Kaushal Kafle

Room 101A, McGlothlin Street Hall, Williamsburg, VA-23187
kkafle@wm.edu | +1 (757) 472-8662 | https://www.kaushalkafle.com/

BIO

I am a PhD student in the Department of Computer Science at William & Mary, being advised by Dr. Adwait Nadkarni. I am the founding member and the lead graduate student at *Secure Platforms Lab (SPL)*, where I currently lead 5 other graduate and 2 undergraduate students. My research analyzes the security and/or privacy of emergent, evolving systems and their implications on the end users. My work on analyzing the security of smart home platforms received the *best paper award* at CODASPY'19, and has been featured in various news outlets. My work on understanding the privacy postures of election campaign websites received the *best poster award* at CCI Symposium'23.

EDUCATION

William & Mary, Williamsburg, USA **August 2017 - Present**
PhD in Computer Science
Advisor: Dr. Adwait Nadkarni

Pulchowk Campus, Tribhuvan University **Nov 2011 - Nov 2015**
BE in Computer Engineering

PUBLICATIONS

Conference Papers

[1] **Kaushal Kafle**, Prianka Mandal, Kapil Singh, Benjamin Andow, and Adwait Nadkarni, "Understanding the Privacy Practices of Political Campaigns: A Perspective from the 2020 US Election Websites", In *IEEE Symposium on Security and Privacy (IEEE S&P)*, Oakland, CA, USA, 2024. *To appear*

[2] Xin Jin*, Sunil Manandhar*, **Kaushal Kafle**, Zhiqiang Lin, and Adwait Nadkarni. "Understanding IoT Security from a Market-Scale Perspective". In *Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS)*, Los Angeles, CA, USA, November 2022. *Co-first Authors. [PDF]

[3] Sunil Manandhar, **Kaushal Kafle**, Benjamin Andow, Kapil Singh, and Adwait Nadkarni, "Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage". In *Proceedings of the 31st USENIX Security Symposium (USENIX)*, Boston, MA, USA, 2022. [PDF]

[4] Amit Seal Ami, Nathan Cooper, **Kaushal Kafle**, Kevin Moran, Denys Poshyvanyk, and Adwait Nadkarni, "Why Crypto-detectors Fail: A Systematic Evaluation of Cryptographic Misuse Detection Techniques," in *IEEE Symposium on Security and Privacy (IEEE S&P)*, 2022. [PDF]

[5] Sunil Manandhar, Kevin Moran, **Kaushal Kafle**, Ruhao Tang, Denys Poshyvanyk, and Adwait Nadkarni. "Towards a Natural Perspective of Smart Homes for Practical Security and Safety Analyses." In *Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P*), San Francisco, CA, USA, May 2020. [PDF]

[6] **Kaushal Kafle**, Kevin Moran, Sunil Manandhar, Adwait Nadkarni, and Denys Poshyvanyk. "A Study of Data Store-based Home Automation." In *Proceedings of the 9th ACM Conference on Data and Application Security and Privacy (CODASPY)*. Dallas, TX, USA, March 2019. ***Best Paper Award*** 🏆 [PDF] [press coverage]

[7] Richard Bonett, **Kaushal Kafle**, Kevin Moran, Adwait Nadkarni, and Denys Poshyvanyk. "Discovering Flaws in Security-Focused Static Analysis Tools for Android using Systematic Mutation." In *Proceedings of the 27th USENIX Security Symposium. Baltimore*, MD, USA, August 2018. [Source code] [PDF]

Journal Papers

[8] Amit Seal Ami, **Kaushal Kafle**, Kevin Moran, Adwait Nadkarni, and Denys Poshyvanyk. "Systematic Mutation-based Evaluation of the Soundness of Security-focused Android Static Analysis Techniques". In *ACM Transactions on Security & Privacy (TOPS),* 2021. [Link]

[9] **Kaushal Kafle**, Kevin Moran, Sunil Manandhar, Adwait Nadkarni, and Denys Poshyvanyk. "Security in Centralized Data Store-based Home Automation Platforms- A Systematic Analysis of Nest and Hue." In *ACM Transactions on Cyber-Physical Systems (TCPS)*, 2020. [Link]

Tool Demo Papers

[10] Prianka Mandal, Sunil Manandhar, **Kaushal Kafle**, Kevin Moran, Denys Poshyvanyk, and Adwait Nadkarni. "*Helion: Enabling Natural Testing of Smart Homes".* In *Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE), Demonstration Track*, December 2023, *To appear.*

[11] Amit Seal Ami, Syed Yusuf Ahmed, Radowan Mahmud Redoy, Nathan Cooper, **Kaushal Kafle**, Kevin Moran, Denys Poshyvanyk, and Adwait Nadkarni. "MASC: A Tool for Mutation-based Evaluation of Static Crypto-API Misuse Detectors". In *Proceedings of the ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE'23), Demonstration Track*, December 2023. *To appear.*

[12] Amit Seal Ami, **Kaushal Kafle**, Kevin Moran, Adwait Nadkarni, and Denys Poshyvanyk. "Demo: Mutation-based Evaluation of Security-focused Static Analysis Tools for Android." In *Proceedings of the 43rd IEEE/ACM International Conference on Software Engineering (ICSE'21), Formal Tool Demonstration,* May 2021, [Link]

Posters

[13] "Security and Privacy in the Smart Home Ecosystem", at the *Annual Virginia Academy of Science, Engineering and Medicine (VASEM) Summit*, Richmond, VA – October 2023

[14] "Expanding Computer Science Learning Opportunities in K-12 Instruction in Virginia Schools", at the *Annual Virginia Academy of Science, Engineering and Medicine (VASEM) Summit*, Richmond, VA – October 2023

[15] "Understanding the Privacy Practices of Political Campaigns", at the *CCI Symposium 2023*, Richmond, VA – April 2023 – ***Best Poster Award*** 🏆

[16] "Smart Home Privacy Demystified", at the *CCI Symposium 2022*, Richmond, VA – April 2022

[17] "A Study of Data Store-based Home Automation", at the *ACM CODASPY 2019***,** Dallas, TX – March 2019

RESEARCH EXPERIENCE

Graduate Research Assistant — *Jan 2018 – Present*

Secure Platforms Lab (SPL)
Department of Computer Science, William & Mary

Research Overview: As a research assistant to Prof. Adwait Nadkarni at SPL, I have worked primarily in the analysis of security and/or privacy of emergent, evolving systems such as IoT systems, election campaigning platforms and security analysis tools.

Projects and Artifacts:

- **Polityzer,** IEEE S&P'24: Designed and developed a framework that assists in analyzing the privacy posture of election campaign websites. Used the framework to analyze the privacy of 2060 election campaign websites in the 2020 US election, leading to various findings that demonstrate various privacy gaps in data collection and sharing among campaigns.
  Source Code: https://github.com/polityzer

- **Security of Centralized Home Automation,** *Best Paper***,** ACM CODASPY'19: Led the research to analyze the architecture and design of various smart home platforms that facilitate automation through a centralized data store. Demonstrated the first Lateral Privilege Escalation in a smart home platform by escalating privilege from a smart switch to compromise a security camera. The project was featured in newspapers, podcasts and TV. Journal Extension published in ACM TCPS'20.
  Press Coverage: https://kaushalkafle.com/publications#press

- **IoTSpotter,** ACM CCS'22: Developed a framework to automatically identify mobile apps as IoT apps using their metadata, and used the framework to perform a large scale security analysis of mobile-IoT apps. Through this analysis, we discover cryptographic violations and the use of vulnerable IoT libraries in mobile-IoT apps potentially impacting security-critical IoT devices.
  Source Code: https://github.com/Secure-Platforms-Lab-W-M/IoTSpotter

- **Smart Home Privacy Policies Demystified**, USENIX'22: Performed a systematic and data-driven analysis of the current state of smart home privacy policies. We generated insights into how hard it is for consumers to find the relevant privacy policy of a smart home product, and when found, how precisely and comprehensively they describe the collection and sharing of sensitive user data collected through these devices.
  Data: https://github.com/Secure-Platforms-Lab-W-M/smart-home-privacy-policies

- **Helion**, IEEE S&P'20: Developed the Helion framework that generates natural home automation scenarios given a set of home events. Helion utilizes a novel concept that smart home event sequences exhibit inherent semantic patterns which can be modeled to generate valid event sequences that are likely to occur in the home next. We leverage Helion to generate security policies for the smart home.
  Source Code: https://github.com/Secure-Platforms-Lab-W-M/Helion-on-Home-Assistant#helion

- **HomeEndorser,** *under submission:* Led the design and development a security framework for smart home platforms to protect the integrity of Abstract Home Objects (AHOs) that enable automation across various third-party integrations in the home. HomeEndorser uses observations from local devices to perform a policy check before proposed changes to AHOs from third-party integrations are endorsed.

- **Mutation-based Soundness Evaluation (MUSE),** USENIX'18: Designed the MUSE framework to analyze the soundness claims of Android static analysis tools by adapting the concepts of mutation testing to the security domain. Discovered undisclosed flaws in multiple prominent Android static analysis tools. Journal Extension published at ACM TOPS'21.
  Source Code: https://secure-platforms-lab-w-m.github.io/muse/

- **Mutation Analysis for evaluating Static Crypto-API misuse detectors (MASC),** IEEE S&P'22: Designed the MASC framework to perform a systematic evaluation of crypto-API misuse detection tools by leveraging mutation testing. We also develop a data-driven taxonomy of existing crypto-API misuse cases which are converted into mutation operators to be leveraged by MASC during the analysis of crypto-detectors.
  Source Code: https://github.com/Secure-Platforms-Lab-W-M/masc-artifact

Lead Graduate Student *June 2022 – Present*
Secure Platforms Lab (SPL)
Department of Computer Science, William & Mary
Responsibilities:
- Provided individual research mentorship and support to other graduate/undergraduate students
- Helped in fostering a good working environment among lab students
- Organized and led student-run weekly meetings
- Led the daily operational activities of the lab

INDUSTRY EXPERIENCE

Virginia Department of Education, Richmond, VA *May 2023 – Aug 2023*

Commonwealth of Virginia Engineering and Science (COVES) Policy Fellow
Mentor: Keisha Tennessee, Virginia Computer Science Coordinator
Responsibilities:

- Support the strategic planning in VA to expand capacity, access, and participation in K-12 Computer Science Education
- Dataset collection, analysis and providing data-based recommendations

Mojo Vision, Tectus Corp., Saratoga, CA *Sep 2022 – Nov 2022*
Graduate Research Intern
Mentor: Dr. Michael Grace
Responsibilities:

- Investigate the security and privacy implications of AR Contact Lens
- Design a new security framework for AR Contact Lens

IBM Research, Yorktown Heights, NY *May 2022 – Aug 2022*
Graduate Research Intern
Mentor: Dr. Kapil Singh
Responsibilities:

- Investigate the feasibility of mapping specific privacy and data policies to the software code behavior

TEACHING EXPERIENCE

Guest Lecturer, William & Mary

- Guest Lecture on "*Practical Integrity in the Smart Home",* in Concepts of Computer Security – CSCI 667 (Graduate-level course) – Spring 2022
- Guest Lecture on "*Ramifications of SSL Issues in Mobile Apps for the Smart Home",* in Mobile Application Security – CSCI 445 (Undergraduate-level course) – Fall 2021
- Guest Lecture on "*Securing a Smart Home*", in IoT Security and Safety – CSCI 680 (Graduate-level course) – Spring 2021

Teaching Assistant, William & Mary *Aug 2017 – May 2019*

- Taught labs and graded assignments in *Computational Problem Solving* – CSCI 141 (133 Students)
- Taught labs and graded assignments in *Programming for Data Science* – CSCI 140 (93 Students)
- Graded assignments in *Mobile App Security* – CSCI 520 – Spring 2018 (20 Students), Fall 2018 (12 Students)

CONFERENCE PRESENTATIONS, INVITED TALKS AND OUTREACH

Conference Presentations

- **"***A Study of Data-store Based Home Automation*" at the **9th ACM CODASPY**, Dallas, TX – March 2019
- "*A Study of Data-store Based Home Automation*" at the **18th Graduate Research** Symposium, William & Mary, Williamsburg – March 2019
- "*Discovering Flaws in Security-Focused Static Analysis Tools for Android using Systematic Mutation*" at the **27th USENIX Security Symposium**, Baltimore – August 2018

Invited Talks and Outreach

- *Leadership in Science Policy Institute (LiSPI)* workshop, invited as a volunteer by **Computing Research Association (CRA)**, Washington DC – November 2023
- "*Understanding the Security of Smart Home Platforms*", as part of the **Emerging Scholar Series**, Public Scholarship Initiative, Williamsburg Regional Library – March 2022
- *"How hackable is your home?",* invited as an expert on smart home security in ***Which? Investigates*** **podcast** (Episode Link) – October 2021
- "*The Security of Smart Home Platforms*", Research talk at the **Journal Club**, William & Mary, Williamsburg – September 2019

- *William & Mary Developer Outreach on "Enabling Safe and Secure Home Automation: Problems, Best Practices and Future Opportunities"*, Williamsburg Developers Group, Williamsburg, VA, July 2019
- *Outreach to High School Students*, invited by **Advanced Technology Center**, Virginia Beach, VA – April 2019
- "*Hacking Your Smart Home*" podcast, invited to discuss my work on smart home security by **News Radio WINA** – December 2018

AWARDS & HONORS

- ***COVES Fellow*****,** VASEM, 2023
- ***Best Poster Award*****,** CCI Symposium 2023, Richmond, VA, USA – April 2023
- ***Best Paper Award***, ACM CODASPY, Dallas, TX, USA - March 2019
- ***GSAB Research Grant*****,** William & Mary - Fall 2021
- ***International Student Opportunity Award*****,** William & Mary - Spring 2020, Spring 2021
- ***USENIX Security Symposium Travel Award*** - 2018

PROFESSIONAL SERVICE

- **Conference Program Committee Member**
  - *USENIX Security Symposium (USENIX)* Artifact Evaluation Committee - 2021, 2022, 2023
  - *Annual Computer Security Applications Conference (ACSAC)* Artifact Evaluation Committee - 2023
- **Conference External Reviewer**
  - *NDSS* - 2020, 2021, 2022, 2023
  - *ACSAC* – 2022, 2023
  - *USENIX* - 2019, 2021
  - *International Conference on Information Systems Security (ICISS)* – 2019, 2022, 2023
  - *Applied Cryptography and Network Security (ACNS)* – 2022, 2023, 2024

OTHER ACTIVITIES

- *Volunteer,* Leadership in Science Policy Institute (LiSPI) workshop, organized by Computing Research Association (CRA), Washington DC, 2023
- *Founding member*, Secure Platforms Lab at William & Mary (Lab website)
- *Volunteer*, IOE Graduate Conference, Pulchowk, Lalitpur, Nepal 2015
- *Volunteer*, Latex Workshop to Graduate Students, Pulchowk, Lalitpur, Nepal 2015
- *Organizer*, Hackathon, Locus 2015
- *Organizer*, Yomari Codecamp, Locus 2015