

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 2020 (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

University of Michigan

Ann Arbor, MI

GRADUATE STUDENT RESEARCH ASSISTANT

Sept. 2015 – Present

- Department of Computer Science & Engineering
- Focus: Secure Execution Platforms, Embedded Systems/IoT Security, Applied Machine Learning
- Advisors: Todd Austin & Kevin Fu

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

UNDERGRADUATE RESEARCH ASSISTANT

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

West Lafayette, IN
Jan. 2014 – April 2015

GE Healthcare

EID SOFTWARE ENGINEERING INTERN

- 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.

Barrington, IL
Summer 2013

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%).

LightSM: a Low-Cost Cryptographic Security Module based on Trusted Execution Environments

OFIR WEISSE, TIMOTHY TRIPPEL, AMIR RAHMATI, MATTHEW HICKS, AND J. ALEX HALDERMAN

Currently under submission.

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

INVITED POSTER

University of Michigan, Ann Arbor, MI

Dec. 2016

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

THaW Annual Review

INVITED PRESENTATION

Vanderbilt University, Nashville, TN

Sept. 2016

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

Analog Devices Inc. Annual Executives Meeting

INVITED PRESENTATION & DEMO

Boston, MA

Jan. 2016

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

THaW Annual Review

INVITED POSTER

Johns Hopkins University, Baltimore, MD

Jan. 2016

“Acoustic Injection Attacks on Implantable Medical Devices”

Teaching Experience

Purdue University

TEACHING ASSISTANT – MICROPROCESSOR SYSTEM DESIGN – ECE362

Course Instructor: David G. Meyer

West Lafayette, IN

Spring 2014

Purdue University

TEACHING ASSISTANT – INTRODUCTION TO DIGITAL SYSTEM DESIGN – ECE270

Course Instructor: David G. Meyer

West Lafayette, IN

Fall 2013

Organizations

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

Awards & Honors

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

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 is to be published at the 2017 IEEE European Symposium on Security & Privacy in Paris, France. Portions of this work are patent pending.

Split QUIC: an Alternative to Split TLS

EECS 589 – ADVANCED NETWORKING

Course Project

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

ECE 477 – DIGITAL SYSTEMS SENIOR DESIGN

Course Project

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

ECE 477 – DIGITAL SYSTEMS SENIOR DESIGN

Course Project

Spring 2015

I designed and architected, using Verilog, a dual core, cache-coherent, 5 stage pipelined microprocessor that supported 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.