Android App Collusion

Ervin Oro
ervin.oro@aalto.fi

Tutor: Jorden Whitefield

Abstract

abstract

1 Introduction

jorden: Need a more general introduction to mobile computing. Things to mention would be that there are two leading phone OS's iOS and Android. Focus of this report is Android. Mention the Android Open Source Project (ASOP) and give an executive summary of project.

Android is estimated to be the most widely used operating system overall [1, 2], running on more than 2 billion active devices [3]. While this is not reflected by malware,

jorden

(OS)

jorden: What is not reflected by malware?

most of which still targets Windows, both the number and complexity of attacks against Android are increasing [4]. McAfee estimates that revenues for mobile malware authors could be in the billion-dollar range by 2020 [5].

~~Taking that into account,~~ Given the lucrative business opportunity for cyber criminals, ~~devices~~ defending Android against malware is an active area of research. Thanks to recent developments,

jorden: What developments? Research efforts? Don't need to write anything but add some citations.

exploit pricing and difficulty are growing [3], indicating that many common attacks can now be detected and protected against. However, ~~especially with increasing incentives,~~ malicious actors are looking for ways to bypass existing protections, and ~~some~~ a number of threats, ~~like~~ e.g., app collusion, can not be reliably detected nor defended against.

jorden

Add citations to these common attacks. Can you add a category of attack and a few citations per category?

App collusion is a secret collaboration between apps with malicious intent [6, 7].

jorden: citation 6 is strange here. From section two perhaps you could move up the quote/verbatim of the definition of collusion? Then with this general definition make it more specific to Android App Collusion.

Android system provides many documented unrestricted channels for apps to communicate with each other [8].

jorden: What is a channel? What types of channels exist (overt/covert)? I think it would be good to have a sentence on each channel type, and then add a forward reference to Section 3.

Additionally, apps can use wide array of covert channels

jorden: Speak about covert channel here without explaining.

to achieve undetected communication [!] . A malicious application that would be detected and blocked with state of the art security systems could be easily split into several applications,

Citation needed:

jorden: What could easily be split across multiple apps? It is not clear.

so that each of them would be categorized as benign when analysed separately [9].

Android app collusion is not a new concept [10], and multiple attempts have been made to develop a suitable detection system.

brief overview of existing approaches

jorden: Mention the figure that literature does, i.e., problem is 2^N, 2 apps and N other possibilities.

However, there still does not exists any robust and usable ways to detect app collusions. Most proposed solutions have large number of false positives due to inability to differentiate collusion from legitimate collaboration.

jorden: what's the difference between collusion and collaboration? Be explicit here.

Furthermore, the only known example of app collusion in the wild [11]

jorden: Will this papers method be explained prior to making this point? If not then I don't understand what is out of scope.

would be out of scope for most current works, as the exponential explosion of having to analyse all combinations of billions [!] of apps has forced authors to focus on a very narrow subset of threats. ~~Approaches attempting to overcome both of these issues have been infeasible thus far.~~ State of the art Android App Collusion detection techniques are limited in their approach, and thus app collusion remains an open research challenge.

Citation needed: number of apps in play store

This report aims to provide ~~a more general~~ an overview of ~~the topic.~~ app collusion on the Android platform. Section 2 discusses ~~the nature of~~ app collusions in general, Section 3 provides specific overview of methods that can be used for colluding on Android, Section 4 ~~briefly~~ describes known examples of colluding apps, and Section 5 gives a more in-depth systematic overview of approaches that have been taken to collusion detection ~~, as well as discusses their shortcomings.~~ and their limitations.

2 Description and definition of app collusion

The Oxford English Dictionary defines collusion as "Secret agreement or understanding for purposes of trickery or fraud; underhand scheming or working with another; deceit, fraud, trickery." [6].

jorden: I think this should be moved up to Section 1. This is a general definition and in section 2 onwards you should be more specific.

~~In this context, [7] defines~~ Asăvoae et al. [7] define app collusion as the situation where several apps are working together in performing a threat. From this, three ~~aspects~~ properties of collusion can be ~~derived:~~ defined:

jorden
I don't understand what you mean. Please clarify.

1. Collusion is secret. Conversely, apps working together in collaboration is common and encouraged practice when such collaboration is well documented [!] .

Citation needed:

2. Collusion is when all colluding parties are in agreement. A distinctly different but related concept is the "confused deputy" attack, where one app mistakenly exposes itself to other installed apps [!] .

Citation needed: Hardy, N.: The confused deputy:(or why capabilities might have been invented. ACM-SIGOPS Operating Systems Review 22(4), 36–38 (1988)

3. Collusion is with malicious intent. In the Android context, it would be the intention to violate one of its security goals,

jorden: What security goals? Should there be a list of these goals earlier or in section 1? I also wonder if it is worth mentioning OWASP Mobile top 10 security... https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

which are to protect application data, user data, and system resources (including the network) [12]. The Android Open Source Project also lists providing "application isolation from the system, other applications, and from the user" as a separate goal, but in this context, collusion would be when apps ~~work together~~ collude to break isolation with some third component, as for two willing parties there exist several legitimate communication channels [8].

jorden: What is a 3rd component? Is this an app or something else? Are two willing parties, two apps?

many things affect, including non technical

difficult to distinguish

3 Methods for colluding

Overt and covert channels

jorden: Anything here about Access Control policies? SEAndroid?

4 Examples of Android app collusion

~~A very widely cited example of collusion is an imaginary situation as follows.~~ Blah et al. [x] define an example of an Android app collusion as follows:

jorden: Make the points below a numbered list perhaps. Easier to follow. With a list of numbered steps I would then also think about if a nice diagram could be made, and numbered to correspond to each step described?

One app , APP_A, has access sensitive information, but no access to internet. Another app, APP_B, ~~on the other hand,~~ has access to internet, but no access to any sensitive information. Many authors [!] argue that in this case, one app could pass information to the other one, which could in turn then exfiltrate the information. Some authors [!] have extended this concept to also cover cases where data is passed to multiple apps before being finally exfiltrated. All current research focuses on detecting such situations.

Citation needed:

Citation needed:

jorden: The steps are not clear as it is mixed in with discussion. Need to spend some time separating these.

There is one known case of Android app collusion in the wild [11]. Interestingly enough, even though this example is also widely referred to [!], it does not follow the pattern described above.

Citation needed: list some references

jorden: This last paragraph is very informal and chatty. This is ok for the draft but would need to be rewritten.

short description of MoPlus SDK

5 Existing methods for detecting collusions

Bibliography

[1] Awio Web Services LLC, “Browser & platform market share,” Dec. 2018.

[2] StatCounter, “Operating system market share worldwide,” Dec. 2018.

[3] Android Open Source Project *et al.*, “Android security 2017 year in review,” Mar. 2018.

[4] AV-TEST GmbH, “Security report 2017/18,” Jul. 2018.

[5] McAfee, “Mobile threat report,” Apr. 2018.

[6] “collusion, n.” in *OED Online*. Oxford University Press, Dec. 2018.

[7] I. M. Asăvoae *et al.*, “Detecting malicious collusion between mobile software applications: the Android™ case,” in *Data Analytics and Decision Support for Cybersecurity*. Springer International Publishing, Aug. 2017, pp. 55–97.

[8] Android Open Source Project, “Application security,” 2019.

[9] H. Chen *et al.*, “Malware collusion attack against machine learning based methods: issues and countermeasures,” in *Cloud Computing and Security*, X. Sun, Z. Pan, and E. Bertino, Eds. Cham: Springer International Publishing, 2018, pp. 465–477.

[10] R. Schlegel *et al.*, “Soundcomber: A stealthy and context-aware sound trojan for smartphones,” in *Proceedings of the Network and Distributed System Security Symposium, NDSS'2011*, Jan. 2011.

[11] J. Blasco *et al.*, “Wild Android collusions,” in *VB2016*, Oct. 2016.

[12] Android Open Source Project, “Security,” 2019.