich.edu
Home: <https://timothytrippel.com>

Education

- 2015–2021 (Expected) **University of Michigan**, Ph.D., Computer Science / Computer Security
Advisor: Prof. Kang G. Shin
- 2015–2016 **University of Michigan**, M.S.E., Computer Science / Computer Security
GPA: 3.85/4.00
- 2011–2015 **Purdue University**, B.S., Computer Engineering
GPA: 3.72/4.00

Ph.D. Dissertation Research

With the proliferation of ubiquitous computing and advancements in artificial intelligence, completely autonomous cyber-physical systems are becoming pervasive. From thermostats and voice assistants, to drones and vehicles, cyber-physical systems often blindly trust a collection of sensors and microprocessors to autonomously execute decisions. From design to deployment, my dissertation takes a red-team/blue-team approach to explore how autonomous cyber-physical systems can be attacked and defended through the foundational hardware they rely on. In doing so, my research aims to increase the trustworthiness and reliability of the autonomous systems entangled in our lives.

Awards and Honors

- [1] NSF Graduate Research Fellowship Recipient (2017)
- [2] Donald C. and Marion E. Currier Scholarship (Purdue University, Full Tuition)
- [3] Purdue University Dean's List (8/8 Semesters)
- [4] Purdue University Semester List (7/8 Semesters)
- [5] Indiana's Top Young Scientist (2011)
- [6] Intel International Science and Engineering Fair Second Place (2011)
Minor Planet named after me by MIT Lincoln Laboratory LINEAR
URL: <https://ssd.jpl.nasa.gov/sbdb.cgi#top> (search "Timtrippel")
- [7] National Junior Science and Humanities Symposium Second Place (2010)

Publications

Refereed

- [1] **Timothy Trippel**, Kang G. Shin, Kevin B. Bush, and Matthew Hicks. "ICAS: an Extensible Framework for Estimating the Susceptibility of IC Layouts to Additive Trojans". IEEE Symposium on Security and Privacy (**Oakland**), May 2020. Acceptance rate: TBD%.
An extensible framework for estimating the vulnerability of IC layouts to fabrication-time Trojaning attacks.
- [2] **Timothy Trippel**, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks". IEEE European Symposium on Security and Privacy (**EuroS&P**), April 2017. Acceptance rate: 19.6%.
First to demonstrate full control over output signals of MEMS sensors with targeted acoustic interference.

Non-refereed

- [1] **Timothy Trippel**, Kang G. Shin, Kevin B. Bush, and Matthew Hicks. “An Extensible Framework for Quantifying the Coverage of Defenses Against Untrusted Foundries”. ARXIV, abs/1906.08836
First to provide a framework for quantifying the security of integrated circuit layouts.
- [2] **Timothy Trippel**, Kang G. Shin, Kevin B. Bush, and Matthew Hicks. “Defensive Routing: a Preventive Layout-Level Defense Against Untrusted Foundries”. ARXIV, abs/1906.08842
A routing-centric preventive defense against stealthy analog hardware Trojans like A2.

Patents Filed

- [1] Kevin B. Bush, Matthew D. Hicks, and **Timothy D. Trippel**. “Defensive Routing and Related Techniques”. *US Patent Application #16/598,293.*
- [2] Kevin B. Bush, Matthew D. Hicks, and **Timothy D. Trippel**. “Integrated Circuit (IC) Portholes and Related Technologies”. *US Patent Application #16/597,013.*
- [3] Kevin Fu, Peter Honeyman, **Timothy Trippel**, and Ofir Weisse. “Protecting Motion Sensors from Acoustic Injection Attack”. *US Patent Application #16/303,495.*

Press

- [1] CNBC April 2017. Hacking with sound waves. Retrieved from <https://www.cnbc.com/video/2017/04/27/hacking-with-sound-waves.html>
- [2] EE Journal April 2017. Cracking a WALNUT A Novel Physical Attack on Accelerometers. Retrieved from <https://www.eejournal.com/article/20170417-walnut/>
- [3] New York Times March 2017. It’s Possible to Hack a Phone With Sound Waves, Researchers Show. Retrieved from <https://www.nytimes.com/2017/03/14/technology/phone-hacking-sound-waves.html>
- [4] IEEE Spectrum March 2017. Smartphone Accelerometers Can Be Fooled by Sound Waves. Retrieved from <https://spectrum.ieee.org/tech-talk/telecom/security/smartphone-accelerometers-can-be-fooled-by-sound-waves>
- [5] Science Friday March 2017. Hacking Via Sound. Retrieved from <https://www.sciencefriday.com/segments/a-proposed-science-budget-hacking-via-sound-and-a-fluorescent-frog/>
- [6] IFL Science March 2017. Sound Waves Can Now Be Used To Hack Into Smartphones. Retrieved from <https://www.iflscience.com/technology/sound-waves-used-hack-smartphones/>
- [7] University of Michigan March 2017. Sonic Cyber Attacks Show Security Holes in Ubiquitous Sensors. Retrieved from <http://www.eecs.umich.edu/eecs/about/articles/2017/sonic-cyber-attacks.html>
- [8] Gizmodo March 2017. Hackers Can Now Use Sound Waves to Take Control of Your Smartphone. Retrieved from <https://gizmodo.com/hackers-can-now-use-sound-waves-to-take-control-of-your-1793259066>
- [9] Fortune March 2017. You Can Hack Fitbits and Smart Phones Using Sound, Researchers Say. Retrieved from <https://fortune.com/2017/03/14/hack-fitbit-smart-phones-using-sound/>
- [10] CNET March 2017. These researchers can hack your phone with sound waves. Retrieved from <https://www.cnet.com/news/hack-fitbit-samsung-sound-waves-researchers/>

- [11] Tom's Hardware March 2017. 'Walnut' Attack Uses Sound To Trick Sensors In Cars, Phones, And Other Devices. Retrieved from <https://www.tomshardware.com/news/walnut-sound-trick-sensors-cars-phones,33901.html>
- [12] The Register March 2017. Boffins Rickroll smartphone by tickling its accelerometer. Retrieved from https://www.theregister.co.uk/2017/03/15/boffins_rickroll_smartphone_by_tickling_its_accelerometer/
- [13] Engineering.com March 2017. Hacking Sensors with Sound Waves. Retrieved from <https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/14511/Hacking-Sensors-with-Sound-Waves.aspx>
- [14] Hacker News March 2017. WALNUT Attack on MEMS Accelerometers. Retrieved from <https://news.ycombinator.com/item?id=13881167>

Professional Experience

2015–	Ph.D. Candidate Computer Science & Engineering Department Advisor: Kang G. Shin	University of Michigan , Ann Arbor, MI
2019	Graduate Research Intern Cyber-Physical Systems Supervisor: Kevin B. Bush Mentor: Matthew Hicks	MIT Lincoln Laboratory , Lexington, MA
2018	Graduate Research Intern Cyber Systems & Operations Supervisor: Kevin B. Bush Mentor: Matthew Hicks	MIT Lincoln Laboratory , Lexington, MA
2017	Graduate Research Intern Cyber Systems & Operations Supervisor: Kevin B. Bush Mentor: Matthew Hicks	MIT Lincoln Laboratory , Lexington, MA
2015	Software Engineering Intern Windows & Devices Group Supervisor: Ted Roberts	Microsoft , Bellevue, WA
2014	Software Engineering Intern Operating Systems Group Supervisor: Mike Dice	Microsoft , Redmond, WA
2013	EID Software Engineering Intern Supervisor: Anand Desikan	GE Healthcare , Barrington, IL

Teaching Experience

2014	Teaching Assistant Microprocessor System Design and Interfacing (ECE 362)	Purdue University
2013	Teaching Assistant Introduction to Digital Systems Design (ECE 270)	Purdue University

Invited Presentations

- [1] Talk “WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks”. 2nd European Symposium on Security & Privacy (EuroS&P), Paris, France. April, 2017.
- [2] Poster “Why Do You Trust Sensors? Analog Cybersecurity Attack Demos”. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA. April, 2017.
- [3] Talk “WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks”. University of Michigan Preliminary Examination, Ann Arbor, MI. January, 2017.
- [4] Talk “WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks”. THaW Annual Review, Vanderbilt University, Nashville, TN. September, 2016.
- [5] Poster “Acoustic Injection Attacks on Implantable Medical Devices”. THaW Annual Review, Johns Hopkins University, Baltimore, MD. January, 2016.

Demos

- [1] “Why Do You Trust Sensors? Analog Cybersecurity Attack Demos”. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA. April, 2017.
- [2] “WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks”. Analog Devices Inc. Annual Executives Meeting, Boston, MA. January, 2016.

Relevant Technical Coursework

Graduate: Computer & Network Security, Micro-architecture, Artificial Intelligence, Machine Learning, Advanced Networking, Advanced Operating Systems

Undergraduate: Computer Architecture, Signals and Systems, Data Structures and Algorithms, Operating Systems, Embedded Systems Senior Design, Computer & Network Security, Microprocessor System Design, Digital Systems Design

Environments, Languages, and Design Tools Experience

Languages: Python, C/C++, Java, Matlab, C#, JavaScript, Verilog, Bash, Assembly, HTML/CSS

Environments: MacOS, Linux, Windows

Design Tools: GTKWave, Innovus, Genus, Spectre, Virtuoso, Icarus Verilog, Calibre nmDRC, COMSOL