

Chapter 5

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 principles¹ 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

DOI: 10.4018/978-1-5225-1016-1.ch005

Authenticity Challenges of Wearable Technologies

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.

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

31 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/authenticity-challenges-of-wearable-technologies/164306

Related Content

AI-Based Wireless Communication

Sanjana T., Lalitha S., Surendra H. H. and Madhusudhan .. K. N. (2022). *Challenges and Risks Involved in Deploying 6G and NextGen Networks* (pp. 42-60).

www.irma-international.org/chapter/ai-based-wireless-communication/306814

Solar Powered Smart Street Light with Maintenance Service System

Thinaharan Ramachandran, Vasaki Ponnusamy and Noor Zaman (2016). *Biologically-Inspired Energy Harvesting through Wireless Sensor Technologies* (pp. 102-120).

www.irma-international.org/chapter/solar-powered-smart-street-light-with-maintenance-service-system/149355

A Simulation Framework for the Evaluation of Frequency Reuse in LTE-A Systems

Dimitrios Biliros, Christos Bouras, Georgios Diles, Vasileios Kokkinos, Andreas Papazois and Georgia Tseliou (2014). *International Journal of Wireless Networks and Broadband Technologies* (pp. 56-83).

www.irma-international.org/article/a-simulation-framework-for-the-evaluation-of-frequency-reuse-in-lte-a-systems/115590

Advanced Spectrum Sensing Techniques

P. T. V. Bhuvaneswari Mohan and Bino Jesu Stephen (2019). *Sensing Techniques for Next Generation Cognitive Radio Networks* (pp. 133-141).

www.irma-international.org/chapter/advanced-spectrum-sensing-techniques/210274

Cooperative Space Time Coding for Semi Distributed Detection in Wireless Sensor Networks

Mohammad A. Al-Jarrah, Nedal K. Al-Ababneh, Mohammad M. Al-Ibrahim and Rami A. Al-Jarrah (2012). *International Journal of Wireless Networks and Broadband Technologies* (pp. 1-15).

www.irma-international.org/article/cooperative-space-time-coding-for-semi-distributed-detection-in-wireless-sensor-networks/85002