Department of Computer Science

Investigating the Latent Security and Privacy Risks in Consumer Software Systems

Kaushal Kafle
William & Mary

Hosted by Martin Kellogg

Date: Monday, March 4, 2024
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
Webex link: https://njit.webex.com/njit/j.php?MTID=m0f06106611883d6fb150712cd8c3ec72

Abstract:
Consumer-oriented software can encompass a diverse range of systems and functionalities; from Internet-of-things (IoT) platforms which interact with the user's physical environment, to online election campaigns which collect and process their political data. Despite the impact on the safety and privacy of consumers, the evolving and disjointed nature make it challenging to analyze the ways in which security and privacy threats manifest in such systems and how stakeholders convey these threats to the consumers. In this talk, I will discuss my work characterizing the security and privacy risks in two domains: IoT platforms, and Election campaign websites. In the first half, I will discuss the security vulnerabilities present in the IoT domain through a systematic study of popular consumer smart home platforms (e.g., Google Nest) and their components (e.g., apps, routines), leading to a novel privilege escalation attack and defense. In the second half, I will discuss an evaluation of the privacy posture of election campaigns through a large-scale analysis of campaign websites from the 2020 US federal elections. In particular, I will discuss the privacy implications of the extensive data collection, privacy disclosure issues and the security risk assessment of the websites in the non-profit context. Finally, I will conclude by providing some insights into how privacy regulations (or lack thereof) have impacted the two domains and discuss my ongoing (and future) research on the mapping of policy requirements to software behavior.

Bio:
Kaushal Kafle is a PhD Candidate in the Department of Computer Science at William & Mary, being advised by Prof. Adwait Nadkarni. He is the Lead Graduate Student of Secure Platforms Lab at William & Mary. His research interest is in the area of security and privacy, with the primary focus on identifying and preventing risks in consumer-oriented software. His work has been featured in various news outlets and has been published in multiple top security venues such as IEEE S&P, USENIX and ACM CCS. He has won the 'Best Paper Award' at ACM CODASPY'19 and the 'Best Poster Award' at Commonwealth Cyber Initiative (CCI) - 2023. He is a Commonwealth of Virginia Engineering and Science (COVES) Policy fellow of 2023.