A Conundrum of Permissions:
Installing Applications on an Android Smartphone

Patrick Gage Kelley, Sunny Consolvo,[2] Lorrie Faith Cranor,
Jaeyeon Jung,[1] Norman Sadeh, David Wetherall[2]

Carnegie Mellon, Microsoft Research,[1] University of Washington[2]

pkelley@cs.cmu.edu, sunny@consolvo.org, lorrie@cs.cmu.edu,
jjung@microsoft.com, sadeh@cs.cmu.edu, djw@cs.washington.edu

Abstract. Each time a user installs an application on their Android phone they are presented with a full screen of information describing what access they will be granting that application. This information is intended to help them make two choices: whether or not they trust that the application will not damage the security of their device and whether or not they are willing to share their information with the application, developer, and partners in question. We performed a series of semi-structured interviews in two cities to determine whether people read and understand these permissions screens, and to better understand how people perceive the implications of these decisions. We find that the permissions displays are generally viewed and read, but not understood by Android users. Alarmingly, we find that people are unaware of the security risks associated with mobile apps and believe that app marketplaces test and reject applications. In sum, users are not currently well prepared to make informed privacy and security decisions around installing applications.

Keywords: privacy, security, android, applications, smartphone, permissions, information design

1 Introduction

Since the launch of the first Android phone in October 2008 the rise of the platform has been meteoric. Android phones accounted for over half of all smartphone sales as of Q3 2011 [6]. With each smartphone sold, more users are downloading applications from the Android Market. As of May 2011, Google reported that over 200,000 applications were available in the Android Market and that those applications had been installed 4.5 billion times in total [2].

Applications are not pre-screened, instead users are given the opportunity to decide which software to install on their phone. Android app rating and recommendation site AppBrain reports that there are now 310,000 applications in the Android market, and that 33 percent of those are rated at "low quality."[1]

[1] http://www.appbrain.com/stats/number-of-android-apps

Additionally, according to a 2011 Juniper Networks report, and follow up press release, they found "a 472% increase in Android malware samples since July 2011 [to November 2011]" [8]. Similar studies from McAfee [11], Kaspersky Lab [12], and Symantec are all reporting continued exploits.

Juniper attributes this rise to the ease of posting Android applications to the market, as they state: "all you need is a developer account, that is relatively easy to anonymize, $25 and you can post your applications. With no upfront review process, no one checking to see that your application does what it says."

While some believe this openness is harmful to users, Google has promoted it. In one of Google's many tributes to openness, Senior Vice President of Product Management, Jonathan Rosenberg wrote, "At Google we believe that open systems win. They lead to more innovation, value, and freedom of choice for consumers, and a vibrant, profitable, and competitive ecosystem for businesses" [13]. As such, there has been no certification process for Android developers, nor prereview of applications before they enter the Android Market, though applications reported as malicious have been later removed.

The market requires users to make two choices when reviewing potential applications for their device.

1. Do I believe this application will compromise the security and function of my phone if I install it?

2. Do I trust this developer and their partners with access to my personal information?

This leaves users left to leverage word-of-mouth, market reviews and ratings, and the Android permissions display to assist users in making decisions that protect their mobile privacy and security. We conducted a series of 20 semi-structured interviews to better understand how users navigate the Android Market, install and use third-party applications, and comprehend the decisions they make at install time.

In the remainder of this paper we will detail related work on users' understanding of privacy and access control concepts as well as the current state of Android security/permissions, our interview methodology, the demographics and expertise of our participants, and finally a collection of participant responses that qualitatively detail their ability to make decisions in the Android ecosystem.

2 Related Work

While Android has only existed publicly since 2008, a significant amount of work has been conducted on studying the Android permissions/security model. Much of this work focuses on creating theoretical formalizations of how Android security works or presents improvements to the system security, and is largely out of scope. Enck et al.'s work with TaintDroid has bridged the gap between system security and user-facing permissions, focusing on analyzing which applications are requesting information through permissions and then sending that data off phone [4].

Follow up work by Hornyack et al. detailed a method for intercepting these leaked transmissions and replacing them with non-sensitive information [7]. This functionality would allow users post-installation privacy-control. In their investigation they detailed the current permission requests of the top 1100 applications in the Android Market as of November 2010. However, our work, which tests users' understandings of the most common of these permissions, finds users have great difficulty understanding the meaning of these terms. Thus, giving users the ability to limit on a case-by-case basis would likely be ineffective without assistance.

Work by Vidas et al. has also studied how applications request permissions, finding prevalent "permissions creep," due to "existing developer APIs [which] make it difficult for developers to align their permission requests with application functionality" [15]. Felt et al., in their Android Permissions Demystified work, attempt to further explain permissions to developers [5]. However, neither of these papers explore end-users understanding of permissions. In our own work we find users attempt to rationalize why applications request specific permissions, trying to understand the developers' decisions, even if their understanding of these requests is flawed.

Others who have looked at Android permissions have attempted to cluster applications that require similar permissions to simplify the current scheme [3] or have attempted a comparison of modern smartphone permission systems [1]. Their work finds that Android permissions provide the most information to users (compared to other modern smartphone OSs such as Symbian, Windows Phone 7, and iOS), however our interviews show that much of the information provided is not understood.

Research in privacy policies, financial privacy notices, and access control have all similarly shown that privacy-related concepts and terms are often not well understood by users expected to make privacy decisions [9, 10, 14]. Our earlier work specifically investigated how the information display of privacy policies could influence understanding, focusing on standardized formats, terms, and definitions. While the Android ecosystem uses a standard format and terms, clear definitions are not readily available to users.

3 Android Permissions and Display

Android app permissions are displayed to users at the time they decide to install any third-party app through the Android Market on the web or on the phone. Apps downloaded from third-party app stores (e.g., onlyAndroid, the Amazon Appstore for Android, etc.) do not necessarily show full permissions on their websites, however upon installing the application package (APK) the user is presented with a permissions screen variant.

Permissions are shown within the Android Market as detailed in the following diagram, Figure 1. A user browses applications using the view shown in Screen 1. Here there is a truncated description, information about ratings, reviews, screenshots, etc. If a user decides to install they click the button labeled with the price of the application, here **FREE.** This brings them to Screen 2,

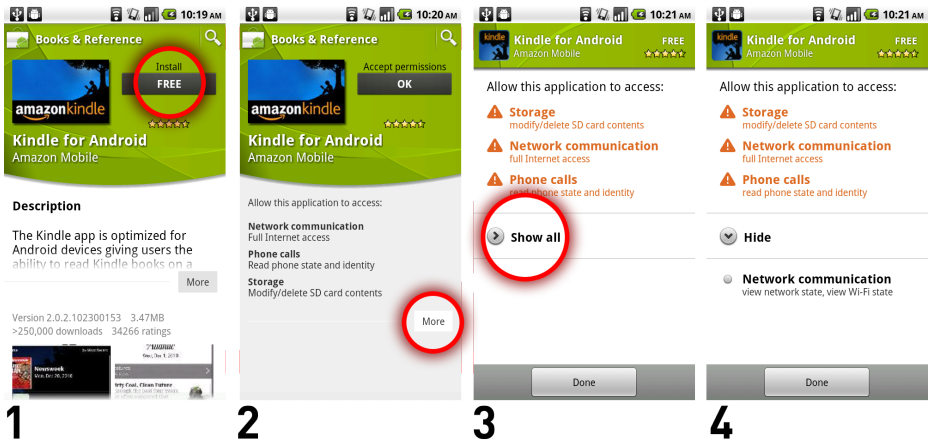

Fig. 1. The figure above shows the workflow for installing applications and viewing application permissions. Screen 1 shows the Amazon Kindle application as displayed in the Android Market. If a user were to click "FREE," circled in red, they are shown Screen 2, which allows them to Accept permissions and install the application, or to click the "Show" button which leads the user to Screens 3 and 4.

where they are given a short list of permissions. If users double tap the **FREE** button on Secreen 1, they skip Screen 2 and essentially approve the permissions without reading. Though Screen 2 serves the sole purpose of an interstitial permissions display between the market and a purchase decision, the complete list of permissions is not displayed.

To explore the full permission request they would click the **More** expander, bringing them to Screen 3. Here they would see a more complete list of permissions with some permissions shown in red and a **Show all** button, which displays the entire list if toggled.

At no point in this process is there an explicit way for users to cancel. The only way for users to not install the application after viewing the permissions is to use the physical back or home buttons on their phone.

The default permissions and groups in the Android SDK are detailed at Android's developer site.[2] The human readable terms are not included in the Android documentation.

4 Methodology

To reach a deeper and more nuanced understanding of how people navigate the current Android ecosystem, we conducted semi-structured interviews in Summer 2011 with 20 participants from Pittsburgh and Seattle. The interviews were exploratory in nature, seeking broad understanding of participants' interactions

[2] `http://developer.android.com/reference/android/Manifest.permission.html` and `http://developer.android.com/reference/android/Manifest.permission_group.html`

with their smartphones as well as diving deeply into issues surrounding the display of permissions, the safety of the Android Market, and possible harms of information sharing.

We recruited participants through flyers around each city and local Craigslist postings. Each candidate filled out a short pre-survey online before the interview, which allowed us to confirm they did use an Android-enabled smartphone. Those participants who opted into the subsequent interview arrived at our labs and completed our consent form allowing us to make an audio recording of their interview. Following the interview participants were given the opportunity to opt-in to share their application information with us, collected through a script running on a local laptop, which we connected their phone to via USB while they watched.

Participants' quotes throughout the remainder of the paper are taken from transcriptions made from the audio recordings of the interviews. Participants were paid $20 for successful completion of the interview, in the form of their choices of Target, Starbucks, or Barnes & Noble gift cards.

5 Demographics and Survey Responses

Our online survey was completed by 77 participants, 20 of whom completed the lab interview. The remainder of this paper will discuss solely those 20 users, whose demographic information and survey responses are summarized in Table 1. Participants P1-P6 are from Seattle, P7-P20 from Pittsburgh. 10 participants are female, and 10 are male. The ages of our participants range from 19 to 48, with an average of 29. Six of our participants were in tech-related fields, the other fourteen were not. Fourteen of our participants have been using Android for less than a year, five participants reported up to two years of use, and only one reported having used Android for more than two years.

6 Results and Discussion

The following sections detail our findings and participants' thoughts on various parts of the Android ecosystem. We begin with the responses to six of the ten permissions we asked participants to explain. These responses highlight the broad range of often inaccurate knowledge around the human-readable terms Android provides to users at application install. Next, we discuss general concerns, response to Android in the media, and awareness of malicious applications.

6.1 Permissions Display Understanding

Half of our participants mentioned the existence of the permissions display before being prompted. When a participant did mention the display, we immediately showed a paper example of one (using the Facebook, Pandora, or Amazon Kindle permissions, Screen 3 of Figure 1). Many reported reading, or at least

Participant overview

#	Gender	Age	Occupation	Phone provider	Phone model	OS version	Time Using Android	# Apps downloaded	# Apps really used
1	Female	24	Education	Verizon	LG Ally	I am not sure	1-6 months	1-10	A few 1-5
2	Male	48	Other	Verizon	HTC Incredible	Froyo	1-6 months	11-25	A few 1-5
3	Male	44	Agriculture	T-Mobile	Motorola Cliq	Cupcake	1-2 years	101+	A ton 20+
4	Male	19	Food Service	T-Mobile	Galaxy S	Eclair	1-6 months	11-25	A bunch 6-20
5	Female	45	Legal	Sprint	HTC EVO 4G	Honeycomb	1-6 months	1-10	A bunch 6-20
6	Female	26	Retail	Sprint	Samsung Replenish	I am not sure	1-6 months	1-10	A bunch 6-20
7	Female	34	Engineering	T-Mobile	LG Optimus	Eclair	7 months-1 year	11-25	A few 1-5
8	Male	23	Computers	Verizon	Motorola Droid X	Gingerbread	7 months-1 year	26-100	A ton 20+
9	Female	25	Other	Verizon	Motorola Droid X	I am not sure	Less than 1 month	1-10	A few 1-5
10	Male	32	Engineering	T-Mobile	HTC G2	Eclair	7 months-1 year	11-25	A bunch 6-20
11	Female	21	Entertainment	Sprint	Something Samsung	I am not sure	1-6 months	1-10	A few 1-5
12	Female	22	Other	T-Mobile	HTC MyTouch 4G	I am not sure	7 months-1 year	11-25	A few 1-5
13	Female	21	Don't work	Sprint	HTC Evo Shift	Gingerbread	1-2 years	1-10	A few 1-5
14	Male	20	Real Estate	Verizon	Motorola Droid X	Gingerbread	1-2 years	101+	A bunch 6-20
15	Male	36	Media / Publishing	Verizon	Motorola Droid 2	Froyo	7 months-1 year	1-10	A few 1-5
16	Male	22	Engineering	Sprint	HTC EVO 4G	Gingerbread	1-6 months	26-100	A bunch 6-20
17	Male	22	Don't work	Verizon	Motorola Droid 2	I am not sure	1-2 years	26-100	A bunch 6-20
18	Female	23	Other	T-Mobile	HTC G2	Gingerbread	More than 2 years	26-100	A bunch 6-20
19	Male	46	Engineering	AT&T	Google Nexus One	Gingerbread	1-2 years	26-100	A bunch 6-20
20	Female	21	Engineering	AT&T	Galaxy S II	Gingerbread	Less than 1 month	1-10	A few 1-5

Table 1. Overview of our 20 survey participants. Columns 2-4, list their age, gender, and industry. Columns 5-8 list their phone provider, phone model, Android OS version, and the amount of time they have primarily used Android devices. Columns 9 and 10 show the number of apps they have downloaded and the number they report frequently using. All information is self-reported.

skimming, these displays with some regularity, though also admitted they did not necessarily understand all of the terms used.

Participants were able to identify these screens, recognized them immediately, and occasionally felt very strongly about them. When asked if he read these screens frequently, one such participant said, "Yeah, all the time. It is just so easy for those apps to do whatever they want, it's a way to protect yourself I guess. Call me paranoid."

Some participants stated that they were not sure how trustworthy the permissions display was. One said of it, "Is it a requirement to be on there [the market] that the software tells you what it is accessing ... Are they required to notify me or not, I don't know."

Unfortunately, most participants do not believe they understand the terms used and have not gone out of their way to learn what they mean. We showed a list of ten permissions with the permission group label, in the fashion they would be shown in the permissions display, to each user and asked them to explain to us their understanding of each term (as if they were explaining it to a relative or friend who was less tech-saavy). Participants reacted to this task with consternation.

Here we present a selection of common, surprising, and strained responses that we received on six of the ten terms we tested.

– **Network communication: full Internet access**

  Of the 1100 applications reported on in Hornyack's work [7], full Internet access is by far the most requested permission, requested by 941 of the 1100 applications, or 85.5% of those surveyed. Our participants were aware of what the Internet is and understood why applications needed it. However how applications have access to it, why they would need to specify it, and how applications would function without it were often unclear.

  - "That you can have access to all kinds of websites, even the protected ones." –P1
  - "I would say, this just requires a data plan, and you would need to have Internet access." –P6
  - "Any app that needs to get information from somewhere other than that is local on the phone." –P7
  - "For this game to be active, it require Internet access, I cannot play it offline." –P11
  - "I would guess that this means, no I don't know. I just assume that it is like taking up data plans. Using stuff with your data plan." –P12

– **Phone calls: read phone state and identity**

  Read phone state and identity is a compound Android permission which leads to participants only correctly anticipating part of the functionality granted. While most of our participants correctly identified functionality related to phone state, the idea that that the phone has unique IDs that are

also being revealed with this permission was lost on most users (P18 notes a phone ID, but adds an incorrect ability, location). While some applications are requesting this permission to actually detect phone state, many current advertising packages require IDs.

- "I would assume it would probably be along the lines of, it knows when my phone is sleeping or in use or in a phone call, and the type of phone" –P2
- "Phone state whether it is on or off, and identity I would assume it is like my telephone number." –P3
- "So it knows whether or not I am in the middle of a call? I don't really know what that part [identity] means." –P13
- "Know where you are, and what phone ID you are on, what type of phone it is." –P18
- "If you are on the phone maybe it shuts itself off. ... Maybe like your carrier? Hopefully not like *who* you are." –P19

– **Storage: modify/delete SD card contents**

Modification and deletion rights themselves were reasonably well understood (largely using metaphors to computers or thumb drives), however what was stored on the phone itself, compared to the external SD card was often misunderstood or simply not disambiguated.

- "That I am about to reach my capacity, or I need to get a new one." –P1
- "Basically, just saving on your memory card or harddrive." –P6
- "That is for games and things to save your play, store information as needed." –P10
- "It can see what is on my SIM card and on the phone itself." –P13

– **Your location: coarse (network-based) location**

While we showed participants both types of location that can be collected within Android, participants largely understood that "fine (GPS) location" meant their exact position. It was the coarse location that seemed to confuse more participants. They all understood it was location related, but there was large deviation on how exact that location was.

- "No, I don't. I haven't the foggiest idea of what that means." –P3
- "Your network based location, I don't know the difference between the GPS, but basically where you are at." –P6
- "This is essentially just where your network is located, based on maybe I guess cellphone tower triangulation." –P10
- "I would guess that this is like the source of your data, like a satellite of some sort." –P12
- "Is coarse location, does that have anything to do with like, when you have phone service and are in range or roaming?" –P13

– **Your personal information: read contact data**

Nearly all participants understood that this permission was requesting their address book, or full contact list. Some gave examples of purposes why this was needed, citing apps that could use this (P7, P18). A few participants were confused due to the permission group label "your personal information." As a result, like P11, they thought it was reading only data about themselves.

- "I would think that would mean my contacts list." –P2
- "Like Facebook, and if it was syncing with contacts." –P7
- "My phone number." –P8
- "My personal information can reach them, my name, address, phone number, email address." –P11
- "Your phone number. They go into your phone, your contacts, and then on Skype they get the number, and he is your friend in your phone. I guess that is what this is." –P18

– **Your accounts: act as an account authenticator**

This permission was rarely correctly identified (P3, while being unsure, has the right idea), and often described as scary. P12 explicitly said it "freaked" her out. The accounts that participant thought could be "authenticated" or, controlled, were frequently not associated with the application itself, with many participants believing applications that asked for this permission would have much wider ranging abilities.

- "Controlling the account? I don't know. I have zero idea." –P2
- "That I don't like, I don't know what it means, ... my impression is that instead of me being able to authorize something, that application is saying it can." –P3
- "That freaks me out. What does that mean exactly, cause I am not quite sure." –P12
- "I dunno is that associated with my T-mobile account?" –P13
- "I don't know, I guess it is in charge of whatever accounts you open up." –P18

As seen above, for each of the permissions we received answers that we would grade as a misunderstanding. For some of the more obscure permissions, participants simply admitted they didn't know, or gave up. None of our participants correctly understood all of the permissions, and most participants simply repeated the words given in the human readable description, a sign they may not have had complete understanding of the of the concepts.

Participants asked questions throughout about why applications needed the access they requested. Participants frequently asked the interviewer for examples of applications that requested the permissions we listed, as well as why they were needed. The relationship between the applications and the permissions they requested seemed, without assistance, unknowable.

One participant, when asked if she thought others understood these permissions said, "No. I mean for me to have to think as much, and I have been using these things, and have been sort of a tech-geek for years. Yeah, thats concerning." With Vidas and Felt finding that developers are misunderstanding permissions, and often applying them without need, and self-proclaimed "tech-geeks" finding the terms difficult, common users are left near helpless. The system and terms as they currently stand have not been created or explained for the average user.

6.2 Application Selection

While permission information is one vector to assist users in selecting which applications to install, many of our participants reported heavy reliance on star ratings, full text reviews, and word of mouth. These other sources of information were better understood and more trusted.

While reading through the reviews was seen as time-consuming, word of mouth was a trusted way to find high quality applications. One participant recounted his frustrations with simply searching the store and why he trusted others' opinions: "I feel it is very much a trial and error exercise. And that, I don't know whether that app is a piece of crap or whether it works. So when I know somebody that tells me that this app is good, that really means a lot to me."

Participants also reported hearing about apps, largely of services and products they already used, through advertisements. One participant described his experience with seeing Android app ads, "I have seen magazines and billboards. The phones and the applications. For instance Time Magazine, they have written you can also download the application."

While most of our participants said they do not purchase apps at all, others said in certain cases they would. P6 said, "I try to look for the free ones first, and if I can't find any free ones I will go ahead and buy it."

6.3 Concern over Malicious Applications

We asked participants if they had heard anything about Android phones or Android applications in the news, media, or on the Internet. Participants told us about Android's increasing market share, comparisons between iOS and Android, and about a few well advertised apps.

When asked a follow up, to specifically inquire on their awareness of malicious applications in the Android Market, our participants were largely unaware of any such activity. While some said they had meant to, or were intending to install anti-virus applications on their phones, most were unconcerned about the threat of malware.

We attribute this lack of concern to two strands we picked up throughout the interviews. The first is an expected coping mechanism that many participants admitted to, a lack of trust in new technology. For example, participants reported an unwillingness to do banking from their phone. One participant said "I don't do banking online through my phone because that doesn't seem particularly safe to me.... I prefer an actual desktop for that because I am paranoid."

The second part of this lack of concern towards malicious apps shows a deeper misunderstanding of the Android ecosystem. All of our participants, without exception, believed (or hoped) that Android, the entity, was pre-screening applications before entrance into the market. Participants elaborately described the reviews that they thought were taking place, screening not just for viruses or malware, but running usability tests (on users!), blocking applications that were too repetitive, or even screening out applications not enough people would want. They believed Android was checking for copyright or patent violations, and overall expected Android to be protecting their brand.

Additionally, people were unaware of who was actually running Android. They saw it as a vague entity, that they could not attribute to any specific parent company. Some knew and some guessed it was Google, others realized they had never stopped to think about that before and were simply unable to attribute the OS to any other company.

7 Conclusion

Users do not understand Android permissions.

Specifically, the human-readable terms displayed before installing an application are at best vague, and at worst confusing, misleading, jargon-filled, and poorly grouped. This lack of understanding makes it difficult for people, from developers to nontechnical users, to make informed decisions when installing new software on their phones. Largely, the permissions are ignored, with participants instead trusting word of mouth, ratings, and Android market reviews.

Users also are largely uninformed about the existence of malware or malicious applications that could be in the Android market. They have difficulty describing the possible harm that could be caused by applications collecting and sharing their personal information. While participants stated they try to find good applications in the market, they believe they are protected by oversight processes which do not exist.

Overall, users are not currently well prepared to make informed privacy and security decisions around installing applications from the Android market.

8 Acknowledgments

The authors would like to thank Intel Labs Seattle for their sponsorship of this work. We acknowledge our colleagues at Intel Labs Seattle, Microsoft Research, the University of Washington, and Carnegie Mellon University, including Seungyeop Han, Peter Hornyack, Jialiu Lin, Stuart Schechter, and Tim Vidas. Additional support was provided by the National Science Foundation under Grants CNS-1012763 (Nudging Users Towards Privacy) and DGE-0903659 (IGERT: Usable Privacy and Security). Additional support was provided by NSF grants CNS-0905562 and DGE 0903659, by the CMU/Portugal ICTI Program, by CyLab at Carnegie Mellon under grants DAAD19-02-1-0389 and W911NF-09-1-0273 from the Army Research Office as well as Google.

References

1. Au, K.W.Y., Zhou, Y.F., Huang, Z., Gill, P., and Lie, D. 2011. Short paper: a look at smartphone permission models. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (SPSM '11).
2. Barra, H. 2011. Android: momentum, mobile and more at Google I/O. The Official Google Blog. http://googleblog.blogspot.com/2011/05/android-momentum-mobile-and-more-at.html
3. Barrera, B., Kayacik, H.G., van Oorschot, P.C., and Somayaji, A. 2010. A methodology for empirical analysis of permission-based security models and its application to android. In Proceedings of the 17th ACM conference on Computer and communications security (CCS '10).
4. Enck, W., Gilbert, P., Chun, B., Cox, L.P., Jung, J., McDaniel, P., and Sheth, A. 2010. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In Proceedings of the 9th USENIX conference on Operating systems design and implementation (OSDI'10).
5. Felt, A.P., Chin, E., Hanna, S., Song, D., Wagner, D. 2011. Android Permissions Demystified. In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11).
6. Gartner. 2011. Gartner Says Sales of Mobile Devices Grew 5.6 Percent in Third Quarter of 2011; Smartphone Sales Increased 42 Percent. http://www.gartner.com/it/page.jsp?id=1848514
7. Hornyack, P., Han, S., Jung, J., Schechter, S., and Wetherall, D. 2011. These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11).
8. Juniper Networks. 2011. Mobile Malware Development Continues To Rise, Android Leads The Way. http://globalthreatcenter.com/?p=2492
9. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R. 2009. A "nutrition label" for privacy. The 5th Symposium on Usable Privacy and Security (SOUPS '09).
10. Kleimann Communication Group, Inc. 2006. Evolution of a Prototype Financial Privacy Notice. Available: http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf
11. McAfee Labs. 2011. McAfee Threats Report: Third Quarter 2011. Available: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2011.pdf.
12. Namestnikov, Y. 2011. IT Threat Evolution: Q3 2011. Available: http://www.securelist.com/en/analysis/204792201/IT_Threat_Evolution_Q3_2011.
13. Rosenberg, J. 2011. The meaning of open. The Official Google Blog. http://googleblog.blogspot.com/2009/12/meaning-of-open.html
14. Smetters, D.K., and Good, N. 2009. How users use access control. In Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09).
15. Vidas, T., Christin, N., and Cranor, L.F. 2011. Curbing Android Permission Creep. W2SP 2011.
16. Wetherall, D., Choffnes, D., Greenstein, B., Han, S., Hornyack. P., Jung, J., Schechter, S., and Wang, X. 2011. Privacy Revelations for Web and Mobile Apps. HotOS'11.

Appendix: Interview Questions

The entire interview guide, as well as additional quotes and some coded data, can be found online at http://patrickgagekelley.com/research/android.