Timothy Trippel

Phone: (574) 607-3954
Email: timothy@trippel.me
Website: `https://timothytrippel.com`

Education

2015–2021	**University of Michigan**, Ph.D., Computer Science Advisor: Prof. Kang G. Shin
2015–2016	**University of Michigan**, M.S.E., Computer Science
2011–2015	**Purdue University**, B.S., Computer Engineering

Summary

My experience / interests lie at the intersection of hardware and software co-design, computer architecture, and embedded systems. I have experience in low-level firmware development, hardware and firmware fuzzing, pre-silicon verification, and developing novel security-focused EDA tools for IC design. I have a background in low-level security research, where I have published several top-tier conferences papers (e.g, USENIX, Oakland, CHES). I am a top-10 contributor to the open-source OpenTitan project.

Professional Experience

June 2021– Present **Senior Software Engineer** — **Google, LLC**, Mountain View, CA
ChromeOS — **Managers:** Neil Hendin; Arun Thomas

Developed firmware (for pre-silicon verification) and fuzzing techniques for OpenTitan: the first open-source silicon root-of-trust.

- Developed a FreeRTOS-based pre-silicon verification test framework for the OpenTitan chip.
- Led the refactoring and completion of 30+ pre-silicon verification device drivers for OpenTitan.
- Stood up several CW310 FPGA boards to emulate OpenTitan hardware for software development purposes.
- Led the final (≈3 months) Meson to Bazel build system migration effort for the OpenTitan codebase.
- Created a top-level test development guide to onboard both company-internal and -external contributors to top-level pre-silicon verification efforts.
- Recruited / Led Ph.D. research itern to develop a novel firmware fuzzing technique to fuzz OpenTitan ROM.

Sept. 2015– May 2021 **Ph.D. Candidate** — **University of Michigan**, Ann Arbor, MI
Computer Science & Engineering — **Advisor:** Kang G. Shin

From design to deployment, my dissertation research developed automated techniques (i.e., fuzzing and EDA tools) to rigorously evaluate hardware designs for the presence of intentional (e.g., Trojans) and unintentional (e.g., bugs) flaws capable of compromising application security.

Summer 2020 **Research Intern** — **Google**, Cambridge, MA
OpenTitan — **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** — **MIT Lincoln Laboratory**, Lexington, MA
Cyber-Physical Systems — **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** — **MIT Lincoln Laboratory**, Lexington, MA
Cyber-Physical Systems — **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 90 nm rad-hard process. Additionally, filed two patents, and submitted technical paper for publication in an academic conference.

Summer **Graduate Research Intern** — **MIT Lincoln Laboratory**, Lexington, MA

2017 Cyber-Physical Systems **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** **Microsoft**, Bellevue, WA
Windows & Devices Group **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** **Microsoft**, Redmond, WA
Operating Systems Group **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** **Purdue University**, West Lafayette, IN
Electrical & Computer Engineering **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 Intern** **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.

Publications

Refereed

[1] **Timothy Trippel**, Kang G. Shin, Kevin B. Bush, and Matthew Hicks. "T-TER: Defeating A2 Trojans with Targeted Tamper-Evident Routing". **ACM Asia Conference on Computer and Communications Security (AsiaCCS)**, July 2023. Acceptance rate: TBD.
A routing-centric preventive defense against stealthy analog hardware Trojans like A2.

[2] Pascal Nasahl, Miguel Osorio, Pirmin Vogel, Michael Schaffner, **Timothy Trippel**, Dominic Rizzo, and Stefan Mangard. "SYNFI: Pre-Silicon Fault Analysis of an Open-Source Secure Element". **IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES)**, September 2022. Acceptance rate: 38%.
A pre-silicon formal verification tool to evaulate fault-injection countermeasures in a secure IC.

[3] **Timothy Trippel**, Kang G. Shin, Alex Chernyakhovsky, Garret Kelly, Dominic Rizzo, and Matthew Hicks. "Fuzzing Hardware Like Software". **USENIX Security Symposium**, August 2022. Acceptance rate: 17.2%.
Adapting coverage-guided greybox software fuzzers for dynamic verification of RTL hardware.

[4] **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: 12.08%.
A dynamic verification technique for eradicating the threat of Ticking-Timebomb Trojans in RTL hardware.

[5] **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.

[6] **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, May 2019.
Quantifiable metrics for evaluating the security of integrated circuit layouts.

Patents

[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.
Integrated circuit layout designs for enhancing post-fabrication imaging of security-critical interconnects.

[2] Kevin Fu, Peter Honeyman, **Timothy Trippel**, and Ofir Weisse. "Protecting Motion Sensors from Acoustic Injection Attack". *US Patent No. 11,209,454.* Issue Date: Dec. 28th, 2021.
Signal filtering mechanisms for coping with periodic interference in motion sensors.

[3] Kevin B. Bush, Matthew D. Hicks, and **Timothy D. Trippel**. "Defensive Routing and Related Techniques". *US Patent No. 11,347,902.* Issue Date: May 31st, 2022.
Integrated circuit routing techniques for hardening interconnects against fabrication-time modifications.

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)

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". 31st USENIX Security Symposium, Boston, MA. August, 2022.

[2] Talk "Bomberman: Defining and Defeating Hardware Ticking Timebombs at Design-time". 42nd IEEE Symposium on Security & Privacy (**Oakland**), San Francisco, CA. May, 2021.

[3] 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.

[4] 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.

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

[6] 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] NewScientist February 2021. *Virtual computer chip tests expose flaws and protect against hackers.* Retrieved from `https://www.newscientist.com/article/2269263-virtual-computer-chip-tests-expose-flaws-and-protect-against-hackers/`

[2] 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`

[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] CNBC April 2017. *Hacking with sound waves.* Retrieved from `https://www.cnbc.com/video/2017/04/27/hacking-with-sound-waves.html`

[5] 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/`

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

[7] 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`

[8] 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/`

[9] 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/`

[10] 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`

[11] 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/`

[12] 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/`

[13] 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`

[14] 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/`

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

[16] 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: C/C++, Python, Bash, LaTeX
Familiar: (System)Verilog, Starlark, MATLAB, Java, C#, JavaScript, HTML/CSS

Platforms/Architectures

Proficient: Linux, Docker, RISC-V
Familiar: FreeRTOS, MacOS

Cloud Platforms/Tools

Proficient: GCP (Compute Engine, Cloud Storage, Cloud Build)
Familiar: Azure (Pipelines), AWS (Route 53, EC2, S3, CodePipeline)

Software Tools

Proficient: Vim, Git, Bazel, Make, GDB, AFL++, Seaborn/Matplotlib, Pandas
Familiar: LLVM, NumPy, pytest, PyPy, kcov, OpenOCD, Jupyter/Colab

Hardware Design Tools

Proficient: Verilator, Icarus Verilog, GTKWave
Familiar: Vivado, FuseSoC, cocotb, Synopsys VCS, Xcelium, Innovus, Genus, Virtuoso, Calibre nmDRC

Hardware Tools/Protocols

Tools: Ocilloscope, Logic Analyzer, Multimeter, Function Generator
Protocols: UART, SPI, I2C, JTAG