Understanding Android Security

Gregor Robinson and George R S Weir

Department of Computer and Information Sciences
University of Strathclyde, Glasgow G1 1XH, UK
gregor.robinson.2013@uni.strath.ac.uk, george.weir@strath.ac.uk

Abstract. This paper details a survey of Android users in an attempt to shed light on how users perceive the risks associated with app permissions and in-built adware. A series of questions was presented in a Web survey, with results suggesting interesting differences between males and females in installation behaviour and attitudes toward security.

Keywords: Mobile security; Android OS, User awareness.

1 Introduction

Android is currently developed and maintained as an open source mobile operating system (OS), by Google. In August 2005, two years after the OS's creation, Google purchased the company behind Android, as a strategic move into the mobile operating system market place. With the subsequent rise in smartphone adoption, along with other handheld devices such as tablets, Android has grown to become the leading mobile operating system in terms of global smartphone market share [1]. Android currently has the largest market share in terms of users and devices, accounting for 84.4% of the smartphone market in 2014 Q3 [2], and over 1 billion active users worldwide across all their device platforms [3]. Android applications have been downloaded and installed over 50 billion cumulative times since its creation in 2003 [4].

Key to Android success is the fact that it is open source, which allows for hardware developers to augment the OS to meet the requirements for their particular device. In turn, this leads to cheaper handsets [5]. In the market to date only Apple is a close competitor in terms of devices and market share [1].

While Apple devices can install a variety of applications from the Appstore, much in the same way as Android devices from Google's play store, Apple takes a more rigid approach to app integrity. This includes sending code to third parties for analysis before being published in the Appstore. In contrast, Google has traditionally relied upon the principle of least privilege [6]. On this principle, a user is only allowed access to what they require in order to complete the task but no more than that. When creating applications, Google entrusts the developers of the application to only code relevant permissions that the application needs to run and no more. However, recent research found that 33% of applications ask for permissions beyond what they require [6]. Results

reported by [6] showed that only 3% of Internet survey respondents could answer permission comprehension questions and only 17% of participants paid attention to permissions during installation.

2 Security Risks

The primary security risks associated with the Android operation system are the misuse of permissions, which may allow developers to install certain types of software onto a device or acquire data from a user. Such risk is primarily associated with Android because there is no relevant party to check comprehensively what applications are released into the Google PlayStore.

Previous attempts to create systems to check for irrelevant or malicious permissions include Droid Ranger [7], which looked at how to detect malicious software in applications. DroidRanger did this by looking for permission-based footprints in order to detect malware families hidden within an application. Despite such attempts at creating an application check, the everyday consumer of Android applications has no reliable way to detect such malicious types of applications. In 2012, Google introduced a security service (codenamed 'Bouncer') that is credited with a 40% drop in the number of malicious apps in its app store, but risks continue both through the Play Store and via third-party app sites.

Many software apps are termed 'grayware'. Such software treads a fine line between legitimate application and malware. Adware is one variety of grayware that automatically displays or downloads adverts within an application [8]. Researchers from antivirus software firm Avast recently discovered three popular applications within the play store that contained Adware [9]. The game Durak, for example, which has between 5-10 million installations, contained Adware that suggested your phone was at risk and that you should protect it by downloading another application. This is a clear threat to user personal information as they were informed that they have to download more applications with different permissions, despite the fact their application and device could have been perfectly fine.

Another security risk associated with Android permissions is that of Spyware, wherein the permissions granted to an application give the ability to spy upon and record private conversations by accessing the device's microphone/camera. The user's recent location and texts could also be vulnerable. This permission group exists because some legitimate applications (such as Skype and Snapchat) need these permissions to function correctly. Recent misuse of this permission recently came to light through the use of voice commands on a range of Samsung smart TVs. The misuse arose in regard to voice recording, when the user issued a voice command, it was then sent across the Internet for analysis without the user knowing [10].

One further serious and sinister use of spyware within Android applications is the ability of spyware to track users. This can be achieved through the location permission enabling the app developer to monitor user locations. Such spyware has been used in the past by suspicious partners and to stalk domestic abuse victims.

Another security and personal information risk that can arise from extraneous permissions in applications is that developers can harvest large amounts of personal data. If handled correctly by the developers, this would fall under the Data Protection Act, requiring that all data given to a third party must be managed in accordance with legally sanctioned data protection principles.

Apps that deploy malicious permissions are able to flout this law, and most users will not realise that data has been taken from them when using the application. With permission granted, the developer can access contact numbers, location, messages, call logs, calendars and other personal information on phones. Such data can be used by the developer or sold to third parties.

3 Survey

In designing an Android user survey, we sought to evaluate the level of user understanding and recognition with regard to permissions. For this purpose, the survey had to shed light on the users' recognition of both permissions and their groups, while looking at how this may affect phone usage. An online survey was implemented using the free survey hosting facility provided by Survey Monkey (www.surveymonkey.com). This allowed us to reach a wide demographic and focus on respondents who had considerable experience of using an Android

The survey comprised several types of question. For example when asking about the respondents' awareness of current issues, this was asked using an open question in order to find out what they knew and what they did not. Closed questions were also used, where a user was presented with a variety of options to choose from as well as 'none of the above' as a response, if they were not inclined to select any of the other answers.

The survey received 52 responses in the two days that it was open. Three of these responses have been filtered out as the individuals concerned had never owned an Android device. The total of responses that were collected and evaluated was 49.

The first question that was asked in the survey, was to find out what sex the respondents where. The main purpose of this was just to find out who was responding, and be able to consider whether different attitudes towards the permission group existed between the genders.

The second question asked the respondents' age. The only age group that is not represented within this survey, is the under 18 age group. Respondents were then asked if they had ever owned an Android device.

Question 4 was the first to specifically address Android permissions and security and asked whether the user recognised any permissions from five permission groups: Location, SMS, Phone, Contact and Photo/Media/File. This was an important question, as one our goals was to gauge the degree to which users recognise permissions and the associated permission groups.

Question 5 was a follow up to question 4 that asked the respondents what exactly they knew about the listed permission groups. This question was designed to find out how much they knew about the permissions and to compare their understanding about permissions and their groups.

Question 6 addressed how users respond when installing applications. This was a key issue since installing an application, is the point in the process where individual permissions are shown to the user.

Question 7 looked into recent news stories discussing Android security problems. In order to understand how wide spread these stories are and how much effect these stories could have on the future of Android popularity with it users and market share. The researcher used an open text box allowing respondents to enter what they knew, instead of discussing a story and seeing if they had any recognition of it.

Question 8 in the survey, was designed to look at how many of the respondents were aware of security issues associated with Android permissions. Question 9 explored what types of Grayware attacks users have been exposed to when using Android applications. The purpose of this question was to gauge what varieties of attack are more prominent among Android applications and draw conclusion on what attacks are the most common and what types of personal information could be lost. In order to gauge what type of attack was more common, respondents were presented with four options: Adware, Spyware, Malware and Other. The user could also specify that they had not seen any attacks or if it was different in nature to those stated.

The final question was included to consider the type of proactive measures that a user can take to protect their Android device. This question asked how many of the respondents had downloaded anti-virus software onto their device.

4 Results

The gender distribution of the respondents shows a slightly larger group of males than females, with 57% male compared to 43% female (Fig. 1).

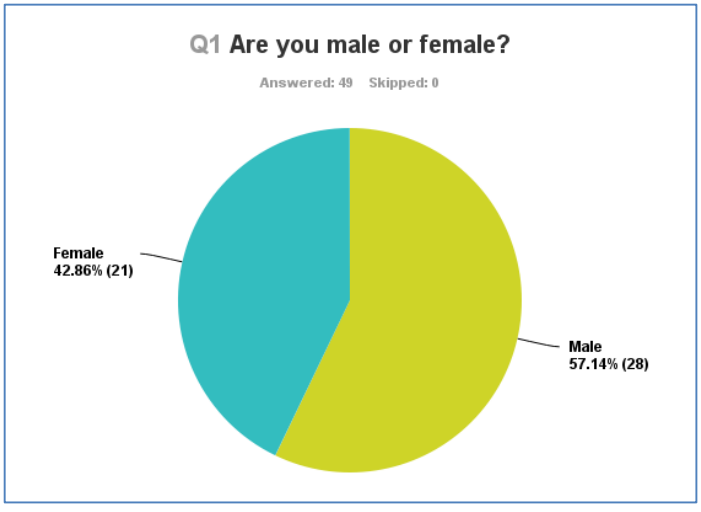

Fig. 1. Gender distribution

Table 1 (below) shows the age range response derived from Question 2.

Age Range	Number	%
18-30	22	44.90
31-45	7	14.29
45-55	8	16.33
55-65	8	16.33
65+	4	8.16

Table 1. Age Range

Question 3 determined how many of the respondents, owned or had owned an Android device, with only 3 of the 52 respondents never owning a device.

The fourth question looked at respondents' understanding and recognition of permission groups. Results show that users have a high level of recognition when it comes to permission groups, with only 10% of respondents not recognizing any of the permission groups. The breakdown of permission recognition is shown in Figure 2.

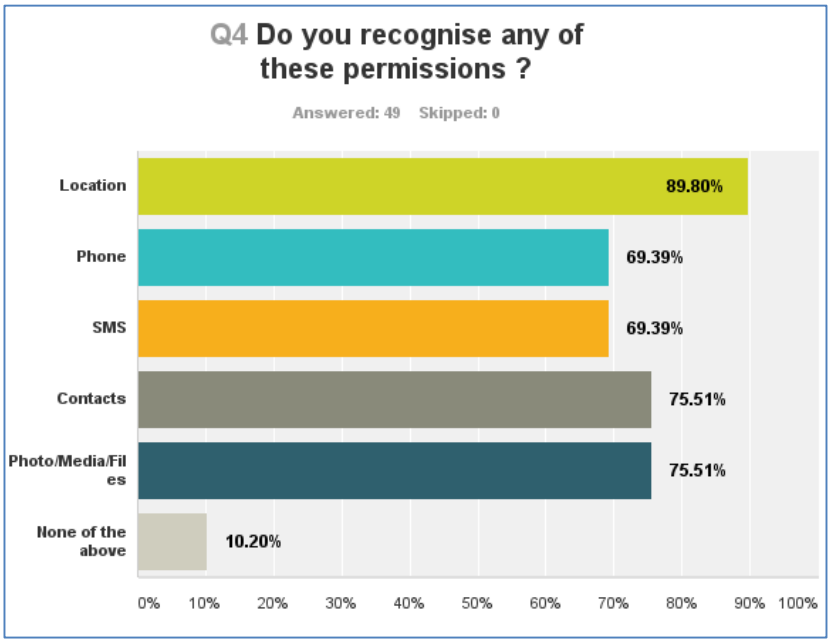

Fig. 2. Recognition of Permissions

Question 5 allowed the user to input what they thought the permission groups, actually did. This was important to ascertain as it went to show how much the user understood about permissions and their groups. The responses ranged from people understanding the permission exactly to people thinking of various permissions in terms of physical attributes that are contained within a device. For example, one response when discussing the Photo/Media/File permission mentioned how they personally stored the media and other files on a their PC: "Having an Android Mobile I already frequently use SMS for messaging, and the contacts folder for address and phone numbers. For my location and destination for weekend car journeys I use Google Maps for information along with a TomTom Satellite Navigation Unit, and in my hobbies of music and photography I keep files in several different formats on my desktop PC at home.

Question 6 of the survey looked at how a user interacts with permission when installing an application to their device. The results for this question are shown in Figure 3 and Table 2 (below).

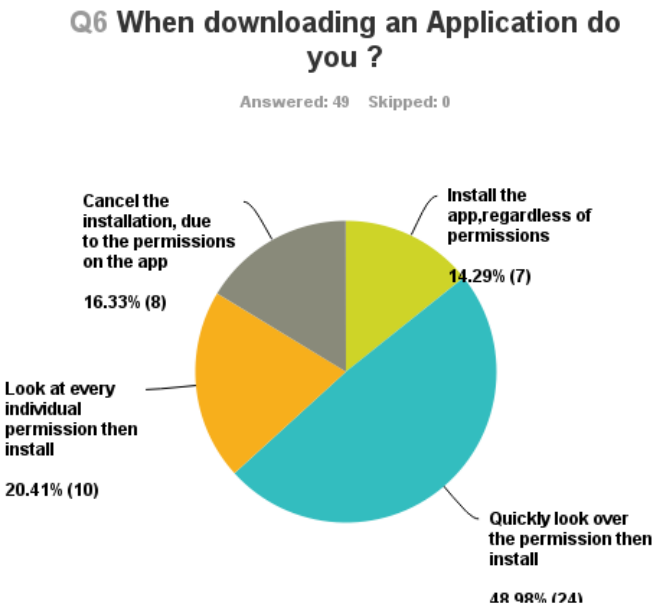

Fig. 3. Installation Responses

Question 7 of the survey built on this by asking if the user had heard of any recent news stories regarding Android security issues. The responses varied, with some respondents mentioning particular programs, such as WhatsApp, to more generic responses related to news stories, but without detailing the particular story they had heard. The more common response, was n/a which meant they either had not heard of any stories, or they had heard of the stories but the story did not change their mind about Android device ownership.

Response	Number	%
Install the app, regardless of permissions	7	14.29
Quickly look over the permission then install	24	48.98
Look at every individual permission then install	10	20.41
Cancel the installation, due to the permissions on the app	8	16.33

Table 2. Installation Responses (Detail)

Question 8 determined how many of the respondents knew about the security risk associated with the permission within an application, with just under 75% of user stating that they were aware of the security risk, the results from this question are shown in Figure 4 (below).

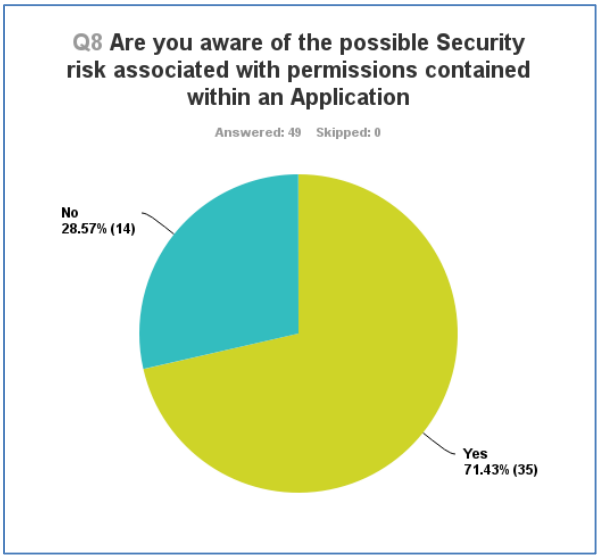

Fig. 4. Permissions Risk Awareness

Results for Question 9 show that the most prominent type of attack was Adware, with over 28% of respondents suffering from this type of Grayware compared to 8% for Spyware and 4.08% for Malware (Figure 5, below).

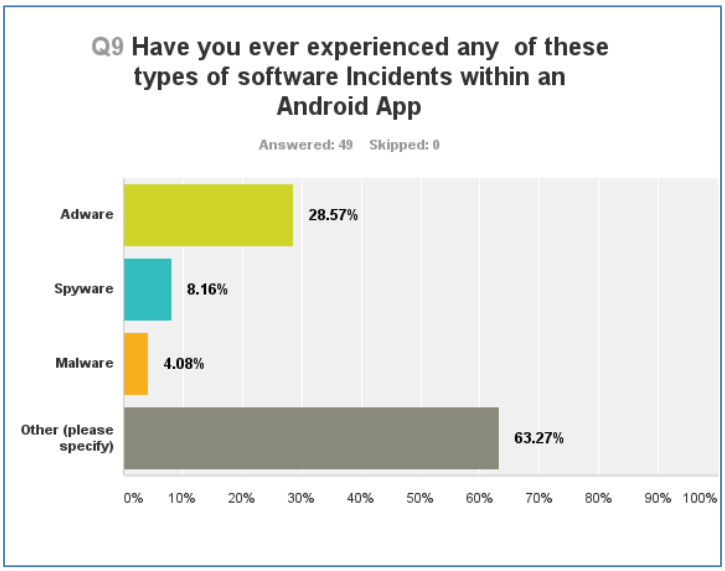

Fig. 5. Experience of Grayware

The final question which was asked in the survey, was Question 10 this looked at how many users installed anti-virus software onto their device. The results for this question are as follows 55% of respondents have installed anti-virus software onto their device compared to 45% who have not. These results are illustrated in Figure 6 (below).

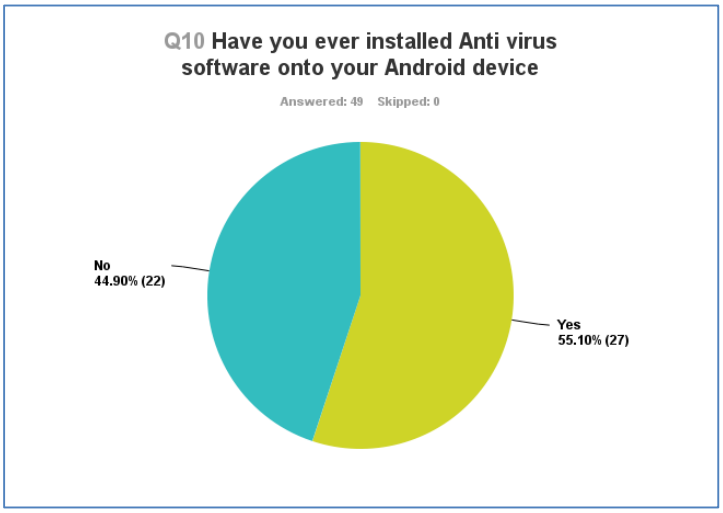

Fig. 6. Android Antivirus Use

5 Conclusions

In analysing the results, we compared our responses to the figures reported by Felt et al [6]. They looked into how many users paid attention when installing an application onto their device and reported 83% [11]. Our survey shows a marginal increase in this to 86% (see Figure 2).

An interesting aspect of attitudes to permission and the installation process was the apparent difference in the way that male and females approach this issue. The survey shows that males tend to be more cautious when installing applications on their devices than females. In the survey results, only 9.52% of female respondents would look at every permission before installing, whereas for males, 20.41% of respondents would look closely at every permission before installing. This suggests that gender has an effect of just under 11% in the approach when installing applications.

More evidence to show that male respondents tended to be more cautious and wary when downloading applications is seen in the fact that 16% of the male respondents would cancel the installation of the application if they were unhappy with the permissions requested by the application. In comparison, only 14.29% of female users would behave in this way.

One final piece of evidence that was observed through this survey would suggest male respondents tend to err on the side of caution compared to females. We see that 57% of females quickly look over the permissions then install, compared to only 49% of male respondents. This was an interesting insight on how users interact with their device, as it shows that males, were more likely to be cautious and alert when installing and protecting their own device from malicious permission, as compared to females. Of course, the survey population was 43% female and 57% male so not equally comprised of males and females and this may slightly skew the gender results.

The next result that was important to compare and contrast was the fact that when Felt et al ran their survey they found that 97% of users could not fully identify every permission that was contained within an application [11]. Following changes in the way that Android implements and displays permissions when installing an application (showing the permission group and not the detailed permissions), it would have been difficult to recreate this exact experiment. To explore this issue we first looked into how many of the respondents recognised the permission and then contrasted this information from Question 5 (in which respondents were asked to give long-hand accounts of permissions). This gave insight into the degree of understanding for permissions against each respondent.

The first permission group evaluated in this fashion was the location permission group. This was the most commonly recognised permission group when the sample was taken as a whole or split by gender. With 89% of respondents recognizing the permission, or 80.95% for females compared to 96.43% for male respondents. Although the recognition of this permission was almost 90% when looking into the responses, we found that only 16% of respondents understood what the permission actually did and could provide a relevant explanation.

The next permission groups to be evaluated were the Phone and SMS permission groups. The reason behind the grouping of these two permissions was that both

achieved the same recognition rate of 69% for the combined sample (despite different rates on the split sample with 66% female and 71% male, respectively). Although it contained a relatively high recognition rate amongst permissions groups, the phone and SMS permission groups actually had one of the lowest level of understanding amongst respondents with only 10% for the phone permission group compared to 12 % for SMS. These results show that although the majority of users can recognise the permission group, the majority struggle to comprehend what is contained within the group and this is why a malicious permission within applications can be so damaging.

The final permission groups to be evaluated were Photo/Media/File and Contacts permission groups. Again, the reason behind the grouping of these two permission was that both achieved the same recognition rate of 75% of the combined sample, unlike the SMS and phone permission group that shared both the same recognition until split between male and female. The contacts permission was recognised by females with a rate of 71% and 78% for males. Whereas the Photo/Media/Files permission had a split of 75% for males and 76% for females, which was the first permission that female respondents recognised more than their male counterparts

Although these permissions consisted of a relatively high recognition rate amongst the permissions groups, the Contact group and Photo/Media/Files had some of the lowest scores in terms of understanding what an application actually does with only 10% of respondents understanding what the Photo/Media/Files permission group can do. This compared to 12% for the Contacts permission group. Again, this demonstrates that although people recognise that these permissions are in most applications, when it comes to understanding how they actually work, the functionality of these permissions and what effect these can have on your device, the gap in knowledge is significant and should be considered in more depth by Android and its developers. This may allow Android to protect their customers against malicious applications that can cause security issues and personal information loss.

One conclusion apparent in this survey is that Android users have a relatively poor understanding of what permissions allow within an application. This can be seen from the fact that although just under 90% of respondents could recognise the location permission group, only 16% of those respondents could give a coherent response to what that the permissions actually could do.

The final area of research that was examined through this survey was the difference between how males and females approach Android permissions and the risk associated with this. Many of our results suggest that males are more cautious and knowledgeable Android users compared to their female counterparts.

One interesting aspect of the results was how different attacks affect the different sexes. This is seen from Question 9 of the survey where the data shows that 32% of males were subjected to some form of Adware attack, compared to 23% of females. This difference could arise from different downloading habits, with males more inclined to download less ‘worthy’ applications than their female counterparts. In comparison when it comes to spyware attacks, females are more likely to be the victim, with 9% respondents informing that they had experienced this type of attack. In comparison, only 7% of males respondents had experience this type of attack. In terms of malware

attacks, the trend for women to be the victim continues with only 3% of males experiencing this issue compared to 5% of females who have experienced this issue.

When looking at these trends it is easy to suppose that because women are seen to be less cautious about their device, when installing any applications, this is why they would experience more security issues than men. But the survey shows that the majority of female Android users actually have installed Anti-virus software onto their device (Question 10). At 57%, this is 4% higher than males. In addition, the majority (66%) of female respondents understood the risk associated with Android permissions (Question 8). Since the male figure for this question was 75%, we can see that both genders are knowledgeable and proactive in securing their phone against threats. However each gender seems more prone to certain types of attacks than the opposite sex.

6 References

1. Hahn, J. (2015), 'Android Claims 81.5% of the Global smartphone OS market in 2014, IOS DIPS to 14.8%'. Available from http://www.digitaltrends.com/mobile/worldwide-domination- android-and-ios-claim-96-of-the-smartphone-os-market-in-2014/ [Accessed 10th March 2015].
2. IDC (2015), Smartphone OS Market Share Q4 2014. Available from: http://www.idc.com/prodserv/smartphone-os-market-share.jsp [Accessed 12th February 2015].
3. Trout, C. (2014) Android Still the dominant mobie OS with 1 Billion active users. Available from: http://www.engadget.com/2014/06/25/google-io-2014-by-the-numbers/ [Accessed 15th March 2015].
4. Statista (2015), Global smartphone operating system market share of Android from 2009-2015. Available from: http://www.statista.com/statistics/216420/global-market-share-forecast-of-smartphone-operating-systems/ [Accessed 20th March 2015]
5. Lee, B. T, (2011), Android Poised to Dominate Developing World. Available from: http://www.forbes.com/sites/timothylee/2011/08/16/android-poised-to-dominate-the-developing- world/ [Accessed 28th March 2015].
6. Felt, P. A. et al. (2010), *Android Permission Demystified*. Available from: http://hibou.cs.wpi.edu/~kven/courses/CS4401-C15/papers/Android-App-Permissions.pdf [Accessed 26th January 2015].
7. Zhou, Y. et al (2011), Hey, you Get, of My Market: Detecting Malicious Apps in Official and Alternative Android Markets. Available from: http://www4.ncsu.edu/~zwang15/files/NDSS12_DroidRanger.pdf [Accessed 2nd February 2015]
8. TechTerms (2015), Adware. Available from: http://techterms.com/definition/adware [Accessed 14th March 2015]
9. Dredge, S. (2015), Several Android Apps Removed from Google Play Store after 'adware' claim. The Guardian. Available from: http://www.theguardian.com/technology/2015/feb/04/android-apps-google-play-adware [Accessed 5th March 2015].
10. BBC News. (2015), Not in front of the telly: Warning over 'listening' TV. Available from: http://www.bbc.co.uk/news/technology-31296188 [Accessed 20th February 2015].
11. Felt, P. A. et al. (2011), Android Permission: User Attention, Comprehension and Behavior. Available from: https://blues.cs.berkeley.edu/wp-content/uploads/2014/07/a3-felt.pdf [Accessed 15th January 2015].