Chapter 32
Security for Hybrid Mobile Development: Challenges and Opportunities

Marcus Tanque
Independent Researcher, USA

ABSTRACT

In recent decades, vendors developed technology infrastructure solutions to integrate with enterprises and consumers' mobile devices. Hybrid development platforms are solution architecture designed to enhance developers' capabilities and provide organizations as well as customers the level of services to support mobile devices capabilities. Hybrid development platform solutions are easy to deploy at various enterprises. These capabilities can be distributed to/or integrated with mobile devices as agile applications and system interfaces. Hybrid mobile devices are designed to further provide users with enhanced technology solutions: cloud computing, big data, the Internet, physical and/or virtual network systems. The development of hybrid mobile platforms provides developers with advanced technology capabilities, necessary for supporting mobile devices once deployed to the marketplace. Technical and security features affecting the development and security of mobile devices are also discussed in this chapter.

INTRODUCTION

In recent years, vendors and information technology practitioners have researched on security solutions necessary, to prevent data breaches and protect user's privacy (Chess, & McGraw, 2004). For many years, mobile devices have been supported by a number of security applications. Thus technical constraints have contributed to organizations and consumer's confidence aimed at protecting user's privacy. Besides, homogeneity and heterogeneity capabilities for mobile devices are designed to support enterprises and consumer's requirements (Ubl, 2011; Rajapakse, 2008; Charland & LeRoux, 2011; Adam & Christ, 2011; Christ, 2011). In the modern time, the mobile industry has designed several technology product solutions to attract enterprises and consumers' business and market attention. Nearly a decade ago, vendors designed commodity hardware and software appliances with embedded capabilities to leverage

DOI: 10.4018/978-1-5225-2599-8.ch032

customer's specifications (Chess, & McGraw, 2004; Burns, 2009). These characteristics include, but are not limited to customized commodity hardware and software appliance, developed to satisfy the user's requirements (Ubl, 2011; Gartner, 2012; Mark, 2013). These features include: faster processing, improved memory and enough storage capacity designed to attract enterprises and consumers' business/market interests. The homogeneity and heterogeneity features mobile devices offer, focused on supporting the enterprises and consumer's business specifications (Fowler, & C. S., 2012; Burns, 2009; Christ, 2011).

BACKGROUND

For many years, securing mobile devices has been one of the challenging issues vendors and policy-makers have dealt with. This includes research on security solutions required, to address any gaps and/or challenges affecting the development of hybrid mobile devices (Thornycroft, 2016). Despite these efforts vendors such as Facebook have been skeptical, in complying with the federal laws, would put organizations/consumers' data protection and privacy policies at risk. Lacking these measures has raised greater concerns to federal and state legislators (Thornycroft, 2016; IBM, 2012). Aside from these policy disagreements between Apple and legislators, yet the U.S. government opted for an eccentric method also known as a "backdoor password solution". Apart from the U.S. government's decision vendors have expressed concerns on how federal laws, must be enforced without impacting on user's privacy. This comprises the development of mobile apps and how such laws must be applied to enterprises and consumers, who have existing contracts with various mobile carriers and providers (IBM, 2012). Despite any differences between Apple and the U.S. federal government, lawmakers vow to uphold the country's constitutional privileges such as national security's interests, and the protection of all citizens' rights. Vendors are confident any existing differences with the federal government must only be resolved through the implementation of suitable legislations to protect data and user's privacy. Apart from these progresses vendors such as Google are developing improved security solutions to protect subscribers' data and privacy. These security solutions are developed to afford users the ability to access and protect data stored on their mobile devices (Thornycroft, 2016; IBM, 2012). In recent years, vendors have developed improved encryption solutions to protect mobile devices, from being compromised by unauthorized personnel. These security tools are developed to protect data and user's privacy. Recently, Android and Apple deployed apps equipped with security capabilities for enterprises and consumers to have the ability to mask the Media Access Control (MAC) addresses stored on their mobile devices. Masking MAC address allows enterprises and consumers to limit any exploitation to mobile devices by unauthorized personnel i.e., attackers, hackers, intruders, via cyber domain sources (Thornycroft, 2016). These technology evolutions have afforded vendors the ability to anonymize requests made or generated from suspected sources, to users' mobile devices. Vendors argue that data and privacy are matters, which require improved security policies and procedures. In recent decade, the discovery of new cryptographic security solutions has significantly reduced the number of threats enterprises and consumers have always encountered from their adversaries (Thornycroft, 2016; Bloice & Wotawa, 2009). For that reason, IT managers and vendors must adopt new security measures to monitor, prevent, deny, moderate and reduce any threats launched against consumers' network resources (Fowler, & C. S., 2012; Chess & McGraw, 2004). Security for hybrid mobile development can be categorized into two different methods (Bloice & Wotawa, 2009; Dickson, 2012; Chess, & McGraw, 2004). These methods involve: single and mul-