NJIT

Department of Computer Science

New Frontiers in Authentication and Side-Channels in Emerging Platforms: 2FA Attacks, Sensor Exploits, and AR/VR Security

Ahmed Tanvir Mahdad
Texas A&M University

Hosted by: Reza Curtmola

Date: Wednesday, December 11, 2024
Coffee: **2:15** PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)

Zoom Link: **https://njit-edu.zoom.us/j/95380544563?pwd=EBkJSN5K9ML6fMl7ELovb0hXZa02W5.1**

Abstract:
Emerging mobile platforms, such as modern smartphones and AR/VR devices, bring new challenges in user verification, data protection, and user privacy. In terms of user verification and data protection, it is important to analyze modern authentication systems that use emerging platforms (e.g., smartphones) and state-of-the-art protocols (e.g., FIDO2) to implement Two-Factor Authentication (2FA) systems. To address this, we developed a novel attack framework and evaluated these authentication systems, uncovering vulnerabilities in all of them. Moreover, to explore user privacy risks on these emerging platforms, we analyzed side-channel vulnerabilities exploiting built-in zero-permission motion sensors of smartphones and AR/VR devices, revealing potential severe privacy leaks. Additionally, we leverage this side-channel information to develop potential defenses against known threats, such as unwanted robocalls and better AR/VR authentication systems.

My presentation focuses on two key areas of my research. First, I will present our designed attack framework that uncovers practical vulnerabilities in 2FA systems, revealing how attackers can bypass FIDO2 key-based and push notification authentication mechanisms without compromising the possession-factor device. Next, I will discuss side-channel privacy risks associated with zero-permission motion sensor data in smartphones and AR/VR devices, highlighting how sensitive information (e.g., user's gender, identity, emotion, and biological info such as vital signs and blood pressure) can be extracted. Finally, I will outline future research directions aimed at strengthening authentication security and safeguarding privacy in various emerging platforms.

Bio:
Ahmed Tanvir Mahdad is a final-year Ph.D. student in the Computer Science and Engineering Department at Texas A&M University. He is currently conducting research under the supervision of Dr. Nitesh Saxena at the SPIES Lab. His research focuses on exploring and mitigating security and privacy issues in modern authentication systems and smart devices (e.g., smartphones, and AR/VR devices). Many of his works have been published in top-tier security and systems conferences and journals, including ACM CCS, IEEE S&P, ACM Mobicom, IEEE ICDCS, and ACM TOPS. Additionally, his research has been featured in various news media worldwide.