

Kaushal Kafle

Room 331, McGlothlin Street Hall, Williamsburg, VA-23187
kkafle@cs.wm.edu | +1 (757) 472-8662 | www.kaushalkafle.com

I am a PhD student in the Department of Computer Science at the College of William and Mary, being advised by [Dr. Adwait Nadkarni](#). My research interests lie in analyzing the security practices of modern operating systems as well as designing practical security frameworks for such systems. I work at the [Secure Platforms Lab \(SPL\)](#) at William & Mary. My work on the security analysis of smart home platforms has been featured in [multiple news outlets](#)!

EDUCATION

College of William and Mary	PhD in Computer Science	August 2017 - Present
------------------------------------	--------------------------------	------------------------------

Advisor: Dr. Adwait Nadkarni

Relevant Courses:

Computer and Network Security, Cybersecurity Research Analysis, Systems Security, Advanced Software Engineering, Practice of Machine Learning, Analysis of Algorithms

Pulchowk Campus, Tribhuvan University	Bachelor's in Computer Engineering	Nov 2011- Nov 2015
--	---	---------------------------

PUBLICATIONS

Journal Papers-----

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. [\[Link\]](#)

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. [\[Link\]](#)

Conference Papers-----

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** [\[PDF\]](#) [\[press coverage\]](#) 🏆

Kaushal Kafle, Kirti Jagtap, Mansoor Ahmed-Rengers, Trent Jaeger and Adwait Nadkarni, "Towards Practical Integrity in the Smart Home with HomeEndorser", *currently in submission*, [\[arXiv link\]](#)

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. [\[Source code\]](#) [\[PDF\]](#)

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, [\[Link\]](#)

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. [\[PDF\]](#)

Amit Seal Ami, Nathan Cooper, **Kaushal Kaffle**, 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. [\[Link\]](#)

WORK EXPERIENCE

Research Assistant, Department of Computer Science, William & Mary

Jan 2018 – Present

Highlights:

Over the course of my research at [SPL](#), I have

- Published at several conferences and journals
- Research paper featured in multiple [news media outlets](#)
- Analyzed and discovered flaws in different smart home systems and apps (e.g. Google Nest, Philips, Hue, Kasa)
- Analyzed and discovered flaws in security tools (e.g. Flowdroid, Amandroid)
- Designed and built various security frameworks to systematically identify and protect against the flaws

Ongoing Research Projects

- **Towards integrity of shared platform resources (Project Lead)**
 - A supplementary security framework for smarhome platforms to protect the integrity of their shared resources such as states shared with 3rd party apps
 - Techniques involved: *reference monitor, integrity checks of smart home objects, automated data scraping, implementation and deployment in a real-world open-source smart home platform*
 - *Under submission*
- **Understanding Privacy in Politics (Project Lead)**
 - *Under submission*

Completed Research Projects:

- **Security of Data-Store Based Home Automation (Project Lead):**
 - Analyzed security of various components of smart home platforms that facilitate automation through *reverse-engineering* or *static analysis*
 - Analyzed components included the *Cloud backend, smart-apps review process, SSL enforcement in third-party smart-apps* of the platforms.
 - Won the **Best Paper Award** in *ACM CODASPY '19*
 - A journal extension was accepted to *ACM TCPS'20*.
 - [Press coverage](#)
- **MUSE (MUtation-based Soundness Evaluation):**
 - Framework for analyzing *soundness claims* of Android static analysis tools leveraging concepts from mutation testing
 - Discovered undisclosed flaws in multiple prominent Android static analysis security tools
 - *USENIX '18*
 - A journal extension was accepted to *ACM TOPS'21*.
- **MASC (MUtation-based Analysis of Static Crypto-misuse detection techniques):**
 - Framework for analyzing the soundness claims of static crypto-misuse detection tools leveraging concepts from mutation testing
 - Designed and created a taxonomy of crypto-flaws commonly found in the wild
 - *To appear at IEEE S&P '22*
- **Helion (Home automation security EvaLUatION):**
 - Conducted a user study to collect and understand smart home routines from real users
 - Designed the gathered data from user-study to be used for automated natural language processing
 - Created safety and security policies by analyzing automation sequences generated from a user's automation preferences
 - *IEEE S&P '20*

Teaching Assistant, Department of Computer Science, William & Mary

Aug 2017 – May 2019

Taught labs and graded assignments for the following classes:

- Computational Problem Solving (CSCI 141), Fall 2017 – 133 Students
- Programming for Data Science (CSCI 140), Spring 2019 – 93 Students

Graded assignments for the following classes:

- Mobile App Security (CSCI 520), Spring 2018 – 20 Students
- Mobile App Security (CSCI 520), Fall 2018 – 12 Students

CONFERENCE PRESENTATIONS & INVITED TALKS

- **Guest Lecture in Mobile Application Security (CSCI 445)** Oct 7th, 2021
 - Ramifications of SSL issues in mobile apps for the smart home
 - William & Mary, Williamsburg, VA
- **Guest Lecture in IoT Security and Safety (CSCI 680)** Feb 7th, 2021
 - “Securing a Smart home”
 - William & Mary, Williamsburg, VA
- **Journal Club** - William & Mary, Williamsburg, VA Sep 26th, 2019
 - “The Security of Smart Home Platforms”
- **9th ACM CODASPY** – Dallas, TX Mar 25th, 2019
 - “A Study of Data-store Based Home Automation”
- **18th Graduate Research Symposium** – William & Mary, Williamsburg, VA Mar 15th, 2019
 - “A Study of Data-store Based Home Automation”
- **USENIX’18** – Baltimore, MD Aug 17th, 2018
 - “Discovering Flaws in Security-Focused Static Analysis Tools for Android using Systematic Mutation”

AWARDS & HONORS

- **GSAB Research Grant**, William & Mary - Fall 2021
- **International Student Opportunity Award**, William & Mary - Spring 2020, Spring 2021
- **Best Paper Award**, ACM CODASPY, Dallas, TX, USA - March 2019
- **USENIX Security Symposium Travel Award** - 2018

PROFESSIONAL SERVICE

- **Reviewer for Conferences**
 - USENIX Artifact Evaluation Committee 2021, 2022
- **Sub-reviewer for Conferences**
 - NDSS - 2020, 2021, 2022
 - Annual Computer Security Applications Conference (ACSAC) - 2022
 - USENIX Security Symposium (USENIX) - 2019, 2021
 - The International Conference on Information Systems Security (ICISS) - 2019

OTHER ACTIVITIES

- Invited to participate in *Which? Investigates* podcast on smart home security ([Link](#)), Oct 2021
- My work featured in various news outlets ([Links here](#))
- One of the founding members of Secure Platforms Lab at William & Mary ([Lab website](#))
- Volunteer, IOE Graduate Conference, Pulchowk, Lalitpur, Nepal 2015
- Volunteer, Latex Workshop at IOE Graduate Conference, Pulchowk, Lalitpur, Nepal 2015
- Organizer, Hackathon, Locus 2015
- Organizer, Yomari Codecamp, Locus 2015

REFERENCES

- *Dr. Adwait Nadkarni (PhD Advisor)*
Assistant Professor, Department of Computer Science
College of William and Mary, VA, USA
Contact: apnadkarni@wm.edu
- *Dr. Trent Jaeger*
Professor, Department of Computer Science
Pennsylvania State University, PA, USA
Contact: trj1@psu.edu
- *Dr. Denys Poshyvanyk*
Professor, Department of Computer Science
College of William and Mary, VA, USA
Contact: denys@cs.wm.edu
- *Dr. Kevin Moran*
Assistant Professor, Department of Computer Science
George Mason University, VA, USA
Contact: kpmoran@gmu.edu