Kaushal Kafle

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

BIO

I am a PhD student in the Department of Computer Science at William & Mary with an expected graduation in Spring 2024. My advisor is Prof. Adwait Nadkarni. I am 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
Expected graduation: March, 2024

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 *Proceedings of the 45th IEEE Symposium on Security and Privacy (IEEE S&P)*, CA, USA, 2024. *To appear* [PDF]

[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, Nov 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 *Proceedings of the 43rd 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, Aug 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. [[PDF]](#)

[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. [[PDF]](#)

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*, Dec 2023. [[PDF]](#)

[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), Demonstration Track*, Dec 2023. [[PDF]](#)

[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, [[PDF]](#)

Posters

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

[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 – Oct 2023 [[PDF]](#)

[15]   "Understanding the Privacy Practices of Political Campaigns"*, at the *CCI Symposium'23*, Richmond, VA – April 2023 – ***Best Poster Award*** 🏆 [[PDF]](#)

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

[17]   "A Study of Data Store-based Home Automation"*, at *ACM CODASPY'19* **,** Dallas, TX – March 2019 [[PDF]](#)

CONTRIBUTION IN AWARDED GRANT

[1]   [NSF Grant CNS – 2132281](#)
   a.   Title*: "Enabling Data-Driven Security and Safety Analyses for Cyber-Physical Systems"*
   b.   PI: Adwait Nadkarni, Kevin Moran, Co-Pi: Denys Poshyvanyk, **Contributor: Kaushal Kafle**
   c.   Award amount: *$799,839*

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:
1. **Polityzer,** IEEE S&P'24 - Source Code: https://github.com/polityzer
2. **Security of Centralized Home Automation,** *Best Paper*, ACM CODASPY'19 - Press Coverage: https://kaushalkafle.com/publications#press
3. **IoTSpotter,** ACM CCS'22 - Source Code: https://github.com/Secure-Platforms-Lab-W-M/IoTSpotter
4. **Smart Home Privacy Policies Demystified**, USENIX'22 - Data: https://github.com/Secure-Platforms-Lab-W-M/smart-home-privacy-policies
5. **Helion**, IEEE S&P'20 - Source Code: https://github.com/Secure-Platforms-Lab-W-M/Helion-on-Home-Assistant#helion
6. **HomeEndorser,** *under submission:* A security framework for securing automations in smart home platforms.
7. **Mutation-based Soundness Evaluation (MUSE),** USENIX'18 - Source Code: https://secure-platforms-lab-w-m.github.io/muse/
8. **Mutation Analysis for evaluating Static Crypto-API misuse detectors (MASC),** IEEE S&P'22 - 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
1. Guest Lecture on "*Practical Integrity in the Smart Home*", in Concepts of Computer Security – CSCI 667 (Graduate-level course) – Spring 2022

2. 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 – Online (over zoom)
3. Guest Lecture on "*Securing a Smart Home*", in IoT Security and Safety – CSCI 680 (Graduate-level course) – Spring 2021 – Online (over zoom)

Teaching Assistant, William & Mary   Aug 2017 – May 2019
4. Taught labs and graded assignments in *Computational Problem Solving* – CSCI 141 (133 Students)
5. Taught labs and graded assignments in *Programming for Data Science* – CSCI 140 (93 Students)
6. Graded assignments in *Mobile App Security* – CSCI 520 – Spring 2018 (20 Students), Fall 2018 (12 Students)

CONFERENCE PRESENTATIONS, INVITED TALKS AND OUTREACH

Conference Presentations
1. "*A Study of Data-store Based Home Automation*" at the **9th ACM CODASPY**, Dallas, TX – March 2019
2. "*A Study of Data-store Based Home Automation*" at the **18th Graduate Research** Symposium, William & Mary, Williamsburg – March 2019
3. "*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
4. *"Guest Post: A PhD Student's Experience at the LiSPI Workshop"*, **Leadership in Science Policy Institute (LiSPI) workshop**, invited by *Computing Research Association (CRA)*, Washington DC – Nov 2023 [Link]
5. "*Understanding the Security of Smart Home Platforms*", as part of the **Emerging Scholar Series**, Public Scholarship Initiative, Williamsburg Regional Library – March 2022
6. *"How hackable is your home?"*, invited as an expert on smart home security in ***Which? Investigates*** **podcast** (Episode Link) – October 2021
7. "*The Security of Smart Home Platforms*", Research talk at the **Journal Club**, William & Mary, Williamsburg – September 2019
8. *"Enabling Safe and Secure Home Automation: Problems, Best Practices and Future Opportunities"*, William & Mary Developer Outreach to Williamsburg Developers Group, Williamsburg, VA, July 2019
9. *Outreach to High School Students*, invited by **Advanced Technology Center**, V. Beach, VA – April 2019
10. "*Hacking Your Smart Home*" podcast, invited to discuss my work on smart home security by **News Radio WINA** – December 2018

AWARDS & HONORS
1. ***Commonwealth of Virginia Engineering & Science (COVES) Policy Fellow,*** Selected by *Virginia Academy of Science, Engineering and Medicine (VASEM)*, Host office - *Virginia Department of Education*, 2023
2. ***Best Poster Award,*** CCI Symposium 2023, Richmond, VA, USA – April 2023
3. ***Best Paper Award***, ACM CODASPY, Dallas, TX, USA - March 2019
4. ***Graduate Studies Advisory Board (GSAB) Research Grant,*** William & Mary - Fall 2021
5. ***International Student Opportunity Award,*** William & Mary - Spring 2020, Spring 2021
6. ***Travel Award*** - USENIX Security Symposium 2018, Computing Research Association (CRA) 2023

PROFESSIONAL SERVICE
1. **Conference Program Committee Member**
   a. *USENIX Security Symposium (USENIX)* Artifact Evaluation Committee - 2021, 2022, 2023
   b. *Annual Computer Security Applications Conference (ACSAC)* Artifact Evaluation Committee - 2023
2. **Conference External Reviewer**
   a. *Top-tier conferences* - NDSS (2020, 2021, 2022, 2023), USENIX (2019, 2021)
   b. *Other conferences* - ACSAC (2022, 2023), ICISS (2019, 2022, 2023), ACNS (2022, 2023, 2024)