

Should the users be informed?

Differences in risk perception between Android and iPhone users

Workshop on Risk Perception at SOUPS 2013,
Newcastle upon Tyne

Zinaida Benenson, Lena Reinfelder

IT Security Infrastructures

University Erlangen-Nuremberg

July 24th, 2013

Motivation: Risk Perception in the Usage of Different Operating Systems

- Do **you** have the same security feeling when doing online banking with
 - Windows / Mac / Linux ?
- Should Linux or Mac users have a virus scanner installed?

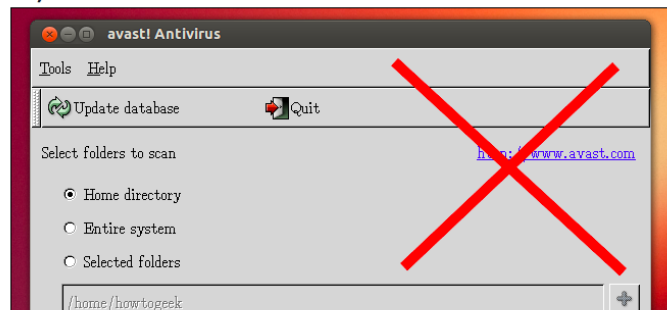


Follow [The Safe Mac on Twitter](#) to stay advised of the latest Mac security news!

Mac Malware Guide : Do I need anti-virus software?

Published June 17th, 2012 at 8:38 PM EDT, modified January 28th, 2013 at 2:25 PM EDT

HTG Explains: Why You Don't Need an Antivirus On Linux (and When You Do)



Believe it or not, there are antivirus programs targeted at desktop Linux users. If you have just switched to Linux and started looking for an antivirus solution, don't bother – you do not need an antivirus program on Linux.



Android vs. iPhone



- When you choose to buy an Android phone or an iPhone, you also choose **the risk communication strategy**
 - iPhone: Apple tradition
 - **We** do everything for you! **Don't worry, be happy.**
 - Hide technical details
 - Don't make users to make "secondary task" decisions
 - Give the users good feelings of belonging and being taken care of
 - Android: Linux tradition
 - **You** are **in control!**
 - Make technical details visible
 - Give the users the freedom of choice
 - Appeal to the open source spirit



Android vs. iPhone iOS



- When you choose to buy an Android phone or an iPhone, you also choose **the risk communication strategy**
 - App market
 - Android: open (decide for yourself!)
 - iOS: closed (App store is safe!)
 - App review process
 - Android: Permissions (user has the control) and a tool (service) called Bouncer
 - iOS: analysis “by hand”? (no tool names are known, no details of the review process)
 - Privacy risks communication
 - Android: Permissions (passive warnings)
 - iOS: runtime warnings (active warnings)

Android vs. iPhone Users

- Apple expects the users:
 - To believe that Apple takes good care of them
 - To develop good feelings about security
- Google expects Android users:
 - To have high technological literacy
 - To be convinced by rational security arguments

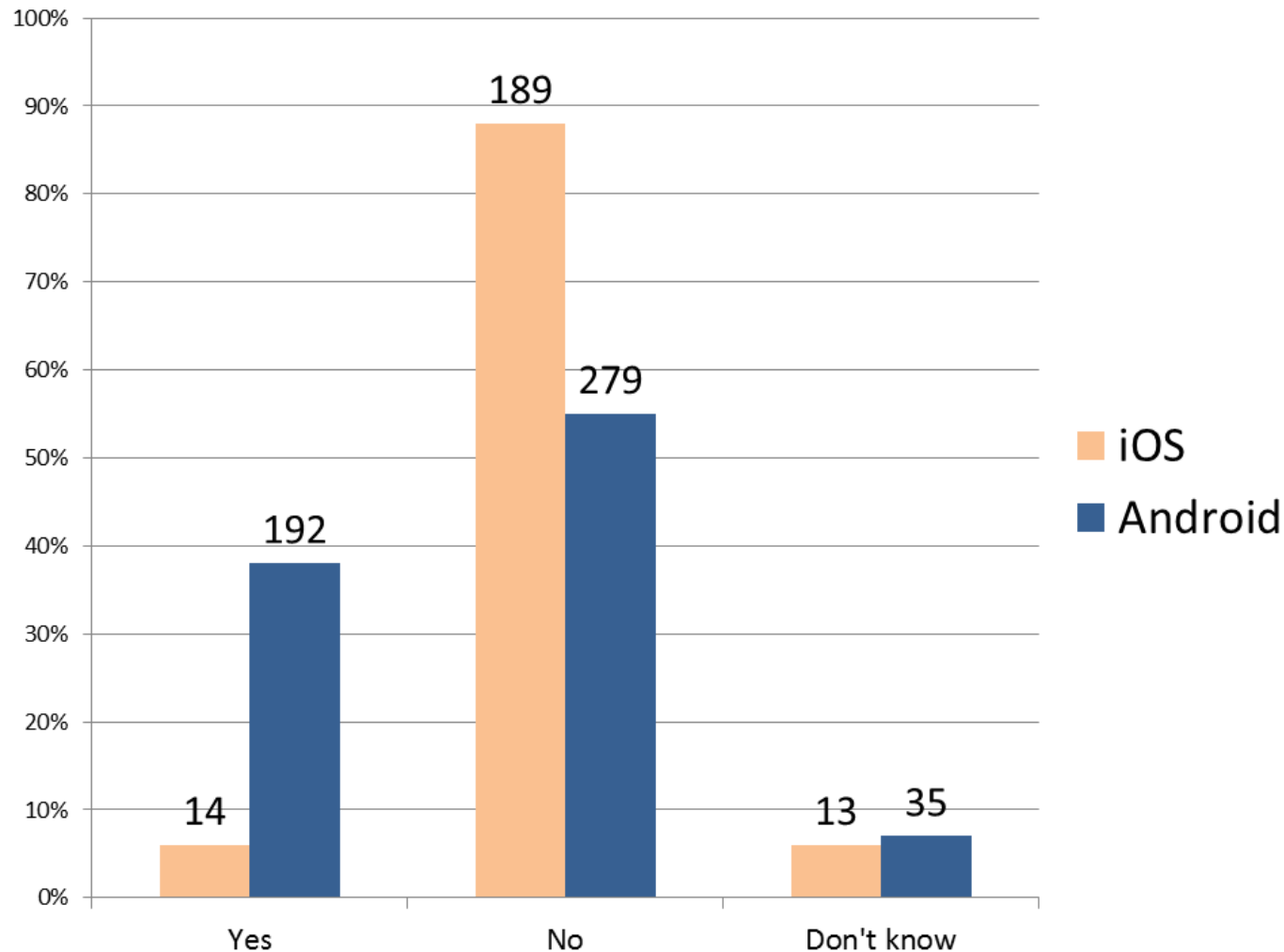
Our Survey

- Research question
 - **Differences between Android and iOS users concerning security and privacy attitudes when using apps?**
- Indicators of S&P awareness
 - What is important to you when you choose a new app?
 - Do thoughts about possible security and privacy risks enter user's mind?
 - Security software installed?
 - Knowledge about possible access to personal data by the apps

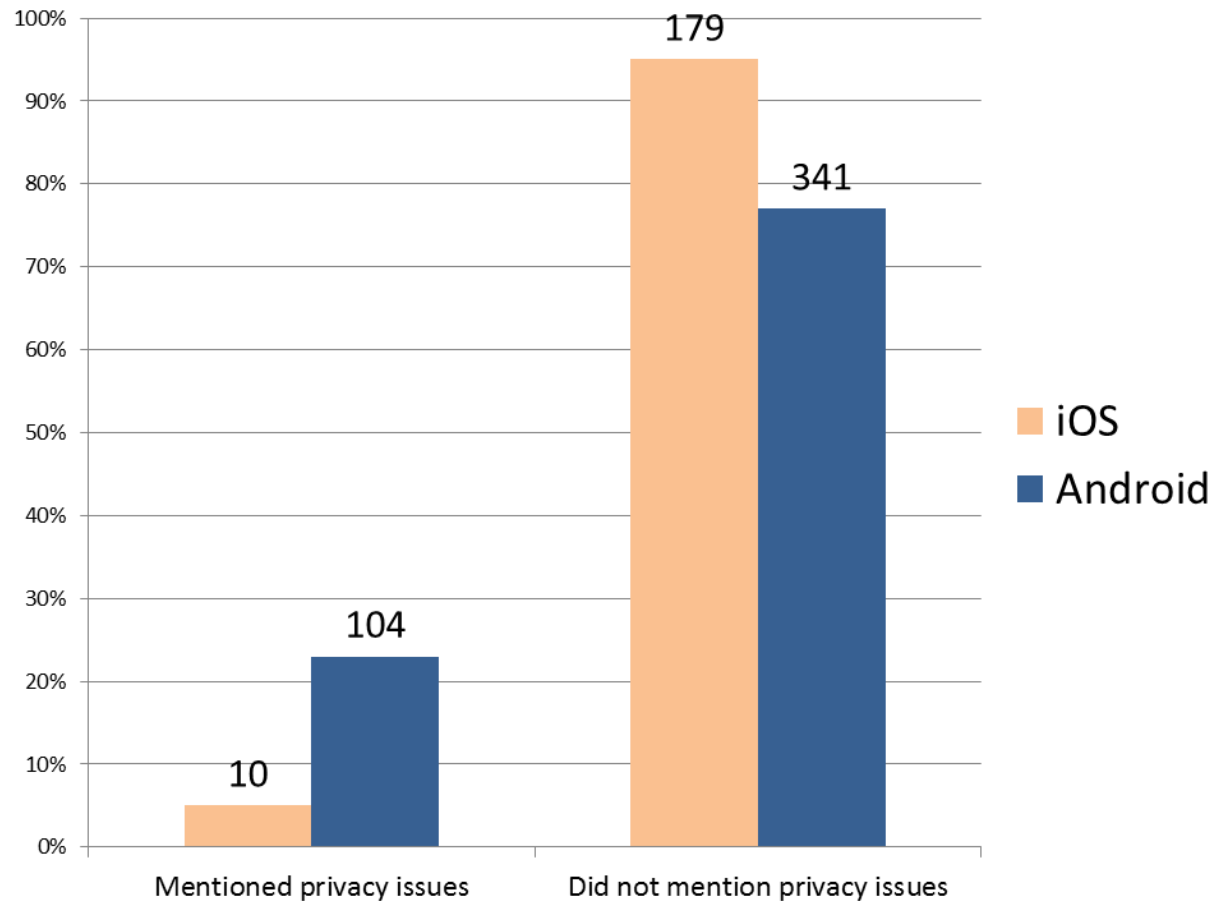
Our Survey

- Participants
 - 506 Android, 215 iOS users
 - 463 male, 258 female
 - 93% of respondents students of our university
 - Technical background
 - Android: 57%
 - iOS: 50%

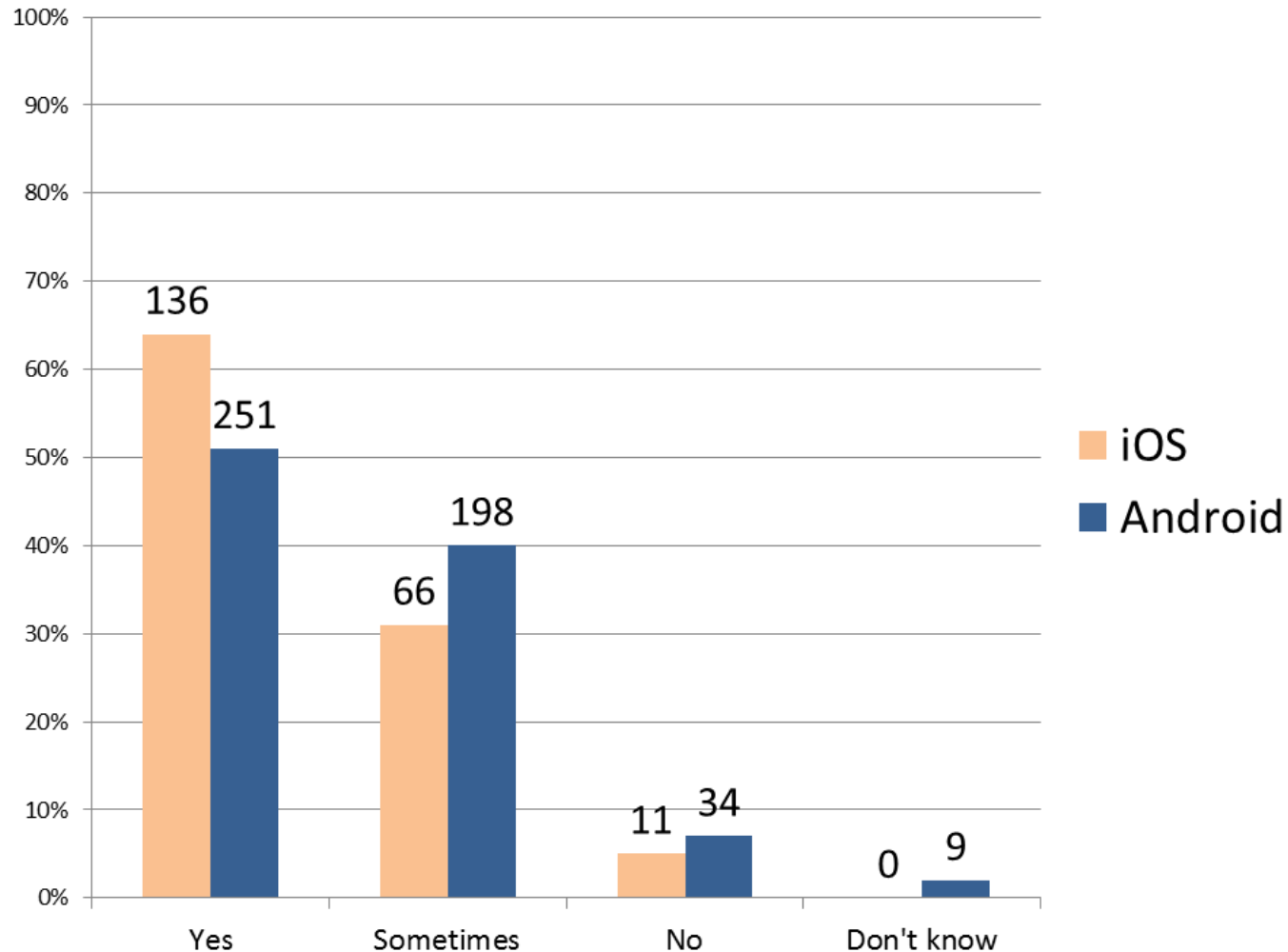
Do you have some security software installed on your smartphone?



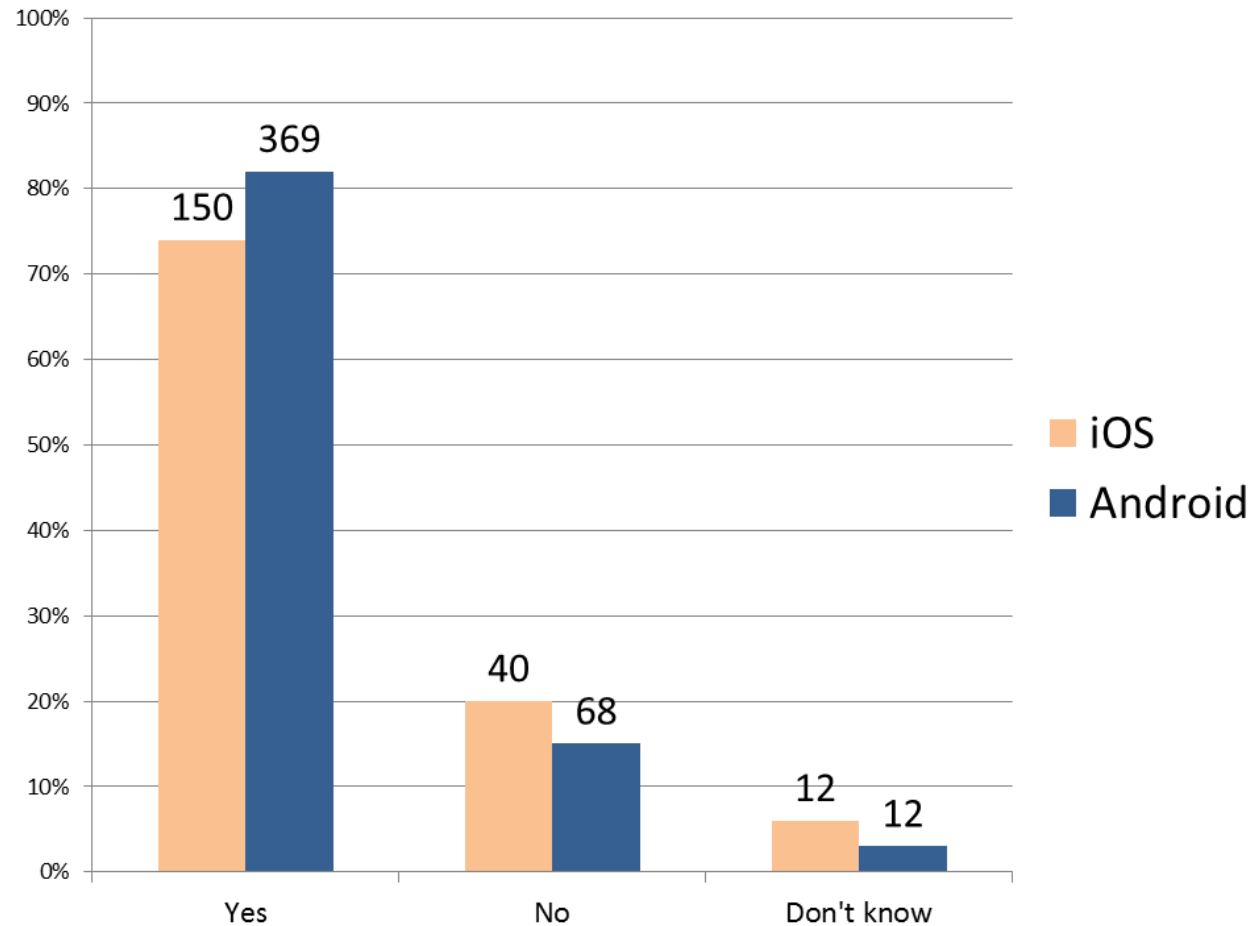
Users that mentioned privacy issues or permissions as an important factor when choosing a new app



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



Did you ever decide against the usage of an app because the app wanted access to your personal data?



If an app wants to access one or several of the following information, I do not use it

Category	Background	iOS	Android
Hidden costs	technical	0 (0%)	22 (4 %)
	non technical	1 (0%)	14 (3%)
Relevance for working	technical	15 (7%)	38 (8%)
	non technical	3 (1%)	9 (2%)
Location	technical	34 (16%)	54 (11%)
	non technical	27 (13%)	44 (9%)
Contact data	technical	27 (13%)	37 (7%)
	non technical	16 (7%)	39 (8%)
reading SMS / MMS	technical	1 (0%)	29 (6%)
	non technical	1 (0%)	26 (5%)
N.a.	technical	33 (15%)	113 (22%)
	non technical	30 (19%)	100 (20%)

Questions

- What is the connection between risk perception and technical literacy of the users?
- Are active runtime warnings more (or less) effectual than passive warning?
 - Do runtime warning probably lead to habituation?
- 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?