Differences between Android and iPhone Users in Their Security and Privacy Awareness

Lena Reinfelder[1], Zinaida Benenson[1], and Freya Gassmann[2]

[1] University of Erlangen-Nuremberg
Martensstr. 3, 91058 Erlangen, Germany
[2] Saarland University
Saarbruecken, Germany

Abstract. This work compares Android and iPhone users according to their security and privacy awareness when handling apps. Based on an online survey conducted with over 700 German respondents (mostly university students) we found out that Android users seem to be more aware of the risks associated with the app usage than iPhone users. For example, iPhone users almost never consider the possibility of apps sending premium-rate SMS or causing other hidden costs. Furthermore, Android users more often mention security, trust and privacy issues as important factors when they decide to use a new app. We hypothesize that the cause of these differences they are likely to arise through differences in app market policies, in app review processes and in presentation of data usage by the apps.

Keywords: Smartphone, iOS, Android, security awareness, privacy awareness.

1 Introduction

Android and iOS are the world's most popular smartphone operating systems [17], whereas their underlying system architectures and business models differ considerably [1,4,28] (see Section 2 for more details).

It is widely believed that the corresponding user communities differ from each other. We could compile a list of differences from personal communication and different press sources [6,1]. A typical Android user is assumed to be male and technically savvy, while having an iPhone is more often attributed to women[1]. Moreover, iPhone users are said to be very loyal to Apple, they buy more apps and are more actively engaged with their devices than Android users.

In this work we assume that the differences of iOS and Android system architecture and apps handling are connected to the differences in perception and behavior of the users with respect to security and privacy. Thus, our main research question is formulated as follows:

[1] For example, according to a 2010 AdMob survey 73 % of Android users versus 57 % of iPhone users were male [6].

C. Eckert et al. (Eds.): TrustBus 2014, LNCS 8647, pp. 156–167, 2014.

Are there differences in attitudes and behavior between Android and iOS users concerning security and privacy when using apps?

Contribution. In this paper we compare Android and iOS users according to their security and privacy awareness, discuss our findings and give directions for future research. To our knowledge, this is the first direct comparison of this kind. We think that the knowledge about these differences can help in design of future security- and privacy-related features of smartphones and of app stores.

Roadmap. The paper is organized as follows: Section 2 provides background information on the differences between iOS and Android. In Section 3, we present related work on security and privacy awareness of Android and iOS users. Section 4 introduces our research methodology and Section 5 presents the results. We discuss limitations of this work in Section 6. Finally, we conclude with a discussion of ongoing and future work in Section 7.

2 Background: Android versus iOS

We focus on differences between Android and iOS that are visible to general public and non-expert users, and we do not discuss technical details of both operating systems here, as the latter are less important for our research question.

2.1 Platforms and App Markets

Apple's iOS (software) is tightly integrated with the iPhone (hardware). Moreover, Apple maintains strict control over app development and distribution. iOS apps can only be developed by subscribers to the iOS Developer Program, and can only be distributed through the official App Store.[2]

Google's Android runs on different hardware platforms. Anyone can develop and distribute Android apps, and although there is the official Google Play store, the apps can also be distributed from any other place.

App developers for either platform can earn money by integrating advertisement networks into their apps [15].

2.2 App Security

Android malware is quite numerous, as anyone can develop and distribute Android apps [26][27]. Although scanning the apps from Google Play for malicious functionality started in 2012, this was found to be not quite effectual [22]. Furthermore, Google introduced the security setting "Verify Apps" to the Google Play Store, which monitors apps at the installation process for malware [9]. This setting is going to be extended to monitor also apps during run time and to check apps that are downloaded from third-party app stores [24]. Still, this security setting can be turned off by the user. Moreover, for the usage of the functionality "Verify Apps" one has to agree to give Google a lot of information, such as

[2] As an exception, organizations that participate in the *iOS Developer Enterprise Program* can develop and distribute in-house apps solely to their employees.

log files, URLs related to the app and also information about one's smartphone (device ID, version of the operating system, IP address) [9].

In contrast, iOS malware is rare [7], because all apps in the App Store undergo a review process in order to ensure that the apps work according to their description. This also means that the apps should not have malicious functionality. However, Wand et al. could present a method how to get malicious apps into Apple's App store [29].

2.3 Handling of Personal Data by the Apps

Android permissions are passive warnings that are automatically generated, if the app accesses or manipulates certain data, such as contacts, messages and system settings. The warnings are presented to the users during the installation process, and they have to agree with all permission requests in order to install the app. Thus, the users only have the "all-or-nothing" choice.

iOS prior to iOS 6 required runtime consent from the users if an app wanted to use location data for the first time. Many other types of user data could be read and manipulated without user's explicit consent [25,5]. iOS 6 (released in September 2012) radically changed the handling of personal data. Now users have to give runtime consent for many more data types, such as contacts, calendar, photos, Twitter or Facebook accounts. Users can also customize their data disclosure policies.

There is evidence that the potential visibility of Android permissions may lead to a more restrictive use of personal data by the app developers [10]. Apps that are available for both Android and iOS, seem to access more sensitive information when programmed for iOS.

3 Related Work

We are only aware of two studies that explicitly mention the differences between Android and iOS users with respect to security and privacy.

In order to analyze privacy concerns and expectations of smartphone users, King [13] conducted interviews with 13 Android and 11 iOS users. The research investigates two dimensions: participants' concerns with other people accessing the personal data stored on smartphones as well as with applications accessing personal data. Almost all participants reported such concerns. King hypothesized that the Apple review process causes iOS users to exhibit more trust into the apps. However, she found out that also Android users thought that Google reviews apps before they are put into the Google Play store (this fact is also confirmed by Kelley et al. [11]), and so no difference between platforms could be observed. Users that believed (falsely or not) that the apps are reviewed felt safer when using apps. iOS users were mostly unaware of data usage by the apps (iOS 6 was not released at that time). In contrast, Android users were aware of the permission screen that is shown during the installation, although the majority of them felt that they do not quite understand what the permissions mean.

Chin et al. [3] examined differences of smartphone users' perceptions and behavior when using laptops versus smartphones. The authors conducted a survey with 30 iOS as well as with 30 Android users. They noticed that Android users had more free apps than iOS users. Furthermore, around 20 % of Android users stated that they always consider permissions when installing apps and additional 40 % stated that they sometimes considered permissions. This is an interesting contrast to the results by Felt et al. [8] that only 17 % of Android users pay attention to the permissions during the installation process.

Independently and concurrently to our work, Mylonas et al. [21] conducted a survey with 458 smartphone users in order to gain insights into their security awareness. The authors found out that most smartphone users do not feel being at risk when downloading apps from official application stores, and that this effect is independent of the smartphone's operating system. Smartphone users also do not pay attention to security messages which are shown by the devices. Further, they could only find a slight correlation between the participants' security background and their awareness of security when using smartphones [20]. In addition to the findings of Mylonas et al., we examine also privacy awareness of smartphone users and compare Android and iOS users in detail.

Android users received the most attention to date in connection with the Android permissions [8,16,2,11]. Although different research strategies and different user pools were considered, the researchers uniformly found that most users pay only limited attention to the permissions and have a poor understanding of their meaning. We are not aware of any studies that specifically concentrated on security- or privacy-related human factors for iOS users.

4 Research Methodology

We conducted a survey with 506 Android and 215 iOS users in order to analyze security and privacy behavior and attitude. We therefore designed an online survey using the LimeSurvey software[3]. The survey consisted of 21 questions including 17 quantitative and 4 qualitative (open-ended) questions and was available online from September 11th to October 4th 2012. In order to avoid priming, we called the survey "How well do you know your smartphone?". The questionnaire is available from the authors.

Participants were recruited via email from the economics department and from the technical department of the University of Erlangen-Nuremberg. Additionally, 250 flyers were distributed in the city of Erlangen in order to increase the amount of non-student participants.

4.1 Hypotheses and Survey Design

According to our research question presented in Section 1, we developed two hypotheses:

[3] `http://www.limesurvey.org`

H1: Android phone users are more security aware than iOS users.
H2: Android phone users are more privacy aware than iOS users.

The hypotheses are based on the assumption that Google's open app market makes Android users more conscious of possible malware infections and that the explicitly presented app permissions draw user attention to the possibilities of data misuse. It is also possible that security and privacy aware users choose Android because it is open source and because they can see in the permissions which data is accessed and manipulated by the apps.

We note that, on the other hand, due to the app vetting process of Apple it might be possible that security and privacy aware people choose iOS. In our ongoing work that is based on the survey presented here we are investigating whether security and privacy awareness is decisive for the choice of smartphone and its operating system, and also whether the choice of smartphone influences security and privacy awareness (see Section 7 for an initial overview).

4.2 Measuring Security and Privacy Awareness

In order to measure security and privacy awareness, we first asked the participants an open-ended question about what is important to them when choosing a new app. This question was asked before mentioning any security or privacy issues in the survey in order not to prime the participants. Users that mentioned security or privacy issues in their answers were classified as security respectively privacy aware.

Later in the survey, we asked the participants whether they have some security software installed on their smartphones, and we also explicitly asked the participants about their knowledge and concerns about the handling of personal data by the apps.

4.3 Participants

We received 917 responses to the survey. After sorting out incomplete questionnaires as well as users that had other kinds of operating systems than iOS or Android, the answers of 721 participants (258 female and 463 male) were left for further analysis.

We received answers from 506 Android and 215 iOS users. More than 80 % of the participants were between 18 and 25 years old and 14 % were between 26 and 30 years old. 93 % (674) of the participants were students, 5 % (37) were employed and 2 % (10) were neither students nor employed.

5 Analysis of the Results

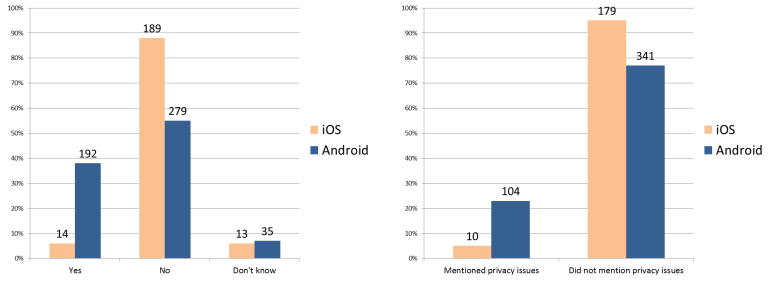
We conducted quantitative as well as qualitative analysis of the answers. For the open-ended questions we used the software for qualitative analysis called

MAXQDA[4] in order to categorize the answers. For quantitative analysis we used SPSS[5].

5.1 Hypothesis 1: Security Awareness

To test hypothesis H1 (Android phone users are more security aware than iOS users), we asked the participants if they have security software such as virus scanner installed on their device. 6 % of iOS users said to have such software installed, while 38 % of Android users stated the same, see Fig. 1(a). The difference is highly significant and there is a medium correlation between the operating system of the smartphone and having security software installed (Cramer's V = .327, p $\leq$.001). This confirms H1.

Mylonas et al. [21] provide similar findings referring to the differences between Android and iOS users. Their survey results show that 33 % of Android users but only 14.7 % of iOS users have security software, especially virus scanners, installed on their smartphones.



(a) Answers to the question *Do you have some security software installed on your smartphone?*

(b) Users that mentioned privacy issues as an important factor when choosing a new app

Fig. 1. Security software question (a); users that mentioned privacy issues (b)

We note, however, that it is not clear whether having a virus scanner can be considered as an independent variable, because there are many virus scanners for Android and virtually no virus scanners for iOS. One may also argue that more security aware people would probably choose iOS because of the Apple review process, and would feel that they do not need any security software in this case.

We further qualitatively analyzed responses to the question: *What is important to you when choosing a new app?* This open-ended question was asked before security or privacy had been mentioned in the questionnaire to avoid priming.

[4] http://www.maxqda.de/

[5] http://www.ibm.com/software/de/analytics/spss

We categorized users as being security aware if they mentioned anything connected to "security", "trust" or "permissions" in their answers (see Table 1). In total, 634 users answered this question. 9 iOS and 96 Android users were categorized as security aware (some participants mentioned more than one security-related issue). We conclude that there is a weak correlation between the operating system and the "security" category that is highly significant (Cramer's V = .206, p $\leq$.000).

Further categories that were derived from the answers to this question can also be found in Table 1. We divided the results into security- and privacy-related categories as well as into those that are not security and privacy relevant.

The above results confirm hypothesis H1: Android users are more security aware, if we consider having security software or mentioning of permissions as indicators of security awareness.

In their survey, Mylonas et al. [21] also asked participants about their application selection criteria, resulting in 8 categories "usefulness", "usability", "efficiency", "cost", "reviews", "reputation", "developer" and "security/privacy". Their most often mentioned category was "usefulness" with 58.8 % and the least mentioned category, "security/privacy", could only be measured in 3.5 % of the answers. In their context, the category security and privacy was e.g. related to not installing an app due to permission requests.

5.2 Hypothesis 2: Privacy Awareness

Although there are some measurement scales for privacy concerns in the literature [18,14], there are not many definitions and scales for privacy awareness [23]. As a first indicator of privacy awareness we analyzed the answers to the question: *What is important to you when choosing a new app?*

We consider users to be privacy aware if they mention anything connected to privacy or personal data, e.g. "privacy", "permissions" or "trustworthy usage of personal data". Although we previously we used the category "permissions" to analyze security awareness of smartphone users, we also use this category for analysis of privacy awareness, as permissions actually refer to both, security-critical actions and personal data access. 10 iOS users and 104 Android users were categorized as privacy aware, see Table 1 and Fig. 1(b). There is a weak correlation between the operating system of smartphones and the categories mentioned above. This correlation is highly significant (Cramer's V = .200, p $\leq$.000).

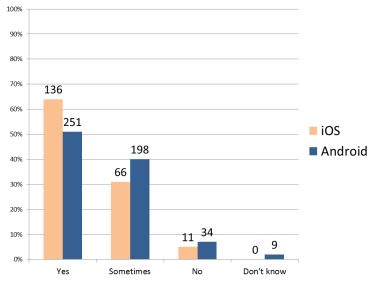
Here, one may be tempted to argue, similarly to H1, that more privacy aware users might choose iOS because they trust that privacy invasive apps will not pass Apple's review process. However, Apple's review criteria are kept secret and iOS apps are known to be quite privacy invasive from the literature [5,25,10].

Table 1. Most frequent categories for the answer to the question "What is important for you when you choose a new app?"

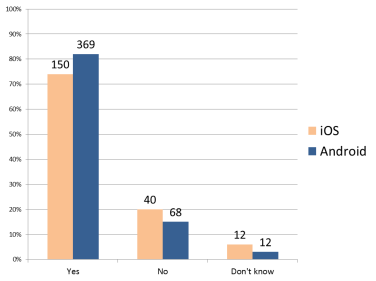
Security- and privacy-relevant	**Description**	**Examples**	**iOS**	**Android**
Security	The term "security" was mentioned	"Data security"	6(3 %)	16(3 %)
Data privacy	"Data privacy" was mentioned or handling of private data	"Protection of private data", "App should not collect or circulate personal data"	6(3 %)	33(7 %)
Permissions	Required permissions of an app; if permissions were mentioned	"Kind of permissions of an app", "If permissions are relevant for the app to function"	3(1 %)	80(16 %)
Not security and privacy relevant	**Description**	**Examples**	**iOS**	**Android**
Usefulness	Useful in daily life, functional volume	"Additionally benefit through app", "Useful benefit"	142(66 %)	318(63 %)
Costs	Costs of an app	"App should be free, because I don't have a credit card", "Free of cost"	90(42%)	205(41%)
Usability	Usability of an app	"App should be user-friendly", "Easy usage"	37(17 %)	72(14 %)
Rating	Recommendations of other users, reviews in app markets	"Experience of other users", "Apps should have good ratings in the store"	26(12 %)	67(13 %)
Entertainment	Entertaining functions such as games	"App should be fun", "Fun factor"	21(10 %)	43(8 %)
Resource usage	Storage space, battery consumption	"App should have a low battery consumption", "App should not waste storage space"	6(3 %)	47(9 %)
Absence of advertisement	No or little advertising being part of an app	"No intrusive advertisement", "No annoying advertisement"	6(3 %)	27(5 %)
N.A.			27(13 %)	61(12 %)

We also asked the participants explicitly about their awareness of data access by the apps. We found no differences between iOS and Android users here, with more than 90 % of the users stating to be aware of the fact. We note, however, one one cannot fully rely on the self-reporting by the users, as this question is suggestive.

In addition, participants were asked whether they pay attention to app accessing personal data. This question was answered by 213 iOS and 492 Android users. If one regards the answers "yes" and "sometimes" together (see Fig. 2(a)), Android and iPhone users both gain about 90 %.



(a) Do you pay attention to whether an app accesses personal data?



(b) Have you ever decided against the usage of an app because the app wanted access to your personal data?

Fig. 2. Questions about privacy awareness

This is interesting if one considers that until iOS 6 emerged, iPhone users were only asked whether they grant the app access to the current location. For all other accesses, users were not directly asked. It remains unclear how iPhone users were able to pay attention to whether an app accesses private data or not. As iOS 6 was actually released exactly in the middle of our survey on September 19th, 2012, we could compare the answers of iOS users that were given before and after the release date. We found no difference in the answers.

Furthermore we found out that 74 % of the iPhone users as well as 82 % of the Android users state to have decided against the usage of an app because the app wanted access to their personal data (see Fig. 2(b)). This question was answered by 202 iOS and 449 Android users. 20 % of iPhone users and 15 % of Android users never decided against the usage of such apps (Cramer's $V = .103$, $p \leq .10$). These differences are not significant.

Finally, we asked the participants an open-ended question about which kind of data access would cause them to abstain from using an application. Here, some differences between iOS and Android users could be identified. "Reading SMS/MMS" is important for 1 % iOS and 12 % Android users. This reflects the corresponding Android permission.

An interesting category is "Apps causing hidden costs" (0 % iOS users and 7 % Android users) that reflects the text of the corresponding Android permission.

It seems that the Android users that pay attention to permissions are the only ones that realize the dangers of malicious apps sending, for example, premium-rate SMS.

The most often mentioned category is "Location" (named by 29 % of iOS and by 20 % of Android users), followed by "Contact data" (20 % of iOS users and 15 % of Android users), with no significant differences between the smartphone types. Moreover, around 10% of users on both platforms gave answers such as "it depends on app's functionality" or "if the data are not related to the core function of the app", indicating that these users make privacy-related trade-offs when deciding to use an app.

The results of this analysis are not straightforward. Are the Android users more privacy aware because they mention one more data type (SMS/MMS) than iOS users? Are the Android users more security aware because a small percentage of them thinks about hidden costs that an app may cause?

On the other hand, significantly more Android users stated in an open-ended question that privacy issues and permissions are important for them when deciding to install a new app (see Fig. 1(b)). They did so before any privacy-related questions were asked. So we make a tentative conclusion that Android users seem to be more privacy-aware than iOS users, confirming hypothesis H2. We note, however, that this issue needs further investigation.

6 Limitations

Our study run form September 11th to October 4th 2012, and iOS 6 was released on September 19th. Thus, the data of iOS users provided after September 19th may be biased because some of them already updated to iOS 6 which requires runtime consent for more data types than location. However, as we noticed no significant differences in the two data sets (data before the introduction of iOS 6 and afterwards), we used all data for our analysis.

Our participants sample was biased towards well-educated young people, as most of them were students, so the generalization of the results cannot be guaranteed. We are investigating other population of participants in our ongoing work.

7 Conclusion and Ongoing Work

The conducted study gave some insights into the interplay between security and privacy awareness and the smartphone choice. Android users seem to be more security and privacy aware, mostly because they notice Android permissions. This may indicate that users need to be presented with a clear overview of the data access by the apps, and that this overview may indeed improve their awareness.

To verify this assumption, and in order to further investigate the relationship between the smartphone type and the users' security and privacy awareness, we

conducted in-depth interviews with 10 Android and 8 iPhone users with various demographic backgrounds and are now analyzing the transcribed interviews using structuring content analysis by Mayring [19].

Furthermore, we are going to develop a model for the interaction between the smartphone type and the security and privacy awareness and to test this model by statistical means, using, for example, structural equation modeling techniques such as LISREL [12].

Acknowledgment. This research was supported by the Bavarian State Ministry of Education, Science and the Arts as part of the FORSEC research association.

References

1. Arthur, C., Dredge, S.: iOS v Android: Why Schmidt was wrong and developers still start on Apple (June 10, 2012), `www.guardian.co.uk`
2. Chia, P.H., Yamamoto, Y., Asokan, N.: Is this app safe?: A large scale study on application permissions and risk signals. In: Proceedings of the 21st International Conference on World Wide Web, WWW 2012 (2012)
3. Chin, E., Felt, A.P., Sekar, V., Wagner, D.: Measuring user confidence in smartphone security and privacy. In: SOUPS (2012)
4. Dediu, H.: Android economics: An introduction (April 2, 2012), `www.asymco.com`
5. Egele, M., Kruegel, C., Kirda, E., Vigna, G.: PiOS: Detecting Privacy Leaks in iOS Apllications. In: NDSS (2011)
6. Elmer-DeWitt, P.: 6 ways iPhone and Android users differ (February 25, 2010), `tech.fortune.cnn.com`
7. Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D.: A survey of mobile malware in the wild. In: SPSM (2011)
8. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: User attention, comprehension, and behavior. In: SOUPS (2012)
9. Google: Protect against harmful apps (February 28, 2014), `https://support.google.com/accounts/answer/2812853?hl=en`
10. Han, J., Yan, Q., Gao, D., Zhou, J., Deng, R.H.: Comparing Mobile Privacy Protection through Cross-Platform Applications. In: Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA (February 2013)
11. Kelley, P.G., Sadeh, L.F.C.N.: Privacy as part of the app decision-making process. In: ACM (2013)
12. Kelloway, E.K.: Using LISREL for Structural Equation Modeling. Sage, Thousand Oaks (1998)
13. King, J.: How Come I'm Allowing Strangers to Go Through My Phone?: Smart Phones and Privacy Expectations, under review (2012)
14. Kumaraguru, P., Cranor, L.F.: Privacy indexes: A survey of Westin's studies. Tech. Rep. Paper 856, Carnegie Mellon University, Institute for Software Research (January 2005)
15. Leontiadis, I., Efstratiou, C., Picone, M., Mascolo, C.: Don't kill my ads!: Balancing privacy in an ad-supported mobile application market. In: HotMobile (2012)

16. Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J.I., Zhang, J.: Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In: ACM UbiComp (2012), http://doi.acm.org/10.1145/2370216.2370290
17. Lipsman, A., Aquino, C.: 2013 Mobile Future in Focus (February 22, 2013), http://www.comscore.com
18. Malhotra, N.K., Kim, S.S., Agarwal, J.: Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research 15(4), 336–355 (2004)
19. Mayring, P.: Qualitative Inhaltsanalyse, 11th edn. Beltz Verlag (2010)
20. Mylonas, A., Gritzalis, D., Tsoumas, B., Apostolopoulos, T.: A qualitative metrics vector for the awareness of smartphone security users. In: Furnell, S., Lambrinoudakis, C., Lopez, J. (eds.) TrustBus 2013. LNCS, vol. 8058, pp. 173–184. Springer, Heidelberg (2013)
21. Mylonas, A., Kastania, A., Gritzalis, D.: Delegate the smartphone user? Security Awareness in Smartphone Platforms 34, 47–66 (2013)
22. Percoco, N.J., Schulte, S.: Adventures in bouncerland. In: Black Hat USA (2012)
23. Pötzsch, S.: Privacy awareness: A means to solve the privacy paradox? In: Matyáš, V., Fischer-Hübner, S., Cvrček, D., Švenda, P. (eds.) The Future of Identity. IFIP AICT, vol. 298, pp. 226–236. Springer, Heidelberg (2009)
24. Raphael, J.: How Google's Android security is about to get even smarter (February 27, 2014), http://blogs.computerworld.com/android/23590/google-android-security
25. Seriot, N.: iPhone Privacy. In: Black Hat USA (2010)
26. Sofos: Security threat report (2013), http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report
27. Spreitzenbarth, M., Freiling, F.: Android malware on the rise. Tech. Rep. CS-2012-04, University of Erlangen (April 2012)
28. Travlos, D.: Five Reasons Why Google Android versus Apple iOS Market Share Numbers Don't Matter (August 22, 2012), http://www.forbes.com
29. Wang, T., Lu, K., Lu, L., Chung, S., Lee, W.: Jekyll on iOS: when benign apps become evil. Presented as Part of the 22nd USENIX Security Symposium, Washington D.C, USA (August 2013)