Securing Mobile Devices - Emerging Threats and Counter Measures

Vir V. Phoha
Prospective Faculty Candidate
W. W. Chew Endowed Professor of Computer Science
Louisiana Tech University
April 4, 2014
3:30 pm
Terry Fuller Petroleum Engineering Research Building Rm 208

Mass proliferation and use of mobile devices, such as phones, tablets, iPods, and iPads, etc. in public places opens these devices to different forms of malicious exploitation. Dr. Phoha's recent work addresses, a class of malicious exploitation algorithms that use direct observation through a readily available camera such as found on mobile phones, to guess PINS and passwords on mobile phones, ATMs, tablets, etc. with *alarmingly high accuracy*. His current work also develops methods and algorithms to defend against such attacks.

Dr. Phoha will present findings on the simplest form of our attack to decode a typed random PIN using spatio-temporal hand dynamics of a user typing on a smartphone to reconstruct the text typed. No language modeling is leveraged. At the heart of the attack is the *deterministic* keyboard design, specifically, the fixed location of the keypad on the phone screen (for any given phone model), the fixed sizes of the keys and the fixed locations of the keys on the keypad. Given video footage that captures: (1) part of a smartphone user's hands during the PIN entry process, and (2) the back side of the smartphone on which typing is being done, the attack operates by algorithmically mapping the position of the typist's hands to the known geometry and position of the keypad during the PIN code entry process.

Their findings raise a number of questions: (1) Should the traditional deterministic keyboard design be reconsidered? (2) Should cameras be completely banned in the vicinity of installations such as ATMs? (3) How can users distinguish between harmless and dangerous video recordings?

To defend against such attacks, Dr. Phoha will present his current *DARPA* project in which they are implementing Active Authentication algorithms that provide a second layer of defense to thwart these kinds of attacks. With a view to build robust systems, he will present our initial results on a new family of robotic attacks on touch-based verification --- the use of touch gestures e.g., swiping, zooming, etc.