Accessibility Service Utilization Rates in Android Applications Shared on Twitter

Shuichi Ichioka[1], Estelle Pouget[1 2], Takao Mimura[3], Jun Nakajima[3], and Toshihiro Yamauchi[1 [0000−−0001−−6226−−5715]]

[1] Graduate School of Natural Science and Technology, Okayama University, Okayama, Japan
ichioka@s.okayama-u.ac.jp, yamauchi@cs.okayama-u.ac.jp
[2] Grenoble INP - Esisar, France
[3] SecureBrain Corporation, Tokyo, Japan

Abstract. The number of malware detected has been increasing annually, and 4.12% of malware reported in 2018 attacked Android phones. Therefore, preventing attacks by Android malware is critically important. Several previous studies have investigated the percentage of apps that utilize accessibility services and are distributed from Google Play, that have been reportedly used by Android malware. However, the Social Networking Services (SNSs) that are used to spread malware have distributed apps not only from Google Play but also from other sources. Therefore, apps distributed from within and outside of Google Play must be investigated to capture malware trends. In this study, we collected apps shared on Twitter in 2018, which is a representative SNS, and created a Twitter shared apps dataset. The dataset consists of 32,068 apps downloaded from the websites of URLs collected on Twitter. We clarified the proportion of apps that contained malware and proportion of apps utilizing accessibility services. We found that both, the percentage of malware and percentage of total apps using accessibility services have been increasing. Notably, the percentages of malware and un-suspicious apps using accessibility services were quite similar. Therefore, this problem cannot be solved by automatically blocking all apps that use accessibility services. Hence, specific countermeasures against malware using accessibility services will be increasingly important for online security in the future.

Keywords: Accessibility Service · Android App · Malware · SNS.

1 Introduction

The number of malware detected has increased annually, with 4.12% of malware found in 2018 reportedly attacking Android phones [6]. A 2018-19 security report by AV-TEST found a total of 5,490,000 Android malware attacks in 2018 [6]. Contrarily, WeLiveSecurity has reported that the number of Android malware is actually decreasing [18]. Either way, the number of Android malware is still large and this poses a significant problem that warrants investigation and prevention.

In 2017, Dr. Web has reported accessibility service (AS) utilization as a recent trend for mobile malware [9]. These services are an Android feature intended for use by people with disabilities, but they have been reportedly used by Android malware as well. For example, a malware called Skygofree, which uses AS to eavesdrop on information on user screens was reported in 2018 [14]. Additionally, in 2019 a malware called Gustuff reportedly used AS to send money unintended by users [11]. Clearly, there have been many malware attacks that exploit these well-intentioned AS.

It is therefore important to investigate the utilization rates of AS by Android applications (apps). There have been reports on the AS utilization rate, specifically by apps that were distributed by Google Play. In November 2017, it was announced that any apps that were using AS for purposes other than supporting users with disabilities would be deleted from Google Play [4]. According to the AS documentation [3]:

> "Although it's beneficial to add accessibility features in your app, you should use them only for the purpose of helping users with disabilities interact with your app."

Therefore, developers could not use Google Play to distribute apps that use AS, except those intended to help users with disabilities. However, many apps that use AS could be distributed by methods other than Google Play, so surveys targeting only Google Play apps are insufficient to investigate the actual distribution of such apps. We must, therefore, investigate the distribution of apps that use AS from all sources to evaluate the overall utilization of AS in malware.

Malware and fake websites have been widely shared on Social Networking Services (SNSs) [13], where many cybercrimes have also occurred [7]. It is therefore important to investigate the true situation around Android apps that use AS so that malware trends can be accurately characterized.

In this study, we collected URLs obtained from Twitter, which is a representative SNS, accessed these URLs, and collected the Android apps that could be downloaded to explore apps distributed from sources other than Google Play. We created a Twitter shared apps dataset that consists of 32,068 apps downloaded from the websites of URLs collected on Twitter. We clarified the proportion of apps that contained malware and proportion of apps utilizing AS.

We used this data to identify the proportion of the total number of shared apps that used AS. This revealed both the threat level presented by apps shared on Twitter and the danger of allowing AS for SNS distributed apps.

In summary, our study makes the following contributions:

- We created a dataset that consists of apps downloaded from the websites of URLs collected on Twitter. As far as we know, there is no dataset that focuses on apps distributed by URLs via Twitter.
- We analyzed the rate at which Android apps shared on Twitter use AS. Focusing on these apps, which are distributed from third party app stores or websites, we identified an accurate summary of apps distributed from these sources in 2018.

```
<service android:permission="android.permission.BIND_ACCESSIBILITY_SERVICE">
    <intent-filter>
        <action android:name="android.accessibilityservice.AccessibilityService"/>
    </intent-filter>
    <meta-data android:name="android.accessibilityservice" android:resource="@xml/accessibility_config"/>
</service>
```

Fig. 1. Extract of manifest declaring AS use

- We show that the proportion of malware is increasing for apps shared on Twitter.
- We find increasing AS usage rates for Android apps shared on Twitter.
- We show some countermeasures that mitigate the threats of apps utilizing AS. We believe that the increasing trend of apps utilizing AS will continue, thus we should carefully check the apps that require AS and their required permissions.

2 Accessibility Services Overview

Following the AccessibilityEvents documentation [1]:

> Accessibility services should only be used to assist users with disabilities in using Android devices and apps. They run in the background and receive callbacks by the system when AccessibilityEvents are fired. Such events denote some state transition in the user interface, for example, the focus has changed, a button has been clicked, etc. Such a service can optionally request the capability for querying the content of the active window.

Notably, apps that use AS can read string data that is displayed on screens and operate other apps [2], making them particularly powerful and potentially dangerous.

For an app to use AS, two things must occur. First, it must be declared in AndroidManifest.xml, an example of which is shown in Fig.1. Second, the user must allow AS in the app settings. A sample settings screen for Android users is shown in Fig.2. When utilizing AS, users must change their settings, as the AS cannot be engaged unless the user permits it.

Malware have been reported to exploit AS. According to Kaspersky, a malware named Skygofree used AS to eavesdrop on messages received by chat apps [14]. Skygofree also hid AS permission requests behind other requests to trick users [14]. Additionally, Group IB reported a malware called Gustuff that automatically filled forms using AS, in mobile banking app, and was thus able to steal money from users [11]. Generally, malware that exploit AS can obtain sensitive information displayed on user screens such as passwords [10]. Further, malware can operate Android phones automatically to download other applications from Google Play and post reviews [15]. Often, attackers trick users into granting access to AS to take advantage of these capabilities.

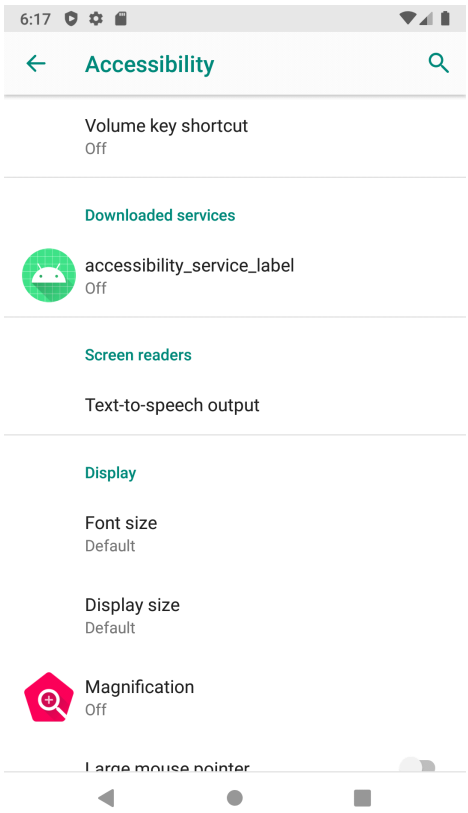

Fig. 2. Sample AS settings screen

3 Investigation of the Ratio of Malicious Apps and their Accessibility Service Utilization Rates

3.1 Purpose of Investigation

Our purpose herein is to investigate the actual AS usage rates of the distributed apps. To this end, we investigated apps shared on SNS, specifically Twitter. We selected Twitter because users can use it anonymously, and a single user can have multiple accounts, making it particularly vulnerable to criminal misuse.

3.2 Method for Collecting Apps on Twitter

As a result of searching for "apk" as a keyword in the public streaming application programming interface (API) [17] of Twitter, we collected the uniform resource locators (URLs) included in all acquired text. We selected "apk" as a keyword because "apk" is used as the file extension for Android apps. We obtained the contents from the websites of the URLs collected from Twitter as

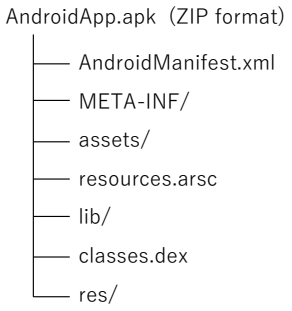

Fig. 3. Android app file structure

Table 1. Number of apps

Month	Number of apps	Number of different certificates
Jan.	3,499	1,220
Feb.	2,702	1,088
Mar.	2,399	936
Apr.	2,848	1,072
May	4,563	1,201
Jun.	2,815	855
Jul.	2,817	988
Aug.	2,384	959
Sep.	1,256	513
Oct.	1,653	631
Nov.	2,913	987
Dec.	2,397	771

well as the contents from the websites contained in the links included on the websites. Android apps include files with unique names such as those shown in Fig.3. Hence, we collected files that met all of the following conditions, which indicate that the file is indeed an app.

A) It is in ZIP format.
B) It includes class.dex and AndroidManifest.xml.
C) It includes a directory named META-INF

For the identified apps, we used VirusTotal to determine whether each was suspicious and to obtain a list of "detected" warnings for users from multiple virus scanners. In this research, one or more "detected" readings determined that the app was suspicious. The app collection period was 1 year, spanning January 1, 2018 to December 31, 2018, and 32,068 total apps were analyzed. The number of apps and different certificates are shown in Table 1. Different certificates indicate different developers. As Table 1 shows, we have collected many apps with different certificates to ensure we obtained a wide range of apps.

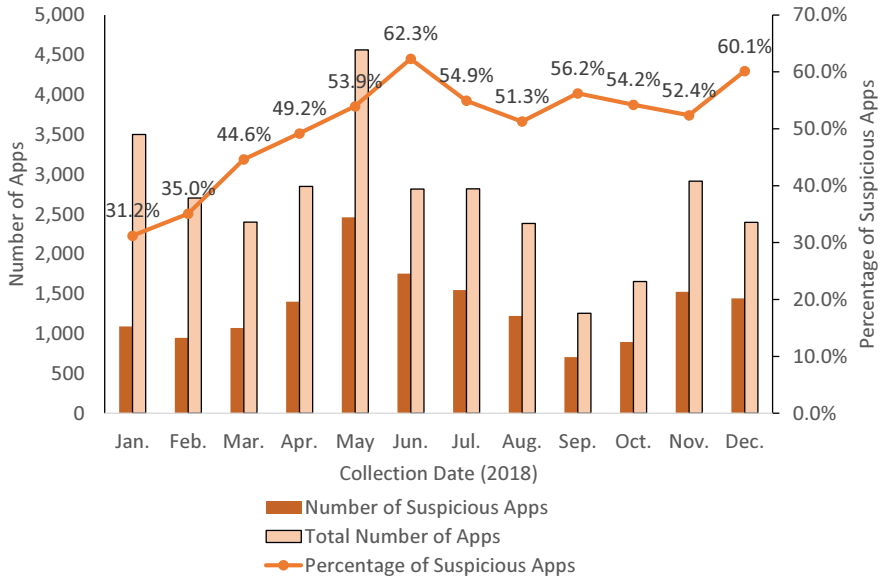

Fig. 4. Percentage of suspicious apps shared on Twitter

3.3 Investigation Method

The flow for analyzing AS usage rates is shown below:

(1) Extract AndroidManifest.xml from the app using Apktool [5].
(2) Search for the following in AndroidManifest.xml:
`android.permission.BIND_ACCESSIBILITY_SERVICE`
(3) If a character string is found as a result of this search, the app is determined to use AS. Apps exhibiting technical issues such as Apktool that abnormally terminated, were excluded from the AS usage rate survey.

This analysis allowed us to collect apps according to their trend of being shared on Twitter. In addition, analyzing AndroidManifest.xml revealed the percentage of apps that can use AS. Therefore, the ratios of suspicious apps shared on Twitter and apps using AS could be clarified.

3.4 Investigation Results

Investigating the ratio of suspicious apps. In Figure 4, the percentage of suspicious apps identified in each month of 2018 is shown, which exhibits an overall increasing trend.

We can infer from these results that the proportion of malware in the apps distributed on Twitter is also increasing. Specifically, the average percentage of suspicious apps was 49.8%. If we generalize this result, we can conclude that about half of all SNS-distributed apps are suspicious, and installing them is dangerous and not recommended.

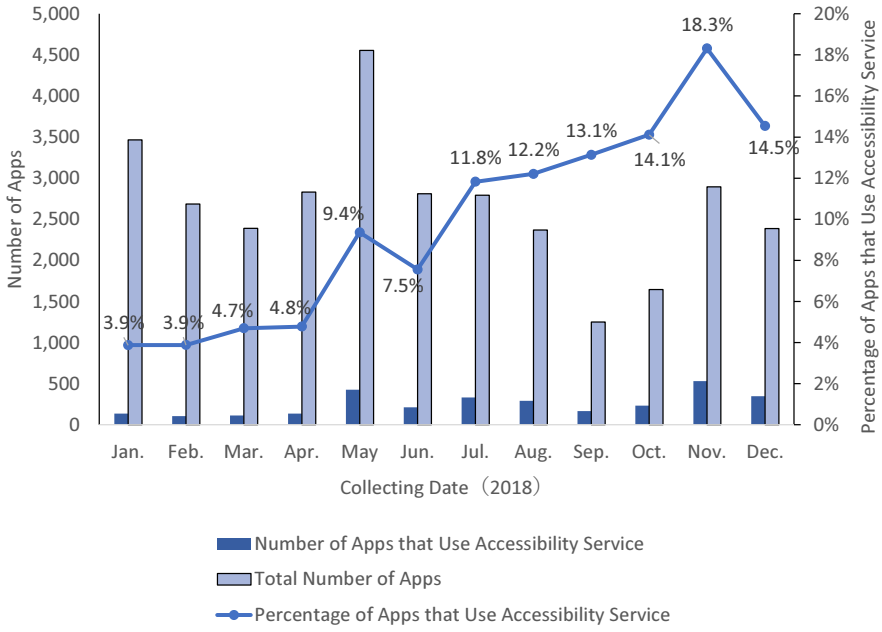

Fig. 5. Percentage of apps that use AS

Investigating the percentage of apps that use accessibility services. In Fig. 5, the AS usage rates for apps shared on Twitter are shown. The rate increased from 3.9% in January 2018 to 14.5% in December 2018, for an overall 3.7 fold increase in 2018. Therefore, we concluded that AS utilization in apps shared on Twitter was on the rise.

Notably, the 2018 AS usage rate for apps distributed on Google Play was reported to be 0.37% [8], while it was 9.4% (3,015 / 32,068) for the apps collected in our study. Thus, the utilization rate found here is quite high. This implies that the AS utilization rates for apps shared on Twitter is higher than that for apps on Google Play. We can thus infer that the proportion of apps that use AS increases for app distribution sources without any AS use restrictions such as those imposed by Google Play.

Analyzing the ratio of apps that use AS for suspicious activity. Figure 6 shows usage rates, classified by whether they correspond to suspicious apps. From Fig. 6, we observe almost no difference in the AS usage rate depending on whether or not an app is suspicious. Therefore, the use of AS cannot on its own be used to identify an app as malware. In fact, the number of suspicious and benign apps that use AS were very similar. However, as the ratio of suspicious apps to all those that use AS was high, about 52.8% (1,591 / 3,015), we can clearly state

Fig. 6. AS usage rates classified by whether they correspond to suspicious apps

that apps shared on Twitter that require AS should not be installed without considering the significant risk of malware.

4 Discussion

As described in Section 3.4, the overall prevalence of malware and overall AS usage rates have been increasing. Thus, the malware risk associated with apps distributed from third-party stores or developer websites has increased accordingly. These are common sources for apps that use AS, likely because Google Play prohibits the distribution of apps that use AS with any intention other than supporting app usage by people with disabilities. Figure 6 clearly indicates that apps that use AS are not necessarily suspicious. Therefore, all apps that use AS cannot automatically be blocked. Therefore, specific countermeasures against malware will become increasingly important for online security in the future.

We believe these countermeasures may include:

- Checking the app developer
  When installing an SNS distributed app, it is important to ensure that the app developer is trust worthy to avoid unintentionally installing malware.

Contaminated apps may be repackaged and distributed, so it is imperative to check with the original developers.
- Allow AS only when needed
  Confirm the reason that an app requires AS, before permitting the AS use. This is expected to reduce AS-exploiting attacks.
- Check permissions required with AS
  Users should check the permissions required with AS, as attacks could be prevented by denying these permissions that may leak information.

5 Related Work

5.1 Identifying AS Vulnerabilities

Kalysch et al. [12] showed that AS could be used to eavesdrop on sensitive user information. They also surveyed the top 1,100 apps on Google Play and found that 99.25% were vulnerable to this type of exploitation. Furthermore, Fratantonio et al. [10] showed that by combining AS with `SYSTEM_ALERT_WINDOW`, which grants permissions to display on top of other apps, an attacker could perform tasks such as clickjacking, keylogger, and password stealing. Additionally, McAfee [15] introduced Click Farm, which uses AS to send fake reviews from devices infected with malware. Collectively, these studies prove that AS can be abused and exploited, highlighting the importance of investigating AS usage among real Android Apps distributed on SNSs. In addition, unsuspicious apps use AS. Thus, it is important to make clear the differences in the AS usage ratios of suspicious and unsuspicious apps.

5.2 Survey of AS usage rates

Wenrui et al. [8] investigated apps distributed by Google Play, and Mohammad et al. [16] reported that 2,815 of these 4,155,414 apps used AS, after investigating their dataset. While these studies investigated AS usage in apps distributed from Google Play, they did not address those from other sources, such as SNS, third-party app stores, and developer websites.

6 Conclusion

We collected URLs from the Twitter streaming API, which is a representative SNS. We then accessed these URLs and collected the Android apps that could be downloaded to investigate apps distributed from sources other than Google Play. We created a data set of the 32,068 apps shared on Twitter in 2018 and showed that 49.8% of these apps are suspicious. Our results also indicate that the proportions of suspicious apps and apps that use AS had been increasing. Installing these apps is dangerous and not recommended. In addition, we showed some countermeasures. The 2018 AS usage rate for apps distributed on Google Play was reported to be 0.37% [8], but it was 9.4% for the apps collected in

our study. This implies that the AS utilization rates for apps shared on Twitter is higher than that for apps on Google Play. Further, the AS usage rates for suspicious apps and benign apps are very similar, demonstrating the increasing importance of malware specific countermeasures in the future of online security.

In future works, malware utilizing AS must be analyzed in detail, and specific countermeasures should be considered and outlined.

Acknowledgement

The research results have been achieved by "WarpDrive: Web-based Attack Response with Practical and Deployable Research InitiatiVE," the Commissioned Research of National Institute of Information and Communications Technology (NICT), Japan.

References

1. Android Developers: AccessibilityService, https://developer.android.com/reference/android/accessibilityservice/AccessibilityService, Last accessed 22 Apr 2020
2. Android Developers: Create your own accessibility service, https://developer.android.com/guide/topics/ui/accessibility/service, Last accessed 26 Apr 2020
3. Android Developers: build more accessible apps, https://developer.android.com/guide/topics/ui/accessibility, Last accessed 22 Apr 2020
4. Android Police: Google will remove Play Store apps that use Accessibility Services for anything except helping disabled users, https://www.androidpolice.com/2017/11/12/google-will-remove-play-store-apps-use-accessibility-services-anything-except-helping-disabled-users/, Last accessed 19 Apr 2020
5. Apktool, https://ibotpeaches.github.io/Apktool/, Last accessed 28 Apr 2020
6. AV-TEST: SECURITY REPORT 2018/19, https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2018-2019.pdf, Last accessed 24 Apr 2020
7. Bromium: Report: Social Media Platforms and the Cybercrime Economy, https://www.bromium.com/resource/report-social-media-platforms-and-the-cybercrime-economy/, Last accessed 19 Apr 2020
8. Diao, W., Zhang, Y., Zhang, L., Li, Z., Xu, F., Pan, X., Liu, X., Weng, J., Zhang, K., Wang, X.: Kindness is a Risky Business: On the Usage of the Accessibility APIs in Android . In: 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019). pp. 261–275. USENIX Association, Chaoyang District, Beijing (Sep 2019), https://www.usenix.org/conference/raid2019/presentation/diao
9. Doctor Web: Mobile malware review for 2017, https://news.drweb.com/show/review/?i=11671\&lng=en, Last accessed 30 Mar 2020
10. Fratantonio, Y., Qian, C., Chung, S.P., Lee, W.: Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop. In: 2017 IEEE Symposium on Security and Privacy (SP). pp. 1041–1057 (2017)

11. Gustuff: Weapon of Mass Infection, https://www.group-ib.com/blog/gustuff, Last accessed 30 Mar 2020
12. Kalysch, A., Bove, D., Müller, T.: How Android ' s UI Security is Undermined by Accessibility. In: Proceedings of the 2nd Reversing and Offensive-Oriented Trends Symposium. ROOTS ' 18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3289595.3289597, https://doi.org/10.1145/3289595.3289597
13. Kaspersky daily: No, you have not won two free airline tickets, https://usa.kaspersky.com/blog/free-airline-tickets-scam/11533/, Last accessed 19 Apr 2020
14. Kaspersky daily:Skygofree - a Hollywood-style mobile spy, https://usa.kaspersky.com/blog/skygofree-smart-trojan/14418/, Last accessed 30 Mar 2020
15. McAfee Mobile Threat Report Q1, 2020, https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf, Last accessed 25 Apr 2020
16. Naseri, M., Borges, N.P., Zeller, A., Rouvoy, R.: Accessileaks: Investigating privacy leaks exposed by the android accessibility service. Proceedings on Privacy Enhancing Technologies **2019**(2), 291 – 305 (2019), https://content.sciendo.com/view/journals/popets/2019/2/article-p291.xml
17. Twitter Developers: POST statuses/filter, https://developer.twitter.com/en/docs/tweets/filter-realtime/api-reference/post-statuses-filter, Last accessed 27 Apr 2020
18. WeLiveSecurity: Semi-annual balance of mobile security 2019, https://www.welivesecurity.com/2019/09/05/balance-mobile-security-2019/, Last accessed 25 Apr 2020