ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Effective Risk Communication for Android Apps

Akshay Jaypatre, Vikas Chavan, Sonali Shivpuje, Prof Amarnath Patil.

Department of Computer Engineering, G.S. Moze College of Engineering, Balewadi, Pune, MH, India

ABSTRACT: The popularity and advanced functionality of mobile devices has made them attractive targets for malicious and intrusive applications (apps). Although strong security measures are in place for most mobile systems, the area where these systems often fail is the reliance on the user to make decisions that impact the security of a device. Android's current risk communication mechanism relies on users to understand the permissions that an app is requesting and to base the installation decision on the list of permissions. Previous research has shown that this reliance on users is ineffective, as most users do not understand or consider the permission information as it required technical knowledge. Also there is security concern known as Pileup flaws, in which an installed app can get the extra permission without user content while updating the app or OS. We propose a system to provide Summary Risk communication to user in friendly manner which is easy to understand and also provide notifications for Pileup flaws

KEYWORDS: Risk communication, Mobile, Malware, Mobile Security

I. INTRODUCTION

IN recent years smart mobile devices have become pervasive. More than 50 percent of all mobile phones are now smart phones [1], and this statistic does not account for other devices such as tablet computers that are running similar mobile operating systems. According to Google, more than 400 million Android devices were activated in 2012 alone. Android devices have widespread adoption for both personal and business use. From children to the elderly, novices to experts, and in many different cultures around the world, there is a varied user base for mobile devices. The ubiquitous usage of these mobile devices poses new privacy and security threats. Our entire digital lives are often stored on the devices, which contain contact lists, email messages, passwords, and access to files stored locally and in the cloud. Possible access to this personal information by unauthorized parties puts users at risk, and this is not where the risks end. These devices include many sensors and are nearly always with us, providing deep insights into not only our digital lives but also our physical lives. The GPS unit can tell exactly where you are, while the microphone can record audio, and the camera can record images. Additionally, mobile devices are often linked directly to some monetary risks, via SMS messages, phone calls, and data plans, which can impact a user's monthly bill, or increasingly, as a means to authenticate to a bank or directly link to a financial account through a 'digital wallet'. This access means that any application (or app) that is allowed to run on the devices potentially has the ability to tap into certain aspects of the information. In the benign case the access is performed to provide Useful functionalities, but in other scenarios it may be used to collect a significant amount of personal information and even as a means to have some adverse impact on a user. Furthermore, the line between benign and malicious is often fuzzy, with many apps falling into a gray area where they may be overly invasive but not outright malicious. Compared to desktop and laptop computers, mobile devices have a different paradigm for installing new applications. For computers, a typical user installs relatively few applications, most of which are from reputable vendors, with niche applications increasingly being replaced by web based or cloud services. In contrast, for mobile devices, a person often downloads and uses many apps from multiple unknown vendors, with each app providing some limited functionality. Additionally, all of these unknown vendors typically submit their apps to a single or several app stores where many other apps from other vendors may provide similar functionality. This different paradigm requires a different approach to deal with the risks of mobile devices, and offers distinct opportunities. The present research focuses on the Android platform, because of its openness, its popularity, and the way in which Android handles access to sensitive resources. In Android an app must request a specific permission to be allowed access to a given resource. Android warns the user about permissions that an app

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

requires before it is installed, with the expectation that the user will make an informed decision. The effectiveness of such a defense depends to a large degree on choices made by the users. Indeed whether an app is considered too invasive or not may depend on the user's privacy preference. Therefore, an important aspect of security on mobile devices is to communicate the risk of installing an app to users, and to help them make a good decision about whether to install a given app.

II. LITERATURE SURVEY

2.1 Security and Usability

Information security and privacy are issues for users of all types of electronic devices. With regard to smart phones, users are more concerned with privacy on their phones than on computers, and they especially worry about the threat of malicious apps [8]. However, although people are shown the permissions an app requests before it is installed, they do not understand them well [8], [10]. Among the recommendations made by Chin et al. [8] was to provide "new security indicators in smartphone application markets to increase user trust in their selection of applications". The addition of new security indicators not only may decrease the frequency of risky user behaviors, but it may also facilitate the use of smart phones for online transactions by more individuals. Staddon et al. [8] found that user's engagement and perception of privacy are strongly associated, and people spend more time in social networks when they are less concerned about their privacy. This relation may be true as well for app installation. People will not use security features properly if they fail to understand the purpose of the features or the information on which their decisions should be based. The security features also will not be used if the users find the features intrusive or too difficult to master. Therefore, interactions between users and the systems need to be simple and user friendly [9]. Despite this need, studies of various security and privacy measures have shown their usability is typically deficient [9], which often leads to user resistance [10], [8]. Studies have also demonstrated that usability can be improved by systematically studying the human information-processing requirements associated with effective use of the measures and incorporating the resulting knowledge into the designs [8], [8], [9]. Usability of security mechanisms has been studied in contexts other than mobile platforms. Biddle et al. [10] laid out some general ground rules concerning the content of security dialogs; e.g., avoid unfamiliar terms, lengthy messages and misleading or confusing wordings. Schwarz and Morris [10] proposed that web search results be augmented with indicators for helping people assess the degree of trustworthiness of web sources. They found that adding such information to search results is useful, but less so when the information is added to web pages, presumably because the content, look, and feel of the page dominate the user's judgment. Cranor et al. [10] developed Privacy Bird specifically with the intent to signal to users whether web sites match their privacy preferences. It provides a red bird icon when visiting a site if the privacy policy does not match the user's preferences and a green bird icon if it does match. They extended this idea to web searches with Privacy Finder, which provides similar information when a search engine returns the results of a query [10]. Studies have found the summary privacy information provided by Privacy Bird (and Privacy Finder) to be effective at improving participant's privacy practices [9], [10]. Egelman et al. [8] directly examined the influence of privacy indicators, which showed privacy ratings of online vendors from low to high as one to four green boxes in a row of four that were green), on Internet users' browsing and purchasing decisions. When the privacy indicators were presented alongside the search results, participants who chose to visit only a single website paid more money for a higher level of privacy. However, when this information was provided after a website had been selected, participants did not alter their initial decision to purchase from a cheaper website with lower level of privacy. Finally, Kim et al. [9] proposed the Online Trust Oracle approach for communicating information regarding programs for Windows desktop environment, the interface lists information regarding why a file may be harmful on the left side of the dialogue and why a file may be safe on the right side of the dialog, and it also uses three colors to distinguish programs of different degrees of risk. To summarize, these studies all suggest that presenting high-level summary risk information will be beneficial, particularly if it is displayed early in the selection process.

2.2 Risk Perception and Decision Making

Users make many decisions that affect the overall state of security of any system with which they interact. For security and privacy, most of these decisions relate to the risk to which the individual or system is exposed. Consequently, improving security decisions by users involves taking into consideration factors that influence a user's risk perception

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

and decision making [9]. Also relevant is risk communication, Which refers to conveying risk to users in a way that allows accurate risk perception and, hopefully, better choices of actions with regard to the actual risks involved [9]. One factor that has been shown to be critical in risky decisions is the way in which losses and gains are framed. With the exact same scenario, the way in which the information is
presented can significantly influence the decision-maker's choice. People are risk-averse when the framing highlights positive outcomes, but risk-seeking when it highlights negative outcomes [9], [8].

2.3 Overview of Android Security

The Android system's in-place defense against malware consists of two parts: sandboxing each app, and warning the user about the permissions that the app is requesting. Specifically, each app runs with a separate user ID, as a separate process in a virtual machine of its own, and by default does not have the ability to carry out actions or access resources which might have an adverse effect on the system or on other apps without requesting permission to do so from the user. The permissions consist of capabilities that an app may require such as accessing geo-location information, sending text messages, receiving text messages, and many more. In total there are around 130 unique permissions in Android depending on the version. Each permission has a name, category, and a high level description of what it allows. An example is the "FULL NETWORK ACCESS" permission in the "NETWORK COMMUNICATION" category with its description as "Allows the app to create network sockets and use custom network protocols. The
browser and other apps provide means to send data to the internet, so this permission is not required to send data to the internet." The risk communication mechanism for permissions relies on the assumption that a user understands and makes an informed decision when presented with a list of permissions requested by an app. For most permissions, risks must be inferred because they are not explicitly stated in the description [8]. When browsing a specific app from the Google Play website, a user is able to see details about the app via a series of tabs at the top of the page. In addition to an overview, user reviews, and 'what's new' section, one of these tabs presents the permission information. When an app has been selected for installation, permissions are displayed before the user confirms installation. When app installation is performed directly on the device, there is a Play Store app which allows users to find and install new apps. The options and information are the same as on the website, with the primary difference being that the screen may be smaller and so when information is displayed, including permissions, a user has to make more of an effort to view that information.

2.4 Risk Communication in Android

Studies have shown that Android users tend to ignore the permissions that an app requests [8], [10], [10], and there are many reasons for ignoring them. Permission descriptions are seen as confusing or difficult to understand by many users [10]. Furthermore, nearly all apps request permissions with some associated risk. Felt et al. [10] analyzed 100 paid and 856 free Android apps, and found that "Nearly all applications (93% of free and 82% of paid) ask for at least one 'Dangerous' permission, which indicates that users are accustomed to installing applications with Dangerous permissions. The INTERNET permission is so widely requested that users cannot consider its warning anomalous. Security guidelines or anti-virus programs that warn against installing applications with access to both the Internet and personal information are likely to fail because almost all applications with personal information also have INTERNET"(p. 6). The implication is that since most apps are considered to be benign, and users see very similar warning information for all apps, the users generally ignore the warnings. Unless a user is highly concerned with security and privacy, and regularly examines the permissions as part of her app selection process, then most likely she has already made the decision to install the app before being presented with the permission information. In Android, a user is able to install the app by clicking a button to 'install' or 'buy' the app. Only then is the user forced to view the permissions that the app is requesting in a final confirmation screen. However, by this point the user has already made the decision to install the app, and this extra warning is often seen as a nuisance and ignored. There is a parallel between Android's permission warning and Windows' User Account Control (UAC). Both are designed to inform the user of some potentially harmful action that may occur. In UAC's case, this happens when a process is trying to elevate its privileges in some way, and in Android's case, this happens when a user is about to install an app that will have all the requested permissions. Recent research suggests the ineffectiveness of UAC in enforcing security. Motiee et al. [10] reported that percent of their survey participants ignored the UAC dialog and proceeded directly to use the administrator account. Microsoft itself concedes that about 90 percent of the prompts are answered as "yes", suggesting

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

that "users are responding out of habit due to the large number of prompts rather than focusing on the critical prompts and making confident decisions" [9]. According to Fathi [9], in the first several months after Vista was available for use, people were experiencing a UAC prompt in 50 percent of their "sessions" - a session is everything that happens from logon to logoff or within 24 hours. With Vista SP1, and over time, this number has been reduced to about percent of the sessions. This reduction suggests that UAC has been effective in incentivizing software developers towrite programs without elevated privileges unless necessary. The difference between Android and UAC is that UAC encourages the developer to work with fewer privileges since this will lead to a smoother user experience. However, with Android there is no obvious feedback loop to the developer at this point other than the fact that a small fraction of the user reviews may complain about an app being over-privileged. An effective risk communication approach for Android could provide an incentive for developers to reduce the number of permissions requested by apps, similar to UAC's impact with Windows software developers. By highlighting requested permissions of apps, such risk communication could potentially change user behavior and drive consumption to apps with fewer permissions, thereby creating a feedback loop to developers and having a positive effect on the app ecosystem.

2.5 Privilege Escalation through Mobile OS Updating

Mobile operating systems (OSes) are evolving quickly. Every a few months, major updates or new overhauls of entire systems are made available, bringing to mobile users brand new apps and enriched functionalities. Conventional wisdom is that such a vibrant ecosystem benefits the phone users, making Mobile systems more usable and also more secure, through timely plugging loopholes whenever they are found. Indeed, for years, major smartphone vendors and system/software developers leverage convenient updating mechanisms on phones to push out fixes and enhance existing protection. However, with such updates becoming increasingly frequent (e.g., every 3.4 months for all Android major updates) and complicated (e.g., hundreds of apps being added or replaced each time by hundreds of different Android device vendors), questions arise about their security implications, which have never been studied before. Security hazards that come with software updates have been investigated on desktop OSes. Prior research focuses on either compromises of patches before they are installed on a target system or reverse-engineering of their code to identify vulnerabilities for attacking unpatched systems. The reliability of patch installation process has never been called into question. For a mobile system, this update process tends to be more complex, due to its unique security model that confines individual apps within their sandboxes and the presence of a large amount sensitive user data (e.g., contacts, social relations, financial information, etc.) within those apps' sandboxes. Every a few months, an update is released, which causes replacement and addition of tens of thousands of files on a live system. Each of the new apps being installed needs to be carefully configured to set its attributes within its own sandboxes and its privileges in the system, without accidentally damaging existing apps and the user data they keep. This complicates the program logic for installing such mobile updates, making it susceptible to security-critical flaws. Also adding to this hazard is fragmentation of mobile OSes, particularly Android, and the most popular system. Multiple official Android versions (from Froyo to Jellybean) co-exist in the market, together with thousands more customized by different vendors (Samsung, LG, HTC, etc.). Those versions are slowly but continuously updated to higher ones, leaving the potential adversary a big window to exploit their update installation process, should its security flaws be uncovered. With the importance of this issue, little has been done so far to understand it, not to mention any effort to mitigate the threat it may pose.

III. PROPOSED SYSTEM

In the below block diagram Permission reader read the permissions required by all apps installed on the device and Controller stores this information in permission database for future reference. Controller also sends this information to Notifier which sends the information in readable format to UI. Controller keeps on waiting for any apps update, when any app get auto updated, controller gets the notification. On getting notification it reads the permission required by the app/s and send the information to Diff Computer. Diffcomputer then compares the info with the information stored in the permission database and if finds any difference in app permission before and after update, it activates the Notifier to send the notification to user regarding the auto permission elevation. User then can make the decision accordingly. If user decides to uninstall the app then controller uninstalls the app from device.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

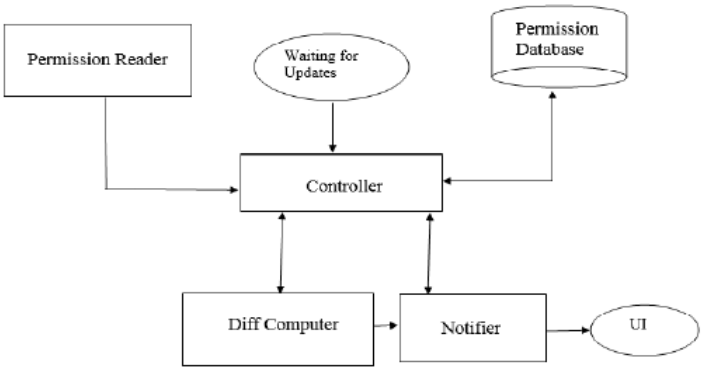

Fig 1. Architecture of proposed system.

Reduce the false ratio of the system. Increase the performance for android system with maximum accuracy.The ubiquitous usage of these mobile devices poses new privacy and security threats. Our entire digital lives are often stored on the devices, which contain contact lists, email messages, passwords, and access to files stored locally and in the cloud. Possible access to this personal information by unauthorized parties puts users at risk, and this is not where the risks end. These devices include many sensors and are nearly always with us, providing deep insights into not only our digital lives but also our physical lives. The GPS unit can tell exactly where you are, while the microphone can record audio, and the camera can record images. Additionally, mobile devices are often linked directly to some monetary risks, via SMS messages, phonecalls, and data plans, which can impact a user's monthly bill, or increasingly, as a means to authenticate to a bank or directly link to a financial account through a 'digital wallet'. This access means that any application (or app) that is allowed to run on the devices potentially has the ability to tap into certain aspects of the information. In the benign case the access is performed to provide useful functionalities, but in other scenarios it may be used to collect a significant amount of personal information and even as a means to have some adverse impact on a user.

Furthermore, the line between benign and malicious is often fuzzy, with many apps falling into a gray area where they may be overly invasive but not outright malicious. Compared to desktop and laptop computers, mobile devices have a different paradigm for installing new applications. For computers, a typical user installs relatively few applications, most of which are from reputable vendors, with niche applications increasingly being replaced by web based or cloud services. In contrast, for mobile devices, a person often downloads and uses many apps from multiple unknown vendors, with each app providing some limited functionality. Additionally, all of these unknown vendors typically submit their apps to a single or several app stores where many other apps from other vendors may provide similar functionality. This different paradigm requires a different approach to deal with the risks of mobile devices, and offers distinct opportunities.

IV. CONCLUSION FUTURE WORK

The proposed system provide strong security provide for android apps.Risk rank translated into categorical values and presented early in the selection process, it will lead users to select apps with lower risk. The results from four user studies validated our hypothesis that when risk ranking is presented in a user-friendly fashion, e.g., translated into categorical values and presented early in the selection process, it will lead users to select apps with lower risk. The majority of participants preferredto have such a risk metric in Google Play Store. We expect that adding a summary risk metric would cause positive changes in the app ecosystem.

When users prefer lower-risk apps, developers will have incentives to better follow the least-privilege principle and request only necessary permissions. It is also possible that the introduction of this risk score will cause more users to pay for low risk apps. Thus, this creates an incentive for developers to create lower risk apps that do not contain invasive ad networks and in general over-request permissions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

REFERENCES

[1] J. Schwarz and M. Morris, "Augmenting Web Pages and Search Results to Support Credibility Assessment," Proc. SIGCHI Conf. Human Factors in Computing Systems, pp. 1245-1254, 2011.
[2] J. Staddon, D. Huffaker, L. Brown, and A. Sedley, "Are Privacy Concerns a Turn-Off?: Engagement and Privacy in Social Networks," Proc. Eighth Symp. Usable Privacy and Security (SOUPS '12), pp. 1-13, 2012.
[3] S. Sternberg, "Inferring Mental Operations from Reaction-Time Data: How We Compare Objects," An Invitation to Cognitive Science: Methods, Models and Conceptual Results, D. Scarborough and S. Sternberg, eds., pp. 703- 863, MIT Press, 1998.
[4] J. Sun, P. Ahluwalia, and K.S. Koong, "The More Secure the Better? A Study of Information Security Readiness," Industrial Management and Data Systems, vol. 111, no. 4, pp. 570-588, 2011.
[5] A. Tversky and D. Kahneman, "The Framing of Decisions and the Psychology of Choice," Science, vol. 211, no. 4481, pp. 453-458,1981.
[6] W. Van Wassenhove, K. Dressel, A. Perazzini, and G. Ru, "A Comparative Study of Stakeholder Risk Perception and Risk Communication in Europe: A Bovine Spongiform Encephalopathy Case Study," J. Risk Research, vol. 15, no. 6, pp. 565-582, 2012.
[7] K.-P.L. Vu, V. Chambers, B. Creekmur, D. Cho, and R.W. Proctor, "Influence of the Privacy Bird User Agent on User Trust of Different Web Sites," Computers in industry, vol. 61, no. 4, pp. 311-317, 2010.
[8] K.-P.L. Vu, R.W. Proctor, A. Bhargav-Spantzel, B. Tai, J. Cook, and E.Eugene Schultz, "Improving Password Security and Memorability to Protect Personal and Organizational Information," Int'l J. Human-Computer Studies, vol. 65, no. 8, pp. 744-757, 2007.
[9] S. Werner and C. Hoover, "Cognitive Approaches to Password Memorability—The Possible Role of Story-Based Passwords," Proc. Human Factors and Ergonomics Society Ann. Meeting, vol. 56, pp. 1243-1247, 2012.
[10] XF. Xie, M. Wang, R. Zhang, J. Li, and QY. Yu, "The Role of Emotions in Risk Communication," Risk Analysis, vol. 31, no. 3, pp. 450-465, 2011.