Timothy Trippel

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

Phone: (574) 607-3954
Email: trippel@umich.edu
Website: 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

From thermostats and voice assistants, to drones and vehicles, autonomous systems often blindly trust integrated circuit (IC) hardware to execute decisions. Making matters worse, the cost and complexity of developing such hardware has pushed many companies, and nation states, to outsource many phases of the design and fabrication processes. Outsourcing, combined with the black-box nature of ICs presents a security risk: *we must trust our hardware has been designed and fabricated to specification.* From design to deployment, my research develops automated techniques to vet hardware for intentional (e.g., Trojans) and unintentional (e.g., bugs) flaws.

Awards and Honors

[1] R&D 100 Award Winner in IT/Electrical for *Defensive Wire Routing for Untrusted IC Fabrication* (2020)
[2] National Science Foundation Graduate Research Fellowship (2017)
[3] Top 10 and Twilio Challenge Award at BoilerMake Hackathon (2014)
[4] Donald C. and Marion E. Currier Scholarship (Purdue University, Full Tuition)
[5] Purdue University Dean's List (8/8 Semesters)
[6] Purdue University Semester Honors (7/8 Semesters)
[7] Indiana's Top Young Scientist (2011)
[8] 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")
[9] National Junior Science and Humanities Symposium Second Place (2010)

Publications

Refereed

[1] **Timothy Trippel**, Kang G. Shin, Kevin B. Bush, and Matthew Hicks. "Bomberman: Defining and Defeating Hardware Ticking Timebombs at Design-time". IEEE Symposium on Security and Privacy (**Oakland**), May 2021. Acceptance rate: TBD.
   A dynamic verification technique for eradicating the threat of Ticking-Timebomb Trojans in RTL hardware.

[2] **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: 12.3%.
   An extensible framework for estimating the vulnerability of IC layouts to fabrication-time Trojaning attacks.

[3] **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. "T-TER: Defeating A2 Trojans with Targeted Tamper-Evident Routing". ARXIV, abs/1906.08842.
A routing-centric preventive defense against stealthy analog hardware Trojans like A2.

Patents

Adjudicated

[1] Kevin B. Bush, Matthew D. Hicks, and **Timothy D. Trippel**. "Integrated Circuit (IC) Portholes and Related Techniques". *U.S. Patent No. 10,839,109*. Issue Date: Nov. 17th, 2020.

Pending

[1] Kevin B. Bush, Matthew D. Hicks, and **Timothy D. Trippel**. "Defensive Routing and Related Techniques". *US Patent Application No. 16/598,293*. Filing Date: Oct. 10th, 2019.

[2] Kevin Fu, Peter Honeyman, **Timothy Trippel**, and Ofir Weisse. "Protecting Motion Sensors from Acoustic Injection Attack". *US Patent Application No. 16/303,495*. Filing Date: May 19th, 2017.

Professional Experience

Sept. 2015–Present	**Ph.D. Candidate** Computer Science & Engineering Department	**University of Michigan**, Ann Arbor, MI **Advisor:** Kang G. Shin
	See Ph.D. Disertation Research above.	
Summer 2020	**Research Intern** OpenTitan	**Google**, Cambridge, MA **Supervisors:** Alex Chernyakhovsky & Garret Kelly
	Developed a *hardware fuzzing* pipeline to fuzz software models of RTL hardware to complement and accelerate traditional design verification efforts across the OpenTitan hardware ecosystem. Additionally, open-sourced project codebase and submitted technical paper for publication in an academic conference.	
Summer 2019	**Graduate Research Intern** Cyber-Physical Systems	**MIT Lincoln Laboratory**, Lexington, MA **Supervisors:** Kevin B. Bush & Matthew Hicks
	Developed a design-time dynamic verification technique to verify hardware is free of Ticking Timebomb Trojans. Additionally, open-sourced project codebase and submitted technical paper for publication in an academic conference.	
Summer 2018	**Graduate Research Intern** Cyber Systems & Operations	**MIT Lincoln Laboratory**, Lexington, MA **Supervisors:** Kevin B. Bush & Matthew Hicks
	Developed techniques to protect the integrity of integrated circuit layouts to fabrication-time attacks enabled by manufacturing them at untrusted foundries. Fabricated prototype hardware on in-house 90nm rad-hard process. Additionally, filed two patents, and submitted technical paper for publication in an academic conference.	
Summer 2017	**Graduate Research Intern** Cyber Systems & Operations	**MIT Lincoln Laboratory**, Lexington, MA **Supervisors:** Kevin B. Bush & Matthew Hicks
	Developed tools to measure the susceptibility of integrated circuit layouts to fabrication-time attacks enabled by manufacturing them at untrusted foundries. Additionally, open-sourced project codebase and submitted technical paper for publication in an academic conference.	
Summer 2015	**Software Engineering Intern** Windows & Devices Group	**Microsoft**, Bellevue, WA **Supervisor:** Ted Roberts
	Worked on the Windows IoT Core team to design and develop point-of-sale (PoS) device emulators for Visual Studio and Windows 10.	

Summer 2014	**Software Engineering Intern** Operating Systems Group	**Microsoft**, Redmond, WA **Supervisor:** Mike Dice

Worked on the Membership Assistance and Connections team to design and develop a web UX customer support feature for Windows 10, and its supporting back-end.

Jan. 2014– Apr. 2015	**Undergraduate Researcher** Electrical & Computer Engineering	**Purdue University**, West Lafayette, IN **Advisor:** Prof. Cheng-Kok Koh

Developed place-and-route algorithms, used by VLSI CAD tools, to automate and optimize integrated circuit layout.

Summer 2013	**EID Software Engineering Inern**	**GE Healthcare**, Barrington, IL **Supervisor:** Anand Desikan

Developed a software life-cycle reporting tool, for use by agile scrum teams, to automate the production of Design History Files required to meet FDA healthcare software regulations. Developed a Python back-end to parse Agile process artifacts, test requirements, and results, that were dumped into a custom internal facing web UX.

Teaching Experience

2014	**Teaching Assistant** Microprocessor Systems & Interfacing (ECE 362)	**Purdue University**, West Lafayette, IN
2013	**Teaching Assistant** Introduction to Digital System Design (ECE 270)	**Purdue University**, West Lafayette, IN

Selected Talks & Presentations

[1] Talk "Fuzzing Hardware Like Software". Google CI2 Verification Team, Virtual. August, 2020.

[2] Talk "ICAS: an Extensible Framework for Estimating the Susceptibility of IC Layouts to Additive Trojans". 41st IEEE Symposium on Security & Privacy (**Oakland**), San Francisco, CA. May, 2020.

[3] Talk "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks". 2nd IEEE European Symposium on Security & Privacy (**EuroS&P**), Paris, France. April, 2017.

[4] Talk "Waging Doubts on the Integrity of MEMS Accelerometers with Acoustic Attacks". THaW Annual Review, Vanderbilt University, Nashville, TN. September, 2016.

[5] Poster "HeartBeats: A study of acoustic injection attacks on medical devices". THaW Annual Review, Johns Hopkins University, Baltimore, MD. January, 2016.

Tutorials

[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] "Acoustic Injection Attacks on MEMS Accelerometers". Analog Devices Inc. Annual Executives Meeting, Boston, MA. January, 2016.

Press

[1]	MIT News	October 2020. *Eight Lincoln Laboratory technologies named 2020 R&D 100 Award winners.* Retrieved from `https://news.mit.edu/2020/lincoln-laboratory-technologies-rd-100-award-winners-1020`
[2]	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`
[3]	CNBC	April 2017. *Hacking with sound waves.* Retrieved from `https://www.cnbc.com/video/2017/04/27/hacking-with-sound-waves.html`

[4] University of Michigan News   March 2017. *Sonic Cyber Attacks Show Security Holes in Ubiquitous Sensors.* Retrieved from `https://news.umich.edu/sonic-cyber-attack-shows-security-holes-in-ubiquitous-sensors-2/`

[5] EE Journal   April 2017. *Cracking a WALNUT A Novel Physical Attack on Accelerometers.* Retrieved from `https://www.eejournal.com/article/20170417-walnut/`

[6] 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`

[7] 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/`

[8] 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/`

[9] 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`

[10] 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/`

[11] 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/`

[12] 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`

[13] 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/`

[14] Engineering.com   March 2017. *Hacking Sensors with Sound Waves.* Retrieved from `https://www.engineering.com/story/hacking-sensors-with-sound-waves`

[15] Hacker News   March 2017. *WALNUT Attack on MEMS Accelerometers.* Retrieved from `https://news.ycombinator.com/item?id=13881167`

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

Languages

Proficient: Python, C/C++, Bash, LaTeX
Familiar: (System)Verilog, MATLAB, Java, C#, JavaScript, HTML/CSS

Platforms

Proficient: Linux, MacOS, Docker, GCP
Familiar: AWS, Windows

Software Tools

Proficient: Vim, Git, Make, AFL, Seaborn/Matplotlib, Pandas
Familiar: LLVM, NumPy, pytest, PyPy, kcov

Hardware Tools

Proficient: Verilator, Icarus Verilog, GTKWave
Familiar: FuseSoC, cocotb, Innovus, Genus, Spectre, Virtuoso, Calibre nmDRC, COMSOL