Should the Users be Informed? On Differences in Risk Perception between Android and iPhone Users.

Zinaida Benenson
Friedrich-Alexander-University
Erlangen-Nuremberg
Erlangen, Germany
zinaida.benenson@cs.fau.de

Lena Reinfelder
Friedrich-Alexander-University
Erlangen-Nuremberg
Erlangen, Germany
lena.reinfelder@cs.fau.de

ABSTRACT

Apple and Google chose very different ways to communicate security and privacy risks to the iPhone and Android users, respectively. iPhone users, in the existing Apple tradition, are actively encouraged to trust into Apple being able to protect their devices through the App Store review process. Android users have at least the possibility to know which data types and which critical actions are used by the app through the permissions that are shown on every app download. Thus, Android users would be better informed about possible risks in case they notice and are able to understand the permissions. In an online survey with over 700 German respondents, we noticed that Android users are indeed better informed than the iPhone users who seem to think less about possible risks. An interesting question is whether the iPhone users really *need* to be informed. Do they need to know about risks that they are probably never going to encounter, such as malicious apps sending premium-rate SMS messages or using their phone cameras to spy on them? The same issue applies to communication of security risks to Mac and Linux users, as well as to the whole field of risk communication: Should risks only be communicated to the high-risk groups?

1. INTRODUCTION

When users choose a smartphone, they also choose a risk communication strategy for the possible security and privacy risks. The difference in risk communication is especially striking if one considers the users of the two most popular smartphone operating systems worldwide, Android and iOS.

Whereas Google's Android appeals to the open source community spirit in giving users more control over their devices, Apple strictly controls the iOS apps and gives the user a good security feeling without going into technical details.

We first describe some relevant features of Android and iOS security and risk communication in Section 2 and then present survey results about security and privacy attitudes of Android and iOS users in Section 3. These results show the differences in risk perception between the respective user communities and give rise to some questions (Section 4).

Symposium on Usable Privacy and Security (SOUPS) 2013, July 24–26, 2013, Newcastle, UK.

2. SECURITY AND PRIVACY RISKS ON SMARTPHONES

2.1 Android Security and Privacy

Android users can decide for themselves where they get their apps, and they are also provided with clues about some (hidden) functionality that the app may have. These clues are passive (static) warnings called *permissions* that describe to which data an app has access (location, contacts, calender) and which critical actions it performs (send SMS, connect to the Internet, make pictures). Unfortunately, not many users pay attention to the permissions, and the technical language in which they are written is poorly understood [6, 5]. On the whole, Google seems to expect Android users to have high technological literacy and be convinced by rational arguments about security. Google uses a tool called Bouncer to scan apps for vulnerabilities [9], and there is also numerous antivirus software for Android. This software is quite useful, as the malware for Android is also numerous [4].

2.2 iOS Security and Privacy

Apple rigidly controls the possibilities of iOS users to download apps. This can only be done in the official Apple Store (apart form the case where organizations and companies participate in the iOS Developer Program that allows them to distribute apps to their employees). Apple tells the users that it reviews the apps for security, such that they don't need to worry about that. The details of the review process are not known. It seems that Apple tries to convey the impression that the apps are reviewed "by hand", e.g. they do not tell which tools they use. All technical details are thus hidden from the users.

Interestingly, for the communication of data usage by the apps Apple takes a more offensive approach than Google. The users receive active (dynamic) runtime warnings about usage of some data types and are asked for informed consent. Prior to iOS6 (that was releasedd in 2012), only location data was considered, such that many other data types could be accessed without user's perception [10, 3]. In iOS 6, 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.

3. SECURITY AND PRIVACY RISK PERCEPTION

In 2012, we conducted a survey about security and privacy attitudes of iOS and Android users among the students of our university. 506 Android and 215 iOS users completed the survey (258 female and 463 male). Among other things, we asked the users to tell us what is important to them when they choose a new app. Only 4% of iOS users mentioned security and privacy, whereas 16% of Android users mentioned permissions. More than two thirds of the latter Android users have technical background (i.e. they study a technical subject).

Moreover, almost 40% of Android users said that they have some security software on their phones, whereas only 6% of iOS users said so.

When asked about which data types they see as critical for an app to access, iOS users could name much less distinct data types than Android users. The only data types that iOS users named more often than Android users were location and contact data. However, this may be due to the fact that in one of the previous questions we gave precisely these data types as examples of personal data. Thus, iOS users might have been primed. "Contact data" (in this precise wording) was mentioned by 20% iOS vs.15% Android users, location was mentioned by 30% iOS vs. 20% Android users. One could also attribute mentioning of location data to Apples's runtime warnings. However, it is still not clear why contact data got this high percentage, unless we consider priming.

There was one type of actions that was left completely unnoticed by iOS users, but was mentioned by almost 20% of Android users: reading and sending SMS. Sending premium-rate SMS is one of the most important malicious functionalities, and iOS users seem to be fully unaware of this possibility. On the whole, iOS users seem to be much less aware of possible security and privacy risks connected with the usage of smartphones.

4. DISCUSSION

Differences in security and privacy risk perceptions of Android and iOS users seem to be connected to the different way in which Apple and Google shape risk communication. Although Android permissions are widely criticized for their poor visibility and cryptic language, they seem to work in raising awareness at least with technically savvy users. Better design could greatly improve the effectiveness of permissions [7].

On the other hand, iOS users seem to be ill prepared to the encounters with malware and spyware. Even runtime warnings seem to be less effective than one might expect. There is evidence that iOS users are less privacy concerned and less privacy aware than Android users [8]. They think that apps need access to more data than is actually needed for the functionality, and are more comfortable with sharing their location.

As some Mac malware emerged in the last years, the Mac OS users and Apple seemed to be ill prepared to deal with the dangerous situations [1]. However, the opinion that Mac OS does not need security protection is still very popular [2]. The argumentation mostly runs in the lines that (1) Mac OS is technically more difficult to attack than Windows and (2) cybercriminals do not make the effort to attack because the Mac OS is not widespread enough to make a good target. At least the second part of this argumentation does not apply in the case of iOS.

In the light of the above discussion, several questions could be discussed:

- What is the connection between risk perception and technical literacy of the users?
- Are active runtime warnings more (or less) effectual than passive warning? In smartphones, runtime warning seem to lead more to habituation than to imporved risk perception.
- Are non-technically savvy users better off if the security of their devices is managed by the vendor? Is it okay for them not to know about possible security and privacy risks?
- What are social and ethical consequences of not informing the users about possible risks?

5. REFERENCES

[1] G. Cluley. History of Mac malware: 1982 - 2011. http://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/2011.

[2] M. Egan. Do Apple Macs need antivirus? OS X security explained. http://www.pcadvisor.co.uk/features/security/3418367/do-apple-macs-need-antivirus-os-x-security-explained.

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

[4] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A survey of mobile malware in the wild. In *SPSM*, 2011.

[5] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: User attention, comprehension, and behavior. In *SOUPS*, 2012.

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

[7] P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. In *Proceedings of the 2013 ACM annual conference on Human factors in computing systems*, CHI '13, 2013.

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

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

[10] N. Seriot. iPhone Privacy. In *Black Hat USA*, 2010.