Abstract

The following paper is a literature review on the topic of Mobile Security. The topic has been chosen due to the rise in mobile applications and the insufficient rise in the topic of the security within those applications. For the purposes of this paper, mobile devices are considered as tablet and cell phones which run a mobile Operating System (OS). More specifically, these are Android (Google), iOS (Apple), or BlackBerry OS (RIM). While it is important to note these terms, this literature review is focused primarily on the Android OS security vulnerabilities. Polymorphic is defined as malware that transforms to be somewhat different than the one before. The automated modifications in code do not modify the malware's functionality, but they can render conventional anti-virus detection technology ineffective against them. An attack vector is most basically described as the approach utilized to assault a specific technology (i.e., a path taken to compromise a system). A botnet is a collection of "zombies" which are remotely controlled for malicious or financial gains [1]. A single botnet often contains hundreds or thousands of devices. When the term "vulnerability" is being utilized within this paper, it is a weak spot which allows an attacker to decrease a system's security. A vulnerability occurs when three elements intersect, including a system weakness or flaw, attacker access to the flaw, and attacker competence to exploit the flaw [2].
Mobile Security: A Literature Review

- ThreatInsight, "Cloned Android Apps: Symbiosis or Parasitic?," F-Secure, 2011.
- Hak5, "Extreme android and google auth hacking with kos," Hak5, 2012.
- The Identity Theft Resource Center, "Breaches: Knowing less and less about less and less," The Identity Theft Resource Center, 2012.

Index Terms

Computer Science
Security
Keywords
Mobile Security polymorphic smartphones Android IOS Blackberry Google Anti-virus BYOD Botnet Vulnerability Information Technology ISA