Chapter 10
Techniques for Analysis of Mobile Malware

Gopinath Palaniappan
Centre for Development of Advanced Computing (CDAC), India

Balaji Rajendran
Centre for Development of Advanced Computing (CDAC), India

S. Sangeetha
National Institute of Technology Tiruchirappalli, India

NeelaNarayanan V
VIT University, India

ABSTRACT

The rapid rise in the number of mobile devices has resulted in an alarming increase in mobile software and applications. The mobile application markets/stores too have created a fundamental shift in the way mobile applications are delivered to users, with apps being added and updated in thousands every day. Even though research progresses have been achieved towards detection and mitigation of mobile security, open challenges still remain and also keep evolving in this area. Several studies reveal that mobile application markets/stores do harbor applications that are either vulnerable or malicious in nature, leading to compromises of millions of devices. This chapter (1) captures the attack surface of mobile devices, (2) lists the various mobile malware analysis techniques, and (3) lays the ground for research on mobile malware by providing mobile malware dataset resources, tools for malware analysis, patent landscaping for mobile malware detection, and a few open challenges in malware analysis.

DOI: 10.4018/978-1-5225-8241-0.ch010

INTRODUCTION

The count of the Mobile devices is increasing dramatically day-by-day. Mobile devices have raised above from just being a digital device or a smartphone, in fact they have turned into a platform for convergence of our personal and digital life because of their rich computing capabilities and its wide range of features such as easier communication, more than one internet connectivity mechanisms, the storage including multimedia and so on. The ubiquitous presence of mobile devices can be understood from the statistics in Figure 1 below. The mobile devices remain online continuously by seamlessly connecting through mobile data or the closest available Wi-Fi, and keeps downloading and uploading data intermittently, increasing the complexities in protecting the data.

There exist several Mobile device vendors who deliver their devices bundled with major mobile operating systems such as Android (by Google), iOS (by Apple) and others. However recent times has seen mentionable increase in the number of Android-based Mobile devices when compared to other mobile operating systems (Figure 2).

The ubiquitous nature of mobile devices has resulted in drastic rise in the number of applications in the mobile market, complicating mobile security further (Imran Ashraf, 2012). These applications are an add-on to the features and capabilities of the mobile devices. They also make the life of the users better by providing them with the functionalities such as financial transactions, entertainment, shopping, games,

Figure 1. Sales of smartphone shipments across the globe from 2009 to 2017 and projections for 2018 to 2022
(Source: The Statistics Portal: www.statista.com)