TEXAS TECH UNIVERSITY
Edward E. Whitacre Jr.
College of Engineering™
Computer Science

Fed up of Advertisers Following you Around? Watch Your Vibe-rations!

Abdul Serwadda, Ph.D.
Tuesday, November 19, 2019 at 3:30 p.m.
Electrical and Computer Engineering, Room 101

Abstract:

The multimedia content that we consume on our phones is strongly correlated with several core attributes of our social life, including our personality traits, moral and political beliefs, criminal behavior, and interpersonal relationships, to mention but a few. Thanks to these strong correlations, advertising companies heavily rely on this information to determine which ads to push out to users. For such functionality to work however, users have to give permission to the relevant apps to access their content, which is not a guarantee in this era where increasingly security-savvy users seek to protect their privacy.
In this talk, we argue that an adverting app (or other malicious app) which has been denied access to the user's multimedia content could very reliably and stealthily learn this information via the motion sensor side-channel. Taking the case of music played on the phone, we design an attack which leverages the accelerometer patterns exhibited during music playback to infer the songs being played by the user. We show, based on the Billboard top 100 during the month of June 2018, that, depending on factors such as the volume at which one plays music, the surface on which the phone rests, the learning paradigm and kind of data used for training, the attack can identify the song being played with an accuracy of over 80%. Although users could mitigate some of the risk by using a phone cover to dampen the vibrations, we show that a sophisticated attacker could adapt the attack to still identify songs with a decent accuracy. On platforms such as Android which do not require explicit user permissions to access motion sensor data, this kind of attack would happen without any sort of suspicion from the user. The study adds to the body of work calling for more stringent restrictions on motion sensor data on mobile platforms.

Bio:

Dr. Abdul Serwadda is an Assistant Professor of Computer Science at Texas Tech University. The majority of his recent research is focused on behavioral biometrics in mobile and wearable settings, spoof attacks on these systems, and the identification and mitigation of the privacy and security threats targeting these devices. His past and present research has been funded by NSF and DARPA grants on which he has had various roles, including PI, Co-PI and senior personnel.