CS Departmental Seminar
Tuesday, November 6, 2018, EC 205 at 3:30-4:30pm

Title: The Gift and the Curse: On the Double-Faced Nature of Sensor-enabled Computing

The motion and orientation sensors embedded in mobile and wearable devices are at the heart of some of today's most innovative apps. However, these sensors are also a vehicle for a series of stealthy side-channel privacy attacks, thanks to the relaxed permission model that mobile Operating Systems apply to them. In this talk, we will present some of our recent findings on the double faced nature of these sensors. First, we will discuss our application of these sensors for the continuous authentication of users based on handwriting patterns. We will present the design of our authentication method, rigorously analyze its performance and showcase its behavior under two different types of spoof attacks. We will then present a privacy attack that exploits these sensors to stealthily make inferences about the applications being used on a smart phone. We will discuss the design of the attack, analyze its performance and discuss the performance of a potential defense mechanism against it. Beyond our work on these sensors, we will also briefly present some of our results from a related study that designs spoof attacks against eye tracking authentication systems.

Dr. Abdul Serwadda is an Assistant Professor of Computer Science at Texas Tech University. His research leverages machine learning to tackle security questions in areas such as user authentication, mobile and wearable sensing and network traffic analytics to mention but a few. He has previously worked as a post-doc at Louisiana Tech University and Syracuse University where his research was supported by two DARPA grants. He is currently a Co-PI on an NSF SaTC project that designs active authentication mechanisms using wearable gadgets, and is the lead PI on a 600K grant training K-12 teachers in cyber security and data science.