Hari Venugopalan

hariv | hari-venugopalan | hariv.github.io | hvenugopalan@ucdavis.edu | 5307608910

Research Interests

I specialize in security and privacy research with a focus on digital identities. My work involves conducting measurements, employing machine learning techniques, and building systems to discover and deploy innovative vectors for establishing digital identities, including hardware and biometrics.

Education

2020 - present	PhD (Computer Science) at **University of California, Davis**
2017 - 2020	MS (Computer Science) at **University of California, Davis**
2010-2014	B.Tech (Production Engineering) at **National Institute of Technology, Tiruchirappalli**

Publications

Aragorn: A Privacy-Enhancing System for Mobile Cameras
Hari Venugopalan, Zainul Abi Din, Trevor Carpenter, Jason Lowe-Power, Samuel T. King and Zubair Shafiq
UbiComp 2024 (Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies)

Doing good by fighting fraud: Ethical anti-fraud systems for mobile payments
Zainul Abi Din, *Hari Venugopalan*, Henry Lin, Adam Wushensky, Steven Liu and Samuel T. King
IEEE Symposium on Security and Privacy 2021

Boxer: Preventing fraud by scanning credit cards
Zainul Abi Din, *Hari Venugopalan*, Jaime Park, Andy Li, Weisu Yin, Haohui Mai, Yong Jae Lee, Steven Liu and Samuel T. King
Usenix Security 2020

Credit Card Fraud Is a Computer Security Problem
Samuel T. King, Patrick Traynor, Christian Peeters, Nolen Scaife, Zainul Abi Din and *Hari Venugopalan*
IEEE Security and Privacy Magazine 2021

Adaptability, Extensibility and Simplicity in the MetabolicOS
Hari Venugopalan, Shreyas Madhav Ambattur Vijayanand and Samuel T. King
BioSys Workshop 2024

FP-Rowhammer: Rowhammer-Based Device Fingerprinting
Hari Venugopalan, Kaustav Goswami, Zainul Abi Din, Jason Lowe- Power, Samuel T. King and Zubair Shafiq
(Under submission at ACM CCS 2024)

GlucOS: A secure, safe and extensible system for automated insulin delivery
Hari Venugopalan, Shreyas Madhav Ambattur Vijayanand and Samuel T. King
(Under submission at Usenix Security 2024)

MultiLock: biometric-based graded authentication for mobile devices
Shravan Aras, Chris Gniady and *Hari Venugopalan*
MOBIQUITOUS: Mobile and Ubiquitous Systems 2019

Open Source Software Computed Risk Framework
Jon Chapman and *Hari Venugopalan*
IEEE International Conference on Computer Science and Information Technologies 2022

Ongoing research

Are bots hiding in plain sight? Inconsistency-based bot detection
Hari Venugopalan, Shaoor Munir, Shuaib Ahmed, Tangbaihe Wang, Samuel T. King and Zubair Shafiq

Javelin: CGM-based authentication for individuals with disabilities
Hari Venugopalan, Shreyas Madhav Ambattur Vijayanand, Jonathan Levitsky, Zubair Shafiq and Samuel T. King

CPU-Print: Power Side-Channels for device fingerprinting
Hari Venugopalan, Kaustav Goswami, Kartik Patwari, Ryan Swift, Jason Lowe-Power, Chen-Nee Chuah and Zubair Shafiq

HammerSim: A System-Level Tool to Model RowHammer
Kaustav Goswami, Ayaz Akram, *Hari Venugopalan*, Zubair Shafiq and Jason Lowe-Power

Work Experience

Graduate Student Researcher, UC Davis, Davis CA Sep 2018 - Present

- Conducted ML and mobile systems research on combating card-not-present credit card fraud.
- Credit card research led to the establishment of a startup that was acquired by Stripe in 2021.
- Led research to design a privacy enhancing system for mobile cameras to protect user privacy.
- Led research to extract device fingerprints from the bit flips produced by the Rowhammer vulnerability.
- Led research to build systems that can safely support any ML-based algorithm in closed loop for automated insulin delivery.
- Currently leading research to study adversarial fingerprints that evade bot detection as well as the inconsistencies they introduce for improved bot detection.
- Currently leading research to extract fingerprints from continuous glucose monitors (CGMs) to build better authentication systems for individuals with disabilities.
- Currently leading research to exploit CPU frequency scaling as a power-side channel for fingerprinting.

ML Reseaerch Intern, Blue Hexagon Inc, Sunnyvale CA Jun 2019 - Sep 2019

- Identified functionality-preserving mutations to Windows Portable Executables (PE files).
- Developed Generative Adversarial Network (GAN) to mutate malicious PE files based on identified mutations to evade detection.

Research Collaborator, UofA, Remote Jan 2015-May 2017

- Collaborated on face recognition research for graded authentication in mobile apps.
- Ran experiments using Haar-Cascades and Local Binary Pattern Histograms for face recognition.

Member of Technical Staff, Oracle India Pvt. Ltd, Bengaluru, India Jun 2014-Jul 2017

- Developed analytics framework to periodically collect data on social network activity for Oracle Social Network (OSN).
- Implemented features for the web client of the same product.

Software Developer Intern, InterviewStreet Technologies, Bengaluru, India May 2012-Jul 2012

- Developed a real-time collaborative editor for interviews.

Awards

- Awarded GGCS summer fellowship by the department of Computer Science at UC Davis in 2022.
- Ranked within the top 200 in India at the regional ACM-ICPC contest in 2013.

Teaching

ECS 152A: Computer Networks Sep 2023-Dec 2023

TA for Dr. Zubair Shafiq
– Designed all programming assignments and programming projects for the course.
– Held weekly office hours to provide hands-on support to students.

ECS 152A: Computer Security Jan 2022-Mar 2022

Lead TA for Dr. Zubair Shafiq
– Designed all programming assignments for the course.
– Led weekly discussions and Held weekly office hours to provide hands-on support to students.

ECS 140: Programming Languages Apr 2018-Jun 2018

Lead TA for Dr. Kurt Eiselt
– Implemented rubric and graded all programming assignments.
– Led weekly discussions and Held weekly office hours to provide hands-on support to students.

ECS 265: Distributed Database Systems Jan 2018-Mar 2018

Lead TA for Dr. Mohammad Sadoghi
– Provisioned cloud instances on Azure for course projects.
– Logged weekly progress for all course projects.

ECS 40: Software Development and Object-Oriented Programming Sep 2017-Dec 2017

TA for Dr. Hao Chen
– Led weekly discussions and office hours to help students get comfortable with Rust.

Skills

Languages	Python, JavaScript, Java, C++, Swift
ML/Data Science Libraries	PyTorch, Tensorflow, Keras, XGBoost, Scikit-Learn, sktime, Pandas, NumPy, OpenCV, Matplotlib
Platforms	Web, Android, iOS
Automation Tools	Puppeteer, Selenium
Cloud Deployment	Heroku, Google Cloud, AWS
DBMS	MySQL, PostgreSQL, Oracle SQL
Hardware	DRAM, CPU Governors, Biometrics (e.g., CGM)
Other	Git, LaTeX, Wireshark, tcpdump

Leadership

- Certified Competent Communicator and Advanced Leader Bronze by Toastmasters International.
- President (Jun 2016-Dec 2016), Lexicon Toastmasters, corporate chapter of Toastmasters International at Oracle India Pvt. Ltd.
- Head (Jul 2013-May 2014), Google Developer Group, NIT Trichy.

Services

- Artifact Reviewer for PETS 2024
- PC member AISec Workshop 2023 (Co-located with ACM CSS 2023)
- PC member SecWeb Workshop 2023 (Co-located with IEEE S&P 2023)
- External reviewer for ACM Interactive Mobile Wearable Ubiquitous Technologies (IMWUT/Ubicomp) 2023
- External reviewer for IEEE Internet of Things Journal 2023

Talks

- Presented a talk titled "eXeGAN: Not all Malware is created Equal" to Blue Hexagon Inc in Sunnyvale, California in Sep 2019. The talk focused on my research using Generative Adversarial Networks (GANs) to automatically mutate malware such that they evade detection by static analysis while preserving their functionality.
- Presented a talk on my paper, "Aragorn: A Privacy-Enhancing System for Mobile Cameras" to the ProperData group in Jan 2022.
- Presented a talk on my paper, "FP-Rowhammer: Rowhammer-Based Device Fingerprinting" to the ProperData group in Feb 2024.
- Presented posters of my paper, "FP-Rowhammer: Rowhammer-Based Device Fingerprinting" at the Noyce Symposium 2022 and the ProperData Symposium 2023.

Media Coverage

- **Stripe acquires Bouncer, will integrate its card authentication into the Radar fraud detection tool**
  TechCrunch article by Ingrid Lunden
- **RAM-ramming Rowhammer is back – to uniquely fingerprint devices**
  The Register article by Thomas Claburn
- **Centauri: Practical Rowhammer Fingerprinting**
  YCombinator News post by Paul Houle
- **Innovative Device Fingerprinting Technique Developed by University of California Researchers**
  Bitdefender article by Vlad Constantinescu
- **Serious Security: Rowhammer returns to gaslight your computer**
  Naked Security article by Paul Ducklin

References

- **Dr. Sam King**
  Associate Professor,
  Department of Computer Science,
  University of California, Davis
  kingst@ucdavis.edu
  bob.cs.ucdavis.edu
- **Dr. Zubair Shafiq**

Associate Professor,
Department of Computer Science,
University of California, Davis
zshafiq@ucdavis.edu
web.cs.ucdavis.edu/∼zubair

- **Dr. Jason Lowe-Power**
  Associate Professor,
  Department of Computer Science,
  University of California, Davis
  jlowepower@ucdavis.edu
  cs.ucdavis.edu/directory/jason-lowe-power
- **Dr. Chen-Nee Chuah**
  Professor,
  Department of Electrical & Computer Engineering,
  University of California, Davis
  chuah@ucdavis.edu
  www.ece.ucdavis.edu/∼chuah/rubinet/people/chuah/bio.html
- **Dr. Yong Jae Lee**
  Associate Professor,
  Department of Computer Sciences,
  University of Wisconsin-Madison
  yongjaelee@cs.wisc.edu
  pages.cs.wisc.edu/∼yongjaelee/