Gaps and Future Directions in Mobile Security Research

Violetta Vylegzhanina, Douglas C. Schmidt, and Jules White
Vanderbilt University, Nashville, Tennessee, USA
{violetta.vylegzhanina, douglas.c.schmidt, jules.white}@vanderbilt.edu

Abstract

The ease with which security flaws in today's mobile devices can be exploited underscores the need for mobile security research. The advent of the Internet of Things (IoT)—where interacting heterogeneous devices surround mobile users and control features in buildings and automobiles—increases the need for robust security mechanisms that can withstand a range of attacks. This paper analyzes the current state of the mobile security research related to supporting the IoT. We survey existing approaches and identify gaps that motivate future research.

Categories and Subject Descriptors D.4.6 [*Operating Systems*]: Security and Protection

Keywords Mobile security; Android; Internet of Things, Research gaps.

1. Introduction

Mobile technology has become pervasive throughout the world. Worldwide sales of smartphones to end users reached 367.5 million units by 2014 [6]. The rapid adoption of mobile computing, however, motivates the need for more resilient security mechanisms. For example, a large portion of HTC devices were rendered vulnerable due to the logging tools used to collect information [3]. This vulnerability allowed any app having a permission to connect to Internet to gain access to user's private information.

This paper surveys current research on techniques to secure mobile devices, focusing on the Android platform, which exceeds 80% of the mobile device market share [6]. Likewise, the growing interest in IoT may significantly increase the reach of mobile devices, which are estimated to reach 26 billion devices by 2020 [5] and will be applied to a range of domains, including home automation applications [1] that will enable mobile devices to interact with many home appliances. We therefore also discuss the IoT, which raises new security concerns and motivates future research directions.

2. Current Mobile Security Research

This section surveys existing approaches for addressing security vulnerabilities and malicious behaviors on Android devices. We categorize whether the approaches can find potential vulnerabilities or actual attacks, detect them, or also prevent them at runtime. We also consider whether the approaches detect the leakage of private information within a single app component, between app components, or between different apps. Moreover, we analyze whether the approaches differentiate between user intended and unintended privacy leaks.

Our survey also examines whether approaches identify cross-process attacks via the Android Binder IPC, standard Android Linux kernel inter-process communication (IPC), hijacking user input, and network channels [4]. Since many malware variants use IPC channels on mobile platforms to perform *permission (privilege) escalation* attacks (such as *confused deputy* and *collusion*) we analyze whether current approaches address this area to detect (and ultimately) prevent permission escalation attacks. In addition, we analyze the *precision* of each approach, *i.e.*, its ability to accurately detect an attack or a vulnerability, with the minimal rate of false positives or false negatives. Finally, we explore whether the approaches just address security on a device or whether they also consider the environment a device interacts with, which is an important consideration in IoT deployments.

3. Research Gaps

Fig. 1 presents a taxonomy that helps to visualize the current research space in mobile security, as well as detect gaps across its multiple dimensions. The space enclosed by the blue line indicates

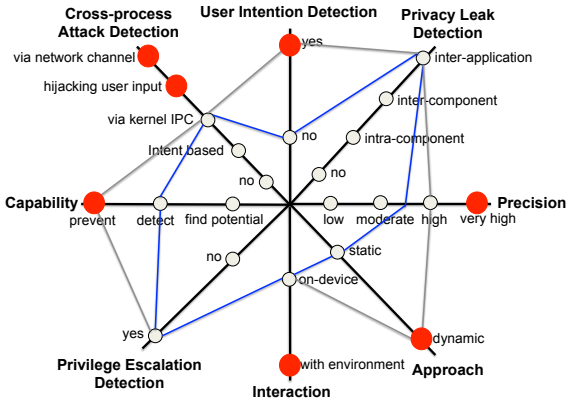

Figure 1. Taxonomy of the Research Space in Mobile Security.

the areas where the current research has mostly concentrated. Conversely, the space enclosed by the grey line represents the areas that are only partially addressed by the current research. Highlighted in red are the research gaps we identified, *i.e.*, these are areas that the current research have addressed either insufficiently or appears not to have addressed at all.

As shown in Fig. 1, the surveyed techniques can detect (and only a few can prevent) inter-application privacy leaks. The majority of these techniques, however, do not consider whether the leakage of a sensitive information is user intended or not. Likewise, most of these approaches detect privilege escalation attacks, but they limit

MobileDeLi '15, October 26 2015, Pittsburgh, PA, USA.

http://dx.doi.org/10.1145/nnnnnnn.nnnnnnn

themselves to Intent-based and kernel IPC-based cross-process attacks, and thus do not consider the trickiest cross-process attacks involving network channel and user manipulations.

Most existing approaches are static, and thus only able to detect a potential vulnerability or attack. Only a limited number of techniques uses dynamic analysis to actually prevent an attack at runtime. In addition, all approaches surveyed incur drawbacks that limit their precision, *e.g.*, FlowDroid [8] is oblivious to multithreading and thus cannot properly resolve reflective calls.

None of the approaches consider the environment a mobile device interacts with. For example, TaintDroid [7] monitors the leakage of sensitive information from a mobile phone, but it cannot detect where this information is being sent once it leaves a device. Such considerations are essential in IoT deployments.

4. Future Research Directions

Our survey of existing research on mobile security identified several fruitful future research directions, including developing dynamic solutions to prevent cross-process privilege escalation attacks that involve user manipulations and intermediate network services [4]. For example, a malicious mobile app can exploit user manipulations by displaying a UI that is overlaid on top of the victim's app UI. A user may touch specific buttons that trigger the delivery of touch events to the malicious app via IPC. The malicious app then forwards these events to victim's app by signaling to the event dispatch mechanism that its process cannot handle the events. As a result, the events are forwarded to the UI elements of a victim's app that the malicious app wants to manipulate.

Likewise, in a network channel attack, a malicious app uses device-specific data to send a message that appears to originate from another process on a device to a network service. The network service believes that the message comes from another on-device process and sends a response to this process. When a benign on-device process receives the message, it triggers an action that is desired by a malicious app. These types of sophisticated cross-process attacks are not adequately addressed by current research.

Another promising research direction is addressing mobile security while simultaneously taking into account the environment in which a mobile device interacts. This work is especially useful as IoT deployments proliferate, *e.g.*, in the context of home automation. Some important research questions that should be addressed include:

- When controlling an appliance at home, how are the user's actions protected to ensure no malicious app overtake the controls without the user's intention?
- When checking the status of controls at home, what policies and mechanisms can ensure the information presented to a user is trustworthy and not presented by a malicious process?

Another example that requires robust mobile security solutions are a mobile device's interactions with its environment, *e.g.*, where a mobile phone is paired with a car and is also senses information from a driver's pace maker. If a driver starts feeling ill, the pace maker sends this information to the phone, which in turn directs the car to pull over, unlock the doors and dial a medical emergency number. It may be possible, however, that a malicious driver behind takes control of the car in front and directs it to stop to conduct a robbery.

Security considerations become especially highly important in such scenarios where a malicious process on a mobile device may not just steal private data or inject malicious data, but can actually physically affect user safety or security. The future research directions outlined earlier can be combined to develop security solutions that consider the environment in which devices operate and interact to dynamically monitor IPC flows to detect and thwart cross-process privilege escalation attacks. The types of attacks to consider should include even the most sophisticated ones, such as attacks via intermediate network services or those involving user manipulations.

Another emerging future research area is the growing fragmentation of Android software (and hardware) [2]. On the one hand, this fragmentation underscores the flexibility of the Android platform, which can be customized to fit particular needs, including being embedded into devices with very small form factors. On the other hand, however, fragmentation can create novel opportunities for exploits that the stock Android OS does not possess, requiring a need to protect many various versions of Android OS that are created.

5. Concluding Remarks

This paper surveyed the current research on mobile security. We identified research gaps and proposed possible future research directions, especially as IoT deployments become more pervasive. The major research directions we identify include developing and evaluating

- Dynamic security tools to prevent cross-process privilege escalation attacks involving user manipulations and intermediate network services.
- Security solutions for mobile devices as they interact with their environment.
- Protective tools concerning Android platoform fragmentation.

References

[1] Android Home. *Google announces Android@Home framework for home automation*. URL http://www.engadget.com/2011/05/10/google-announces-android-at-home-framework/.

[2] InformationWeek. *8 Android Security Concerns That Should Scare IT*, March 2015. URL http://ubm.io/1xnfmTq.

[3] A. Russakovskii. *Massive Security Vulnerability In HTC Android Devices (EVO 3D, 4G, Thunderbolt, Others) Exposes Phone Numbers, GPS, SMS, Emails Addresses, Much More*. URL http://bit.ly/1FO2W81.

[4] J. White. *CAREER: Automated Detection and Prevention of Cross-process Attacks on Mobile Platforms*. Dept. of Electrical and Computer Engineering, Virginia Tech, 2012.

[5] Gartner14. *Gartner Says the Internet of Things Will Transform the Data Center*. Gartner, March 2014. URL http://www.gartner.com/newsroom/id/2684616.

[6] Gartner15. *Gartner Says Smartphone Sales Surpassed One Billion Units in 2014*. Gartner, March 2015. URL http://www.gartner.com/newsroom/id/2996817.

[7] W. Enck, P. Gilbert, S. Han, V. Tendulkar, 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. *ACM Transactions on Computer Systems*, 32(2):5:1–5:29, June 2014.

[8] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. Le Traon, D. Octeau, and P. McDaniel. Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps. In *Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI '14, pages 259–269, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2784-8. .