Talk Title: Smartwatch-Based Inference Attacks on Keyboards and Context-Aware Protection Mechanisms

Date: April 8th (Friday)
Time: 05:30 PM to 06:30 PM
Venue: Jabara Hall (JB-127), WSU

Speaker Biography: Dr. Murtuza Jadliwala obtained his Doctoral (Ph.D.) and Masters (M.S.) degree in Computer Science from the Computer Science and Engineering Department at the University at Buffalo, State University of New York in September 2008 and June 2004, respectively. He was a Post-doctoral Research Fellow with the Laboratory for computer Communications and Applications (LCA1) at the Swiss Federal Institute of Technology (EPFL) in Lausanne, Switzerland from September 2008 until December 2011. He is currently an Assistant Professor in the Electrical Engineering and Computer Science department at Wichita State University where he directs the SPriTE (Security, Privacy, Trust and Ethics in Computing) Research Lab. His research interests are in the broad areas of computing systems and network security & privacy, especially, security and privacy issues in human-centered cyber-physical and socio-technical systems. His research is funded by the NSF, AFOSR, AFRL-Information Institute and the Power Systems Energy Research Center (PSERC).

Talk Abstract: The popularity of wearable mobile devices such as smartwatches and fitness trackers is soaring. These smart wearable devices feature a wide range of highly precise sensors required for useful applications, including, but not limited to, personal assistance, health and wellness monitoring, personal safety, and corporate solutions. However, malicious applications on these devices can misuse some of these sensors in unintended ways. In this talk, I will discuss how any application having access to a smartwatch’s ‘motion sensors’ can be used to recover text typed on an external QWERTY keyboard. Our attack characterizes wrist movements (captured by the motion sensors of the smartwatch worn on the wrist) observed during typing, based on the relative physical position of keys and the direction of transition between pairs of keys. Eavesdropped keystroke characteristics are then matched to candidate words in a dictionary. To prevent such attacks, I will also outline the details of a nonintrusive context-aware protection framework which can be used to automatically disable (or downgrade) access to motion sensors, whenever typing activity is detected. I will also present some other attack scenarios on user privacy that can be accomplished using sensors on-board these wearable devices and what we can do to overcome those.

P.S: Please RSVP to CSA@wichita.edu by April 7th (Thursday)