

EVIN JAFF

Graduate Student in Computer Science & Biomedical Engineering

@ evin@wustl.edu

+1 425-785-1644

evinjaff.github.io

github.com/evinjaff

in bit.ly/evinjaff

EDUCATION

Washington University in St. Louis

PhD, Computer Science

Finished with Masters Degree

Aug. 2023 – Dec. 2024 St. Louis, MO

Washington University in St. Louis

Bachelors, Biomedical Engineering & Computer Science

Aug. 2019 – May 2023 St. Louis, MO

TECHNICAL SKILLS

- Programming Languages:** Python, Swift, MATLAB, C++, Java, C, JavaScript, TypeScript, PHP, C#
- Libraries & Tools:** Simulink, Jupyter, NumPy, Pandas, Scikit-learn, PyTorch Django, SwiftUI, OpenCV, Git, Docker
- Machine Learning:** Classifiers, Large Language Models, Adversarial Example, Penetration & Security
- Testing:** JUnit, XCodeUI, Django TestCase, .NET Unit Test

WORK EXPERIENCE

Graduate Researcher

Washington University Security and Privacy Lab

August 2023 – Present St. Louis, MO

Graduate researcher in Cyber-Physical System security, adversarial machine learning, and untrusted LLM app evaluation. Led multiple rapid prototyping efforts. Culminated in Masters' project on deepfake audio detection and prevention.

Software Engineering Intern - iOS

Zillow

May 2023 – August 2023 Seattle, WA

Intern for iOS app team at Zillow. Built "Learn More" feature for ShowingTime+ listings that explains the benefits of premium listings. Also utilized a new internal CDN to the app for low-frequency static images that reduced app size by 15 MB.

Software Engineering Intern - Bio-instrumentation

Garmin Ltd.

May 2022 - August 2022 Olathe, KS

Intern with Garmin Health. Worked on development of a machine learning model to monitor blood pressure optically. Developed clinical study, wrote firmware patches, and built models on received data with competitive accuracy.

PUBLICATIONS

- 2024 (ACM CCS Workshop) Chang, Li, Jaff, Chang, Wang, Zhang, Hsiao *AdapBox: Adaptive Sandboxing in Medical Systems with eBPF*
- 2024 (preprint), Jaff, Wu, Iqbal, Zhang: *Data Exposure from LLM Apps: An In-depth Investigation of OpenAI's GPTs*
- 2024 (preprint - accepted into second round at IEEE Symposium on Security and Privacy) Chang, Liu, Jaff, Lu, Zhang *SoK: Security and Privacy Risks in Medical AI*

PROJECTS

CardioConnect EKG Shirt

- For undergraduate capstone, designed and built working prototype of a wearable EKG shirt with dry electrodes that could take EKGs compliant with AHA standards. Wrote sampling software, and designed circuit that utilized a custom RP 2040 board with a shunt chip to accurately sample an EKG from the electrodes. Competed in the SlingHealth competition and won 3rd place at the Washington University BME Day competition. (link: bit.ly/ekgshirt).

Detection of Iatrogenic Ureteral Injury

- Led software/electronics for a SlingHealth venture team trying to detect injury during robotic ureteral surgery. Built a surgical stent embedded with thermistors to infer the proximity of a heated scalpel to the ureter. (link: bit.ly/ureteral-injury)

Connections Button

- Invented new use for an IoT button using AWS IoT and Twilio that relays a distress signal to a crisis hotline for students in need of rapid assistance. Partnered with local school to develop beta program. Interviewed by local news (link: bit.ly/k5evin). Featured in Skandalaris Creator's Gallery and Washington University in St. Louis' Engineering Magazine. (link: bit.ly/evinbutton)

HONORS & AWARDS

- Skandalaris Center Honors in Innovation and Entrepreneurship, (2023)
- Award of Excellence in Technical Writing with a Computer Science Focus, (2022)
- Olin Big IdeaBounce Finalist, (2020)
- Washington State Academic Honors, (2019)
- Eagle Scout with Gold Palm, (2017)