Chapter 3
Watch What You Wear:
Smartwatches and Sluggish Security

Joseph Ricci
University of New Haven, USA

Ibrahim Baggili
University of New Haven, USA

Frank Breitinger
University of New Haven, USA

ABSTRACT

There is no doubt that the form factor of devices continues to shrink as evidenced by smartphones and most recently smartwatches. The adoption rate of small computing devices is staggering and needs stronger attention from the cybersecurity and digital forensics communities. In this chapter, we dissect smartwatches. We first present a historical roadmap of smartwatches. We then explore the smartwatch marketplace and outline existing smartwatch hardware, operating systems and software. Next we elaborate on the uses of smartwatches and then discuss the security and forensic implications of smartwatches by reviewing the relevant literature. Lastly, we outline future research directions in smartwatch security and forensics.

DOI: 10.4018/978-1-5225-1016-1.ch003

INTRODUCTION

Smartwatches have recently become a novel consumer product especially with the release of the Apple Watch, which has certainly galvanized the wearable-tech market. eMarketer, an independent market research company expects smartwatches will lure consumers away from fitness trackers - which is currently the most popular wearable device (eMarketer, 2015). Smartwatches process a variety of personal data, different from data processed by current smartphones, making the study of smartwatches from the security and forensics perspectives important.

Since the advent of smartphones, law enforcement, criminals, and organizations have been able to collect a plethora of personal data about their consumers allowing service providers and device manufacturers to profile their users. Smartphones can collect data such as shopping preferences, Global Positioning System (GPS) coordinates, weight, gender, and age just to name a few examples. Undoubtedly, people have become personally and emotionally attached to these devices (Thorsteinsson & Page, 2015). Notwithstanding, we have now entered the era of smartwatches as device factor continues to decrease in size. Now that smartwatches such as the Samsung Gear 2 Neo, LG G, and Apple Watch have a flourishing adoption rate and employ many of the similar capabilities as smartphones, one may ask the question *What additional personal data are these smart devices able to collect and how safe is that data during transit and storage?* We posit that smartwatches will become fully integrated personal digital assistants that not only will receive notifications from a one's smartphone but also monitor one's health.

Research on smartwatch security is sparse, which is why it is important to understand their functionality and their vulnerabilities. The security of data that is stored and transmitted from and to a smartwatch suggests that encryption is important to protect data from prying eyes. Identifying potential challenges may make users aware of the likely risks from using smartwatches and may assist in preventing sensitive data from being leaked. While we observe the size of smart devices shrinking over time, it is not difficult to imagine the possibility for smartwatches replacing smartphones one day.

In this chapter, we first outline the history of smartwatches, and the current smartwatch marketplace in an effort to familiarize the reader with this technology. Next, existing smartwatch hardware, operating systems and software are delineated to provide insight into how one could implement methods and technologies in smartwatch security and forensics. We then follow that with the uses of smartwatches to provide an understanding of how they operate. Then, the security implications of smartwatches are discussed, followed by a review of the preliminary forensic