Divide-and-Conquer: Why Android Malware cannot be stopped

Dominik Maier Tilo Müller Mykola Protsenko
Friedrich-Alexander-Universität
Erlangen-Nürnberg, Germany
{*dominik.maier, tilo.mueller, mykola.protsenko*}*@fau.de*

***Abstract*—In this paper, we demonstrate that Android malware can bypass all automated analysis systems, including AV solutions, mobile sandboxes, and the Google Bouncer. We propose a tool called *Sand-Finger* for the fingerprinting of Android-based analysis systems. By analyzing the fingerprints of ten unique analysis environments from different vendors, we were able to find characteristics in which all tested environments differ from actual hardware. Depending on the availability of an analysis system, malware can either behave benignly or load malicious code at runtime.**

We classify this group of malware as *Divide-and-Conquer* attacks that are efficiently obfuscated by a combination of fingerprinting and dynamic code loading. In this group, we aggregate attacks that work against dynamic as well as static analysis. To demonstrate our approach, we create proof-of-concept malware that surpasses up-to-date malware scanners for Android. We also prove that known malware samples can enter the Google Play Store by modifying them only slightly. Due to Android's lack of an API for malware scanning at runtime, it is impossible for AV solutions to secure Android devices against these attacks.

***Keywords*-Android Malware, Mobile Sandboxes, AV, Google Bouncer, Static and Dynamic Analysis, Obfuscation**

I. Introduction

The time when we used mobile phones solely for placing calls are long gone. Today, modern phones are used more like tablet PCs and are generally called *smartphones*. Actually, they have become so smart that we do not only store our family, friends, and business contacts on them, but also check for emails, visit social networks, and even access bank accounts to transfer money. We handle both private and business life more and more over smartphones, and we entrust our personal data to them, including photos, GPS movement profiles, and text messages. As of today, the largest operating system for smartphones is Android with a market share of 81.9% [1]. This makes Android an ideal target for shady IT practices.

Android versions on older phones do not get updated quickly, and sometimes not at all. As a consequence, publicly available exploits can be targeted towards a large number of users for a long period of time. The *Android Market*, which is today re-branded to *Google Play Store*, has had its share of many malware installations in the past. Besides the Play Store, the open source nature of Android allows vendors to ship their devices with markets from other companies, like the *Amazon Appstore*, and also holds an option for users to install apps directly from the Internet or their computer.

A. Contributions

In the quest to understand the attack surface on current Android smartphones, we look at the Android ecosystem from an attacker's point of view. We explore ways for malware to evade sandboxes and static analysis tools, such as anti-virus scanners. While errors in normal apps can lead to exploitable code, our work revolves around malware that is delivered as an app, namely an Android APK file, and can hence be analyzed by security scanners.

To hide Android malware from automated analysis tools, we were able to create malware samples that behave benignly in the presence of analysis, and maliciously otherwise. Automated static analysis scans all code that is locally present in cleartext, while dynamic analysis executes the code and observes its behavior. To surpass both analysis techniques, we study *Divide-and-Conquer* attacks that (1) divide malware samples into benign and malicious parts, and (2) conquer security scanners by showing only benign behavior within an analysis environment.

In detail, our contributions are as follows:

- As part of this work, a fingerprinter for Android sandboxes has been developed called *Sand-Finger*. With Sand-Finger, we were able to gather information about ten Android sandboxes and AV scanners which are available today, such as *BitDefender* and the *Mobile Sandbox* [2].
- With the results of Sand-Finger, we show that Android malware can easily gather information to surpass current AV engines by ambivalent behavior. We provide proof-of-concept samples that use a combination of fingerprinting and dynamic code loading to enter the Google Play Store. We also revise the effectiveness of so-called *collusion attacks* [3], that split the behavior of an app in two apps with distinct permission sets. We classify both attacks as *Divide-and-Conquer*.
- Finally, we give an overview about sandbox improvements and countermeasures that have been previously proposed to help prevent Divide-and-Conquer attacks. We argue, however, why these improvements are difficult to implement on Android and why malware detection generally fails in practice today.

To sum up, we show that Divide-and-Conquer attacks not only evade sandboxes and static scanning, but also effectively surpasses all available security mechanisms for Android, including on-device AV scanners.

B. Related Work

How to surpass virtualization-based sandboxes on x86 has been shown by Chen et al. in 2008 [4]. A comprehensive security assessment of the Android platform has been given by Shabtei et al. in 2010 [5]. The security of automated static analysis on Android, especially concerning virus scanners, has recently been evaluated in 2013, for example, by Rastogi et al. [6], Fedler et al. [7], and Protsenko and Müller [8]. However, none of these approaches focus on bypassing dynamic analysis of automated Android sandboxes. The bytecode-based transformation system PANDORA [8], for example, complicates static analysis by applying random obfuscations to malware, but cannot surpass dynamic analysis because it does not change its behavior.

From an attackers point of view, semantics-preserving obfuscation that confuses static analysis is outdated due to the increasing use of Android sandboxes, like the Mobile Sandbox [2], and at the latest since the initial announcement of the Google Bouncer in 2012 [9]. A short time after the announcement of the Bouncer, it was proven that dynamic analysis cannot be entirely secure by Percoco and Schulte [10], as well as Oberheide and Miller [11]. Most recently, in 2014, Poeplau et al. have shown that dynamic code loading can bypass the Google Bouncer [12]. Poeplau et al. come to the conclusion that dynamic code loading is unsafe in general and must be secured on Android. However, obfuscation and packing techniques that bypass all Android sandboxes and AV scanners have not been investigated in a large-scale study yet.

C. Outline

The remainder of this paper is structured as follows: In Sect. II, we provide necessary background information for available anti-malware technologies on Android, such as AV scanners and sandboxes. In Sect. III, we describe our approach to fingerprinting of analysis environments by the tool *Sand-Finger*. In Sect. IV, we show that Android malware can easily bypass automated security scanners by acting according to the principle of Divide-and-Conquer. In Sect. V we discuss how this problem can be tackled in the future by looking closer at proposed countermeasures. Finally, in Sect. VI, we conclude and outline the potential direction of the future work.

II. Background Information

We now provide background information about automated malware analysis for Android. In Sect. II-A, we illustrate static analysis, pointing out some advantages and problems. In Sect. II-B, we focus on dynamic analysis.

A. Static Analysis

Static analysis is the art of analyzing code without actually running it. Static analysis tries to find out the control flow of an application in order to figure out its behavior [13]. It is also often applied for finding programming faults and vulnerabilities in benign applications, and is furthermore used to detect malicious behavior without having to run an application. This paper uses the term static analysis for every analysis that is performed statically as opposed to running code dynamically. Note that static analysis is often understood as the task of *manually* analyzing malware, which is very time consuming and requires specially trained analysts. The Divide-and-Conquer principle, which is discussed in this paper, cannot defeat manual analysis. However, as it is nearly impossible to perform manual analysis for all apps that are uploaded to the Play Store, we confine ourselves to automated analysis.

Currently, virus scanners on Android are not allowed to monitor running apps, but can only statically analyze them. Due to these restrictions, monitoring an app's behavior on real devices is close to impossible. Tests show that static virus scanners on Android can easily be evaded; proof has been released by various authors [8], [6], [7], [12]. For manual static analysis, sophisticated tools exist for both DEX bytecode and compiled ARM binaries. Contrary to that, considering automated static analysis on Android, native binaries are often black boxes for malware scanners since the tools focus on DEX bytecode. In native code, however, root exploits can open the doors for dangerous attacks.

B. Dynamic Analysis

As a solution to the shortcomings in automated static analysis, running code in a sandboxed environment received attention. By running code instead of analyzing it, automated tools can trace what an app really does. The logging files can then be rated automatically, or be examined manually. Although approaches for running software on *bare-metal* exist [14], dynamic analysis of mobile apps is almost exclusively done on virtualized environments. Virtual machines considerably simplify the design of sandboxes because (1) changes in a VM state can be monitored by the host system, and (2) a VM can be reset to its initial state after an analysis.

Sandboxes for desktop malware have existed for years, including the *CWSandbox* proposed by Willems et al. [15] as well as *Anubis* [16]. With the rise of smartphones, sandboxes for mobile systems were also proposed at that time [17], [18]. After the introduction of touch-centric OSs for smartphones, in particular iOS and Android, old smartphone systems quickly declined in sales and researchers started to adopt sandboxes for the new platforms. On the one hand, the openness of Android leaves the possibility to spread malware more easily, but on the other hand, thanks to this openness, it has proven to be easier to implement a sandbox for Android than for iOS [19]. Recent sandbox technologies are mixing static and dynamic analysis for the best results. As shown in our comparison of sandboxes in Sect. III-B, many sandboxes also use AV vendors to detect Android malware.

III. Fingerprinting Analysis Environments

In this section, we introduce our fingerprinting tool *Sand-Finger* (Sect. III-A), and give a comparative overview of available sandboxes (Sect. III-B).

A. The Sandbox Fingerprinter

Smartphones are usually embedded devices with built-in hardware that cannot be replaced and, as opposed to desktop PCs, they are aware of their specific hardware environment. Many different kernel and Android versions exist with various features for different hardware. Additionally, smartphones are actively being used and are not run as headless servers. In other words, users install and start different apps, interact with the GUI, lock and unlock the screen, move the device, and trigger numerous other system events. All this device information, including the specific hardware, location data, and user generated input, can be exploited to differentiate systems, which are used by humans, from automated analysis environments. Hence, this information can be exploited to detect dynamic analysis environments.

During the development of the Sand-Finger fingerprinter, we collected as much data as possible from sandboxed environments and submitted it to a server for evaluation. Building a VM close to actual hardware is a sophisticated task due to the large number of sensors, e.g., accelerometer, gyroscope, camera, microphone, and GPS. In short, we could not find any sandbox with hardware that is entirely indistinguishable from real hardware. In addition to hardware, malware can read settings and connections to find out whether it is running on a real device or not. For example, constraints like "the device needs at least n saved WiFi-networks", "the device must have a paired Bluetooth device", "the device must not be connected via cable", "the device IP must not match a specific IP range", and "the device must have at least n MB of free space", can easily be put in place and require dynamic analysis tools to emulate realistic environments.

Note that the examples given above are not far-fetched, because at the moment no emulator we analyzed has an active or saved WiFi connection. Also note that detection rates with a small number of false positives do not prevent malware from being spread. To get accurate fingerprint results, additional oddities can be taken into account. For example, the default Android emulator does not forward the ICMP protocol used by ping. Whenever an obvious problem, like the empty WiFi list or missing ICMP forwarding, gets fixed, malware authors will come up with new ideas. Instead, static analysis must be used to reach high code coverage and to skip the fingerprinting part of malicious apps [20]. However, according to our results, none of the tested analysis environments can fool simple fingerprinting and reach high control flow coverage.

The app that we developed for this work, namely Sand-Finger, sends an automatically generated JSON-encoded fingerprint to a remote web service via HTTPS. JSON *(JavaScript Object Notation)* is a human-readable data format for which many parsers exist. HTTPS is used to prevent the filtration of fingerprint data. While performing our tests, we noticed that some requests were filtered and never reached our server. Some of these sandboxes, however, could then be assessed without encryption.

When executed in a sandbox, the fingerprinter gathers information available on the virtual device. Around 100 unique values are extracted, depending on the platform version. The information includes static properties like the device "brand", "model", "hardware", "host name", "http agent", and a value named "fingerprint". Information about the underlying Linux system is extracted as well, such as "Kernel version", the "user", and the "CPU/ABI". On top of this static information, a lot of device settings are gathered, such as the timezone, the list of WiFi connections, and whether debugging is enabled. Additional data is gathered from the surroundings, namely the current phone's cell network status and neighboring cell info. Our analysis also checks if the device has been rooted by searching for the *su* binary. Moreover, it lists the directories of the SD card and the system's bin-folder and transmits all available timestamps.

According to our tests, it is very useful to know how long a system has already been running, since analysis systems are often reset. We also send a *watermark* back to our server, which is a constant string that is specified at the compile time of Sand-Finger to identify the origin of each test run. Thanks to this, the redistribution of malware samples between sandboxes and AV vendors can be traced. For example, the Mobile Sandbox passes on suspicious samples to companies like *BitDefender* and *Trend Micro*, if a sample was not marked as private.

Last but not least, two pings to `google.com` and our own server are performed on the command line. By using this test, we learned that the VM *QEMU*, in the default mode for the Android emulator, does not forward packages other than UDP and TCP. Without a ping reply, the app is presumably inside a default emulator, and hence, the values returned by ping are also added to our JSON-fingerprint. After a complete fingerprint is received by the server, it is stored inside a database together with the server's timestamp and the sender's IP address. Sand-Finger can also embody malware, that combines dynamic code loading against static analysis with an ambivalent behavior, making it invisible to automated static and dynamic testing. The client listens for server responses, and only if an expected response is received, does Sand-Finger extract its payload and run it using `System.load()`.

B. Comparing Android Sandboxes

In this section, we give an overview about available Android sandboxes and AV scanners, and compare these analysis environments based on the results of our fingerprinter Sand-Finger. Anti-virus companies often receive samples from sandboxes; for example, according to the identification of our watermarks, the Mobile Sandbox forwards samples to several online AV scanners, including BitDefender and Trend Micro. The IP of one fingerprint we received for the watermarked Sand-Finger sample that was submitted to the Mobile Sandbox belongs to the anti-virus company BitDefender, while another was sent from a system with the model *TrendMicroMarsAndroidSandbox*. Contrary to that, the Google Bouncer does not forward submitted samples to AV scanners. Moreover, the Google Bouncer does not

seem to connect to any internet service, including our web server waiting for fingerprints. Consequently, we could not reliably fingerprint the Google Bouncer (but we were still able to surpass it with simple Divide-and-Conquer attacks, as explained in Sect. IV-A).

As the JSON file generated by Sand-Finger has over 100 entries to identify a system, we focused on values in which all analysis environments greatly differ from real hardware. Altogether, we found about ten of such values, as listed in Fig. 1. The hardware we used as a reference value is the *Nexus 5* from Google, but we confirmed our results on other hardware, too. As a second reference value, we used the official emulator of the Android SDK. The meaning of the columns in Fig. 1 is:

- *Android Version*: The version number of Android.
- *CPU Architecture*: The actual CPU architecture. In some cases, the CPU/ABI differs from the *os.arch* type in Java, so the latter was used.
- *Resembles Hardware*: Some sandboxes try to adapt the virtualization environment to resemble real devices, mostly Google Nexus. However, others just use stock values or something completely different.
- *Successful Ping*: The official Android emulator cannot forward pings, only UDP and TCP packets are routed.
- *Correct Timestamp*: The timestamp in virtualized environments is oftentimes inaccurate, but accurate timestamps can be received from the Internet. This column lists if the timestamp is close to correct.
- *Hardware not Goldfish*: The virtual hardware of the Android emulator is called *Goldfish*. This column lists if the tested environment uses a different hardware.
- *WiFi Connected*: A real device is usually connected to the Internet either via cell-tower or WiFi, otherwise the fingerprint could not reach our server. Sandboxes are often connected via cables instead.
- *Cell Info*: If the device is a real phone, it has some kind of cell info describing the current mobile connection. Sandboxes often omit this info.
- *UpTime >10 min.*: As a normal phone or tablet runs the whole day, the probability of a device running longer than 10 minutes is high. Sandboxes are often reset after each analysis.
- *Consistent*: A consistent fingerprint from a real device does not show two different Android versions, or two different CPU architectures.
- *Untraceable*: A sandbox that gives away its own location or its IP address in its fingerprint is traceable; otherwise it is untraceable.

In the following, we discuss the results of ten fingerprinted sandboxes and AV scanners in alphabetical order: *Andrubis*, *BitDefender*, *ForeSafe*, *Joe Sandbox Mobile*, *Mobile Sandbox*, *SandDroid*, *TraceDroid*, *Trend Micro*, and two systems from unknown vendors. The unknown systems stem from the redistribution of malware samples among sandboxes. We received several fingerprints from these sandboxes, but could not identify their operator.

Andrubis: This is the mobile version of *Anubis*, a well-known sandbox for desktop PCs [16]. Andrubis performs static as well as dynamic analyses and allows uploading APK files. It also offers an Android app to submit APK files. A problem about the APK files, however, is the size restriction of seven MB [21]. Andrubis has an extensive feature set, including support of the native code loading. Like many other sandboxes, it is based on open source projects like *DroidBox*, *TaintDroid*, and *Androguard* [22]. The Andrubis sandbox, despite its usefulness when it comes to detection of malware, can easily be fingerprinted. Its environment is similar to the official emulator, and it even uses test keys (meaning it is self-signed). Another drawback is, that it still runs on Android version 2.3.4, probably because of its dependency on the popular analysis software TaintDroid [23]. As on most sandboxes, also on Andrubis, a ping did not reach its destination. The static IP address used by Andrubis ends at the Faculty of Informatics of the TU Vienna. Regarding this sandbox, we noticed strange behavior when an app closes: Andrubis just taps on the desktop wildly, launching the music app or executing a Google login, for example.

BitDefender: In the few weeks of our analysis, while we were working on the fingerprinter, the BitDefender sandbox apparently was updated. First, the VM was inconsistent, actually being a 4.1 Android that claims to be 4.4. Then the system changed, and since then consistently shows Android 4.3. This makes it the most recent Android version among the group of tested sandboxes. However, BitDefender is not the stealthiest environment because values like “Batmobile” for manufacturer and “Batwing” for the product can easily be fingerprinted. But note that as long as nobody fingerprints these values, they are more secure than the stock names from the Android emulator, because it is impossible to white-list all Android devices. Interestingly, BitDefender was the only sandbox that contained cell information to emulate a real phone. The static IP address used by this sandbox is registered for BitDefender.

ForeSafe: The ForeSafe sandbox not only offers a web upload but also a mobile security app for Android. After analysis, ForSafe shows an animation of the different UI views it passed while testing. It is not the only Sandbox that captures screenshots, but the only one with actually moving screenshots [24]. ForeSafe uses Android 2.3.4 and hence, probably builds on TaintDroid. Despite heavy fingerprinting and the possibility to execute native code, Sand-Finger was flagged as benign by this scanner. ForeSafe executed the sample a few times and was the only scanner with an uptime exceeding ten minutes. This is important as malware could simply wait longer than ten minutes before showing malicious behavior.

Joe Sandbox Mobile: This is a commercial sandbox which has a free version as well. Just like the sandboxes above, it is possible to upload APK files for automated testing. According to our tests, this sandbox performs very extensive tests, combining static and dynamic analysis, and it even detects some anti-VM techniques in malware. Roughly speaking, it is the most exotic sandbox in our test set. First, we found out that Joe Sandbox uses

	Sandbox	Android Version	CPU Architecture	Resembles Hardware	Successful Ping	Correct Timestamp	Hardware not Goldfish	WiFi Connected	Cell Info	UpTime >10 min.	Consistent	Untraceable
	Google Nexus 5	4.4.2	armv7l	✓	✓	✓	✓	✓	✓	✓	✓	-
	SDK Emulator (x86)	4.4.2	i686	X	X	✓	X	X	✓	X	✓	-
1	Andrubis	2.3.4	armv5tejl	X	X	X	X	X	X	X	✓	-
2	BitDefender	4.3	i686	X	X	✓	X	X	✓	X	✓	X
3	ForeSafe	2.3.4	armv5tejl	X	X	✓	X	X	X	✓	✓	✓
4	Joe Sandbox Mobile	4.2.1	i686	✓	✓	X	✓	X	X	X	✓	✓
5	Mobile Sandbox	4.1.2	armv7l	✓	X	✓	✓	X	X	X	✓	-
6	SandDroid	2.3.4	armv5tejl	X	X	X	X	X	X	X	✓	-
7	TraceDroid	2.3.4	armv5tejl	X	X	✓	X	X	X	X	✓	X
8	Trend Micro	4.1.1	armv7l	X	X	X	X	X	X	X	✓	X
9	Unknown ARM	4.1.2	armv7l	✓	X	X	X	X	X	X	X	✓
10	Unknown x86	4.0.4	i686	✓	X	X	✓	X	X	X	X	✓

Figure 1. Fingerprinting ten Android sandboxes with Sand-Finger. The eleven most revealing values (out of over 100) are listed here as examples.

the anonymous Tor network as proxy and is thereby untraceable. Second, it is the only sandbox that does not build upon the official Android emulator, but uses an x86 build of Android for the *Asus Eee PC*. In addition to the x86/ABI, Joe Sandbox specifies "armeabi" as "CPU2/ABI", meaning that Intel's *libhoudini.so* is probably installed to run binary translated ARM code. Most likely, Joe Sandbox Mobile is running on VMware; the build settings, however, are adapted to mimic a Galaxy Nexus. As it is based on a different virtualization technology, pings can reach their destination. Moreover, the build is rooted. The sandbox itself was generally hard to trick, e.g., some anti-virtualization techniques are detected.

Mobile Sandbox: Another advanced sandbox with many features in the making, like machine learning algorithms, is the Mobile Sandbox. It offers a web platform to submit malware samples and is based on a modified version of DroidBox for dynamic analysis. It also applies static analysis and monitors usage of native libraries as well as network traffic. The camouflage of Mobile Sandbox is the most advanced within our test set. Just by looking at its properties, it is indistinguishable from a Samsung *Nexus S*, even replacing the Goldfish hardware string with a real device string. Moreover, a telephone number was given, and it has a more recent Android version than most sandboxes we tested. Interestingly, this sandbox sent the most fingerprints over a time period of 20 minutes, meaning it restarted the app over and over, probably trying to maximize code coverage. Mobile Sandbox also applies some machine learning algorithm to the results and sent data. However, it shares some of the flaws all Android emulator-based sandboxes have, like the missing ping and a static IP address.

SandDroid: SandDroid is a Chinese online analysis tool [25]. This sandbox performs detailed static analysis which it presents graphically to the user. It is powered by Androguard and DroidBox, and allows to upload APK files of up to 20 MB. Besides its rich static analysis, it features a dynamic analysis and also gives a security rating. The fingerprint of Sand-Finger never reached our web server, so HTTP is probably sandboxed, too. Requests returned "302:Found". However after uploading a non-HTTPS version of Sand-Finger, the fingerprint results could simply be copied from SandDroid's traffic capturing. The timestamp inside the sandbox is wrong. According to the low Android version, SandDroid probably uses TaintDroid.

TraceDroid: The *TraceDroid Analysis Platform (TAP)* is the only sandbox that rarely performs static analysis and does not rate the results [26]. Instead, it packs all results in an archive that can then be downloaded from a web service. The data is useful, especially the control flow graphs. Regarding the fingerprint, it is interesting that many log files are stored on the SD card. TraceDroid uses *Monkey Executor* to generate random user input. The sandbox is easily traceable because the IP of the sandbox is equal to the static IP of the TraceDroid web server located at the VU University Amsterdam.

Trend Micro: Another anti-virus scanner that is used by the Mobile Sandbox and sends fingerprints to our web server is Trend Micro. The fingerprinted sandbox of Trend Micro has the model string *TrendMicroMarsAndroidSandbox* and its IP address is located in Japan (where this company is located). It is a sandbox running a rather recent

Android version, namely 4.1., and probably builds upon DroidBox. Interestingly, the user name is always "mars" and the SD card contains a PCAP-file and a file named *mars_conf.txt*. Hence, this environment can be fingerprinted with static strings.

Unknown ARM and x86: We received fingerprints from more AV engines that we could not match to a specific operator yet. These fingerprints were watermarked with the Sand-Finger samples that we submitted to the Mobile Sandbox. The Mobile Sandbox submits samples to more AV companies, including *ClamAV*, *Kaspersky*, *Sophos*, and others. The yet unknown ARM-based sandbox seems to be built on DroidBox and its IP address is located in China, pointing to a Chinese AV company. The sandbox is rooted but has no super user APK installed. While the fingerprint states the device is a *google/occam/mako*, thus mimicking the Google *Nexus 4*, the Android version in reality is 4.1.2 and is based on the Goldfish hardware. The unknown x86 sandbox is similar and also mimics a Nexus device with a higher fingerprint than the platform version. It claims to be the *google/soju/crespo*, i.e., a Nexus S, but only runs Android 4.0.4. Moreover, it claims to be an "armeabi-v7a" architecture although it is actually x86-based. This implies that, just as Joe Sandbox Mobile, this emulator has the ARM-to-x86 binary translator *libhoudini.so* installed. The x86 sandbox runs on a dedicated server in France.

C. Summary

All of the fingerprinted sandboxes in our test set have specific elements in common: (1) None of the analysis environments could send an ICMP ping packet except Joe Sandbox Mobile. (2) No sandbox has been up for more than ten minutes except the ForeSafe sandbox, which has been up for 15 minutes. This implies that no sandbox ran our Sand-Finger sample for more than 15 minutes. (3) None of the tested sandboxes returned a WiFi connection or stored any WiFi SSIDs. Only one sandbox was virtually connected to a cellphone network, but real devices can send back their fingerprints only if either a WiFi or a cellphone network is connected. (4) Most of the VMs are simply based on the emulator hardware Goldfish. (5) The timestamp was often incorrect. The timestamp, however, is clearly not the best sandbox detection method.

Considering current versions of the sandboxes we tested, we can conclude that using the uptime of a system in combination with its hardware string and a list of connected networks is a reliable indicator to differentiate between virtualized environments and real devices today. The false positive rate of this combination would already be minimal, possibly concerning only devices that were recently switched on. Of course, some of these indicators can be fixed by sandboxes in the future, but in turn the indicators used by ambivalent malware could be changed, as well. Hence, creating an Android sandbox that cannot be distinguished easily from real devices remains an interesting research topic for malware analysis.

IV. Defeating Analysis Environments

Insights from our fingerprinting tool Sand-Finger can be deployed to build ambivalent malware that behaves maliciously on real devices, but gets classified as benign in analysis environments. To defeat sandboxes in general, we focus on a technique that we call *Divide-and-Conquer* attacks. These attacks divide malware samples into a benign and malicious part, such that the malicious part is hidden from analysis by packing, encrypting or outsourcing of the code. As a consequence, the malware sample outwardly appears benign and hence, conquers the AV engine. Only when running on real devices, does ambivalent malware show its true behavior. These methods are especially effective, as they are hiding from both static and dynamic analysis. Malicious code segments are split in such a way that a sandbox is not aware of critical code.

Note that Divide-and-Conquer attacks are especially successful against restrictive operating systems like Android. On an unrooted Android phone, it is impossible for an app to scan another app during runtime, preventing on-device AV scanners from applying heuristics after a sample has unpacked itself. Contrary to that, proper virus scanners for Windows desktop PCs cannot be tricked as easily, as they run in a privileged mode and monitor the address space of third party apps at runtime. Indeed, many apps exist for Android that suggest effective AV scanning, but technically these apps can only scan a sample statically before runtime.

A. Dynamic Code Loading defeats the Google Bouncer

In this section, we describe how ambivalent malware can be combined with dynamic code loading to enter the Google Play Store. To enter the Play Store, an Android app must pass the Google Bouncer, which is the most prominent example of dynamic analysis for Android today.

With respect to dynamic code loading, Android imposes minimal restrictions inside an app (whereas Apple, for example, tries to restrict dynamic code loading). From an AV engine's point of view, the problem is that dynamic code loading is a common practice in many benign Android apps, too. Just like on Windows, Android apps are free to load whatever they please at runtime. On Windows, however, effective malware scanners can be installed that monitor other apps at runtime. For example, on Windows, the RAM of a program can be scanned for malicious contents when certain files are accessed. Hence, Windows malware has to struggle to trick the heuristics of AV scanners.

As opposed to this, on Android every app runs its own Dalvik VM instance that cannot be accessed by other apps. While this is, on the one hand, secure because apps are not allowed to alter other apps in a malicious way, *apps can do anything they have permissions for*. Once an Android malware sample defeats the Google Bouncer and enters the Play Store, e.g., based on ambivalent behavior, there is no effective authority that monitors an app while running on real devices. All an AV scanner can do on Android is to scan suspicious samples in advance, either statically, or by submitting them to a sandbox for dynamic analysis, as

discussed in the last section. This shortage makes Divide-and-Conquer attacks particularly easy against Android.

From a technical point of view, dynamically loaded code in Android can either be a DEX file or a native library. It can be downloaded from the Internet, copied from SD card, loaded from other apps packages or be shipped encrypted or packed in the apps resources [7], [27]. Apart from static analysis, which is naturally not able to find dynamically loaded code, dynamic analysis can be defeated when it is combined with fingerprinting techniques. Even a thoroughly scanned app can do anything after the scanner stops watching [12].

As we revealed during our analysis in Sect. III, it is currently impossible to fingerprint the Google Bouncer because it blocks any Internet traffic to custom servers (or does not execute uploaded APKs at all). This, however, has been different in the past. Oberheide and Miller were able to fingerprint the Google Bouncer in 2012 [11]. For example, they found out that the Google Bouncer is based on the Android emulator as it creates the file */sys/qemu_trace* during boot. As part of this work, the Google Bouncer was revisited. Since most devices are regularly connected to the Internet today, the missing Internet connection itself can be used as a fingerprint. That is, malware can disable malicious code on a missing Internet connection to evade dynamic analysis of the Google Bouncer. While cutting the Internet connection on a sandbox hinders fingerprinting, there is no way of executing malware that relies on connectivity to a command and control server.

For our tests, we equipped an otherwise benign app with a root exploit that is executed as soon as a certain command is received from a C&C server which is regularly contacted. For our first test, we included the root exploit as a plain native ARM binary into the app. Containing an executable root exploit, the app should be rejected based on static analyses of the Google Bouncer and not become available for download. As we expected, this variant was indeed classified as malicious and got rejected by the Bouncer soon after upload. As a consequence, the author's Google Play account was banned. Unfortunately, Google managed to link the banned account to all test accounts, although those were issued with fake identities, such that all of four developer accounts were closed at once. It is worth mentioning that the rejected sample was neither blacklisted by *Verify Apps* nor uploaded to the Google-owned *VirusTotal*, despite its being banned from the store.

Surprisingly, to confuse static analyses by Google's Bouncer, it turned out to be sufficient to zip the root exploit. Contrary to our own expectations, it was neither necessary to encrypt the root exploit, nor to dynamically download it from the C&C server. The Google Bouncer never contacted our server during its analysis, but the malicious APK became available for download on the Play Store a few hours after submission. To verify our approach, we downloaded the binary to a vulnerable Samsung Galaxy S3 device and ran the exploit. Note that, as our server always declined execution requests from unknown clients, there was no danger for Android users at any time. Only when the server permitted execution was the binary unpacked and executed. We also removed our sample from the Play Store within 24h after all tests had been applied, and we did not count any download of the app other than ours.

To sum up, Divide-and-Conquer apps hiding a root exploit can easily surpass widespread security checks for Android. Malware without root exploits, however, would still require declaring its permissions in the manifest file. But first of all, permissions alone cannot be consulted to classify malware due to numerous legitimate apps with massive permission overuse. And second, permissions can be hidden up to a certain point by another type of Divide-and-Conquer attacks, so-called *collusion attacks*, as described in the next section.

B. Collusion Attacks defeat VirusTotal Scanners

Automated analysis usually consists of a static and a dynamic part. In the static phase, sandboxes first identify granted permissions in the manifest file, scan through constants, embedded URLs, and possibly library calls. Afterwards, they execute the code, oftentimes tapping on the screen more or less randomly, and finally rate the sample. Commonly, Android permissions play a central role in this rating. By doing so, sandboxes can classify ordinary apps that come as single APK files. Malware, however, can also be divided into two complementary apps.

Due to the way Android's permission system works, an app can access resources with the help of another app, in such a way that it does not need to have all permissions declared in its own manifest. Those attacks are called *collusion attacks* [3]: Assuming the app with the desired permissions has already been trusted by the user on installation, another app can send the requests to perform a certain action by IPC mechanisms, like sockets or even covert channels. On a system as complex as Android, many covert channels can be found, for example shared settings. Even using the volume as a 1-bit channel has been proposed [28]. However, social engineering techniques have to be used to get a user to download the complementary app. But it is a common practice to provide additional app packages, like game levels, plug-ins, and more.

The collusion attack is effective against automated static and dynamic analysis alike, because automated analysis looks at only one app at a time. Also note that the collusion attack is currently the only method, besides root exploits, that can trick the analysis of permissions. To evaluate this approach, we used the open source malware *AndroRAT (Android Remote Administration Tool)*. This software connects to a server which then controls the whole Android system remotely. Many AV scanners detect the installation of AndroRAT as malware, namely 15/50 AV solutions on *VirusTotal*. Microsoft's Windows Defender even stopped the compilation of AndroRAT from source.

As part of this work, we created three variants of AndroRAT, called *AndroRAT-Welcome*, *AndroRAT-Pandora* and *AndroRAT-Split*. AndroRAT-Welcome simply includes

an anti-automation screen that must be touched by the user before the app continues. AndroRAT-Pandora is a obfuscated version of AndroRAT that we created with the transformation framework PANDORA [8] to confuse static analysis. AndroRAT-Split finally divides the app into two and performs a collusion attack as described above. Technically, we kept the main service class in one APK and added the activity classes to a second app. Thanks to Android's IPC mechanisms, this approach was straightforward to implement.

While the detection rate of the original AndroRAT sample on VirusTotal is 15/50, the detection rate of AndroRAT-Welcome declined to 9/15. Thus, six AV engines were either not able to bypass the welcome screen, or detecting the original version was based on static signatures, like a hash sum of the AndroRAT APK. While these detection rates are already fairly low, our goal was to decrease them further. The detection rate of AndroRAT-Pandora declined to 4/15, probably defeating static analysis systems in the first place. The detection rate of AndroRAT-Split finally declined to 0/15 for both of the separated apps, since none of them shows malicious behavior without the other.

We also tested the collusion attack against our test set of dynamic sandboxes. When analyzing with TraceDroid, a sandbox without static analysis, none of the malicious methods was detected. On sandboxes that combine static and dynamic analysis, however, only the activity app was rated as benign. This is plausible, as without the service class, the app has no harmful code. The service app was generally considered less harmful but still precarious. Hence, we could not surpass all sandboxes with a simple collusion attack. More advanced variants of AndroRAT-Split would be required that either split up the permissions into more apps, or combine the collusion attack with fingerprinting and dynamic code loading, as described before.

V. Countermeasures

We now discuss countermeasures that have been proposed against Divide-and-Conquer attacks in the literature.

A. Secure IPC Mechanisms for Android

As shown by collusion attacks in Sect. IV-B, IPC mechanisms on Android can be used to unite the permissions of two distinct apps. An app can use the permissions of another app without a user's approval. To tackle this problem, *XManDroid* [28] has been proposed by Bugiel et al. to patch the Android platform against the risk of privilege escalations [29]. XManDroid claims to also stop collusion attacks that communicate via channels other than Android's standard IPC mechanism.

B. Taming Dynamic Code Loading

The Android OS lacks a way to prevent Divide-and-Conquer attacks based on dynamic code loading. Fedler et al. proposed an anti-virus API for Android that allows certified scanners to monitor the file system and third party apps on demand [30]. For example, live change monitoring on the file system becomes possible similar to AV solutions on Windows. This API, if it were included in standard Android, could help to mitigate the risks of dynamic code loading. Fedler et al. also proposed several methods to secure the Android platform against the execution of malicious native code, especially root exploits [27]: An executable bit for Javas *System.load()* and *System.loadLibrary()* methods, a permission based approach where execution is granted per app, and the ability to load libraries only from specified paths.

A more sophisticated approach towards dynamic code loading, regarding both native code and bytecode, has been presented by Poeplau et al. [12]. Poeplau et al. suggest disallowing the execution of unsigned code entirely. They propose a patch to the Android system that allows multiple signing authorities and hence fits the Android ecosystem such that other companies, apart from Google, can still offer software in their own stores. If code is always required to be signed, so that only trusted code can be executed, on-device AV scanners would no longer be needed. Revising and signing all code of an app store, however, is obviously a bottleneck.

C. Improving Sandboxes

Many of the ideas that are used in mobile malware and mobile sandboxes, have been found on desktop PCs before. For the case of desktop PCs, Kirat et al. proposed to run malware analysis on *bare-metal* [14], i.e., on real devices rather than virtualized environments. To our knowledge, a similar approach has not been proposed or implemented for Android yet. From the hardware perspective, it would be feasible though, building upon the possibility to root devices and by communicating with an analysis PC via Android's debugging bridge.

Additionally, also for desktop PCs, Sun et al. proposed a system to detect virtualization resistant behavior in malware [31]. To this end, they measure the distance in behavior between running an app on real devices and running it inside VMs. A similar approach is taken by Lindorfer et al. [32]. Their tool figures out evasive malware by running in different environments. However, this tool does not compare the run to a real device, but compares runs on different VMs. In the future, similar approaches could also be taken on Android to tackle Divide-and-Conquer attacks and fingerprinting.

As opposed to the aforementioned improvements to run Android malware on bare-metal, another future research project could involve the implementation of a transparent malware sandbox in software. As seen in Sect. III, today it is rather simple to fingerprint available Android sandboxes. The implementation of a solution that is almost indistinguishable from real hardware remains an interesting future task. As a starting point, the fingerprinting tool SandFinger could be used as an opponent that must be defeated. Obvious flaws such as the missing ability to ping hosts on an unaltered QEMU emulator must be addressed. In addition, personal phone data could be faked, like sensor data, photos and contacts.

D. Machine Learning

Instead of playing the ongoing game of cat-and-mouse between AV scanners and malware authors, many researchers propose using machine learning and anomaly detection algorithms [33], [34]. In theory, a well-trained machine learning algorithm not only identifies known malware samples, or those matching certain heuristics, but also yields to correct results for yet unknown malware. As an advantage, machine learning algorithms evolve over time and can learn from a few known malware samples that were analyzed manually. With a growing set of analyzed apps, the detection rate of machine learning becomes more accurate. Hence, this approach is particularly suitable for sandboxes, and some of the sandboxes we tested already started to apply machine learning algorithms, like the Mobile Sandbox.

VI. Future Work and Conclusions

On-device AV scanners for Android have little possibilities of counteracting threats. Once a malware sample is installed, there are no possibilities to analyze it at runtime, i.e., no possibilities to detect its malicious behavior. As a consequence, the Google Bouncer was introduced to reject suspicious apps and to keep the Play Store clean. As shown by our work, however, the Google Bouncer can be surpassed by Divide-and-Conquer attacks today. Moreover, we have shown that most sandboxes in our test set can easily be fingerprinted, thus enabling attackers to create ambivalent malware.

A. Future Work

The fingerprinting tool Sand-Finger proposed in Sect. III, at the moment, can successfully fingerprint the tested analysis frameworks. In the future, however, these analysis frameworks might evolve and apply anti-fingerprinting techniques. In that case, Sand-Finger must be improved further. At this time, only one snapshot of the state of a device is taken. On actually moving devices, however, more information about the surroundings can be collected to reveal the variation of sensors over time. A huge amount of variable data, like the battery charge level, the signal strength, and the GPS localization, can be gathered. Possible future additions also involve the recording of sound samples and the comparison of subsequently taken camera photos. Moreover, there is still static data to be collected that we omitted so far, such as the screen resolution and pixel density.

B. Conclusions

As part of this work, ten unique sandboxes have been fingerprinted using a custom-built fingerprinter called *Sand-Finger*. Moreover, we argued that results of our fingerprinter can be applied to Android malware to perform so-called *Divide-and-Conquer* attacks that defeat automated analysis frameworks. To substantiate our approach, we demonstrated that dynamic code loading can be used to bypass the Google Bouncer, and successfully uploaded an Android root exploit to the Play Store. We also revised the effectiveness of so-called *collusion attacks* based on the AV detection rates of VirusTotal. Both dynamic code loading and collusion attacks can be classified as Divide-and-Conquer attacks.

To conclude, neither automated static nor dynamic analysis of Android APKs can be considered entirely secure today. Static analysis has no possibility of analyzing code which an app dynamically downloads or unpacks at runtime before execution. Dynamic analysis, on the other hand, can easily analyze code loaded at runtime, but it cannot analyze code which is not executed inside an analysis environment either. Hence, from an attackers point of view, the trick is to behave differently in analysis environments than on real devices. On desktop PCs, such malware samples are also known as *split-personality malware* [35]. But in contrast to desktop PCs, on Android such malware samples cannot be detected by on-device AV scanners because monitoring of third party apps at runtime is not possible.

Acknowledgments

The research leading to these results was supported by the *Bavarian State Ministry of Education, Science and the Arts* as part of the FORSEC research association.

References

[1] Gartner. (2013, Nov.) Gartner Says Smartphone Sales Accounted for 55 Percent of Overall Mobile Phone Sales in Third Quarter of 2013. [Online]. Available: http://www.gartner.com/newsroom/id/2623415

[2] M. Spreitzenbarth, F. C. Freiling, F. Echtler, T. Schreck, and J. Hoffmann, "Mobile-sandbox: Having a deeper look into Android applications," in *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, ser. SAC '13. New York, NY, USA: ACM, 2013, pp. 1808–1815.

[3] C. Marforio, H. Ritzdorf, A. Francillon, and S. Capkun, "Analysis of the Communication Between Colluding Applications on Modern Smartphones," in *Proceedings of the 28th Annual Computer Security Applications Conference*, ser. ACSAC '12. New York, NY, USA: ACM, Dec. 2012, pp. 51–60.

[4] X. Chen, J. Andersen, Z. Mao, M. Bailey, and J. Nazario, "Towards an understanding of anti-virtualization and anti-debugging behavior in modern malware," in *Dependable Systems and Networks With FTCS and DCC, 2008. DSN 2008. IEEE International Conference on*, June 2008, pp. 177–186.

[5] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer, "Google Android: A comprehensive security assessment," *IEEE Security and Privacy*, vol. 8, no. 2, pp. 35–44, Mar. 2010.

[6] V. Rastogi, Y. Chen, and X. Jiang, "Droidchameleon: Evaluating Android anti-malware against transformation attacks," in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '13. New York, NY, USA: ACM, 2013, pp. 329–334.

[7] R. Fedler, J. Schütte, and M. Kulicke, "On the effectiveness of malware protection on Android," Fraunhofer AISEC, Berlin, Tech. Rep., 2013.

[8] Mykola Protsenko and Tilo Müller, "PANDORA Applies Non-Deterministic Obfuscation Randomly to Android," in *8th International Conference on Malicious and Unwanted Software*, Fernando C. Osorio, Ed., 2013.

[9] H. Lockheimer. (2012, Feb.) Android and Security. Google Inc. [Online]. Available: http://googlemobile.blogspot.de/2012/02/android-and-security.html

[10] N. J. Percoco and S. Schulte, "Adventures in Bouncerland: Failures of Automated Malware Detection with in Mobile Application Markets," in *Black Hat USA '12*. Trustwave SpiderLabs, Jul. 2012.

[11] J. Oberheide and C. Miller, "Dissecting the Android Bouncer." Presented at SummerCon 2012, Brooklyn, NY, 2012. [Online]. Available: https://jon.oberheide.org/files/summercon12-bouncer.pdf

[12] S. Poeplau, Y. Fratantonio, A. Bianchi, C. Kruegel, and G. Vigna, "Execute This! Analyzing Unsafe and Malicious Dynamic Code Loading in Android Applications," in *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2014.

[13] A. Moser, C. Kruegel, and E. Kirda, "Limits of static analysis for malware detection," in *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, Dec 2007, pp. 421–430.

[14] D. Kirat, G. Vigna, and C. Kruegel, "Barebox: Efficient malware analysis on bare-metal," in *Proceedings of the 27th Annual Computer Security Applications Conference*, ser. ACSAC '11. New York, NY, USA: ACM, 2011, pp. 403–412.

[15] C. Willems, T. Holz, and F. C. Freiling, "Toward automated dynamic malware analysis using cwsandbox," *IEEE Security and Privacy*, vol. 5, no. 2, pp. 32–39, Mar. 2007.

[16] U. Bayer, I. Habibi, D. Balzarotti, E. Kirda, and C. Kruegel, "A view on current malware behaviors," in *Proceedings of the 2Nd USENIX Conference on Large-scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More*, ser. LEET'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 8–8.

[17] M. Becher and F. C. Freiling, "Towards dynamic malware analysis to increase mobile device security," in *Sicherheit*, ser. LNI, A. Alkassar and J. H. Siekmann, Eds., vol. 128. GI, pp. 423–433.

[18] M. Becher and R. Hund, "Kernel-level interception and applications on mobile devices," University of Mannheim, Tech. Rep., may 2008.

[19] T. Bläsing, L. Batyuk, A.-D. Schmidt, S. Camtepe, and S. Albayrak, "An Android application sandbox system for suspicious software detection," in *Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on*, Oct 2010, pp. 55–62.

[20] M. Spreitzenbarth, "Dissecting the Droid: Forensic Analysis of Android and its malicious Applications," Ph.D. dissertation, 2013, Friedrich-Alexander-Universität Erlangen-Nürnberg.

[21] M. Lindorfer. (2012, Jun.) Andrubis: A Tool for Analyzing Unknown Android Applications. iSecLab. [Online]. Available: http://blog.iseclab.org/2012/06/04/andrubis-a-tool-for-analyzing-unknown-android-applications

[22] Anthony Desnos. Androguard: Reverse engineering, Malware and goodware analysis of Android applications. [Online]. Available: http://code.google.com/p/androguard/

[23] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," in *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation*, ser. OSDI'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1–6.

[24] ForSafe, "Forsafe mobile security," Whitepaper, 2013. [Online]. Available: http://www.foresafe.com/ForeSafe_WhitePaper.pdf

[25] Botnet Research Team. (2014) SandDroid: An APK Analysis Sandbox. Xi'an Jiaotong University. [Online]. Available: http://sanddroid.xjtu.edu.cn

[26] V. Van der Veen, "Dynamic Analysis of Android Malware," Master Thesis, VU University Amsterdam, Aug. 2013. [Online]. Available: http://tracedroid.few.vu.nl/thesis.pdf

[27] R. Fedler, M. Kulicke, and J. Schütte, "Native code execution control for attack mitigation on Android," in *Proceedings of the Third ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*, ser. SPSM '13. New York, NY, USA: ACM, 2013, pp. 15–20.

[28] S. Bugiel, L. Davi, A. Dmitrienko, T. Fischer, A.-R. Sadeghi, and B. Shastry, "Towards Taming Privilege-Escalation Attacks on Android," in *19th Annual Network & Distributed System Security Symposium*, ser. NDSS '12, Feb. 2012.

[29] L. Davi, A. Dmitrienko, A.-R. Sadeghi, and M. Winandy, "Privilege escalation attacks on Android," in *Proceedings of the 13th International Conference on Information Security*, ser. ISC'10. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 346–360.

[30] R. Fedler, M. Kulicke, and J. Schütte, "An antivirus API for Android malware recognition," in *Malicious and Unwanted Software: "The Americas" (MALWARE), 2013 8th International Conference on*, Oct 2013, pp. 77–84.

[31] M.-K. Sun, M.-J. Lin, M. Chang, C.-S. Laih, and H.-T. Lin, "Malware virtualization-resistant behavior detection." in *ICPADS*. IEEE, 2011, pp. 912–917.

[32] M. Lindorfer, C. Kolbitsch, and P. Milani Comparetti, "Detecting environment-sensitive malware," in *Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection*, ser. RAID'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 338–357.

[33] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, ""Andromaly": a behavioral malware detection framework for Android devices," *Journal of Intelligent Information Systems*, vol. 38, no. 1, pp. 161–190, 2012.

[34] D. Arp, M. Spreitzenbarth, M. Hubner, H. Gascon, and K. Rieck, "DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket," in *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS)*, San Diego, CA, February 2014.

[35] D. Balzarotti, M. Cova, C. Karlberger, C. Kruegel, E. Kirda, and G. Vigna, "Efficient detection of split personalities in malware," in *In Proceedings of the Symposium on Network and Distributed System Security (NDSS)*, San Diego, CA, Mar. 2010.