Imposing Security Awareness on Wearables

Submitted by grigby1 on Wed, 05/17/2017 - 1:51pm

Title: Imposing Security Awareness on Wearables
Publication Type: Conference Paper
Year of Publication: 2016
Authors: Walter, Charles, Hale, Matthew L., Gamble, Rose F.
Conference Name: Proceedings of the 2Nd International Workshop on Software Engineering for Smart Cyber-Physical Systems
Publisher: ACM
Conference Location: New York, NY, USA
ISBN Number: 978-1-4503-4171-4
Keywords: bluetooth security, composability, Human Behavior, privacy, pubcrawl, Resiliency, security, situational awareness, wearables, wearables security

Abstract
Bluetooth reliant devices are increasingly proliferating into various industry and consumer sectors as part of a burgeoning wearable market that adds convenience and awareness to everyday life. Relying primarily on a constantly changing hop pattern to reduce data sniffing during transmission, wearable devices routinely disconnect and reconnect with their base station (typically a cell phone), causing a connection repair each time. These connection repairs allow an adversary to determine what local wearable devices are communicating to what base stations. In addition, data transmitted to a base station as part of a wearable app may be forwarded onward to an awaiting web API even if the base station is in an insecure environment (e.g. a public Wi-Fi). In this paper, we introduce an approach to increase the security and privacy associated with using wearable devices by imposing transmission changes given situational awareness of the base station. These changes are asserted via policy rules based on the sensor information from the wearable devices collected and aggregated by the base system. The rules are housed in an application on the base station that adapts the base station to a state in which it prevents data from being transmitted by the wearable devices without disconnecting the devices. The policies can be updated manually or through an over the air update as determined by the user.