Chapter 7
Survey in Smartphone Malware Analysis Techniques

Moutaz Alazab
Isra University, Jordan

Lynn Batten
Deakin University, Australia

ABSTRACT
Smartphone Malware continues to be a serious threat in today’s world. Recent research studies investigate the impacts of new malware variant. Historically traditional anti-malware analyses rely on the signatures of predefined malware samples. However, this technique is not resistant against the obfuscation techniques (e.g. polymorphic and metamorphic). While the permission system proposed by Google, requires smartphone users to pay attention to the permission description during the installation time. Nevertheless, normal users cannot comprehend the semantics of Android permissions. This chapter surveys various approaches used in Smartphone malware detection and investigates weaknesses of existing countermeasures such as signature-based and anomaly-based detection.

INTRODUCTION
The production and use of smartphone devices are increasing rapidly, with technological advancements resulting in lighter and more powerful devices. In 2015, the growth in smartphone popularity convinced society, on both a macro and micro level, to turn away from traditional computers in exchange for what the smartphone market was offering (Halleck, 2014).

Nowadays, consumers are not restricted to only making phone calls and sending text messages via their mobile phones. The smartphone market offers a number of features that were previously unheard of, with the consumer being able to browse the internet, upload and share their photos, access and send emails, view social networking sites such as Facebook and Twitter, and have the convenience of countless applications offering everything from online banking to online market.

Smartphones are the most in-demand phone amongst consumers across the entire phone market (Gartner, 2015). The growth in popularity has prompted manufacturers to develop the phone’s functionality
even further, which explains the existence of company giants such as HTC, Apple and Samsung who are competing to release more improved and advanced smartphones.

With this dramatic growth in the smartphone market (Bureau, 2012; Svajcer, 2014), there has been a detection of high amounts of prohibited malicious applications designed to specifically target smartphones. For example, the most common type of malware is known as a Trojan. This specific malware appears to be clean, but in fact can harm the smartphones without the user even noticing. The authors of such malicious applications are able to produce malevolent files by gaining access to operating system documents of the smartphones targeted. Such documents are used to find gaps that they can penetrate, and then used to create smartphone malware. In addition, the developments of smartphone applications are considerably more complicated than the development of traditional windows software. In comparison, this makes smartphone malware more complicated to understand.

Smartphone misconduct through cybercriminals is not a new area, with the latest reports CNCCS (2013); (Fossi et al., 2011; Victor Chebyshev & Roman Unuchek, 2014) showing that various kinds of malicious codes are being developed for the mobile handsets. The well-known antivirus engine Kaspersky produced a report Kaspersky (2012) on the IT threat evolution, which indicated that smartphone attacks are becoming more frequent, and attention has been given to target open source operating systems, such as the Android. In their report, findings confirm that almost 150,000 “zero day” malicious applications harm the Android operating system annually, with 49% of those smartphone malware being a centralised Trojan, which has the capability of stealing users’ data by connecting smartphones to a remote server.

The damage caused by malicious applications usually has two results:

- Malware that causes physical damage to the smartphone handset by taking up memory space and switching on extra features such as the Bluetooth. This, in turn, damages smartphone speed and performance. This kind of malware primarily affects the handset’s resources i.e. battery life, CPU speed and memory capacity.
- The software effect, where some other malicious binary may cause innumerable problems to confidential data, includes the threat of hackers accessing and stealing the mobile user’s private emails, passwords, contacts, photos, videos and various other personal files. It can also affect the mobile user’s service bill, with hardware glitches that yield calls and messages that result in the user exceeding their usual fixed bill.

Smartphone antivirus applications are becoming widely deployed amongst smartphone users, and have proven to be very efficient in offering protection against different types of smartphone malware threats. Commercial smartphones are all protected by antivirus engines and firewalls. Indeed there are various real-time anti-malware and anti-theft protection for smartphones, accessible in the smartphone markets, which are free to the consumer. These antivirus applications usually protect users from harmful Viruses, Trojans, Spyware and help to preserve the safety of the mobile users’ private data. There are incomplete forms of protection available for these devices that can offer cellular network firewalls and antivirus protection (Zhao, Zhang, Ge, & Yuan, 2012; Zhou & Jiang, 2012). Malicious writers produce malevolent files to exploit new weaknesses, security retailers have to find it first and then react with a new antivirus signature(s) that require smartphones users to complete the installation through the Internet (Wi-Fi or cellular network). Therefore, fresh malicious attacks do not have the time they need to spread throughout smartphones.