Willy R. Vasquez

wrv@utexas.edu

https://alum.mit.edu/www/wrv/

EDUCATION

The University of Texas, Austin, TX
Candidate for Ph.D. Electrical and Computer Engineering **Expected Ph.D.**: Summer 2024

- **Current Research:** Finding and Protecting from Vulnerabilities in Media Parsing Libraries
- **Adviser:** Prof. Hovav Shacham

Massachusetts Institute of Technology (MIT), Cambridge, MA September 2017
Master of Engineering (M.Eng.) in Computer Science and Engineering

- **M.Eng. Thesis:** Auditable Private Ledgers
- **Adviser:** Dr. Neha Narula

Massachusetts Institute of Technology (MIT), Cambridge, MA June 2015
B.S. in Computer Science and Engineering

- **Undergraduate Thesis:** Optimizing SAT/SMT Solvers with Machine Learning and Program Synthesis
- **Adviser:** Prof. Armando Solar-Lezama

RELEVANT SKILLS

Programming	Python, Rust, Java, Go, C, C++; Android; Git
Security	Ghidra, gdb, Corellium
Language	Fluent in Spanish

PUBLICATIONS

Yingchen Wang, Riccardo Paccagnella, Zhao Gang, **Willy R. Vasquez**, David Kohlbrenner, Hovav Shacham, and Chris W. Fletcher. *GPU.zip: On the Side-Channel Implications of Hardware-Based Graphical Data Compression*. In IEEE Security and Privacy. San Francisco, CA, 2024.

Willy R. Vasquez, Stephen Checkoway, Hovav Shacham. *The Most Dangerous Codec in the World: Finding and Exploiting Vulnerabilities in H.264 Decoders*. In Usenix Security. Anaheim, California, 2023.

Neha Narula, **Willy Vasquez**, and Madars Virza. *Privacy-preserving Auditing on Distributed Ledgers*. In Usenix NSDI. Renton, Washington, 2018.

EXPERIENCE

UT Systems Security Lab – Video Decoder Security
Research Assistant with Hovav Shacham August 2019 – Present

- Evaluate the security of hardware video decoders on mobile devices by constructing malformed H.264 encoded videos.
- Built H26Forge, a Rust tool to decode, mutate, and encode H.264 videos abiding by the H.264 spec and the entropy encoding process.
- H26Forge can also be used to modify and re-encode existing H.264 videos for targeted syntax exploration, or as a part of a fuzzing process for evaluating video decoder resilience against spec-compliant, correctly encoded, out-of-bounds syntax elements.
- Associated CVEs: CVE-2022-48434, CVE-2022-42850, CVE-2022-42846, CVE-2022-32939, and CVE-2022-3266
- Presentations: REcon 2023, Black Hat USA 2023, USENIX Security 2023, Demuxed 2023, BSidesDFW 2023.

UT Systems Security Lab – Media Library Sandboxing
Research Assistant with Hovav Shacham January 2022 – Present

- Add WASM SIMD support to RLBox, a toolkit for sandboxing third-party C libraries, by incorporating the SIMD Everywhere library into The WebAssembly Binary Toolkit utility wasm2c. RLBox with SIMD enables sandboxing performance-critical C libraries, such as browser media parsers.
- SIMD-enhanced RLBox was used to sandbox libSoundTouch and released in Firefox 120. [Mozilla Bugzilla 1673285]

Trail of Bits – Zero-knowledge Proofs of Exploits
Intern in the Research and Engineering Group February 2023

- Designed and implemented approach to incorporate the file system into zero knowledge proofs for exploits of x86 program vulnerabilities.

Cirrus Logic – Hardware Security Verification
Intern in the Design Verification Team Fall 2021

- Evaluated System-on-Chip design for potential security vulnerabilities.
- Synthesized HW security literature to establish security verification methodology in line with customer requirements.

UT Spark Research Lab – Verifiable Computation
Research Assistant with Mohit Tiwari August 2017 – July 2019

- Research and understand verifiable computing primitives, including SNARKs, Interactive Proofs, and arithmetic circuit compilation.
- Build upon existing verifiable computing constructions to improve prover overhead.

Samsung Austin Research Center (SARC) – Evaluating Samsung Processor Security
Research Intern in the Samsung Performance Architecture (SPA) Team Summer 2019

- Evaluated hardware fixes related to Spectre Variant 2.
- Provide design recommendations to ensure side-channel resistant processor components.

Microsoft Research – Optimizing Verifiable Computing
Research Intern in the Security and Privacy Group Summer 2018

- Improve the performance of a verifiable state machine system called Spice (OSDI '18) with memoization techniques.
- Design balanced tree data structures in Python that minimizes the number of balance operations with minimal depth.

MIT Digital Currency Initiative (DCI) – Auditable Private Ledgers
Research Assistant with Neha Narula August 2016 – August 2017

- Research technologies and tools to add privacy-enabling technologies to blockchains.
- Design and implement zero-knowledge proofs and homomorphic commitment schemes atop distributed ledger technologies in Go.
- Paper accepted to NSDI '18.

Raytheon BBN Technologies – Cybersecurity Group
Associate Cyber Research Scientist August 2015 – August 2016

- Contributed to the design and analysis of DARPA funded cybersecurity efforts.
- Designed behavioral malware signatures that rely on results from static analysis results of Android applications.
- Engineered suggestors and constraint solvers for the generation of potential vulnerabilities in commodity devices.
- Participated in business development initiatives by providing new ideas and performing feasibility research.
- Organized biweekly group tech talks with internal and external speakers.

MIT Sloan School of Management – Vulnerability Research and Vulnerability Market Analysis
Research Assistant with Michael Siegel May 2015 – August 2015

- Fuzzed multiple versions of a popular program using AFL to provide evidence for a model of cyber vulnerability discovery.

Benemérita Universidad Autónoma de Puebla (BUAP) – School of Computer Science
Research Assistant with Miguel Angel León Chávez June 2015 – July 2015

- Developed iPhone and server applications that used pairing based cryptography to perform an electronic voting protocol.
- Explored the implementation of Barreto-Naehrig curves with the Optimal-Ate pairing in Java and C implementations.

MIT Undergraduate Research Opportunity (UROP) - Computer-Aided Programming Group: Synthesizing a Synthesizer
Undergraduate Research with Armando Solar-Lezama September 2014 – May 2015

- Parsed output from a SMT-LIB v2 parser using Python to a Sketch Domain Specific Language directed acyclic graph (DAG) format.
- Implemented a testing suite to discover common operations in DAGs to transform into rewrite rules for SMT solvers.
- Presented work at EECScon 2015 and work became part of a larger NSF grant.

MIT UROP - Theory of Computation Group: Proof of Work Attribute Based Encryption
Undergraduate Research with Shafi Goldwasser June – August 2014

- Devised a protocol to combine Attribute Based Encryption (ABE) with proof of work (POW) schemes for a POW decryption mechanism.
- Collaborated with a graduate student; Explored lattice cryptographic schemes to implement them and develop a library.

Symantec Corporation (Twice), Waltham, MA
Mobility Software Solutions Intern June – August 2013, 2014

- Designed and developed internal use Android application for management and administration of Mobility Manager, formerly App Center.
- Developed a load testing script to mimic iOS devices using Apache JMeter for performance analysis of Mobility Manager.

Secunetics, Reston, VA
Associate Consultant January 2014

- Assisted in securing the U.S. Department of Interior's network from malicious external and internal activity.
- Developed a web dashboard to mimic security incident and event management (SIEM) capabilities by gathering logs and reports from intrusion detection and prevention systems using Meteor and Rickshaw for manual correlation.

LEADERSHIP

GraduatE ECE (GREECE) @ UT
Co-President and Co-Founder January 2018 – December 2019

- Founded GREECE to promote an ECE-wide community of graduate students through social, academic, and corporate events.
- Lead a board of 9 other students in achieving our mission through event organization and promotion, partnering with the ECE department, and partnering with corporate sponsors.

MAES (Latinos in Science and Engineering) Boston Professional Chapter
Vice President July 2016 – July 2017

- Coordinate and plan networking and outreach opportunities to Boston area Latino STEM Professionals.
- Support Boston area MAES Student Chapters by exposing them to professionals and providing chapter governance support.

MAES Student Chapter (http://mymaes.org)
National Student Representative, Vice President of Marketing for Local Chapter September 2013 – May 2015

- Represent all the East Coast MAES chapters on the National Board of Directors and help fulfill MAES's vision nationwide.
- Design MIT MAES's website and advertising material for campus wide events.
- Increased MIT MAES's alumni donations with targeted design changes to the website.

MITSec (MIT Security Club) (superseded by TechSec https://techsec.mit.edu)
President, Cofounder May 2013 – May 2015

- Partnered with a fellow classmate to bring together MIT's talent in applied and theoretical security.
- Organize meetings and lectures to teach the MIT populace about network and computer security.

MIT LUChA (La Unión Chicana por Aztlan) (http://lucha.mit.edu/)
President, Vice President, Webmaster, Social Chair, ECCSF Chair, Academic Chair December 2011 – May 2015

- Coordinated and planned ECCSF Conference at MIT for 150 participants from all over the East Coast.
- Designed new LUChA webpage using Twitter Bootstrap as a frontend.
- Organized, advertised for, and ran the logistics of campus wide events, such as our Independence Day BBQ and Day of the Dead Party.

TEACHING

The University of Texas at Austin CS 361s: Computer Security – Teaching Assistant
Support student learning and develop autograders for RISC-V exploitation and defense labs. Austin, TX. Spring 2024.

Ringer0 Reverse Engineering of Android Malware – Teaching Assistant
Support student learning and review course material for consistency. Virtual. February 2024.

The University of Texas at Austin I 320: Applied Cybersecurity Foundations – Guest Lecture
"Cryptography and Encryption" Austin, TX. January 2024.

The University of Texas at Austin I 320: Applied Cybersecurity Foundations – Guest Lecture
"Automatic Updates and Encryption" Austin, TX. September 2023.

The University of Texas at Austin EE 319K: Introduction to Embedded Systems – Teaching Assistant
Introduce students to programming embedded systems in C and Arm Assembly. Austin, TX. Spring 2019.

PRESENTATIONS

BSidesDFW 2023 – Presentation
"*The Most Dangerous Codec in the World: Finding and Exploiting Vulnerabilities in H.264 Decoders*" BSidesDFW.
Denton, TX. November 2023.

Demuxed 2023 – Presentation
"*Having H26Fun with H26Forge: Vulnerability Hunting, Datamoshing, and More!*" Demuxed.
San Francisco, CA. October 2023.

USENIX Security 2023 – Presentation
"*The Most Dangerous Codec in the World: Finding and Exploiting Vulnerabilities in H.264 Decoders*" USENIX Security.
Anaheim, CA. August 2023.

Black Hat USA 2023 – Presentation
"*The Most Dangerous Codec in the World: Finding and Exploiting Vulnerabilities in H.264 Decoders*" Black Hat USA.
Las Vegas, NV. August 2023.

REcon 2023 – Presentation
"*The Most Dangerous Codec in the World: Finding and Exploiting Vulnerabilities in H.264 Decoders*" REcon.
Montreal, Canada. June 2023.

WORKSHOPS/HACKATHONS

Atlantic Council Cyber 9/12 Strategy Challenge, Austin Regional, February 2023 – Semi-finalist
Competed in a team of three responding to a crisis on the US cobalt supply chain. Won best Decision Document.

MIT Policy Hackathon, October 2022 – Finalist – Presentation
The MIT Policy Hackathon aims to address relevant societal challenges via data and policy analysis. In a team of five, provided recommendations to The Omidyar Network and BeVigil on how to improve mobile app cybersecurity in the Global South.

MIT Policy Hackathon, October 2021 – Finalist – Presentation
In a team of four, analyzed government takedown requests to online service providers, provided by The Lumen Database, to construct policy that balances equities of affected communities.

Atlantic Council Cyber 9/12 Strategy Challenge, Geneva Regional, May 2021 – Semi-finalist
The Cyber 9/12 Strategy Challenge is an annual cyber policy and strategy competition where students from across the globe compete in developing policy recommendations tackling a fictional cyber catastrophe. Competed in a team of four responding to an EU-wide disruption of hospitals during a pandemic. Experience documented via the UT Strauss Center and The Manu<Script> Podcast.

Atlantic Council Cyber 9/12 Strategy Challenge, Washington D.C. National, March 2021 – Semi-finalist
Competed in a team of four responding to cyber-attacks on maritime infrastructure.

Atlantic Council Cyber 9/12 Strategy Challenge, Austin Regional, January 2021 – Semi-finalist
Competed in a team of four responding to ransomware attacks on US hospitals.

Atlantic Council Cyber 9/12 Strategy Challenge, New York City Regional, November 2019 – Semi-finalist
Competed in a team of three responding to an insider threat situation in government.

Atlantic Council Cyber 9/12 Strategy Challenge, Washington D.C. National, March 2019
Competed in a team of four responding to potential vulnerabilities in the 2020 census.

Atlantic Council Cyber 9/12 Strategy Challenge, Austin Regional, December 2018 – Semi-finalist
Competed in a team of four responding to denial-of-service attacks of Internet of Things (IoT) and critical infrastructure.
DeepSpec Summer School 2017
Deep dive into formal methods using the Coq Theorem Prover for high assurance systems and design formally verified software. Explored technologies such as CompCert, Vellvm, QuickChick, CertiKOS, and many more. Also participated in the Coq Intensive, reviewing Benjamin Pierce's Software Foundations textbook.
Technologies used: Coq Theorem Prover

LATISM El Hackathon 2015 – Consejera (1st Place)
Web platform for guiding parents who are not familiar with the US school system on how to best support their child, while providing security and privacy guarantees from used technology.
Technologies used: Mylar (Meteor.js), MongoDB, Bootstrap

Battelle Cyber Auto Challenge 2014 – Automobile CyberSecurity
First-hand experience exploring the security of automobiles, from attacks, defenses, and policies.
Technologies used: SocketCAN, VehicleSpy, Python

Facebook Summer of Code 2013 – Facemood
Semantic analysis of Facebook friend's statuses to determine if they are having a good day or a bad day.
Technologies used: PHP, Facebook API, Heroku, Semantic API

Hopper Storm and Finagle+ Hackathon 2013 – Storm Hackathon
Semantic analysis of tweets combined with geographic data to determine regional perception of topics.
Technologies used: Twitter Storm, Semantic API, Google Map API

HONORS AND ACHIEVEMENTS

Strauss Center Brumley Next Generation Fellow (2019, 2020, 2021) • Virginia & Ernest Cockrell, Jr. Fellowship in Engineering (2018, 2019, 2020) UT Austin Whaley Engineering Fellowship Scholar (2017) • BeVisible 2016 Most Inspiring Latinx Engineers • MIT Office of Multicultural Programming Excellence Through Adversity Award (2015) • MAES National Leadership Conference First Place Presentation (2013)