TWC: Small: Authenticating Smart Wearable Devices Using Unique Human Body Movement Patterns
Zhang, Rutgers University

1 Introduction

After generations of technological revolutions; from wired to wireless communications, stationary to mobile machines, and large-sized to hand-held devices, we are now witnessing what can be deemed as the next phase of mobile technology: widespread *wearable computers*. Research in wearable computers can be dated back at least to the 1980s when Steve Mann experimented with backpack computers and developed a prototype of heads-up-display goggles [58]. Thanks to the advances in hardware miniaturization technology, cheap sensors/processor chips, and low-power sensing/computing, today, wearables are now available off-the-shelf and on the way to become an integral part of human lives [2, 4, 1]. In this proposal, we focus in this proposal, we focus on special-purpose wearable devices that are worn close to the body as opposed to the more general-purpose computing/communication platform like smartphones or tablets. Examples are smart glasses, smart wristbands, and smart watches, smart jewelry, and devices embedded in clothing like jackets or shoes. Such devices are typically very small and impose severe resource constraints.

With the proliferation of such wearable devices, they can be expected to be subjected to malicious attacks and preserving the security and privacy of these devices will become increasingly important. Much of the collected data on such devices is personal in nature and often relates to the user's health. Any security and privacy solution for such devices, however, also has to strike an appropriate balance with user convenience, especially as users are interacting with an increasing number of such specialized devices. A fundamental building block for safeguarding the security and privacy of user data acquired on or accessed through wearable devices are user authentication techniques, since many solutions are only effective as long as the device itself is authenticated to the right user/owner.

Authentication on most commercially available wearable devices today [1, 4] relies on an indirect mechanism, where users can log in to their wearables through their phones. This requires the wearable device to be registered and paired to the user's mobile device, which makes it inconvenient as the user has to carry both devices. The security of this approach is also in question as it increases the chance of hacking into both the devices if either of the devices are lost or stolen. Some devices including Google Glass [2] and FitBit's health tracker [1] also allow linking the device to online accounts instead of the phone for user's convenience; however, this does not add any security benefit.

Even though it has such fundamental shortcomings, indirect authentication is still the dominant paradigm for wearables because these devices are *seriously* constrained in many aspects: battery power, computing capability, storage, and input/output methods. As a result, if the community simply borrows the authentication methods designed for more powerful devices, the only plausible solution is to implement these methods on more powerful devices through indirect authentication. In this proposal, however, we take the viewpoint that in order to make a wearable device an independent unit, we must break it away from the smartphone or other more powerful devices most of the time, and we thus seek to develop suitable *direct authentication* methods that are both accurate and light-weight.

Before we design direct authentication methods for wearable devices, let us first consider the available solutions for other mobile systems, especially smartphones and tablets. Broadly speaking, there are two categories of direct authentication methods that are commonly adopted across different systems: password based authentication and biometric based authentication. However, we argue that neither of these two methods is really suitable for wearable devices: typing passwords on wearable devices can be quite cumbersome due to their small input/output units, while collecting and recognizing physiological biometrics (such as DNA, fingerprint, hand/finger geometry, iris, odor, palm-print, retinal scan, voice, etc.) is highly subject to the availability of the sensing hardware and the computing capability on the wearable units.

In addition to these two common methods, there is a third class of direct authentication method that is gaining popularity in the research community: we can rely upon the uniqueness of human behavior characteristics such as human walking gait, arm swings, typing patterns, body pulse beats, eye-blinks, etc. This way of authenticating users is called *behavioral* biometrics, which has been studied in the context of authenticating smart phones and tablets [73, 21, 81, 68, 65, 49, 14, 23]. The main advantage of using behavioral biometrics for mobile devices is that the signatures can be readily generated from raw data of built-in sensors