Title: Security Leaks and Defenses in Smart Wearables

Speaker: Prof. Diksha Shukla (Assistant Professor, University of Wyoming)

Abstract:

The scope and usage of smart devices are expanding day by day in our everyday life and hence the need to make them more secure. In the near future, we may need to authenticate emerging smart devices such as electronic doors, exercise equipment, power tools, medical devices, and smart TV remote control. Recent research trend focuses on developing new behavioral biometric-based methods to authenticate these smart devices and there is an increase in brain wave and hand gesture-based authentication systems and IOT applications

This talk will focus on the user's sensitive information leakage through their hand movements patterns while they interact with their devices. The talk will introduce the threat model utilizing the video and motion sensor-based side channels to steal the user's sensitive information exploiting the users' hand movements patterns. I will present algorithms and methods to learn the user's pin, password, and brain wave patterns. My talk will also include novel, low effort authentication systems that utilizes the user's unique hand gestures and provides enhanced security.

Speaker Bio:

Diksha Shukla is an Assistant Professor of Computer Science in the College of Engineering and Applied Sciences, University of Wyoming, USA. She received Ph.D. degree in Computer & Information Science and Engineering from Syracuse University, USA, in 2019, M.S. degree in Mathematics from Louisiana Tech University, USA, in 2014 and the M.C.A. degree from Jawaharlal Nehru University, New Delhi, India, in 2011. Her research interest includes machine learning, computer vision, and cybersecurity. Her research spans applications of these areas to wearable devices, authentication, biometrics, and side channel attacks. Diksha's current research focuses on uncovering security threats and building secure authentication solutions for smart wearable devices. She has published in top-ranked machine learning and security journals and conferences including IEEE TIFS, ACM TOPS, ACM CCS, and ACM DTRAP, etc.