Information Sciences 321 (2015) 193–204

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Simple and effective method for detecting abnormal internet behaviors of mobile devices

Patrick Shicheng Chen [1], Shu-Chiung Lin *, Chien-Hsing Sun

Department of Information Management, Tatung University, 40, Sec.3, Zhongshan N. Road, 104 Taipei, Taiwan, ROC

ARTICLE INFO

Article history:
Received 2 April 2014
Received in revised form 11 April 2015
Accepted 16 April 2015
Available online 4 May 2015

Keywords:
Smartphone
Malware
Trojan
Mobile communications security

ABSTRACT

Smartphones are becoming the primary mobile communications device. Because of the rich data stored in smartphones, data theft and Trojan threaten mobile security and account for most attacks. Most antivirus systems function using a signature-based approach. However, this study proposes an effective solution for detecting abnormal behaviors of mobile malware according to its communication characteristics on the Internet. Malware usually establishes external connections to transmit compromised data to a specified host; the proposed method detects abnormal behaviors by monitoring outward communicating packets. The method involves a three-step check action: identify the HTTP POST/GET packets, check for the transmission of sensitive data, and verify the rationality of the remote server. Behavior characteristics of malware and normal software were experimentally compared for verifying the efficacy of the method; a collection of malicious, legitimate, and common application programs were used in the experiment. The results revealed that the proposed method effectively identifies abnormal Internet behavior without constructing a complex detection environment. It detects anomalies in all mobile operating platforms. In addition, the method can be easily implemented by users and enterprises for enhancing information security in mobile communications.

1. Introduction

In this decade, many smartphone applications have been developed for conveniences and services, such as teaching and learning [41], transportation and traffic [43], online search and purchase [7], news and entertainment [60], social networking [35], environmental monitoring [44], and health management [22]. The development of mobile communication devices and application services has radically changed online user behavior [28]. Smartphones are becoming the primary device for mobile communications; therefore, implementing secure mobile and wireless networks is crucial for enterprises operating in the Internet-based business environment [4]. The high level of integration of mobile communications services in people's daily lives has led to a large amount of data, such as text messages, addresses, photographs, GPS coordinates, and even corporate data, being stored in their smartphones, all of which are potential data theft targets [58].

According to Gartner Inc. surveys released in February 2014 and March 2015 [19,20], the two most popular smartphone operating platforms were Android and iOS, with Android having 78.5% and 80.7% of the market share in 2013 and 2014, respectively (Table 1). In January 2012, Trend Micro Inc. reported that smartphone bulk replication malware was the severest

* Corresponding author. Tel.: +886 2 25925252x3614; fax: +886 2 25853966.
E-mail addresses: chenps@ttu.edu.tw (P.S. Chen), sclin@ttu.edu.tw (S.-C. Lin), rubysun2006@yahoo.com.tw (C.-H. Sun).

[1] Tel.: +886 2 25925252x3609; fax: +886 2 25853966.

http://dx.doi.org/10.1016/j.ins.2015.04.035
0020-0255/© 2015 Elsevier Inc. All rights reserved.

Table 1
Market share of smartphone operating systems in 2012–2014 (thousands of units). Source: Gartner (February 2014 and March 2015).

Operating system	2014 Units	2014 Market Share (%)	2013 Units	2013 Market Share (%)	2012 Units	2012 Market Share (%)
Android	1,004,675	80.7	761,288	78.5	451621.0	66.4
iOS	191,426	15.4	150,786	15.5	130133.2	19.1
Windows	35,133	2.8	30,714	3.2	16940.7	2.5
BlackBerry	7,911	0.6	18,606	1.9	34210.3	5.0
Others	5,745	0.5	8,327	0.9	47203.0	6.9
Total	1,244,890	100.0	969,721	100.0	680108.2	100.0

threat in 2011, and that it worsened in 2012 [1]. Between 2009 and 2011, 46 types of malware operating on the iOS, Android, and Symbian platforms were reported [18]. Furthermore, malware attacks on Android smartphones increased 14.1-fold between January and July 2011 [39]. In 2012, over 120,000 malicious Android applications were identified [1] and over 32.8 million Android devices were infected by malware [38].

This study focused on the Android operating system (OS) because of its dominant market share. An analysis of Android malware (Fig. 1) revealed that private data theft accounted for 24.3% of the attacks, followed by remote control attacks (22.6%) and malicious fee charging (21.5%). Furthermore, the compromised private data include geographical location (35.2%), mobile phone model information (24.3%), address books (17.5%), and text messages (14.5%) [36]. Remote control attacks, private data theft, and malicious fee charging by Android malware grew rapidly to 26.3%, 24.2%, and 23.5%, respectively [37]. The two severest threats were advertising Trojans, which accounted for 83% of remote control attacks, and geographical information theft, which accounted for 61% of private data thefts.

Malware is designed for various functions such as keyboard sniffing, password sniffing, network monitoring, backdoor access, spying, and rootkiting [57]. This study distinguishes three types of malicious data access behaviors: anomalous information dissimilation, anomalous information leakage, and unauthorized data use. Malware usually launches an attack in the following manner: (1) infect the target, (2) perform the specified activities, and (3) propagate to other devices [6]. Mobile phone viruses often carry attachments and propagate through bulk multimedia messaging [26].

Malware detection techniques can be signature or anomaly based [2]. Currently, the majority of mobile malware detection techniques are signature based [15,46]; that is, the antivirus software examines the contents of the scanned files against its dictionary of virus signatures [13]. Virus signatures are extracted from viral codes, and detecting a virus signature in a file is equivalent to detecting the virus. On detection, the antivirus software can remove the virus. However, antivirus software is less likely to acquire the dynamic data of other applications in operation because of permission restrictions in mobile systems [56]. Although signature-based approaches are generally effective, they cannot detect new malware unless samples have been obtained and signatures documented [27,46,47,55]. Therefore, signature-based approaches are ineffective in detecting the latest and unknown viruses, especially metamorphic viruses, which encrypt or disguise themselves to avoid being matched to the documented signatures [13]. Such viruses can cause considerable damage before their signatures are created. Moreover, most signature-based approaches scan all files and programs residing on the mobile device, rendering them invasive. Cha et al. [11] proposed a signature-based antimalware system called SplitScreen that filters client files during signature detection, thus preventing private data transmission; however, most signature-based approaches scan users' private data and risk data disclosure. Therefore, behavior-based detection approaches have been intensively studied [24,61].

In recent years, several behavior-based malware detection techniques for mobile devices have been developed: AMAL [34], MMDS [24], NEMESYS [21], Crowdroid [9], pBMDS [54], WMMD [15], and JStill [56]. Some methods are specifically used to detect viruses operating on particular operating systems (OSs), for example, Symbian [8], Windows Mobile [15], Android [9,42,47,53] and iOS [16]. Other methods provide static analysis [21,45,47,53,55] wherein programs residing in the mobile devices are analyzed to understand their behavior. Certain approaches entail complex environments, such as those used in intrusion detection systems (IDSs) and intrusion prevention systems [16,22]. Several systems facilitate decision support by collecting experiences of human-user behaviors [34], abnormal behaviors [15], sensitive application behaviors [62], and system weaknesses [29] to construct a knowledge base for reasoning.

Because mobile phones are convenient and continually used devices, their security must be regularly monitored. Antivirus software can effectively protect mobile phones from known viruses. For new, self-updating, polymorphic viruses, a behavior-based approach can be adopted [48]. A review of the current literature showed that some behavior-based systems are OS dependent and invasive in providing static analyses, entail complex detection environments, and are not easy to use. In addition, corporate professionals often save critical corporate data in their mobile devices and are reluctant to secure their devices by using invasive applications. Therefore, developing a simple, effective, and noninvasive behavior detection approach is desirable. We propose an intuitive approach that monitors device network traffic, sniffs network packets, and analyzes behavior patterns. Because the proposed approach can distinguish malware and safe behavior, it can detect malware without requiring its signature; that is, the approach effectively detects unknown and varying mobile malware.

The rest of the manuscript is organized as follows. Section 2 discusses literature on virus infections and the behavioral patterns of mobile malware. Section 3 describes the experimental environment, and Section 4 presents the experimental results. The concluding section presents discussions and future research potential.