Timothy **Trippel**

2260 Hayward St, Rm. 4944, Ann Arbor, MI 48109

trippel@umich.edu https://timothytrippel.com

Education

University of Michigan *Ann Arbor, MI*

PH.D. IN COMPUTER SCIENCE & ENGINEERING *Sept 2015 – May 2019 (Expected)*

M.S.E. IN COMPUTER SCIENCE & ENGINEERING *Sept 2015 – Dec 2016*

- Advisor: Kang G. Shin
- Cumulative GPA: 3.85/4.00

Purdue University *West Lafayette, IN*

B.S. IN COMPUTER ENGINEERING *Aug 2011 – May 2015*

- Cumulative GPA: 3.72/4.00

Computer Skills

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

Platforms & Software: macOS • Windows • Linux • Intel SGX • Visual Studio • Eclipse • Git

Coursework

Graduate: Computer & Network Security • Artificial Intelligence • Machine Learning Advanced Networking • Microarchitecture • 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

Professional Experience

MIT Lincoln Laboratory *Lexington, MA*

SUMMER GRADUATE RESEARCH INTERN *May 2017 – Sept 2017*

- Cyper Systems and Operations Group
- Developed tools to protect ASIC hardware from fabrication-time attacks enabled by manufacturing them at untrusted foundries

University of Michigan *Ann Arbor, MI*

GRADUATE STUDENT RESEARCH ASSISTANT *Sept 2015 – Present*

- Department of Computer Science & Engineering
- Focus: Hardware Supply Chain Security, Embedded Systems/IoT Security
- Advisor: Kang G. Shin

Microsoft *Bellevue, WA*

SOFTWARE ENGINEERING INTERN – WINDOWS DEVICES GROUP *Summer 2015*

- Worked on IoT Core Team
- Designed and developed Windows 10 point-of-sale (PoS) device emulators for integration into Visual Studio.
- Designed both UX and back-end for PoS device emulators primarily in XAML, C#, and C++.

Microsoft *Redmond, WA*

Software Engineering Intern – Operating Systems Group *Summer 2014*

- Worked on Membership Assistance and Connection Team
- Designed and developed a remote assistance customer support feature, and its supporting back-end for Windows 10.
- Developed web UX and back-end using ASP.NET MVC5, SignalR, Twitter Bootstrap, jQuery, Jasmine.js, and Windows Azure services.

Purdue University *West Lafayette, IN*

Undergraduate Research Assistant *Jan. 2014 – April 2015*

- Department of Electrical & Computer Engineering
- Focus: VLSI CAD Tool Algorithms
- Advisor: Cheng-Kok Koh

GE Healthcare *Barrington, IL*

EID Software Engineering Intern *Summer 2013*

- Designed and developed a software development 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

WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks
Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu
2nd Annual IEEE European Symposium on Security and Privacy (EuroS&P)
April 2017. Paris, France. (Conference acceptance rate: 19.6%).

Presentations

2017 IEEE European Symposium on Security and Privacy (EuroS&P) *Paris, France*

Conference Presentation *April 2017*

"WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks"

CFAR Annual Review *University of Michigan, Ann Arbor, MI*

Invited Poster *Dec 2016*

"WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks"

THaW Annual Review *Vanderbilt University, Nashville, TN*

Invited Presentation *Sept 2016*

"WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks"

Analog Devices Inc. Annual Executives Meeting *Boston, MA*

Invited Presentation & Demo *Jan 2016*

"WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks"

THaW Annual Review *Johns Hopkins University, Baltimore, MD*

Invited Poster *Jan 2016*

"Acoustic Injection Attacks on Implantable Medical Devices"

Teaching Experience

Purdue University *West Lafayette, IN*

Teaching Assistant – Microprocessor System Design – ECE362 *Spring 2014*

Course Instructor: David G. Meyer

Purdue University *West Lafayette, IN*
Teaching Assistant – Introduction to Digital System Design – ECE270 *Fall 2013*
Course Instructor: David G. Meyer

Organizations

2017 **Michigan Data Science Team** *Ann Arbor, MI*
2014 **Eta Kappa Nu Electrical and Computer Engineering Society** *Beta Chapter*

Awards & Honors

2017 **National Science Foundataion (NSF) Graduate Research Fellowship** *Ann Arbor, MI*
2016 **University of Michigan Summer Graduate Research Fellowship** *Ann Arbor, MI*
2012 **Donald C. and Marion E. Currier Undergraduate Scholarship** *West Lafayette, IN*
Full Tuition and Living Stipend for 3 years
2011–2015 **Purdue University Deans List**, 7 Semesters *West Lafayette, IN*
2014 **Twilio Challenge Award**, Purdue University BoilerMake Hackathon *West Lafayette, IN*
2011 **Indiana's Top Young Scientist** *Bloomington, IN*
$10,000 Scholarship
2011 **2nd Place**, Intel International Science and Engineering Fair *Los Angeles, CA*
$1,500 and naming of a minor planet in my honor by MIT Lincoln Labs
2010 **2nd Place**, National Junior Science and Humanities Symposium *Bethesda, MD*
$8,000 and paid trip to London International Youth Science Forum

Projects

Algorithmic Financial Modelling and Company Valuations
MDST Project *Spring 2017*
Worked with Michigan Data Science Team members to develop an algorithmic model for predicting company valuations. Project currently ongoing.

LightSM: a Low-Cost Cryptographic Security Module based on Trusted Execution Environments
Research Project *Spring 2017*
Worked on a 5 person team to build a lightweight software "hardware security module (HSM)" to protect cryptographic key material and operations in untrusted virtual cloud environments from being comprised by untrusted operating systems, hypervisors, or hardware. LightSM utilizes the security guarantees provided Trusted Execution Environments (specifically Intel SGX technology). LightSM was integrated into lighttpd and a Linux PAM used for password authentication.

Subverting the Linux RNG via the Xen Hypervisor *Course Project*
EECS 588 – Computer and Network Security *Spring 2016*
Worked in a three person team to design and develop random number generation attacks on virtual machines (VMs) running on top of the Xen hypervisor. Our attacks programmatically control the output of /dev/random and /dev/urandom, as well as the generation of private keys for Diffie-Hellman key exchanges in Apache2/OpenSSL from the hypervisor, without modification to the VM. Additionally, we explored artifacts of these attacks and proposed detection methods to combat use in the wild.

Spoofing MEMS Accelerometers with Acoustic Injection Attacks

Research Project *Spring 2016*

I developed a novel acoustic side-channel attack against MEMS accelerometers. I demonstrated how adversaries can spoof arbitrary acceleration output signals from a capacitive MEMS accelerometer using intentional acoustic interference. Additionally, I provided defense mechanisms to thwart such attacks. This work was published at the 2017 IEEE European Symposium on Secuirty & Privacy in Paris, France. Portions of this work are patent pending.

Split QUIC: an Alternative to Split TLS *Course Project*

EECS 589 – Advanced Networking *Fall 2015*

Worked in a three person team to design and develop an alternative to Split TLS, which is commonly used in enterprise network environments to enable network admins to introspect on corporate network traffic. We demonstrated our design on top of the QUIC protocol. “Split QUIC” leaks TLS session keys in real-time to a trusted network gateway to allow network traffic introspection, while maintaining end-to-end encryption between a client and server.

Stratus: Wireless WiFi Flash Drive *Course Project*

ECE 477 – Digital Systems Senior Design *Spring 2015*

Worked in a four person team to design and develop a wireless Wi-Fi flash drive. Stratus was designed to be a “wireless cloud storage device in your pocket”. Stratus consisted of a micro SD card and wireless (Wi-Fi) network interface SoC built around a central microprocessor. Mobile devices could read and write to the SD card over Wi-Fi. We designed Stratus from the ground up including: printed circuit board, system architecture, firmware, interfacing iOS application, and physical packaging.

Custom MIPS Dual-Core Cache Coherent Pipelined Processor *Course Project*

ECE 477 – Digital Systems Senior Design *Spring 2015*

I designed and architected, using Verilog, a dual core, cache-coherent, 5 stage pipelined microprocessor that suported a subset of the MIPS instruction set. The project was broken down into building basic processor functional units (register file, ALU, control unit, memory controller, branch predictor, caches, etc.) and assembling them together. The end result was a fully functional RTL design that was synthesized and tested on an FPGA clocked at 25 MHz. The RTL was written in Verilog and simulated using ModelSim.