Analyzing unnecessary permissions requested by Android apps based on users' opinions

Jina Kang[1], Daehyun Kim[1], Hyoungshick Kim[1] and Jun Ho Huh[2]

[1]Department of Computer Science and Engineering, Sungkyunkwan University, Korea
[2]Honeywell ACS Labs, USA

Abstract. Many existing mobile apps request for unnecessary permissions knowing that users often ignore permission warning messages. We conducted an online user study to investigate how users feel about permissions being requested by both free and paid Android apps. Results show that users tend to feel that free Android apps request for more unnecessary permissions compared to paid apps. Users also felt that older apps (those that are previously released and have gone through several updates) request for more unnecessary permissions than those that are newly released. Based on that observation, we surmise that many developers initially publish apps that require a small set of permissions (so that users are not discouraged from installing an app), and gradually add more permissions to their apps through updates.

Keywords: permission; Android; smartphones; usable security

1 Introduction

When a user tries to install a mobile application (or an app) from `Google Play` (marketplace for Android apps), a list of *permissions* required by that app is shown to the user before initiating the installation process. Android asks the user if she or he wishes to continue installing the app and grant those permissions to that app. Most casual users, however, are not too interested in those permissions. Recent studies [5, 7, 6] have shown that the majority of users tend to ignore permission warning messages at installations time. Warning messages pop up on the screen when users have already decided to install an app; at that stage, users probably just want to continue with the installation without being interrupted [2, 7]. Even for users who pay careful attention to permissions being requested, permission descriptions are often confusing and are hard to understand.

This is a big concern because more and more apps are increasingly asking for access to sensitive information on your phone to function properly. Facebook Messenger, for instance, asks to "record audit with the microphone (at any time without your confirmation)", "access the phone's call logs", "read data about contacts stored on the phone", etc. In fact, a study shows that 96% of iOS apps require email permissions, 92% require address book, 84% require location permissions, 52% require camera permissions, and 32% require calendar permissions [8]. Companies like Facebook, Twitter and Linkedin with huge userbase

have recently figured out how to generate strong revenue through mobile advertisements (e.g., through sponsored ads and posts). To enhance the relevance and success of their ads (i.e., targeted ads), such companies will try to gather as much personal data as possible and the worst is yet to come in terms of apps requesting for unnecessary permissions.

As an extension of recent studies on permissions, we investigate how end-users feel about the level of permissions being requested by popular Android apps, asking which permissions seem unnecessary or necessary for an app to function properly. Users gave their opinions on the necessity of requested permissions; e.g., 'Angry Birds' (a free popular Android game) requiring a permission to read phone state and identity information is questionable. In many cases, such assessments for excessive permissions will be subjective. To strengthen the analysis, we gathered 234 popular Android apps from `Google Play` and conducted a user study with 125 participants, asking each participant to give their opinions on permissions being requested by all 234 apps. As mentioned above, since permission warnings are typically ignored by the majority of users [5, 7, 6], it is integral to identify unnecessary permissions and remove them (or highlight them) to follow the least privilege principle [9]. This study might be the cornerstone of identifying such unnecessary permissions in apps. Our key contributions can be summarized as follows:

- We identified the lists of permissions that are frequently considered by users as unnecessary or incomprehensible. About 24% of the permissions we tested with were frequently considered as unnecessary. More permissions from the `PERSONAL_INFO`, `LOCATION`, and `MESSAGES` permission groups were considered to be unnecessary than those from the other groups. Some permissions were totally incomprehensible even for security experts. Many permissions defined by developers (e.g., `com.skt.aom.permission.AOM_RECEIVE`) were not well defined.
- We showed that users are more concerned with the permissions in free Android apps than with those in paid apps. Free apps tend to ask for more permissions that would allow them to collect sensitive personal information (e.g., 'Read your contact data'), implying that free apps rely more on the collection of personal data.
- We found that the numbers of unnecessary permissions in older apps (that have gone through several updates) are significantly greater than those in newly released apps. We surmise that many developers initially publish apps with a small set of permissions, but, through updates, incrementally add more unnecessary permissions.
- We observed that users with more awareness of permissions were more sensitive and careful about unnecessary permissions. This might be an evidence that security education can help users identify unnecessary permissions and make better decisions.

We believe those observations can help build more effective and reliable permission models for the Android platform. For example, permissions that are

frequently considered as unnecessary can be highlighted to inform users about potentially dangerous permissions.

2 Related work

The Android permission system limits access to sensitive data (SMS, contacts, calendar), resources (battery or log files) and system interfaces (Internet connection, GPS, GSM). To invoke sensitive APIs, users should grant the relevant permissions for an app at install time. Even though Android 4.3 provides a hidden feature called "App Ops", which allows users to selectively revoke unnecessary permissions on a per-app basis, users are still relied upon to determine the permissions that should not be granted.

Many researches have been concerned with understanding permissions used in Android. Kelley et al. [7] showed that most users cannot understand permission screens. Felt et al. [5] showed that Android permissions fail to clearly inform the majority of users about their privileges. To that end, Kelley et al. [6] suggested the use of a new design called 'privacy checklist' to display (potential) privacy risks of using an app, and showed that the proposed display does significantly affect users' app selection decisions compared with the current interface.

Felt et al. [4] surveyed 100 paid and 856 free apps to identify the most frequently used dangerous permissions (i.e., which generate permission warning notification) and showed that there was a significant gap between the free and paid apps in the frequency of dangerous permissions being requested; for example, 14% of free apps ask for the `INTERNET` permission, but only 4% of paid apps ask for the same permission. This disparity supports the hypothesis in [1] where free apps may frequently ask for the `INTERNET` permission in order to load advertisements. We extend their work by considering the relationship between the apps and the permissions. Unlike ours, Felt et al. [4] used a fixed set of common permissions categorized as `Normal`, `Dangerous` and `Signature` by Google but some apps even use `Dangerous` permissions legitimately.

One of the most important challenges for a better permission system is to develop automated tools to detect overprivileged and (potentially) malicious apps. Stowaway [3] was designed to detect overprivileged Android apps by checking whether an app asks for more permissions than what is needed. Felt et al. [3] found that about one-third of 940 Android apps are considered overprivileged. Vidas et al. [11] proposed a static analysis tool for finding the actual (minimum) set of permissions that an app uses to behave correctly.

3 User Study

3.1 Study Design

Our study was designed to answer the following research questions:

– **RQ1.** What are the most frequently reported unnecessary or incomprehensible permissions in Android apps?

Fig. 1: An example of survey questions: (1) a randomly chosen app's screenshot (captured from `Google play`) was shown in the leftmost window; (2) the description of the app (obtained from `Google play`) was presented in the middle-upper window; (3) questions about comprehensibility of the permissions requested by the app were displayed with using two scales (incomprehensible–comprehensible) radio buttons in the middle-bottom window; and (4) when clicking the 'comprehensible' button for a permission, another question about excessiveness of the permission was displayed with using a three scales (not excessive–maybe–excessive) radio button in the rightmost window.

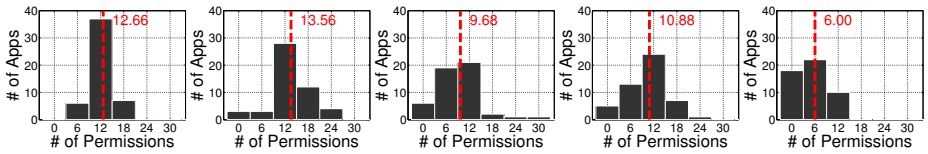
- **RQ2.** Do free apps demand more unnecessary permissions than paid apps?
- **RQ3.** Does the number of unnecessary permissions requested by an app significantly increase over time?
- **RQ4.** Are users with more awareness of permissions also more sensitive toward unnecessary permissions being requested?

Answers to those research questions will help us understand more clearly how smartphone users behave when they install apps, and help them make better decisions by identifying unnecessary permissions requested by apps.

We conducted an online user study to examine the level of Android users' understanding and concerns about the permissions requested by apps. The survey could be accessed in an anonymous way by both PC and mobile users.

A pilot study was first conducted with four subjects (who were familiar with Android) to identify issues with the study and to get a sense of how well the questions and user interfaces were designed. Final modifications were made on the questionnaire based on the observations from the pilot study. Here is an overview of study design:

1. First, we gathered the participants' consent and asked them to complete a background questionnaire to obtain demographic information (gender, age,



(a) `T--G` (b) `T--F` (c) `T--P` (d) `T--N--F` (e) `T--N--P`

Fig. 2: Histograms of the number of permissions for the apps in each of the five categories (`Top Grossing`, `Top Free`, `Top Paid`, `Top New Free`, and `Top New Paid`) in `Google Play`. The red dotted lines represent the mean of the number of permissions over the all apps in each category.

job, and Android version) and data to assess their familiarity with Android permissions. To assess familiarity with Android permissions, we asked the following two questions: (Q1) Do you know what permissions mean when installing Android apps? and (Q2) Do you pay attention to permission information when downloading an app?.

2. Second, we provided an example (training) survey to increase participants' familiarity with our survey procedure. It was designed to help participants learn how to complete the tasks: given an app, participants were asked to read the description of the app and then carefully select incomprehensible or unnecessary permissions from the list of permissions requested by that app.
3. Third, in the real study, participants were asked to complete the same set of tasks for five randomly selected apps (see an example in Fig. 1). An app was randomly selected from each of the following five categories in `Google Play`: `Top Grossing`, `Top Free`, `Top Paid`, `Top New Free`, and `Top New Paid`.

3.2 Android Apps Used in Our Survey

We downloaded the top 50 Android apps from each of the five categories (`Top Grossing`, `Top Free`, `Top Paid`, `Top New Free`, and `Top New Paid`) in the Korean `Google Play` store. Some categories were not mutually exclusive though. For example, 10 apps from the `Top Grossing` category were also shown in `Top Free` and `Top Paid` categories. Consequently, we compiled a total of 73 permissions from 234 popular Android apps. Those permissions represent only a portion of all Android permissions, but are the most frequently used ones.

Histograms in Fig. 2 show the distributions of the number of permissions required all the apps in each category. From those histograms, we can see that `Top Free` and `Top Grossing` have relatively more permissions than the other categories.

3.3 Demographics

We recruited participants who own a smartphone by posting fliers about our study on bulletin boards in a university. We clarified the academic motivations

Gender	
Male	72.73%
Female	27.27%
Age group	
18–29	97.98%
30–49	2.02%
Highest level of education completed	
High school	85.86%
College/University	14.14%
Smartphone platforms	
Android	95.96%
iOS	4.04%
Do you know what permission means when installing apps?	
Yes	56.57%
Maybe	28.28%
No	15.15%
Have you paid attention to permission at install time?	
Yes	25.00%
Maybe	28.57%
No	43.43%

Table 1: The demographics of the participants

behind this study to encourage participants to pay more attention to our study. Participants also received a $2 honorarium for completion of the user study after investigating the validity of their responses.

During a week period, 125 participated in the survey, and 99 respondents (out of that 125) correctly completed the questionnaire. The majority of the respondents were male (72.73%) and were in the age group of 18–29(97.98%). 56.57% said that they are aware of permissions, while only 25% of them actually paid attention to permissions during app installation (See Table 1).

4 Study Results and Discussion

This section analyses the results collected from the user study, and discusses the participants' levels of concerns with Android permissions with respect to their necessity and comprehensibility.

4.1 Incomprehensible Permissions

We first present the list of permissions that were frequently mentioned by participants to be *incomprehensible* (see Table 2). In order to identify those permissions, we used "yes" or "no" type of questions, asking whether a participant thinks a permission is incomprehensible.

Type	Permission
Android (3)	– Allows an application to call killBackgroundProcesses(String) – Allows an application to read from external storage – Allows an application to perform I/O operations over NFC
Google (1)	– Use the authentication credentials of an account
Third-party (1)	– `com.skt.aom.permission.AOM_RECEIVE`

Table 2: The list of frequently mentioned incomprehensible permissions. The number inside the parentheses in each type indicates the number of permissions included in the type.

In general, a permission can be considered incomprehensible when "yes" responses are more likely to occur than "no" responses. After counting the numbers of "yes" and "no" responses, respectively, for each permission, the binomial exact test (one-tailed) was used to test whether the number of "yes" responses was significantly greater than the number of "no" responses (i.e., the expected probability of the "yes" response is significantly greater than 0.5).

From the study results, only 5 of 73 permissions (about 6.8%) were frequently identified as incomprehensible permissions. Table 2 shows those incomprehensible permissions. We observed that all of those permissions contained a technical terminology or a jargon (e.g., 'NFC' or 'killBackgroundProcesses') that a casual user may not know. Three Android-defined permissions were also included in that list (see the number inside the parentheses in the 'Android' type). This shows that even some of the official, Android-defined permissions were not well understood.

Our results were quite different from a previous study [7], which showed that the majority of permissions were not well understood by Android users. Contrastingly, only about 6.8% were seen as incomprehensible permissions in our study. The different demographics in the two studies may have caused that: Section 3.3 shows that our sample of users, on average, are younger (97.98% of them were aged between 18 and 29) and have higher education (all participants were university students) than those who have participated in the previous study [7].

4.2 Unnecessary Permissions

In this section, we present the list of permissions that were frequently mentioned by participants to be *unnecessary*.

To ask whether a permission seems unnecessary for a given app, only those who understood the meaning of a permission were sequentially asked to respond to a question about the necessity of that permission. A three-point Likert scale ranging from 0 ("disagree") to 2 ("agree") was used to answer that question. A permission is considered unnecessary when "agree" responses occur more than "disagree" responses. After counting the numbers of "agree", "neutral" and "disagree" responses for each permission, the one-tailed t-test was used to test whether the mean score was significantly greater than 1.0, which indicates the neutrality level.

Category	Permission
`system tool` (2)	– Allows an application to call killBackgroundProcesses(String) – Changing the general settings of the system
`phone call` (1)	– Reroute outgoing calls
`personal information` (5)	– Allows an application to read the user's contacts data – Allows an application to read the user's call log – Allows an application to write (but not read) the user's call log – Allows an application to write (but not read) the user's calendar data – Allows an application to read the user's calendar data
`location` (3)	– Allows an application to access precise location from location sources such as GPS, cell towers, and Wi-Fi – Allows an application to create mock location providers for testing – Allows an application to access extra location provider commands
`message` (1)	– Allows an application to read SMS messages

Table 3: The list of frequently mentioned excessive permissions. The number inside the parentheses in each category indicates the number of permissions included in the category.

From the results, 12 of 73 permissions (about 16.4%) were frequently identified as unnecessary permissions (see Table 3). To analyze the characteristics of those permissions, we also looked at their category information defined by Google (see more details in `http://developer.android.com/reference/android/Manifest.permission_group.html`). We observed that participants were particularly concerned about the permissions that would allow apps to access personal data such as contacts, call logs, calendar, or locations. For example, 5 of 11 personal data permissions (about 45.45%) were frequently mentioned as unnecessary, and 3 of 4 location permissions (75%) were considered as unnecessary. On the other hand, participants considered only 2 of 26 permissions (about 7.69%) in system tools as unnecessary. Moreover, participants were not too concerned with the permissions that would give apps direct access to hardware components like audio or camera. Such a lack of concern could have serious security and privacy implications as discussed in several previous studies (e.g., [12, 10]). For instance, a malicious app that has requested for the camera permission could silently take pictures or record videos of private moments and transfer them over the air.

4.3 Comparing Free Apps and Paid Apps

This section analyses participants' responses to permissions in *free* apps compared with those in *paid* apps. We divided the apps into free (`Top Free` and `Top New Free`) and paid (`Top Paid` and `Top New Paid`) apps and analysed the differences in the required level of unnecessary permissions as opinionated by the

participants – if the score is high for an app, that app can be considered risky in terms of the number of unnecessary permissions that it has.

From the study results, the mean score for the free apps was 5.9495 with the standard deviation of 6.4231 while the mean score for the paid apps was 4.3939 with the standard deviation 5.9085. We statistically tested the difference between free and paid apps using unpaired one-tailed t-test ($P \leq 0.05$) and obtained the P-value of 0.0063. From that test result, we can state with statistical significance that the mean score for free apps is higher than the mean score for paid apps, indicating that free apps (`Top Free` and `Top New Free`) request for more unnecessary permissions and tend to be riskier than paid apps (`Top Paid` and `Top New Paid`).

4.4 Comparing Top Apps and Top New Apps

This section analyzes participants' responses to excessive permissions in *top* apps compared with those in *top new* apps. To demonstrate this, we divided the apps into top (`Top Free` and `Top Paid`) and top new (`Top New Free` and `Top New Paid`) apps and analysed their differences in the number of excessive permissions.

From the study results, the mean score for the top apps was 6.5455 with the standard deviation of 7.4244 while the mean score for the top new apps was 3.7980 with the standard deviation of 4.2973. We statistically tested the difference between top and top new apps using unpaired one-tailed t-test ($P \leq 0.05$) and obtained a very small P-value ($\ll 0.0001$). From that test result, we can state with statistical significance that the mean score for top apps is significantly higher than the mean score for top new apps, indicating that top apps request for more unnecessary permissions and turned out to be riskier than the newly released apps.

This observation is interesting since it indicates that the developers might deliberately include less permissions in the initial version of an app – to make it look safer to use – but could be gradually adding more permissions through updates. In depth study of a randomly selected sample of apps (that requested a large number of permissions) reinforced that observation: for example, an app designed to allow home screen customization requested for unnecessary permissions like 'Allows an app to access precise location from location sources such as GPS, cell towers, and Wi-Fi','Allows an application to read SMS messages' and 'Allows access to the Gmail content provider' when it pushed out updates that did not have noticeable new features.

If a small number of extra permissions are requested incrementally through each update it would be harder for users to notice it, even if Google Play informs users about newly requested permissions. It might also be true that this trend is due to developers adding more features to their apps through updates and requiring more permissions as a result.

4.5 In Depth Analysis of Free Apps

It is our intuition that most free apps would heavily rely on mobile advertisements to generate revenue, and for such a reason, they tend to request more

unnecessary permissions than the paid apps (to analyse personal data and enhance advertisement relevance). In this section, we study the number of free apps that have mobile advertisements and request for unnecessary permissions. We use static analysis tools and manual validation for this analysis.

We studied with 76 different free apps. To count the number of free apps that have in-app advertisements, we used three advertisement detectors (`Lookout Ad Network Detector`, `TrustGo Ad Detector`, and `AppBrain Ad Detector`), which cover most popular advertisement networks such as `AdMob`, `TapJoy`, `Cauly` and `InMobi`. From our observations, 29 of 76 free apps (about 38.16%) had in-app advertisements. In particular, many free game apps (e.g., `Bouncing Ball` and `Psychological Test`) used advertisement networks. Among the remaining 47 apps, 10 apps requested for permissions to access personal data, and at least 6 apps requested for unnecessary permissions that seemed irrelevant to their core functions.

4.6 Effects of Users' Interests in Permissions

From the demographics in Section 3.1, we found that 56.57% of participants answered 'Yes' to the question 'Do you know what permission means when installing apps?'. To check whether those who answered 'Yes' are more sensitive toward unnecessary permissions (than those who answered 'Maybe' or 'No'), we divided participants' responses according to their answers ('Yes': 56.57%, 'Maybe': 28.28%, 'No': 15.15%) and analysed the differences in how they perceived excessiveness of permissions.

As mentioned before, each participant evaluated the excessiveness of every permission in each of five randomly selected apps using a three-point Likert scale, ranging from 0 ("disagree") to 2 ("agree"). Based on the sum of a participant's ratings for all the permissions in five apps, those who answered 'Yes' scored the highest with 5.7500 on average (standard deviation: 4.9036). The mean score for those who answered 'Maybe' is 3.8214 (standard deviation: 3.7718) and 3.4667 (standard deviation: 3.6227) for those who answered 'No'.

Unpaired one-tailed t-tests ($P \leq 0.05$) were used to compare their answers in a statistical manner. From these results (`Yes` vs `Maybe`: 0.0357, `Yes` vs `No`: 0.0486, `Maybe` vs `No`: 0.3836), we can see that there were significant gaps between participants who answered 'Yes', 'Maybe', and 'No' except for the case of 'Maybe' and 'No'. On the basis of those testing results, we surmise that subjects who are more aware of the meaning of permissions are more picky and careful when it comes to reading permission requests of apps. That finding, to some extent, can support the claims about how security education can help users identify permissions that seem unnecessary given the functions of an app, and make better decisions about upon installing it.

We ran similar tests on the question 'Have you paid attention to permission at install time?' but did not find any statistically significant differences among the participants.

5 Limitations

Our study has three limitations that are worth mentioning. First, we analyzed only 73 permissions from 234 popular apps rather than the full list of Google-defined permissions (145 Android-defined permissions).

Second, in the user studies, we asked the participants for their opinions on the necessity of the permissions based on the description of app features and functions. Fully understanding app functions and accurately selecting unnecessary permissions by just reading app descriptions could have been difficult for some participants.

Third, all of our participants are from a single pool of users. Finding an online survey tool (e.g., Amazon's Mechanical Turk in the U.S.) and surveying a random pool of participants in Korea was not easy. To that end, we conducted an online survey within an university campus, and, as a result, all of the participants were university students. That could have affected the results for identifying incomprehensible permissions. We originally expected that many participants would have low level of understanding of permissions and their terms, but the results showed that only about 7% of the participants struggled with the terms of permissions. Participants' education level and age have probably affected that.

6 Conclusion

We studied how participants feel and think about Android permissions in terms of how 'unnecessary' and/or 'incomprehensible' they might be. We studied 73 permissions in total, where 12 of them have been frequently opinionated by the participants to be unnecessary: such permissions can leak personal/sensitive information about users and may even cause damages to the mobile devices.

Not surprisingly, free apps tend to ask for more permissions, where those permissions often lead to collection of personal information. Free apps heavily rely on advertisements as their primary monetization means, and that is one reason why we suspect that those apps ask for more permissions. We rated participants' answers based on a simple Likert scale to measure how much free apps and paid apps rely on unnecessary permissions. Free apps scored higher to indicate that they require more number of permissions that are frequently opinionated by users as unncessary. From just the perspective of the permissions that an app has, those free apps seem to be relatively more dangerous and risky than paid apps. On those lines, our study shows that users are more concerned with permissions requested by free apps since they clearly ask for more permissions.

Interestingly, newly released apps (whether they are paid or free) tend to have much smaller number of permissions than those that have been released some time ago and have gone through several updates. It seems that the developers are putting a small number of permissions in their first releases (newly released apps), but gradually adding more permissions as they release more updates. Hence, users should be aware that the permissions they allow on a newly installed app might look completely different after installing a few updates on it.

7 Acknowledgements

This research was partly supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (NIPA-2014-H0301-14-1010) supervised by the NIPA (National IT Industry Promotion Agency) and is funded in part by the ICT R&D program (2014-044-072-003 , 'Development of Cyber Quarantine System using SDN Techniques') of MSIP/IITP.

References

1. David Barrera, H Güneş Kayacik, Paul C van Oorschot, and Anil Somayaji. 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)*, 2010.
2. Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the 27th ACM conference on Human factors in computing systems*, 2009.
3. Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. Android permissions demystified. In *Proceedings of the 18th ACM conference on Computer and communications security (CCS)*, 2011.
4. Adrienne Porter Felt, Kate Greenwood, and David Wagner. The Effectiveness of Application Permissions. In *Proceedings of the 2nd USENIX Conference on Web Application Development (WebApps)*, 2011.
5. Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android Permissions: User Attention, Comprehension, and Behavior. In *Proceedings of the 8th Symposium on Usable Privacy and Security (SOUPS)*, 2012.
6. Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy as part of the app decision-making process. In *Proceedings of the 31st ACM conference on Human factors in computing systems*, 2013.
7. PatrickGage Kelley, Sunny Consolvo, LorrieFaith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In *Proceedings of the 16th Financial Cryptography and Data Security*. 2012.
8. John Leyden. The TRUTH about LEAKY, STALKING, SPYING smartphone applications. The Register, 2014.
9. Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.
10. Roman Schlegel, Kehuan Zhang, Xiaoyong Zhou, Mehool Intwala, Apu Kapadia, and XiaoFeng Wang. Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones. In *Proceedings of the 18th Network and Distributed System Security Symposium (NDSS)*, 2011.
11. Timothy Vidas, Nicolas Christin, and Lorrie Cranor. Curbing android permission creep. In *Proceedings of the 5th Workshop on Web 2.0 Security and Privacy (W2SP)*, 2011.
12. Nan Xu, Fan Zhang, Yisha Luo, Weijia Jia, Dong Xuan, and Jin Teng. Stealthy Video Capturer: A New Video-based Spyware in 3G Smartphones. In *Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec)*, 2009.