Chapter 46
Authenticity Challenges of Wearable Technologies

Filipe da Costa
University of Minho, Portugal

Filipe de Sá-Soares
University of Minho, Portugal

ABSTRACT

In this chapter the security challenges raised by wearable technologies concerning the authenticity of information and subjects are discussed. Following a conceptualization of the capabilities of wearable technology, an authenticity analysis framework for wearable devices is presented. This framework includes graphic classification classes of authenticity risks in wearable devices that are expected to improve the awareness of users on the risks of using those devices, so that they can moderate their behaviors and take into account the inclusion of controls aimed to protect authenticity. Building on the results of the application of the framework to a list of wearable devices, a solution is presented to mitigate the risk for authenticity based on digital signatures.

INTRODUCTION

For a long time information security management has been based on the CIA triad, the acronym denoting the principles[1] of Confidentiality, Integrity, and Availability. Over time, the sufficiency and appropriateness of these three cornerstone principles of information security have been challenged by several authors. In 1998, Parker complemented them with three new principles, namely Ownership, Authenticity, and Utility (Parker, 1998). The arrival of the new millennium with the need for organizations to adopt more agile and flat structures led Dhillon and Backhouse (2000) to argue for the inclusion of four people-related principles, known under the RITE acronym, meaning Responsibility, Integrity, Trust, and Ethicality. More recently, Teixeira and de Sá-Soares (2013) proposed a revised framework composed of thirteen information security principles and five sub-principles.

DOI: 10.4018/978-1-5225-5484-4.ch046

In a sense, these sets of information security principles convey worldviews concerning the theory and practice of information security. But new technology may alter our worldviews. An illustrative case is the emergence and evolution of wearable technologies and mobile computing devices offering us true information systems in our pocket, on our wrist, or through our glasses. These technologies are being equipped with ever-stronger information acquisition, storage, processing, display, and communication capabilities. By adopting and using wearable technologies in our daily activities, we are on the verge of a revolution that brings the potential to change the way we live, think, feel, and act.

What challenges will this new era bring us? What will be the impact of wearable technologies on our current accepted information security principles? Will we need to revamp them? Will we be forced to add new principles? Or will we even have to abandon principles once taken as a mainstay?

Wearcams connected to the Internet and sharing images in real time pose new challenges to confidentiality. Wearable GPS (Global Positioning System) devices (as simple as most common cell phones) shrink the frontiers of personal privacy. Losing our smartphone puts us out of sync with the world and makes us unavailable to others. These all exemplify issues that wearable technologies may raise to information security principles. But among the principles, we are particularly interested in the impacts of wearable technologies on *authenticity*, here defined as "Information is in accordance with a particular reality, and its genuineness and validity are verifiable, or an individual, entity or process is who it claims to be" (Teixeira & de Sá-Soares, 2013). This interest in authenticity stems from the fact that, in a scenario where all people are connected, not directly, but through their devices or wearable technology, it is crucial to develop mechanisms to ensure that information received is real and that the subjects we interact with are who they claim to be.

Wearable technologies may be conceived as cognitive prostheses that expand our human capabilities. Increased volumes of information; virtual and augmented reality; sensors feeding us real time news, opinions, restaurant suggestions, and likes from friends; apps a fingertip away, all extend what we know, and shape what we do or choose. Radio-Frequency IDentification (RFID) tags make now possible the Internet of Things (IoT). In fact, in an "all connected" society, wearable technologies make possible the Internet of People (IoP). Will we exchange wearable technologies or are one's own wearable technologies so personal that without them one will feel naked? It will not take much for wearable technologies to become blended with the body, in a morphing process of technology and human tissue (e.g. implantables), giving rise to bionic entities and redefining our identity, raising many new questions.

How will we assure that the information we receive through our wearable technologies is in accordance with reality? How will we verify the genuineness and validity of that information? Rather, will that even be possible? How can we be sure that an individual, entity or process that digitally addresses us is whom it claims to be? How can we ascertain who we really are? Will we know who we really will be? How do we prove that we are authentic? Will the machines we wear become autonomous and when they are capable of self-programming will look at us, as we look now at things, as other devices? Can these devices impersonate us? How much control will we have over our wearable technologies? Will we be aware of providing our information to third parties without any guarantee about which information is really shared? Will we measure up with our wearable devices in terms of intelligence? Will we inherit the bugs of the devices we wear? Will the Nokia slogan "Connecting people" in the future make no sense? Maybe we will know the interface for people, not the persons.

Against this background, this chapter begins by reviewing the concepts of authenticity and wearable technology. Then, it presents the "wearable ecosystem" and its underlying dangers, discussing how current and foreseeable wearable technologies may impact on the authenticity of information and subjects.