NJIT

Department of Computer Science

Security Vulnerabilities and Defenses in Emerging Mobile Applications (AR/VR and Voice Assistant Systems)

Cong Shi
Rutgers University, NJ

Hosted by Jing Li

Date: Wednesday, February 9, 2022
Time: 11:00 AM - 12:00 PM
Location: https://njit.webex.com/njit/j.php?MTID=mb7229a38631700a09550d0db330f154a

https://cs.njit.edu/seminars

Abstract: With the advancement of mobile technologies, mobile devices play an important role in enabling many emerging applications, such as augmented reality (AR)/virtual reality (VR), voice assistant systems, human-computer interactions (HCI), through combining various sensing and machine learning techniques. My research explores the security vulnerabilities in the sensing interfaces and built-in machine learning models, with the hope of addressing these inherited security issues and bringing trustworthiness to end users. My research work also explores emerging sensing modalities (e.g., acoustic, vibration, visible lights, and WiFi) to enable convenient and secure interactions with mobile systems, by developing authentication schemes and defense techniques against various attacks. The first part of my talk reveals important privacy leakage against voice interfaces on face-mounted AR/VR devices. As AR/VR headsets are closely mounted on the user's face, the headset can be impacted by the underlying facial dynamics as the wearer speaks, which encodes private biometrics and speech. By leveraging the facial dynamics captured by zero-permission built-in motion sensors, a malicious actor can infer highly sensitive information from live human speech, including speaker gender, identity, and speech content. The second of my talk describes a training-free voice authentication system that leverages the cross- domain speech similarity between the audio domain and the vibration domain to provide enhanced security to the popular voice assistant systems. When a user gives voice commands, the designed system exploits motion sensors on the user's wearable device to capture the aerial speech in the vibration domain and verify it with the speech captured in the audio domain via the voice assistant device's microphone. Compared to existing approaches, our cross-domain user authentication solution is low-effort and privacy-preserving, as it neither requires users' active inputs nor stores users' privacy-sensitive voice samples for training. In addition, our solution exploits the distinct vibration sensing interface and its short sensing range to sound to verify voice commands and defend against various acoustic attacks. Finally, I would like to share some new research directions to pursue with the aim of influencing the future of mobile security.

Bio: Cong Shi is currently a Ph.D. candidate in the Wireless Information Network Lab (WINLAB), Rutgers University, under the supervision of Prof. Yingying (Jennifer) Chen. His research interests include Cyber Security and Privacy, Security in Machine Learning (ML)/Artificial Intelligence (AI), Mobile Sensing, Smart Healthcare and Internet of Things (IoT). His research explores novel machine learning, sensing, signal processing techniques to classify and model research problems related to security and privacy, healthcare, human-computer interaction (HCI), and augmented reality (AR)/virtual reality (VR), with a strong emphasis on system implementation and validation in real-world scenarios. During his Ph.D. study, he has published 23

journal and conference papers in premium conferences and peer-reviewed journals including ACM CCS, ACSAC, ACM MobiCom, ACM MobiSys, ACM MobiHoc, ACM SenSys, AAAI, ACM UbiComp, IEEE ICASSP, and IEEE TMC. He is the recipient of two industry- sponsored fellowships by Cisco System and Siemens Corporate Research. His research has been reported by various media outlets such as BBC News, Yahoo News, NBC New York, Science Daily, etc.

.