Android and iOS Users' Differences concerning Security and Privacy

Zinaida Benenson
University of Erlangen-Nuremberg
D-91058 Erlangen, Germany
zinaida.benenson@cs.fau.de

Freya Gassmann
Saarland University
D-66041 Saarbrücken, Germany
f.gassmann@ceval.de

Lena Reinfelder
University of Erlangen-Nuremberg
D-91058 Erlangen, Germany
lenareinfelder@googlemail.com

Copyright is held by the author/owner(s).
CHI 2013 Extended Abstracts, April 27–May 2, 2013, Paris, France.
ACM 978-1-4503-1952-2/13/04.

Abstract
We compare Android and iOS users according to their demographic differences, security and privacy awareness, and reported behavior when installing apps. We present an exploratory study based on an online survey with more than 700 German students and describe directions for further research.

Author Keywords
Smartphone; iOS; iPhone; Android; Personal Data; Security Awareness; Privacy Awareness

ACM Classification Keywords
D.4.6 [Software]: Security and Protection; H.1.2 [User/Machine Systems]: Human factors; K.4.2 [Public Policy Issues]: Privacy.

Introduction
Smartphones are increasingly powerful personal devices that offer novel ways of communication, information search and sharing, and entertainment. Most popular smartphone operating systems worldwide are Google's Android that comes with a wide variety of smartphones and Apple's iOS that is used in iPhones. The system architectures and business models underlying both operating systems differ considerably [1, 15], as presented in the sidebar on page 2.

Android Business Model

Google provides free services and sells ads there, Android being one of the services.

Apps handling: Anyone can develop and distribute Android apps. Although there is the official *Google Play* store, the apps can also be distributed from any other place.

iOS Business Model

Apple has the *integrated model*, where iOS (software) is integrated with the iPhone (hardware).

Apps handling: iOS apps can only be developed by subscribers to the *iOS Developer Program*, and can only be distributed through the official *App Store*.

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

Ad Networks Integration

App developers for either platform can earn money by integrating *ad networks* into their apps. This business model for app developers should not be confused with Google's business model.

It is widely believed that also the user communities of Android and iOS differ from each other. Although we could not find reliable scientific data, we could compile a list of differences from personal communication and different press sources [5, 1]. Probably most poignantly these differences are pictured in the cartoon by Idan Schneider (Fig. 1). The Android users are assumed to be mostly male and technically savvy, the iPhone users are said to be very loyal to Apple and be more brand-aware in general.

An app is usually written by a third party. It has to be downloaded and installed from an app store, and the users has limited possibilities for knowing which information the app might collect about them, or what hidden functionality the app might have. Thus, app usage is often connected to security and privacy risks. The differences between Android and iOS apps concerning security and privacy are presented in sidebars on pages 3 and 4.

In this work we assume that these differences are connected to the differences in perception and behavior of the users with respect to security and privacy. We note that it is not clear in which direction the influence might work, and we do not attempt to answer causal questions here. Thus, our main research question is formulated as follows:

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

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.

Figure 1: "iPhone vs. BlackBerry vs. Android", Cartoon courtesy of Idan Schneider, C-Section Comics, `www.csectioncomics.com`.

Chin et al. [3] primarily investigated differences in perceptions and behavior of users when they are using a laptop vs. a smartphone. However, as they chose to test 30 Android users as well as 30 iOS users, they noticed that Android users had more free apps than iOS users.

Android and iOS Security
Android malware is quite numerous [7], as anyone can develop and distribute Android apps. Although scanning of the apps from Google Play for malicious functionality started in 2012, this was found to be not quite effectual [13]. Besides, nothing prevents users from downloading malicious apps from elsewhere [16].
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. Nevertheless, some malware and spyware found its way into the store [14, 2].
Jailbreaking iOS or Rooting Android gives the users privileged (root) access to their devices. This way the users get much more control (e.g., the iOS users can install apps from other sources than App Store). However, the devices loose protection given by their operating systems and become an easy target for malware.

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.

King [11] explicitly compares 13 Android and 11 iOS users according to their privacy concerns and expectations. She 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 (this fact is also confirmed by Kelley et al. [10]), 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.

As Apple and Google chose quite different ways of informing users of apps' data usage (see sidebar on page 4), some differences in privacy concerns and privacy awareness emerged during the study. 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 always shown during the installation, although the majority of them felt that they do not quite understand what the permissions mean. This feeling is confirmed by other user studies [10, 8, 12].

Furthermore, iOS users were less privacy concerned and less privacy aware than Android users. They thought that apps needed access to more data, and were more comfortable with data sharing. Moreover, iOS users were much more comfortable with real-time location sharing than Android users. This difference is probably influenced by the runtime consent that iOS users need to give for location-aware apps.

Android users received the most attention to date in connection with the Android permissions [10, 8, 12]. 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.

Study Design and Data Collection

As not much data is available about the comparison of Android and iOS users, we conducted an exploratory study using a short online questionnaire.

Hypotheses

We were primarily interested in the differences between Android and iOS users concerning security and privacy issues. We also wanted to check if there is a grain of truth in the demographic differences as depicted in Fig. 1. Therefore, we formulated the following five hypotheses.

H1: Female users are more likely to have an iPhone.

H2: If users have a technical background, then they are more likely to have an Android phone.

H3: If users are brand-aware, then they are more likely to have an iPhone.

H4: Having an Android phone is positively correlated to being more security aware.

H5: Having an Android phone is positively correlated to being more privacy aware.

The last two hypotheses are based on the reflection that Google's open app market makes Android users more

Handling of Personal Data in Android and iOS
Android permissions are warnings that are automatically generated from the app code if the app accesses or manipulates certain data, such as contacts, messages, 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 from the users *runtime consent* 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 [14, 4]. **iOS 6 (released on 19 Sept. 2012)** radically changed the handling of the personal data. Now users have to give runtime consent for many more data types, such as contacts, calendar, photos, Twitter or Facebook account. Users can also customize their data disclosure policies using a wide set of privacy settings.

conscious of possible malware infections, and that the explicitly presented app permissions draw user attention to the possibilities of data misuse. On the other hand, 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.

Operationalization of Variables

Technical background (H2) was operationalized in two ways: (1) study of a technical subject or work in a technical field, and (2) interest in technology. The latter was measured using five new items in the style of the questionnaire developed by Karrer et al. [9].

We define *brand-awareness* (H3) as the extent to which the product's brand influences the decision to use the product. We asked the participants to rate the importance of smartphone manufacturer (such as Apple, Samsung, Nokia etc.) for the choice of their gadget.

For hypotheses H4 and H5, we decided to look for indicators that people think about security and privacy when using their smartphone. We first asked participants an open-ended question about factors that influence them when choosing an app. After that we asked if the participants have a virus scanner installed. Participants that mentioned security- or privacy-related factors for their app choice without priming were considered security vs. privacy aware. Participants that have a virus scanner were considered security aware.

Data Collection

We conducted an online survey with the students of the economics department and of the technical department at the University of Erlangen-Nuremberg in September 2012. The link to the questionnaire was distributed via email. In order to avoid priming, we called the survey "How well do you know your smartphone?".

iOS 6 was released on 19th September 2012, in the middle of our study. As new features and release date of new iOS versions are usually treated in a manner of a "state secret", we were not fully aware of the iOS 6 changes, and so we did not ask the users to provide the version of their operating system. Thus, we cannot use the data of iOS users provided after September 19th for analysis of anything concerning privacy. Moreover, according to statistical data [6], around 60 % of German iOS users updated their devices to iOS 6 by the beginning of October.

Thus, we ended up with two data sets. We use the full data set for analysis of hypotheses H1 to H4 that are not connected to privacy, and we use a restricted set of data collected before September 19th for analysis of H5.

Results

Demographics of Participants

We received 917 completed questionnaires. After sorting out inconsistent data and users that had other kinds of smartphones, 722 valid answers remained. From these, 506 (70 %) were Android and 216 (30 %,) were iOS users. More than 80 % of the participants were between 18 and 25 years old, and 14 % were between 26 and 30. 36 % were female and 64 % male.

Evaluation of Hypotheses

Hypotheses H1 to H4 were evaluated on the full data set using logistic regression with IBM SPSS Statistics 20. We used the operating system as the dependent variable (Table 1).

	β	β^*
Gender	0.445^{+} (0.234)	1.902
Tech. subject	0.088 (0.214)	0.411
Interest in technology	-0.351^{**} (0.129)	-2.721
Technical features	0.535^{***} (0.115)	4.652
Hardware producer	-0.717^{***} (0.092)	-7.793
Friend's opinion	-0.231^{**} (0.081)	-2.852
Virus scanner	1.265^{***} (0.194)	6.521
Constant: 0.433, n: 722 Nagelkerkes R^2: 0.293		
$^{+}p < 0.10, ^{*}p < 0.05,$ $^{**}p < 0.01, ^{***}p < 0.001$ $\beta^* = standardized\ \beta$		

Table 1: Logistic regression with operating system as dependent variable. Variables representing age and occupation are omitted. They were not significant. *Tech. subject* indicates technical study subject or field of work (7 % of respondents were not students). *Interest in Technology* was derived from five technology interest questions (see page 4) using factor analysis (principal component analysis with Varimax rotation). All other variables are explained in the text.

H1: Female users are more likely to have an iPhone.
This hypothesis is weakly supported ($p < 0.1$). However, this may be due to the large sample size.

H2: If users have a technical background, then they are more likely to have an Android phone.
Studying a technical subject or working in a technical field were not correlated to having an Android phone. However, if technical features are an important factor for the choice of the smartphone, the person is significantly more likely to have an Android phone (variable *Technical features*, $p < 0.001$).

On the other hand, the variable *Interest in Technology* has a negative effect. Persons interested in technology (as measured by our questionnaire items) are much more likely to have an iPhone ($p < 0.01$). To summarize, H2 needs further investigation, especially the scale for measuring interest in technology should be reconsidered.

H3: If users are brand-aware, then they are more likely to have an iPhone.
This hypothesis is supported. Persons that stated that the phone manufacturer's brand influenced them when choosing a smartphone, are significantly more likely to have an iPhone ($p < 0.001$). Also persons that said that the opinion of friends, family and colleagues affected them when choosing their smartphone, are more likely to have an iPhone (variable *Friend's opinion*, $p < 0.01$).

H4: Having an Android phone is positively correlated to being more security aware.
Persons who stated to have a virus scanner installed on their smartphone are significantly more likely to have an Android phone ($p < 0.001$). 38 % of all Android users said that they have a virus scanner installed.

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. This question needs further investigation.

H5: Having an Android phone is positively correlated to being more privacy aware.
Hypothesis 5 had to be evaluated on the data received before the release of iOS 6. As an indicator of privacy awareness we took answers to the open-ended question "Which factors are important to you when you consider to install an app?" Persons that mentioned personal data or permissions were considered privacy aware. Out of 322 participants that answered the survey before September 19th, 20% of Android users and 5% of the iOS users were privacy aware (Fig. 2). This difference is highly significant (Cramer's V=0.207, $p < 0.001$). Thus, H5 is supported.

Here, one may be tempted to argue, similarly to H4, 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 [14, 4].

Limitations

Due to different policies of the two considered university departments for sending mass emails, we started the survey on September 11th in the economics and on September 23th in the technical department. Between the two email waves, iOS 6 was released. As we did not ask the participants about their iOS version, we could not separate iOS 6 users from the others. Therefore, for all

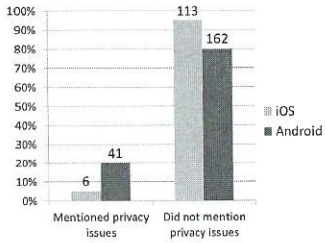

Figure 2: Participants that mentioned or not mentioned (in an open-ended question) privacy issues as a factor that they consider when installing apps.

reliable results that concern privacy awareness we could only use the data of the economics department students. Unfortunately, in this way we could not see if there is a correlation between technical background and privacy awareness.

Our results concerning the indicators of technological interest are ambiguous. That is, we are not sure what we actually measured with our five technology-related questions, and we are going to analyze this in more depth.

Conclusions and Future Work

Additional data from the presented study will be analyzed in order to generate hypotheses for the next stage of our examination. For example, the participants provided answers to an open-ended question "If the app wants to access the following data, then I do not use it." We are going to categorize the data and look there for differences between the operating systems. Subsequently, we are going to conduct a set of experiments and quasi-experiments using specially developed Android and iOS apps, complemented by in-depth interviews.

References

[1] Arthur, C., and Dredge, S. iOS v Android: why Schmidt was wrong and developers still start on Apple. `www.guardian.co.uk` Jun. 10, 2012.

[2] Bonnington, C. First Instance of iOS App Store Malware Detected. `www.wired.com` May 7, 2012.

[3] Chin, E., Felt, A. P., Sekar, V., and Wagner, D. Measuring user confidence in smartphone security and privacy. In *SOUPS* (2012).

[4] Egele, M., Kruegel, C., Kirda, E., and Vigna, G. PiOS: Detecting Privacy Leaks in iOS Apllications. In *NDSS* (2011).

[5] Elmer-DeWitt, P. 6 ways iPhone and Android users differ. `tech.fortune.cnn.com` Feb. 25, 2010.

[6] Etherington, D. Europeans Quickest To Adopt iOS 6. `techcrunch.com` Oct. 13, 2012.

[7] Felt, A. P., Finifter, M., Chin, E., Hanna, S., and 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., and Wagner, D. Android permissions: User attention, comprehension, and behavior. In *SOUPS* (2012).

[9] Karrer, K., Glaser, C., Clemens, C., and Bruder, C. Technikaffinität erfassen – der Fragebogen TA-EG. In *8. Berliner Werkstatt Mensch-Maschine-Systeme.* (2009).

[10] Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., and Wetherall, D. A conundrum of permissions: Installing applications on an android smartphone. In *USEC Workshop* (2012).

[11] King, J. How Come I'm Allowing Strangers to Go Through My Phone?: Smart Phones and Privacy Expectations. under review, 2012.

[12] Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., and Zhang, J. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *ACM UbiComp* (2012).

[13] Percoco, N. J., and Schulte, S. Adventures in bouncerland. In *Black Hat USA* (2012).

[14] Seriot, N. iPhone Privacy. In *Black Hat USA* (2010).

[15] Travlos, D. Five Reasons Why Google Android versus Apple iOS Market Share Numbers Don't Matter. `www.forbes.com` Aug. 22, 2012.

[16] Zhou, Y., Wang, Z., Zhou, W., and Jiang, X. Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets. In *NDSS* (2012).