Smartphone Privacy in Mobile Computing: Issues, Methods and Systems

Rui LIU[◇] Jiannong CAO[♠] Lei YANG[♣]

The ubiquitous and ever-more-capable smartphones bring forth unprecedented performance in mobile computing. The pursuit of high quality mobile mobile applications and services may however compromise user privacy, which is a pivotal issue in mobile computing. In this article, we survey the state of the art on smartphone privacy, focusing on current issues, proposed methods and existing systems. We discuss the characteristics of smartphone privacy in mobile computing and then investigate a number of related work and on-going research in detecting and mitigating privacy risks in the smartphone. According to our findings, we point out future challenges of smartphone privacy in mobile computing.

1 Introduction

Taking advantage of increasing storage resources, powerful computing capacity, high-quality networks and sophisticated embedded sensors, a lot of mobile devices including smartphones, PDAs, tablets, Mobile PC and wearable devices provide us various services in our daily life [1]. These almost always-on devices make our life and work more comfortable, as well as monitor our activities. It is not uncommon that users' privacy is disclosed when they are using their mobile devices. One of the most threatening of all is smartphone since people spent much time on it every day [2]. No one can deny that smartphones have already penetrated into different aspects of our life, ranging from our photos, email, social networking accounts to financial information. Our information stored in our smartphones may disclose accordingly. Therefore, privacy of smartphone users is a pivotal issue in mobile computing.

Mobile computing is an interaction technology by which a computer is expected to be a mobile device that enables access to resources at any time, from any location. There are several layers in the typical architecture of mobile computing for smartphones: mobile operating system, mobile application, mobile communication. The smartphone application interacts with users and provides services to them directly. These applications are generated based on plentiful APIs and resources, which are provided by different mobile operating systems. The mobile operating systems, like Android and iOS, are supported by increasing storage resources, powerful computing capacity, high-quality networks and sophisticated embedded sensors in hardware layer. The communication is another important function of smartphone in mobile computing. Under various kinds of network, users can access network, share data and receive information. Much attention goes into the privacy leaks in mobile communication from connectivity perspective [3–5]. Mobile sensing is a novel sensing paradigm which utilizes embedded mobile sensors to collect and share data. It is becoming mature and involved in our life. It, unfortunately, may disclosure users' information since the people have no awareness what can be inferred from the sensory data. Mobile sensing has revealed the public privacy concerns.

Therefore, in this survey, we study privacy issues of smartphone users in terms of three aspects: mobile operating system, mobile application and mobile sensing, as shown in Fig. 1. Our main contribution is to investigate the characteristics of smartphone privacy, point out the privacy issues according to three aspects in Fig. 1 and provide a taxonomy of existing methods and systems which can detect, analyze and mitigate privacy issues of smartphone users.

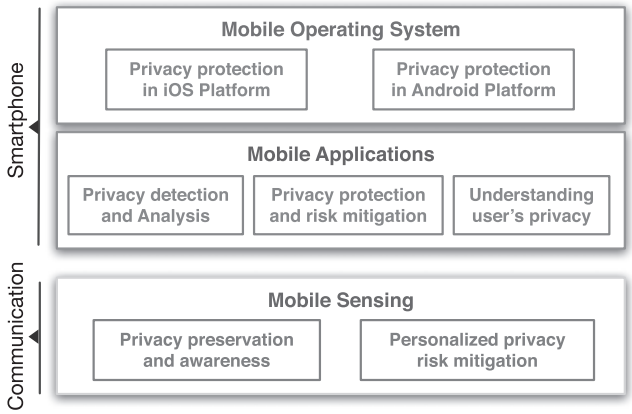

Fig. 1: The framework of the survey

The remainder of this paper is organized as follows, we illustrate and characterize smartphone privacy from human-centric and technology-centric perspectives in section 2. Subsequently, we point out some issues of smartphone privacy in section 3. In section 4, we present and classify a number of related works to solve the privacy issues on mobile operating system, mobile application and mobile sensing. Finally, we identify some future research directions in section 5 and conclude the article in section 6.

2 Characteristics of Smartphone Privacy

Since understanding privacy served as the underpinning of the smartphone privacy research, we discuss some existing privacy definitions and describe important characteristics of smartphone privacy in this section. The characteristics will be applied throughout the remainder of this paper.

Privacy is by no means a fad of modern society. In 1890,

◇ Department of Computing, The Hong Kong Polytechnic University csrliu@comp.polyu.edu.hk
♠ Department of Computing, The Hong Kong Polytechnic University csjcao@comp.polyu.edu.hk
♣ Department of Computing, The Hong Kong Polytechnic University csleiyang@comp.polyu.edu.hk

Two U.S. lawyers proposed a prevalent definition, private life, habits, act, relations and the right to be alone [6]. With the proliferation of information technology, Wesin proposed that privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others, and it came to be known as information privacy [7]. These two acknowledged definitions both emphasized that privacy to users should be an ability to express themselves selectively. Moreover, as proposed by Bellotti and Sellen [8], privacy definition is not static and monolithic but should emphasize different aspects due to new technology, patterns of use and social norms development.

In order to cater to the specific characteristics of smartphone, we express smartphone privacy from two perspectives, human-centric and technology-centric.

2.1 Human-centric Privacy

Based on previous definitions and discussion, a number of definitions emphasize that people's concern is one of the most important factors. When people use smartphone, on one hand, it is routine for them to provide their information for better services. On the other hand, they are reluctant to exposure sensitive data due to privacy concern [9]. Therefore, human-centric smartphone privacy in mobile computing focuses on the balance between privacy and services [10]. Human-centric privacy of smartphone in mobile computing mainly includes expectation, awareness and authorization.

- **Expectation** means people's expectation about how their information can be used by smartphones. Namely, the data usage in smartphone should meet the users' expectation. For instance, users' expectation of a game application is entertainment rather than accessing many other kinds of information. Some game applications require a plethora of data, including users' accounts, approximate location information, personal photos and device ID, which may be not necessary for functioning [11]. The information abuse make smartphones' behaviors beyond users' expectation. A number of research have been carried out to investigate users' expectation about their information in the smartphones [12–14].
- **Awareness** explains the degree of agreement between users' awareness and actual behaviors of smartphones. It is a curial issue since many free applications in Android and iOS platform collect users' data without their awareness and intervention [15]. A lot of research works concentrate on it [16, 17], since users' awareness is significant in human-centric smartphone privacy.
- **Authorization** expresses all decisions about users' data in the smartphone, including removing, collecting, analyzing, publishing, should be made by themselves. Some researchers try to built tools, systems and frameworks to protect users' privacy in the light of their own decisions [18, 19].

Noted that the ultimate goal of human-centric smartphone privacy is to find balance between services and privacy. Namely, according to the nature of human-centric privacy, protecting users' privacy in smartphone is based on their attitude, concern, preference.

2.2 Technology-centric Privacy

Technology-centric smartphone privacy concentrates on protecting or preserving privacy using technique according to different context for various goals, such as designing algorithms, developing mechanisms and building systems to prevent sensitive information from stealing and attacking. Technology-centric smartphone privacy mainly includes sensitivity and anonymity.

- **Sensitivity** refers to sensitive information stored in the smartphone. These information should be protected as much as possible. Users' privacy can be disclosed after obtaining some sensitive data or inferring according to the data [20, 21]. More particularly, the sensitive data may include time, location, acoustic and visual data, acceleration, environment context and biometric information.
- **Anonymity** usually considers the probability of their data can be hided after releasing [22]. Since completely protecting information is an impossible mission, the advent of anonymity technology has aroused wide concern. Some works like k-anonymity [23], l-diversity [24] and t-closeness [25] are proposed for guaranteeing the appropriate usage of data. Likewise, some research works try to achieve anonymity of smartphone data, currently most of them focus on location data in the smartphone [26, 27].

By comparison with human-centric smartphone privacy, the research on technology-centric privacy put much value on how to protect information using technology without considering users' privacy concerns and preferences. Furthermore, it should be noted that the technology-centric privacy is different from security in the smartphone. Security is usually referred to as the confidentiality, availability, and integrity of data. Namely, the objective of security is to ensure the data is accurate, reliable and only accessed by authorized individuals or organizations. Technology-centric privacy however mainly focuses on achieving appropriate use of data in smartphone through methods, tools and systems. In other words, the data in the smartphone should be used according to the agreed purposes between users and stakeholders.

3 Issues of Smartphone Privacy

In this section, we point out some issues of smartphone privacy from three perspectives: mobile operating system, mobile application and mobile sensing.

The operating system is built in smartphones and further provides a plethora of applications aimed at making our life convenient [28]. However, there may be some innate flaws in mobile operating systems, which can lead users' privacy leakage. As we know, iOS and Android are the two of most popular mobile operating systems but many reports, news, investigations reveal that some drawbacks exist in the systems, which can be used by malicious users [29–31].

Likewise, many smartphone applications, especially malicious ones, also face privacy risks. However, most applications are released as a encapsulated package or a executable program. From viewpoint of technology-centric privacy, it is arduous to learn what information can be disclosed. One important issue therefore is to detect and analysis the mobile applications so that we can know the privacy risk of them.

In the Android system, each application has a permission list to claim what kind of data or function the app can use. The application will hold the permission when the users approve it. Actually, the users have to agree it since it is a necessary step for installing the application. Thus, a lot of applications try to get as much permissions as they can which may lead permission abuse. Users' information can be stole or destroyed if some malicious applications can access personal data stored in the smartphones. It is also dangerous even normal application can get some unrelated data for application running. There is no such permission mechanism in iOS platform, however the privacy settings make users face to the similar problem. Thus, another issues is to address data abuse of smartphone apps. From human-centric privacy angle, individual concern to privacy differs from person to person, background to background. It is improper to assume that everyone has the same privacy preferences. Understanding users' privacy thus is becoming a problematic issue in smartphone privacy. Overall, mobile applications try to provide better services to the people. The ultimate goal of smartphone privacy from application perspective is that how to balance the apps' functionality and users' privacy. The final issue is the tradeoff between utility and privacy.

The mobile communication is another vital function of smartphone in mobile computing. Under various kinds of network, users can access network, share data and receive information. Mobile communication research has paid more attention to privacy leakage when users share their data from connectivity perspective [4, 3]. In this field, mobile sensing is becoming popular due to the proliferation of sensor-equipped smartphones. It is a novel sensing paradigm which utilizes embedded mobile sensors to collect and share data. It is very different from traditional privacy preserving scenarios. In mobile sensing, on one hand, it is not uncommon for users to share their information with others in mobile sensing tasks. On the other hand, they are reluctant to exposure sensitive data due to privacy concern. Unfortunately, it is arduous for users to choose proper information for sharing in appropriate participatory sensing tasks since they are unaware of what can be inferred from the sensory data. Hence, one issue is that how to share sensory data and preserve personal privacy as well.

4 Countermeasures to Smartphone Privacy Leakage

In this section, we review the existing works about understanding, detecting and mitigating smartphone privacy risks. As shown in Fig. 1, smartphone privacy disclosure happens due to, the flaws of mobile operating systems, the data abuse of some applications and users' unawareness when they output data for different goals, especially in mobile sensing campaigns. Thus, we investigate a number of existing works from these three directions respectively, classifying them based on privacy characteristics and their targets. We do not present details of the works since the aim of this section is to provide an unambiguous overview of the current works about smartphone privacy.

4.1 Countermeasures for Mobile Operating System

According to a recent report, Android has over 84% and iOS has 11.7% of the global market share in the third quarter of 2014 [32]. The copious applications are produced based on the mobile systems and used by people everyday. These two popular systems both claim that they take users' personal information and privacy very seriously and retain the users' information just for better services [33]. The users of Android and iOS however still faced the scads of privacy issues and risks. We therefore analyze these two mobile systems since they hold the two biggest application market globally.

4.1.1 iOS platform

We discuss Apple iOS in this section, concentrating on its privacy features. For guaranteeing the privacy, code-signing, encryption and sandboxing are developed in iOS. More particularly, code-signing mechanism only allows code which is verified by Apple to run. Encryption prevents the code from reverse-engineering and ensures the applications only can be launched by the purchasers. Sandboxing is designed for preserving users' privacy, preventing an application from accessing users' information in the smartphone. Rather, iOS offers a gamut of APIs with developers that allows applications to communicate with each other using parameters.

However, many applications in iOS are designed to access shared information and resources, including sensitive data like location, photos, emails, contacts, for better utilities and services. What's worse is that considering the tenet of iOS is to provide elegant and intuitive interface, the scads of interactions are hidden. For example, there is no alert or notification to users about their privacy when they are installing the applications. Recognizing the need for protecting user privacy, iOS introduces popup notifications, users can setting the permission for the data when an application want to access some personal information. However according to some reports and survey, most people think the notification is intricate and few of them will read it [34].

Normally, iOS applications are distributed and reviewed via the App Store held by Apple. The review process currently includes static analysis to make sure only authorisze APIs are used and runtime analysis to ensure that applications would not obtain information by evading sandbox mechanism. Unfortunately, it is very arduous to scrutinize each application due to scads of iOS applications submitted. Moreover, sometimes a number of malicious applications actually pass the review process. Besides getting applications from App Store, another way is jailbreaking, which is not supported by Apple. However, it is prevalent for users, even some research works to protect user privacy are based on jailbreaking [31]. In this case, the code-signing will be removed and applications can be installed from other sources, such as Cydia Store. We do not discuss the jailbreaking since it is out of this article but it is obvious that jailbreaking iOS devices may lead to more privacy risks.

Since iOS is considered as closed source system, there is few work that can improve privacy preserving of iOS except Apple itself. From iOS 4-8, privacy preserving technology and policy have been ameliorated, but the users' data are still

in dangerous. Therefore, many researchers develop methods and tools, which are installed in iOS as applications to mitigate privacy risk. We will further illustrate them in section 4.2.

4.1.2 Android platform

Android is a Linux kernel based mobile operating system. It is designed for various mobile devices, especially smartphones. Its applications are written in Java and compiled into a custom byte code, which is known as ART and its predecessor Dalvik [35]. We briefly discuss Android mobile operating system and its ecosystem from a privacy perspective before describing the proposed system.

Android privacy is based on sandbox, cryptography, secure IPC. Android applications run in a sandbox environment called Android Application Sandbox, which isolates a particular application's data and code execution from other applications, so that other processes on the system cannot access it. Cryptography and secure IPC actually include some implementations of common security functionality. More specifically, a wide array of algorithms using cryptography and an encrypted filesystem have been implemented to protect data. Meanwhile, Android provides plentiful APIs for developers to access local data in the smartphone and shared information by others [36]. Although these APIs help applications to produce better services, most of accessed data are sensitive to users, including location, contacts, photos and so forth [5, 3].

To address this issue, Android introduces permission mechanism in Android Play Store and access notification in the smartphone. Permission mechanism is a feature allows applications explicitly share resources and obtain additional capabilities not provided by the basic sandbox due to their needs [37]. All the applications in Play Store will show their data permissions before installing [38]. The data access notification will pop up when the app require some pieces of information. Unfortunately, few people will read the list and figure out why they need to hold such permissions they just touch the accept or ignore button [39]. Furthermore, even if people read and reject those permissions, services will then not be provided due to the scarcity of required data [40]. Compromise is users' only choice.

Furthermore, Google introduces Bouncer to automatically scrutinize applications to prevent malicious applications. However, a plethora of applications can circumvent the Bouncer and appear on the store. Beside Play Store, Android allows APK to distribute and install application software. This feature extremely expands application ecosystem and may lead more information disclosure [41, 42]. Since these software were not in Android Play store, it is difficult for users to know their specification [43]. These features and issues of Android system make us believe that it is curial to help users make proper decisions about their Android applications based on their own preferences.

4.2 Countermeasures for Mobile Application

There has been a great deal of works on providing privacy to users for smartphone applications. We provide an overview of some existing literatures. We classify related work into three categories: (1) Privacy detection and analysis (2) Privacy protection and risk mitigation (3) Understanding users' privacy for different applications. After reviewing existing works, we compare some representative research works about smartphone applications privacy in table 1.

4.2.1 Privacy detection and analysis

With the proliferation of smartphone applications in mobile operating systems, the scads of drawbacks have aroused much public concern. Thus research community has put much effort on detecting and analyzing the potential privacy risk of smartphone applications. Two mainstream methods are static analysis and dynamic analysis, some methods are also proposed from different perspectives besides.

The static detection and analysis methods analyze the source code of smartphone applications to generate a control flow graph (CFG) rather than actually executing the applications. After covering all the paths of CFGs, the methods will detect and analyze the potential privacy risk of each smartphone applications. In the most cases, the applications is often detected and analyzed by an automated tool or system. Some such works have been designed. LeakMiner is tool to detect disclosure of sensitive information on Android based on static analysis [44]. It can identify 145 real leakages in a set consists of 1750 applications, even though with 160 false positives. Mann and Starostin [35] design a framework to detect privacy leakage for Android applications through static static information flow analysis. It tries to identify whether the Dalvik bytecode implementation of an Android app conforms to a given privacy policy. AndroidLeaks a static analysis framework for finding potential leaks of sensitive information in Android applications on a large scale [45]. It found that there are 57,299 potential privacy leaks in 7,414 applications among 24,350 tested applications. ComDroid has been proposed to help developers to analyze their own applications before release since custom code has potential privacy risk since the code is usually unjustified [46]. Some static analysis tools also have been developed to automatically detect attempts to load external code using static analysis techniques [47]. Applying the static analysis to Android permission mechanism is also a telling method. Android permission mechanism allows each application has permissions to perform any operations that would adversely impact other applications, the system and users. The permission abuse however also can lead data leakage. Woodpecker is a tool which try to identify the permissions or capabilities abuse of applications using static analysis [41]. It found that 11 permissions were leaked among 13 privileged permissions examined. All aforementioned tools and systems are based on Android platform, PiOS is a tool which allows people to statically analyze applications for potential information disclosure in iOS platform [48]. According their findings, it claims that most applications respect personal identifiable information stored on user's devices in the light of testing of over 1,400 iOS applications.

The static detection and analysis methods have to spend more time on scrutinizing the source code of smartphone applications and generating CFG for further analysis, yet they actually have no time performance overhead since processing is done before the applications are launched. Furthermore, there is no prerequisite for static analysis like mobile devices

or simulation environment, which are necessary for dynamic detection and analysis.

Unlike static detection and analysis, dynamic detection and analysis methods monitor the applications when they are running. In other words, the actual behaviors of smartphone applications would be analyzed in dynamic detection. Data flow analysis (DFA) is a popular technique to achieve the goal by tracking the flow of sensitive data of users [49]. However, as we discuss in the static analysis, the dynamic detection and analysis is based on real mobile devices or simulation environment. The time performance overhead is another drawback of dynamic analysis since it performance when the applications are ran.

TaintDroid [50] is a dynamic taint tacking and analysis system, which involves some aforementioned methods to simultaneously tracking multiple sources of sensitive data. It can provide realtime analysis by leveraging Android's virtualized execution environment. In the architecture of TaintDroid, it predefines nine situations of the information is taint. After monitoring and analyzing the behavior of 30 third-party Android applications based on the situations, TaintDroid finds 68 instances of potential misuse of users' private information across 20 applications. DroidScope is proposed as an dynamic analysis platform using virtualization-based malware analysis [51]. It focuses on reconstructing both the OS-level and Java-level semantics, by mirroring three aspects of an Android device: hardware, OS and Dalvik Virtual Machine. Dynamic detection and analysis via graphical user interface is another telling methods. AndroidRipper can test Android application based on a user-interface driven ripper that explores the app's GUI with the aim of exercising the application in a structured manner [52].

Currently, more and more detection and analysis methods have emerged besides static and dynamic analysis. It is an intuitive idea to combine these two analysis methods to improve performance of analysis. Smartdroid is a hybrid static and dynamic analysis method to reveal UI-based trigger conditions in Android applications [53]. More particularly, it firstly uses static analysis to extract expected activity switch paths and then takes advantage of dynamic analysis to scan each UI elements and explore the UI interaction paths towards the sensitive APIs. It is however too resource-consuming when we do such analysis in the smartphone. Thus, Paranoid Android is proposed to address the issue by leveraging cloud-based analysis [54]. Most analysis work will be finished by the server, which does not have as smartphone like constraints.

Crowdsourcing also has been used for determining vulnerabilityies in the smartphone due to its unprecedented ability of data collection. Crowdroid is a framework for collection of traces from an large number of real users based on crowdsourcing [55].

4.2.2 Privacy protection and risk mitigation

Privacy protection for smartphone applications is a challenging issue. A number of research have focused on how to preserve users' privacy and application's functionality at the same time. We classify the existing works into three groups, (1) permission removal (2) access control (3) data mock.

As we discuss in section 4.1.2, Android system provides a permission mechanism to protect users' data. The permission list of an application will be shown to users before they install applications from the app store. Only when the applications get approbation does they can be installed. After installation, the applications can access the resources and information according to their permission lists. Obviously, Android permission mechanism intends to improve users' awareness of the privacy about the applications and preserve the privacy.

However, most Android users have defective understandings about the permission. To make things worse, they paid limited attentions to the permission list which is shown on the screen just before installation [39]. Corroborating this point, a laboratory study show that Android users have little attention and comprehension to applications and permissions of data usage [11]. Thus, a feasible way to mitigate data abuse is to establish a system with the ability to prevent applications from accessing resources without the stated permissions [29]. In this case, users will know what kind of information will be obtained by the app. However, some developers always ask for unnecessary permissions due to ambiguous API documentations and bad develop habits [56]. This abuse of permissions also lead unexpected information disclosure. An immediate idea is to remove or constrain suspected permissions. Permissions removal has been proposed to mitigate the privacy leak in Android smartphone [57]. It is a kind of reverse engineering process which aims to remove an app's permission to a resource when the permission is unrelated to the application. The repackaged app can run in the smartphone again. It also claims that a key challenge is that how well-integrated the different permission are within an app.

Access control provides a different perspective of detecting and protecting privacy in smartphone. FlaskDroid [19] privodes mandatory access control on Android's middleware and kernel layers to prevent information disclosure. All these works put much efforts on analyzing and protecting security for Android applications. However, as we discussed before, protecting users' information unilaterally cannot meet their requirements since users have different concerns towards Android applications.

AppIntent provides a framework which try to control data transmission to prevent Android applications from stealing sensitive data, meanwhile identify if transmission is from users' intention [58]. For each data transmission, it can generate a sequence of GUI manipulations corresponding to the sequence of events. Thus, it can help analysts to determine if the data transmission is user intended or not. TrustDroid is designed to isolate data and communication at different layer of the Android software stack, including the middleware layer, kernel layer and network layer [59]. AppFence is a method which aims to empower users to protect their data from exfiltration by permission-hungry applications [60]. It can covertly substitute shadow data in place of data that the user wants to keep private, and block network transmissions that contain data the user made available to the application for on-device use only.

However, as suggested by Ghosh et al. [61], current privacy control mechanisms are static and cannot preserve privacy in the dynamic context-aware environment. According to recent systematically research, several vulnerabilities

have existed in Android applications. Their presence even in some extremely popular applications [62]. Thus, plenty of work focuses on privacy of Android platform and its applications. Techniques and tools that can detect and prevent information from being leaked in Android applications have been widely studied [47, 19]. Permission analysis is a telling method to detect sensitive information potential leakage. It can scrutinize Android app to know whether the developers follow least privilege with their permission requests. In the light of results of a detailed analysis, limitations of Android's UID sharing method coerce developers to write custom code rather than rely on OS-level mechanisms [63].

Data mock can play an expected role in preserving privacy since some applications cannot run without accessing specific information. TISSA [64] and MockDroid [65] can provide artificial data instead of real one to the applications such that they can still function. In this case, there is, actually, no risk for users because the data is fake. However, due to the same reason, applications cannot provide competent services to users.

All aforementioned works provide us some techniques and tools to detect and mitigate privacy risk on Android applications. However, these works did not tell users about the kinds of information to be offered and data to be preserved. Understanding users' privacy concern therefore become a significant role in smartphone privacy.

4.2.3 Understanding users' privacy

Understanding user's privacy is based on human-centric privacy as illustrated in section 2. Namely, privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [7]. Therefore, privacy of applications should emphasize that users have adequate awareness and understanding to their personal and sensitive information. According to a recent survey [66], Android users hold quite different viewpoints due to their demographic characteristics, privacy awareness, and reported behaviors when installing applications. It is probably surprised for users to realize data collection and distribution activities of smartphone applications [67].

It is challenging to recognize users' perceptions of whether a given action is legitimate, or how the action makes them feel with respect to privacy. A model, privacy as expectations, is proposed to capture people's expectations of privacy [13]. Appprofiler [68] is an approach to provide users with knowledge for decision-making about Android application through analyzing privacy-related behaviors of applications and users opinions. After understanding user's perceptions, it is important to assess privacy risk and predict user's privacy preferences. An approach is proposed for assessing the privacy risk of Android users based on impact valuation from users and their profiles [69]. Super-Ego [70] is a crowdsourcing framework which can predict the user's privacy preferences for different location on the basis of the general user population. Altman's theory of boundary regulation and Nissenbaum's theory of contextual integrity are also adopted to explore the privacy gap between users' privacy expectations and smart phone usage.

4.3 Countermeasures for Mobile Sensing

In this section, we review the related work about smartphone privacy in mobile sensing. The mobile sensing is a novel sensing paradigm using smartphones. In the mobile sensing, smartphone users need to provide sensory data, by comparison with other data communication in smartphone, mobile sensing have more possibilities to access users' information legally. We therefore study some works which want to preserve privacy in mobile sensing.

For better understanding of existing works, we firstly provide a overview of system model of mobile sensing. The typical architecture of mobile sensing system is illustrated in Fig. 2. Normally, there are two significant roles in mobile sensing applications, participant and stakeholder [71]. The participants refer to the people who are allocated to and accept the sensing tasks, and collect the data from physical world. Noted that the participants capture the data using different mobile devices, while our work focuses on the smartphone. Stakeholders refer to the people who benefit from the data. They usually initiate a mobile sensing application, and then access the sensory data for further analysis or presentation. A number of participatory sensing applications have been emerged recently [71]. However, users' privacy concern is an obstacle for long-term deployment [72]. Based on the characteristics of smartphone privacy, we classify related work into twe categories: (1) Privacy preservation and awareness (2) Personalized privacy risk mitigation.

4.3.1 Privacy preservation and awareness

Privacy preserving is a long-standing issue and prompts a wide discussion in mobile sensing systems which target the pervasive collection of information. As we mentioned before, privacy issue may be the cardinal obstacle [73]. Many works on privacy preserving mechanism has been proposed.

PiRi, a privacy-aware framework for participatory sensing systems, which addressed the privacy issues based on an untrusted central data server model and enabled participation of the users without compromising their privacy [74]. PEPSI, a Privacy-Enhanced Participatory Sensing Infrastructure, explores realistic architectural assumptions and a minimal set of formal requirements aiming at protecting the privacy of both data producers and consumers with low additional computational cost and overhead claimed by the authors [75]. AnonySense is a privacy-aware architecture for realizing pervasive applications based on participatory sensing by mobile devices. It allows applications to submit sensing tasks that distributed across anonymous participating mobile devices, later receiving verified, yet anonymized, sensor data reports back from the field, thus providing the first secure implementation of this participatory sensing model [76]. SensorSafe is an architecture for managing personal sensory information in a privacy-preserving way, which consists of multiple remote data stores and a broker so users can retain the ownership of their data and management of multiple users can be well supported. Also, it provides a context-aware ne-grained access control mechanism by which users can dene their own sharing rules based on various conditions including context and behavioral status [77]. Jedrzejczyk

Table 1: Comparison of some representative research work about smartphone applications privacy

Methods/Systems	Privacy Characteristics	Objectives	Platform	Summary
Woodpecker [41]	Technology-centric	Privacy detection and analysis	Android	13 privileged permissions were examined and 11 were leaked, with individual phones leaking up to eight permissions.
TaintDroid [50]	Technology-centric	Privacy detection and analysis	Android	30 popular Android applications were examined, 68 instances of potential misuse of users' privacy were found across 20 applications.
AndroidLeaks [45]	Technology-centric	Privacy detection and analysis	Android	24,350 Android apps were examined, 57,299 potential privacy leaks in 7,414 Android applications were found
PiOS [48]	Technology-centric	Privacy detection and analysis	iOS	More than 1,400 iOS apps were analyzed, 656 Apps use ad library code which may disclose devices ID, 36 Apps leak GPS location and 5 Apps leak contacts.
LeakMiner [44]	Technology-centric	Privacy detection and analysis	Android	It is an automatic and static taint analysis method. After analyzing 1750 apps, it can identify 145 real leakages in this app set.
ComDroid [46]	Technology-centric	Privacy detection and analysis	Android	It can be used by developers to analyze their Apps before release, by application reviewers to analyze Apps in the Android Market, and by end users. It analyzed 20 applications with the help of ComDroid and found 34 exploitable vulnerabilities; 12 of the 20 applications have at least one vulnerability.
FlaskDroid [19]	Technology-centric	Privacy protection	Android	It provides mandatory access control simultaneously on both Android's middleware and kernel layers. The evaluation is based on the empirical testing using the security models, testbed of known malware and synthetic attacks.
TrustDroid [59]	Technology-centric	Privacy protection	Android	It is a framework, which can isolate data and applications at different layers (middleware layer, kernel layer, network layer) with a negligible overhead, small cost on battery's life-time
MockDroid [65]	Technology-centric Human-centric	Privacy protection	Android	It is a modified version of the Android which allows a user to provide artificial data instead of real one to the apps such that they can still function (possibly with reduced functionality). A random sample of twenty-three popular applications can successfully run in the MockDroid.
AppIntent [58]	Human-centric	Privacy protection, Privacy detection and analysis	Android	It is an analysis framework, which can provide a sequence of GUI manipulations corresponding to the sequence of events to determine if the data transmission is user intended or not. The evaluation is based on a set of 750 malicious apps and 1,000 top free apps from Google Play.
Privacy as expectations [13]	Human-centric	Understanding users' privacy	Android	It is a system which capture users' expectations of what sensitive resources mobile apps use through crowdsourcing. It found that both users' expectation and the purpose of sensitive resources can affect users' feelings and their decisions. Also, properly informing users of the purpose of resource access can ease users' privacy concerns to some extent.
ProtectMyPrivacy [31]	Human-centric	Understanding users' privacy	iOS	PMP was in use for over nine months by 90,621 real users and 225,685 unique Apps were reviewed. Based on the crowdsourcing, PMP can recommend users the decisions for their permission settings in iOS.
Appprofiler [68]	Human-centric	Understanding users' privacy	Android	It provides users the knowledge needed to make informed decisions about the applications they install. It has three findings: (1)The permission system is not fine-grained enough. (2)Differentiating between actions performed by users and actions in the background is important. (3)There are significant differences between third-party library code and code written as part of a specific application.

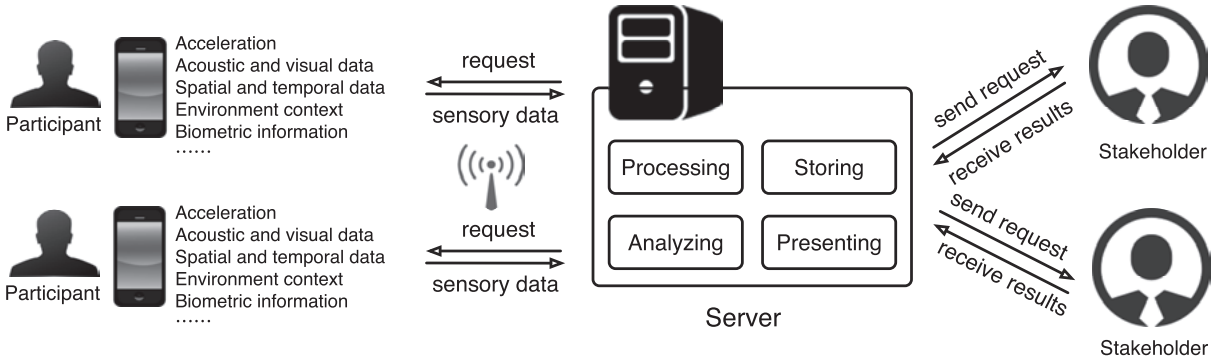

Fig. 2: The typical architecture of mobile sensing system

et al. [78] observed anonymous users of a location-based social networking application in their natural environment and demonstrated how to re-identify them based on that data.

Besides the framework, a privacy-preserving mobile sensing scheme for multidimensional data which uses negative surveys has been presented. In this scheme, the server can reconstruct the probability density functions of the original distributions of sensed values, without knowing the participants' actual data [79]. Location privacy is another important concern in mobile sensing systems [80]. A decentralized mechanism to preserve location privacy during the collection of sensor readings has been proposed, which can exchange the sensor readings of users in physical proximity for jumbling the location information [81]. An algorithm to address kNN queries for datasets which grouped by users based on locality-sensitive hashing in mobile sensing systems [82]. User-side privacy-protection scheme can adaptively adjusts the parameters of participatory sensing for satisfying individual location privacy protection requirements against adversaries in a measurable manner [83].

4.3.2 Personalized privacy risk mitigation

Unlike privacy preserving mechanism, personalized privacy methods consider users' requirements in mobile sensing, which served as the unpinning of further protection. Muslukhov et al. [84] hold the viewpoint that users' privacy requirements in mobile sensing system are heterogeneous. Different targets and form of utilizing personal data can affect users' concerns. For example, Barkhuus and Dey [85] present an experimental case study that examines people ' s concern for location privacy. They find that location tracking services generate more concern for privacy than position-aware services.

They design a user-side privacy protection adaptively adjusts parameters to meet personalized privacy. Gedik and Liu [26] provide a privacy personalization framework to support location k-anonymity for context-sensitive personalized privacy requirements. Each mobile node is specified the desired minimun level of anonymity and maximum temporal and spatial resolutions.

A suite of scalable spatio-temporal cloaking algorithms, CliqueCloak, which aims at avoiding or reducing known location privacy threats before forwarding requests. Gong et al. [86] propose a dynamic privacy management system aimed at enabling tangible privacy control and feedback in a pervasive sensor network. A key contribution is to conduct a user study to show some insight of privacy/benefit tradeoff from various sensing capabilities and how privacy settings and user behavior relate. Freudiger et al. [87] push the understanding of the privacy risk in the location-based services.

5 Future research directions

We have discussed the privacy issues and presented surveyed a number of methods and systems to address them. According to our investigation, even though much attention goes into protecting and preserving smartphone privacy in mobile computing, tailored and practical solutions are scarce and fundamental research in the area of smartphone privacy in still in its infancy. In the following, we highlight future research challenges of smartphone privacy in mobile computing, both from the perspective of the surveyed work as well as from our own perspective; note that our list of given challenges is by no means exhaustive, but contains our subjective impression of the most relevant challenges at the time of writing this article.

Challenge 1: Human Privacy and Smartphone Interaction. According to our discussion about human-centric smartphone privacy, a key challenge for the future is to build a system or framework based on interaction with human to protect privacy. As we emphasized in the section 2, people' concerns are heterogeneous [30]. Therefore, understanding people's privacy preference, concern and attitude should be an key challenge.

In the future, the integration of the human in the smartphone privacy should be supported by concepts and methodologies issued from various disciplines, such as psychology, computer science and behavioristics.

Challenge 2: Active Defence in Smartphone Privacy. With comparison with human-centric privacy, active defence in smartphone privacy would focus on protecting privacy even without people's awareness and intervention. The active defence may collect users' behaviors data for learning and protect users' information accordingly. Malicious apps currently have a plethora of ways to attack smartphones, even through an official application [92].

To address such problem, active defence technology is a future direction. It would involve privacy risk detection, privacy analysis, and protection. The adaptive version of active

Table 2: Comparison of some representative research work about privacy in mobile sensing

Methods/Systems	Privacy Characteristics	Objectives	Summary
AnonySense [22]	Technology-centric	Privacy preserving	It allows the sensing tasks distribute anonymously to the participating mobile devices. The sensory data also will be reported back in a verified and anonymized way.
Sensorsafe [77]	Technology-centric	Privacy preserving	It is a system for managing personal sensory information in a privacy-preserving way with supporting multiple users. Users can dene their sharing rules based on different context through ne-grained access control mechanism.
PEPSI [75]	Technology-centric	Privacy preserving	The main contribution is the work is based on some realistic assumptions and a minimal set of formal requirements aiming at protecting privacy of both data producers and consumers. Meanwhile, adding low computational cost and communication overhead is another lightspot.
PiRi [88]	Technology-centric	Privacy preserving	PiRi is a privacy-aware framework, which aims to guarantee predefined users' privacy when they participate in mobile sensing system. Thus, defining privacy is one of the main contribution.
Prisense [89]	Technology-centric	Privacy preserving	It is a privacy-preserving data aggregation method which is based on data slicing, data mixing and non-additive aggregation functions to against a tunable threshold number of colluding users and aggregation servers.
PoolView [90]	Technology-centric	Privacy preserving	It provides privacy guarantees on stream data for participatory sensing application, which is based on data perturbation and reconstruction techniques. The actual data is applied in the evaluation for demonstrating the privacy-preserving aggregation functionality.
Adaptive Personalized Privacy [83]	Human-centric	Personalized privacy	It considers heterogeneous user privacy requirements in mobile sensing system. A user-side privacy protection adaptively adjusts parameters to meet personalized privacy is proposed, which wants to balance the privacy and utility. The evaluation is based on synthetic and real data.
CliqueCloak [91]	Human-centric	Personalized privacy	It provides a privacy personalization framework to support location k-anonymity for context-sensitive personalized privacy requirements. Each mobile node is specified the desired minimun level of anonymity and maximum temporal and spatial resolutions. CliqueCloak is proposed to avoid or reduce known location privacy threats before forwarding requests.
Dynamic Privacy Management [86]	Human-centric	Personalized privacy	It is a dynamic privacy management system aimed at enabling tangible privacy control and feedback in a pervasive sensor network. A key contribution is to conduct a user study to show some insight of privacy/benefit tradeoff from various sensing capabilities and how privacy settings and user behavior relate.

defence may also consider people's concerns and preferences.

Challenge 3: Smartphone Privacy Measurement and Analysis. Different criteria and metrics are currently being used to evaluate the performance of the proposed solutions in terms of privacy protection for different context [14, 93, 94]. To achieve more precise and usable privacy-preserving in the smartphone, measurement and analysis for individual privacy in different environment should be proposed and applied. While it might be arduous or even impossible to propose an one-size-for-all measurement and analysis mechanism, the need to define generalized metrics is widely acknowledged.

Challenge 4: Smartphone Privacy Policy Modeling. It is not uncommon to realized that from scientific and technological point, there is no clear and absolute definition of privacy. Instead, there are some meaningful and acknowledged statements about privacy, which have been presented and discussed in section 2. A key challenge for the future is to propose a model as a unifying approach to formally state our smartphone privacy. The unified model can be not only a method to protect users' smartphone privacy but also a common metric to verified different algorithms, tools and systems. Even it can be a reference for lawmakers to legislate to protect citizen's information.

6 Conclusions

Smartphone privacy has been widely concerned due to the ubiquity of mobile phones. In this paper, we provided a comprehensive of recent research on smartphone privacy in mobile computing, focusing on issues, methods and systems to mitigate privacy risk. We firstly discussed the definition and characteristic of smartphone privacy in mobile computing

from two perspectives human-centric and technology-centric, and illustrated some potential issues of smartphone privacy. We subsequently reviewed the existing works about understanding, detecting and mitigating smartphone privacy risk, mainly concentrating on mobile operating system, mobile application and mobile sensing which are three places of privacy disclosure. We list and compare some representative research work about privacy in smartphone applications and mobile sensing. Finally, we highlight and discuss future challenges according to our survey and findings.

[Acknowledgments]

[Bibliography]

[1] T. Imielinski and H. F. Korth, *Mobile computing*. Springer, 1996, vol. 353.

[2] "79% Of People 18-44 Have Their Smartphones With Them 22 Hours A Day," http://www.mediabistro.com/alltwitter/smartphones_b39001.

[3] D. F. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, "Location leaks on the gsm air interface," *ISOC NDSS (Feb 2012)*, 2012.

[4] S. B. Wicker, *Cellular Convergence and the Death of Privacy*. Oxford University Press, 2013.

[5] N. Cheng, X. Wang, W. Cheng, P. Mohapatra, and A. Seneviratne, "Characterizing privacy leakage of public wifi networks for users on travel," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2769–2777.

[6] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard law review*, vol. 4, no. 5, pp. 193–220, 1890.

[7] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, p. 166, 1968.

[8] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous computing environments," in *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93*. Springer, 1993, pp. 77–92.

[9] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao, "Understanding and capturing people's privacy policies in a mobile social networking application," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 401–412, 2009.

[10] V. M. García-Barrios, "User-centric privacy framework: Integrating legal, technological and human aspects into user-adapting systems," in *Computational Science and Engineering, 2009. CSE'09. International Conference on*, vol. 3. IEEE, 2009, pp. 176–181.

[11] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 3.

[12] J. L. B. L. N. Sadeh and J. I. Hong, "Modeling users ' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[13] J. Lin, S. Amini, J. I. Hong, N. Sadeh, J. Lindqvist, and J. Zhang, "Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing," in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM, 2012, pp. 501–510.

[14] A. Braunstein, L. Granka, and J. Staddon, "Indirect content privacy surveys: measuring privacy without asking about it," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 2011, p. 15.

[15] B. Fu, J. Lin, L. Li, C. Faloutsos, J. Hong, and N. Sadeh, "Why people hate your app: Making sense of user feedback in a mobile app store," in *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2013, pp. 1276–1284.

[16] H. Zhu, H. Xiong, Y. Ge, and E. Chen, "Mobile app recommendations with security and privacy awareness," in *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2014, pp. 951–960.

[17] S. R. Murillo and J. A. Sánchez, "Enhancing privacy awareness through interaction design," in *Proceedings of the XV International Conference on Human Computer Interaction*. ACM, 2014, p. 44.

[18] P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2013, pp. 3393–3402.

[19] S. Bugiel, S. Heuser, and A.-R. Sadeghi, "Flexible and fine-grained mandatory access control on android for diverse security and privacy policies," in *Usenix security*, 2013, pp. 131–146.

[20] P. Mohan, V. N. Padmanabhan, and R. Ramjee, "Nericell: rich monitoring of road and traffic conditions using mobile smartphones," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*. ACM, 2008, pp. 323–336.

[21] H. Lu, J. Yang, Z. Liu, N. D. Lane, T. Choudhury, and A. T. Campbell, "The jigsaw continuous sensing engine for mobile phone applications," in *Proceedings of the 8th ACM Conference on Embedded Networked Sensor Systems*. ACM, 2010, pp. 71–84.

[22] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: privacy-aware people-centric sensing," in *Proceedings of the 6th international conference on Mobile systems, applications, and services*. ACM, 2008, pp. 211–224.

[23] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[24] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, p. 3, 2007.

[25] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity." in *ICDE*, vol. 7, 2007, pp. 106–115.

[26] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *Mobile Computing, IEEE Transactions on*, vol. 7, no. 1, pp. 1–18, 2008.

[27] H. P. Li, H. Hu, and J. Xu, "Nearby friend alert: location anonymity in mobile geosocial networks," *Pervasive Computing, IEEE*, vol. 12, no. 4, pp. 62–70, 2013.

[28] "Number of available android applications," http://www.appbrain.com/stats/number-of-android-apps.

[29] C. Orthacker, P. Teufl, S. Kraxberger, G. Lackner, M. Gissing, A. Marsalek, J. Leibetseder, and O. Prevenhueber, "Android security permissions–can we trust them?" in *Security and Privacy in Mobile Information and Communication Systems*. Springer, 2012, pp. 40–51.

[30] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns," in *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2012, pp. 33–44.

[31] Y. Agarwal and M. Hall, "Protectmyprivacy: detecting and mitigating privacy leaks on ios devices using crowdsourcing," in *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*. ACM, 2013, pp. 97–110.

[32] "Smartphone OS Market Share, Q3 2014," http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

[33] "Your privacy is important to apple. So we've developed a Privacy Policy that covers how we collect, use, disclose, transfer, and store your information." https://www.apple.com/legal/privacy/en-ww/, 2014.

[34] J. Lin, M. Benisch, N. Sadeh, J. Niu, J. Hong, B. Lu, and S. Guo, "A comparative study of location-sharing privacy preferences in the united states and china," *Personal and ubiquitous computing*, vol. 17, no. 4, pp. 697–711, 2013.

[35] C. Mann and A. Starostin, "A framework for static detection of privacy leaks in android applications," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*. ACM, 2012, pp. 1457–1462.

[36] C. Mulliner, "Privacy leaks in mobile phone internet access," in *Intelligence in Next Generation Networks (ICIN), 2010 14th International Conference on*. IEEE, 2010, pp. 1–6.

[37] B. Konings, C. Bachmaier, F. Schaub, and M. Weber, "Device names in the wild: Investigating privacy risks of zero configuration networking," in *Mobile Data Management (MDM), 2013 IEEE 14th International Conference on*, vol. 2. IEEE, 2013, pp. 51–56.

[38] S. Holavanalli, D. Manuel, V. Nanjundaswamy, B. Rosenberg, F. Shen, S. Y. Ko, and L. Ziarek, "Flow permissions for android," in *Automated Software Engineering (ASE), 2013 IEEE/ACM 28th International Conference on*. IEEE, 2013, pp. 652–657.

[39] 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 *Financial Cryptography and Data Security*. Springer, 2012, pp. 68–79.

[40] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "Little brothers watching you: Raising awareness of data leaks on smartphones," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 12.

[41] M. C. Grace, Y. Zhou, Z. Wang, and X. Jiang, "Systematic detection of capability leaks in stock android smartphones." in *NDSS*, 2012.

[42] T. Vidas, D. Votipka, and N. Christin, "All your droid are belong to us: A survey of current android attacks." in *WOOT*, 2011, pp. 81–90.

[43] E. K. Choe, J. Jung, B. Lee, and K. Fisher, "Nudging people away from privacy-invasive mobile apps through visual framing," in *Human-Computer Interaction–INTERACT 2013*. Springer, 2013, pp. 74–91.

[44] Z. Yang and M. Yang, "Leakminer: Detect information leakage on android with static taint analysis," in *Software Engineering (WCSE), 2012 Third World Congress on*. IEEE, 2012, pp. 101–104.

[45] C. Gibler, J. Crussell, J. Erickson, and H. Chen, *AndroidLeaks: automatically detecting potential privacy leaks in android applications on a large scale*. Springer, 2012.

[46] E. Chin, A. P. Felt, K. Greenwood, and D. Wagner, "Analyzing inter-application communication in android," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*. ACM, 2011, pp. 239–252.

[47] S. Poeplau, Y. Fratantonio, A. Bianchi, C. Kruegel, and G. Vigna, "Execute this! analyzing unsafe and malicious dynamic code loading in android applications," in *NDSS*, vol. 14, 2014, pp. 23–26.

[48] M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "Pios: Detecting privacy leaks in ios applications." in *NDSS*, 2011.

[49] B. Lokhande and S. Dhavale, "Overview of information flow tracking techniques based on taint analysis for android," in *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*. IEEE, 2014, pp. 749–753.

[50] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: an information flow tracking system for real-time privacy monitoring on smartphones," *Communications of the ACM*, vol. 57, no. 3, pp. 99–106, 2014.

[51] L.-K. Yan and H. Yin, "Droidscope: Seamlessly reconstructing the os and dalvik semantic views for dynamic android malware analysis." in *USENIX Security Symposium*, 2012, pp. 569–584.

[52] D. Amalfitano, A. R. Fasolino, P. Tramontana, S. De Carmine, and A. M. Memon, "Using gui ripping for automated testing of android applications," in *Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering*. ACM, 2012, pp. 258–261.

[53] C. Zheng, S. Zhu, S. Dai, G. Gu, X. Gong, X. Han, and W. Zou, "Smartdroid: an automatic system for revealing ui-based trigger conditions in android applications," in *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2012, pp. 93–104.

[54] G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos, "Paranoid android: versatile protection for

smartphones," in *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM, 2010, pp. 347–356.

[55] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: behavior-based malware detection system for android," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011, pp. 15–26.

[56] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 627–638.

[57] Q. Do, B. Martini, and K.-K. R. Choo, "Enhancing user privacy on android mobile devices via permissions removal," in *System Sciences (HICSS), 2014 47th Hawaii International Conference on*. IEEE, 2014, pp. 5070–5079.

[58] Z. Yang, M. Yang, Y. Zhang, G. Gu, P. Ning, and X. S. Wang, "Appintent: Analyzing sensitive data transmission in android for privacy leakage detection," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 1043–1054.

[59] S. Bugiel, L. Davi, A. Dmitrienko, S. Heuser, A.-R. Sadeghi, and B. Shastry, "Practical and lightweight domain isolation on android," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011, pp. 51–62.

[60] P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, "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*. ACM, 2011, pp. 639–652.

[61] D. Ghosh, A. Joshi, T. Finin, and P. Jagtap, "Privacy control in smart phones using semantically rich reasoning and context modeling," in *Security and Privacy Workshops (SPW), 2012 IEEE Symposium on*. IEEE, 2012, pp. 82–85.

[62] Y. Zhou and X. Jiang, "Detecting passive content leaks and pollution in android applications," in *NDSS*, 2013.

[63] D. Barrera, J. Clark, D. McCarney, and P. C. Van Oorschot, "Understanding and improving app installation security mechanisms through empirical analysis of android," in *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2012, pp. 81–92.

[64] Y. Zhou, X. Zhang, X. Jiang, and V. W. Freeh, "Taming information-stealing smartphone applications (on android)," in *Trust and Trustworthy Computing*. Springer, 2011, pp. 93–107.

[65] A. R. Beresford, A. Rice, N. Skehin, and R. Sohan, "Mockdroid: trading privacy for application functionality on smartphones," in *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*. ACM, 2011, pp. 49–54.

[66] Z. Benenson, F. Gassmann, and L. Reinfelder, "Android and ios users' differences concerning security and privacy," in *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2013, pp. 817–822.

[67] I. Shklovski, S. D. Mainwaring, H. H. Skúladóttir, and H. Borgthorsson, "Leakiness and creepiness in app space: perceptions of privacy and mobile app use," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2347–2356.

[68] S. Rosen, Z. Qian, and Z. M. Mao, "Appprofiler: a flexible method of exposing privacy-related behavior in android applications to end users," in *Proceedings of the third ACM conference on Data and application security and privacy*. ACM, 2013, pp. 221–232.

[69] A. Mylonas, M. Theoharidou, and D. Gritzalis, "Assessing privacy risks in android: a user-centric approach," in *Proceedings of the 1st international workshop on risk assessment and risk-driven testing (RISK-2013), Springer, Turkey (November 2013)*, 2013.

[70] E. Toch, "Crowdsourcing privacy preferences in context-aware applications," *Personal and ubiquitous computing*, vol. 18, no. 1, pp. 129–141, 2014.

[71] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," *Communications Magazine, IEEE*, vol. 48, no. 9, pp. 140–150, 2010.

[72] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys (CSUR)*, vol. 45, no. 1, p. 3, 2012.

[73] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall, "Toward trustworthy mobile sensing," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*. ACM, 2010, pp. 31–36.

[74] L. Kazemi and C. Shahabi, "Towards preserving privacy in participatory sensing," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*. IEEE, 2011, pp. 328–331.

[75] E. De Cristofaro and C. Soriente, "Short paper: Pepsi—privacy-enhanced participatory sensing infrastructure," in *Proceedings of the fourth ACM conference on Wireless network security*. ACM, 2011, pp. 23–28.

[76] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, and N. Triandopoulos, "Anonysense: A system for anonymous opportunistic sensing," *Pervasive and Mobile Computing*, vol. 7, no. 1, pp. 16–30, 2011.

[77] H. Choi, S. Chakraborty, Z. M. Charbiwala, and M. B. Srivastava, "Sensorsafe: a framework for privacy-preserving management of personal sensory information," in *Secure Data Management*. Springer, 2011, pp. 85–100.

[78] L. Jedrzejczyk, B. A. Price, A. K. Bandara, and B. Nuseibeh, "I know what you did last summer: risks of location data leakage in mobile and social computing," *Department of Computing Faculty of Mathematics, Computing and Technology The Open University*, pp. 1744–1986, 2009.

[79] M. M. Groat, B. Edwards, J. Horey, W. He, and S. Forrest, "Enhancing privacy in participatory sensing applications with multidimensional data," in *Pervasive Computing and Communications (PerCom), 2012 IEEE In-*

ternational Conference on. IEEE, 2012, pp. 144–152.

[80] R. P. Minch, "Privacy issues in location-aware mobile devices," in *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*. IEEE, 2004, pp. 10–pp.

[81] D. Christin, J. Guillemet, A. Reinhardt, M. Hollick, and S. S. Kanhere, "Privacy-preserving collaborative path hiding for participatory sensing applications," in *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*. IEEE, 2011, pp. 341–350.

[82] K. Vu, R. Zheng, and J. Gao, "Efficient algorithms for k-anonymous location privacy in participatory sensing," in *INFOCOM, 2012 Proceedings IEEE*. IEEE, 2012, pp. 2399–2407.

[83] B. Agir, T. G. Papaioannou, R. Narendula, K. Aberer, and J.-P. Hubaux, "User-side adaptive protection of location privacy in participatory sensing," *GeoInformatica*, vol. 18, no. 1, pp. 165–191, 2014.

[84] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding users' requirements for data protection in smartphones," in *Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on*. IEEE, 2012, pp. 228–235.

[85] L. Barkhuus and A. K. Dey, "Location-based services for mobile telephony: a study of users' privacy concerns." in *INTERACT*, vol. 3. Citeseer, 2003, pp. 702–712.

[86] N.-W. Gong, M. Laibowitz, and J. A. Paradiso, "Dynamic privacy management in pervasive sensor networks," in *Ambient Intelligence*. Springer, 2010, pp. 96–106.

[87] J. Freudiger, R. Shokri, and J.-P. Hubaux, "Evaluating the privacy risk of location-based services," in *Financial Cryptography and Data Security*. Springer, 2012, pp. 31–46.

[88] L. Kazemi and C. Shahabi, "A privacy-aware framework for participatory sensing," *ACM SIGKDD Explorations Newsletter*, vol. 13, no. 1, pp. 43–51, 2011.

[89] J. Shi, Y. Zhang, and Y. Liu, "Prisense: privacy-preserving data aggregation in people-centric urban sensing systems," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9.

[90] R. K. Ganti, N. Pham, Y.-E. Tsai, and T. F. Abdelzaher, "Poolview: stream privacy for grassroots participatory sensing," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*. ACM, 2008, pp. 281–294.

[91] B. Gedik and L. Liu, "Location privacy in mobile systems: A personalized anonymization model," in *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on*. IEEE, 2005, pp. 620–629.

[92] W. Diao, X. Liu, Z. Zhou, and K. Zhang, "Your voice assistant is mine: How to abuse speakers to steal information and control your phone," in *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*. ACM, 2014, pp. 63–74.

[93] X. Page, K. Tang, F. Stutzman, and A. Lampinen, "Measuring networked social privacy," in *Proceedings of the 2013 conference on Computer supported cooperative work companion*. ACM, 2013, pp. 315–320.

[94] N. Mohamed and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from malaysia," *Computers in Human Behavior*, vol. 28, no. 6, pp. 2366–2375, 2012.

Rui LIU

Rui Liu is currently a MPhil candidate in the Department of Computing at Hong Kong Polytechnic University. He received the BSc degree from Northeastern University, China, in 2012. He is a recipient of Research Studentships in Hong Kong Polytechnic University. He is an Outstanding Graduate in Liaoning Province. He is a recipient of the Google Excellence Scholarship. His research interests include participatory sensing systems, privacy measurement, recommendation system, and pervasive computing. He is now a student member of IEEE Computer Society.

Jiannong CAO

Jiannong Cao is currently a chair professor and the head of the Department of Computing at Hong Kong Polytechnic University. He received the BSc degree from Nanjing University, China, in 1982, and the MSc and PhD degrees from Washington State University, USA, in 1986 and 1990, all in computer science. His research interests include parallel and distributed computing, computer networks, mobile and pervasive computing, fault tolerance, and middleware. He coauthored 4 books, coedited 9 books, and published more than 300 technical papers in major international journals and conference proceedings. He has directed and participated in numerous research and development projects and, as a principal investigator, obtained over HK$25 million grants. He is a fellow of IEEE, a member of ACM, and a senior member of China Computer Federation. He has served as the Chair of IEEE Technical Committee on Distributed Computing, an associate editor and a member of editorial boards of many international journals, and a chair and a member of organizing and program committees for many international conferences.

Lei YANG

Lei Yang received his Ph.D degree from Department of Computing, The Hong Kong Polytechnic University, in 2014, the MSc degree from Institute of Computing Technology, Chinese Academy of Science, in 2010, and the BSc degree from Wuhan University, in 2007. He is currently a postdoc in Department of Computing, The Hong Kong Polytechnic University. His research interest includes mobile cloud computing, RFID systems, and social computing.