2012 Tenth International Conference on ICT and Knowledge Engineering

A Review of Mobile Location Privacy in the Internet of Things

Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung
School of Computing, Engineering and Mathematics
University of Western Sydney
Sydney, Australia

***Abstract*—The goal of Internet of Things (IoT) research is to extend computing and connectivity to anything, anyone, anywhere and anytime. While there are apparent benefits in using IoT systems, the convergence of technologies has begun to challenge the privacy of users. Powered by location based services, these systems have the potential to enable a systematic mass surveillance and to impinge on the personal privacy of users, especially their location privacy. This paper overviews some of the existing location privacy issues found on mobile devices. Particular attention is paid to the current access permission mechanism used on the Android, iPhone and Windows Mobile platforms. It is anticipated that the current privacy issues in mobile platforms are more likely to be inherited if not magnified in the IoT.**

***Keywords*—Location Based Services, Location Privacy, Mobile Computing, Internet of Things.**

I. INTRODUCTION

The inventions of the Internet, computers, mobile devices, wireless networks, GPS enabled devices and other types of communications took place rapidly given that humanity took thousands of years before the inventions of the wheel. With this rapid advancement of technology, the Internet of Things (IoT) is no longer seen as a vision of the future. It is becoming a reality. IoT is where networks of objects are connected together using wireless technologies, RFID, 3G and 4G networks, Bluetooth, GPS systems and other communication technologies. The interconnected network of everyday objects, along with backend systems that seek out patterns of activity among those objects, in tandem with cloud computing environments, web portals, and mobile computing will allow the 'Things' to communicate with each other. Over the next couple of years, the prediction is that the industrial value of the Internet of Things will surpass that of the Internet 30 times over, and it is expected to become a market that is worth more than $100 billion [1].

The convergence of location based services (LBSs), communication and computing technologies in the Internet of Things arena will enable a revolution in our everyday activities, where both technologies become sophisticated. Location based services, especially on mobile devices, are now becoming more mainstream. Mobile devices, mobile applications and location based service technologies will be the key elements in the emerging Internet of Things. Recent studies on the Internet of Things show the importance of mobile devices in this domain. Examples are the integration of RFID technology in mobile devices [2] and the combinational application of mobile networks and IOT technology for a mobile logistic information collection [3].

While there are apparent benefits in using IoT systems, this combination of technologies is going to challenge the protection of privacy of users. Powered by LBS, these systems have the potential to enable systematic mass surveillance and to impinge on the personal privacy of users especially their location privacy. Location privacy concern by itself is not new. What is new is the increased scope of the problem. The automation in gathering and analyzing users' information, in the IoT environment, gives location privacy an added dimension. This work is an attempt to highlight the issue of location privacy in the IoT. The paper is organized as follows: Section 2 discusses location based services and location technologies. Section 3 covers the issues of location privacy. The location privacy in mobile devices in relation to the IoT is discussed in Section 4. Conclusions and other issues are presented in Section 5.

II. LOCATION BASED SERVICES

In mobile computing, there are wide-spread adoptions of LBSs in smart phone applications. Mobile applications such as those which run on the iPhones or the Android enabled devices give mobile users the ability to access remote data anytime and anywhere, and to improve availability of services e.g. group calendar, mobile banking, and social networking. Searching for a restaurant nearby or exploring the current area for shopping deals or discounts are some examples of LBSs in use today on almost every smart phone.

Sharing location information has improved the way people communicate. Mobile location based services have facilitated the exchange of location information between people, making socializing easier. A couple of years ago, some studies in Europe [4], found that most teenagers used SMS to connect with their friends and arrange meetings. Lately, SMS communication has evolved significantly with the penetration of mobile applications in the mobile industry. With the wide spread of iPhones, Android and Windows mobile phones, SMS and VOIP applications, operating over 3G networks, are taking over traditional SMS. Some of these applications also offer location sharing with friends. These applications are referred to as social location disclosure applications [5]. The cross mobile platform applications "Whatsapp" and "Viber" for example, enable mobile users to exchange, using an Internet connection, text messages, images, audio and video messages, and location

978-1-4673-2317-8/12/$31.00©2012 IEEE

information with one another at no cost. Other location based services have emerged and applications such as child location services are becoming popular [6].

A. Location Awarness

Traditionally, computers only have the ability to determine the identity of users using traditional methods of authenticating individuals or computers by usernames and passwords, digital certificates, and other credentials. They also have the ability to record the times of access and in some cases the IP addresses of users. Location awareness is a term which has become popular only recently. The term originated from configuration settings in networking. Network location awareness (NLA) services collect network configuration and location information, and notify applications when this information changes [6]. With the advent of global positioning systems and radio-equipped mobile devices, the term has evolved ever since. Obtaining location information becomes more useful in combination with identity authentication in mobile and pervasive computing. This combination leads to the use of the term location based services.

Hopper describes the three methods usually used to record location information [7]: (1) coordinates: a two- or three-dimensional vector of real numbers representing the distance of an entity from a well-defined origin; (2) proximity: a real number (usually rounded to a binary value) representing how close two or more entities are to one another; and, (3) containment: a value representing the amount of interaction between entities ,e.g. a laptop is inside a room.

Recent development in mobile computing has enabled portable devices to obtain location information using various methods. Access to location information can be initiated using GPS satellite tracking, cellular tower triangulation, or the device's media access control (MAC) address on a Wi-Fi network. The following sections describe different location technologies.

B. Location via GPS

Research into the Global Positioning System (GPS) can be dated back to 1972 when the United States Air Force (USAF) conducted developmental flight tests of two prototypes of GPS receivers over White Sands Missile Range, using ground-based pseudo-satellites. Consequently, GPS satellites were widely used for the first time in 1990 during the gulf war [8]. A device equipped with a GPS receiver calculates its position by precisely timing the signals sent out by the GPS satellites. Usually, signals from 3 satellites are required for the two dimensional (2D) operational mode. The 2D operation mode will provide only horizontal coordinates without elevation readings. For the 3D operation mode, at least 4 satellites are needed. In this scenario the horizontal and elevation coordinates can be obtained. Messages sent by satellites include the time when a message was transmitted and the satellite's position at the time of sending the message. Therefore, using messages received from a minimum of four satellites, a GPS receiver is able to determine the times sent and therefore the positions of the satellites corresponding the times sent. The location process is as follows: The GPS receiver starts by locating four or more satellites, calculates the distance to each satellite, and uses the distances from all the satellites to determine its own location. This process is based on a mathematical principle know as trilateration. Trilateration is the process of determining the absolute or relative locations of points by measurement of distances, using the geometry of circles, spheres or triangles. Therefore, a GPS navigation device provides latitude and longitude information, and some have the ability to provide altitude information.

C. Location via Wi-Fi

With the rapid growth of wireless technologies, in general, and wireless local areas networks (WLANs), locating wireless device based on Wi-Fi signals, known as Wi-Fi-based positioning system (WPS), is attracting more applications. The localization mechanism used for positioning in Wi-Fi access points is based on two methods. The first is by measuring the intensity of the received signal and the second is known as WLAN fingerprinting [9].

A location fingerprinting technique, also known as a scene analysis or pattern matching technique, observes the operating environment and estimates a device's current location based on these observations [10]. This method assumes that every physical location has a unique fingerprint in the wireless signal space, i.e. different characteristics, similar to the fingerprint of human. The operating procedure of this technique mainly consists of two phases. The first phase consists of an offline sampling where WLAN scanning is performed and map construction is performed, and an online locationing. In the second phase, the location of the WLAN device is determined based on real-time WLAN measurements. The wireless geo-location techniques are usually based on a mathematical calculation of the time of arrival (TOA), the time difference of arrival (TDOA) and the direction of arrival (DOA) of the signals [11].

D. Location through Cellular Network

Obtaining the location of a device through the cellular network is known as GSM localization. Localization is performed using the multilateration of radio signals between the radio towers of the network and the device. Multilateration is a navigation technique based on the measurement of the differences in distance to two or more stations at known locations that broadcast signals at known times [12]. Interestingly, this process of localization does not require an active phone call. GSM is based on the signal strength to nearby antenna masts. The GSM localization method works as follows. The base station has the responsibility of processing calls from a GSM enabled device. Therefore, a base station can determine the general geographic area of a device. Other base stations also make contact with the GSM enabled device and once information from several base stations has been gathered, the location of the device can be narrowed down using triangulation. Triangulation is the process of determining the location of a point by measuring angles to it from known points at either end of a fixed baseline [13], rather than measuring distances to the point directly known as trilateration. Accuracy can be to within a few hundred meters in city areas where the base stations are not far from each other; while in rural areas, the system is less accurate.

III. LOCATION PRIVACY

Locations based services offer numerous benefits to users as well as financial benefits. However, the possibility of unauthorized disclosure of location information is one of the major concerns and it poses a serious threat to users' privacy. In such an environment, users are unable to manage their location disclosure settings effectively as they lack the control over the location sharing. Consequently, a user may wish to stay anonymous and may not want to be identified by LBS providers, especially when the information reveals the location of the user. Researchers have long been aware of the potential privacy risks associated with LBSs as the problem has received a considerable attention from users and, in some cases, from service providers and government organization.

While better services can be provided if personalization is allowed, not all LBSs require the personal identification of a user. However, the problem is that positioning information in the form of a specific location can actually lead to personal identification of the user and their behaviors. The study in [14] showed that a driver's home location can be inferred from the GPS data collected from his vehicle even if the location information was anonymized. It further shows that the reconstruction of an individual's route could provide a detailed movement profile that allows inferences. For example, recurring visits to a medical clinic could indicate illness and visits to activist organizations could hint at political opinions. In [14], it has been found that using clustering techniques, locations of users can be exposed even when the GPS traces, collected by the location-based services, are anonymized. In [15], it was found that there are ethical issues associated with the use of GPS with public users. Adequate safeguards need to be in place to avoid the abuse of location information gathered through GPS technology.

In another study [16], it has been shown that the future movements' of users can be predicated from location information collected over a period of time. The authors used GPS data from a single volunteer collected over a four month period and used it to derive the location context of a user. They developed an algorithm which extracted locations of importance from the GPS data and used it to design an intelligent predictive model of the user's future movements. In a similar study, a protocol was developed which had the ability to identify and infer the home location and the identity of a user. Data were collected from 172 individuals. A reverse geo-coder was able to infer home locations of roughly 5% of the participants correctly [17].

A. Should Apps Developers be Trusted?

A law suit was filed in 2012 against Twitter, Apple, Facebook, Instagram, and some mobile application companies, accusing them of distributing privacy-invading mobile applications [18]. Lookout, a security firm specialized in anti-virus products, revealed the results of its 'App Genome Project' report, showing that around 300,000 applications for both iPhone and Android phones have the capability to access users' personal data [19]. The reports also showed the percentage of free applications that have the capability to access user's locations and contact data, and the ability to execute third party codes which enable users' data to be collected and these data may be analyzed to reveal user's location information.

B. Android, Apple and Windows Mobile Phones

The hundreds of Android threats, reported by McAfee in the middle of 2011, have jumped into thousands in the first quarter of 2012 [20]. Similarly, F-secure (a well-established anti-virus and computer security company) reported that Android malwares have been growing exponentially [21]. Some of these malwares were targeting the users' personal information.

TaintDroid project [22], has identified that some Android applications are releasing users' private information to online advertisers. TaintDroid is a joint study by Intel Labs, Penn State, and Duke University. An application was developed to provide real-time monitoring services that precisely monitor the traffic of a particular application and detect when private information was released to a third party. In a study of the 30 most popular applications, TaintDroid found that 15 applications were sending users' geographic location to remote advertisement servers. The study also found that seven of the 30 applications sent the unique phone (hardware) identifier, and, in some cases, the phone number and SIM card serial number to developers. These 30 applications were randomly selected out of the 358 most popular free applications on the Android Play that have access to both the Internet and privacy information such as geographic location, camera, audio, and phone information. The TaintDroid project results are summarized in Table 1.

In [23], the authors reported that hackers could take control of a phone by maliciously crafting SMS messages. An attacker can get full control of the user's phone by sending 500 messages without being noticed by the victim. In March 2011, another study found that 7.5% of the total applications on the Android OS had the capability to access the user's stored contacts, while 28% of them had access to the user's location [19]. In December 2011, Google removed 22 applications from the Android market saying that these applications were stealing and hacking user data [24].

TABLE I. TAINTDROID PROJECT SUMMARY

Statistical Significance	30 Applications, 8% of the top 50 popular free applications in each category that had access to privacy sensitive information were monitored and analyzed (at the time of the experiment).
Users Awareness	The installed applications do not inform the user when or why personal data are collected. The declaration of permission request during installation does not provide enough information on when and to whom private information are sent.
Periodicity of Transfer	Some applications shared location information with advertisement servers only when displaying ads to the user. Some applications shared location information even when the user was not running the application. Some applications shared location information frequently as every 30 seconds.
Limitations	The study only covers the Android platform.

Similarly, Apple pulled out the MogoRoad - Swiss road traffic information application from its App Store. It was because Apple received many user complaints that, by using this application, users were getting phone calls from marketing companies. Also, a federal lawsuit in the US was filed against the Storm8 iPhone application maker. They were accused of harvesting users' phone numbers using their game application without any encryption [25]. Seriot also pointed out that another iPhone's application which violated users' privacy. The application was called Hollywood Gossip and it was available to download for free on the App Store. Besides providing clues about celebrities and stars, the application was found to be secretly accessing users' address books and changing email addresses. The application developer knew that people from the film industry were most likely to use this application. The developer intended to use the application to collect private information from celebrities [26].

Another study published by "The Wall Street Journal" analyzed the 101 most popular smart phone applications running on different operating systems, including the Windows phone, iPhone and Android phone [27]. It was reported that out of the 101 applications, 56 transmitted the unique phone IDs to other companies without the users' authorizations. Forty-seven applications were caught transmitting location information to third parties. The other five applications were found to be stealing other information like information about genders and ages.

Prashant Gupta published a review on the applications running on the Window Mobile platform on McAfee website [28]. He pointed out that some applications had the capability to access a user's picture library, video library, webcam's video feed, microphone's audio feed, location, and other information related to the Internet connection. Some of these applications also have had ability to add, change or delete files from both the picture and video libraries.

In 2011, a study detailed the vulnerability of the RIM BlackBerry device [29]. The author developed a spyware targeted to blackberry devices. The spyware was able to access and transfer sensitive data back to a server without the user's notice. It showed the impact on the integrity, and availability of corporate data if similar spywares infiltrate BlackBerry devices connected to corporate assets.

IV. MOBILE PRIVACY & THE IOT

The previous Section reported some privacy incidents from the use of Mobile applications on the Android, Blackberry, iPhone, and Windows platforms. Some service providers were found stealing users' private information, such as the contact addresses or location information of the user. In this section, we examine the application permission mechanism used in mobile devices in order to develop a better understanding of the flaws in the application permission mechanism being used. It is anticipated that mobile devices are going to be the major player in the IoT. Therefore, the privacy issues found in the current privacy model are more likely to be inherited if not magnified in typical IoT scenarios.

Apple iOS is generally considered as a closed platform. Unlike Android, Windows Phone and BlackBerry platforms

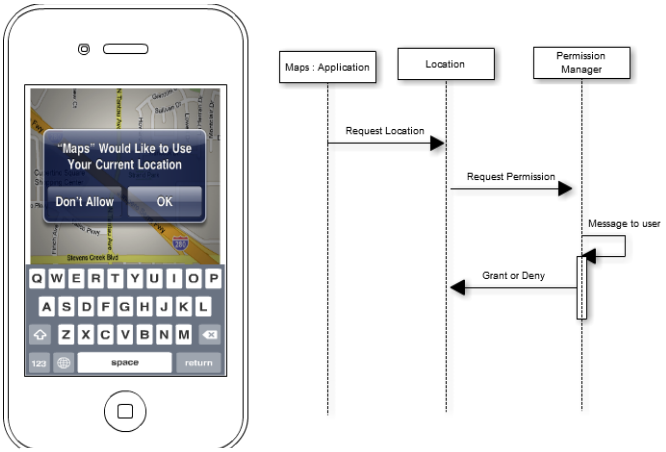

Figure 1. iPhone Location Permission Request

where an application must declare the required application privileges for inspection and approval by the end-user prior to installation, iPhone applications have access to everything in the mobile by default and the OS only alerts users when an application accesses their location. The Android and Windows models present choices to the end-users, while Apple prefers the OS making the decision on application permission during the installation process. The following sections describe the access permission mechanism used during the installation of application s on mobile devices.

A. Application Permission on iPhone

Users in the iOS platform are only notified by the application when a certain application requests access to location information. This notification is in the form of a popup message in which a user has the choice of granting or denying access to his/her location. Fig. 1 shows the popup message from an iPhone. While, this method gives users the control over their location information, there are no other settings/features provided to control the rest of the personal information, such as the contact address.

Beside, notifying a user for every possible application permission request will end up in a large number of messages presented to the user. This will impose much of the administrative burden on a user.

B. Application Permission on Android and Windows Mobile

In the Android and Windows Mobile platforms, in order to access certain data or capabilities on the mobile phones, an application requests some access permissions when the application is being installed. Its application framework enforces the permission-based security policy that only allows installed applications to access other parts of the system when they are explicitly permitted to do so. The permission is granted by the human user when an application is installed on the mobile device. Some permission requests allow access to standard phone capabilities such as the Internet, while others involve accessing sensitive information such as location information or text messages. As of location permission, they can be of two types. A fine GPS permission allows applications to determine the user's location when the GPS is on. The other option is related to access to coarse location

information in the database of the mobile phone network; and the majorities of applications have access to both. There are 22 different permissions that an application could obtain in the Android platform. Permissions are enforced by Android at runtime, but must be accepted by the user at installation time.

When users install a new application in Android, they are prompted to accept or deny the permissions requested by the application. Permissions are also described in a more user friendly language at installation time. These descriptions attempt to give a brief, technical explanation for the permissions, but do not disclose what the developer intends to use access to those resources for. In its simplest form, access to each user's personal information, referred to as a component such as contact address or location, by an application, is restricted by assigning it to an access permission label. The reference monitor looks at the permission labels assigned to its application and if the target component's access permission label is in that collection, then it allows establishment of access to proceed. If the label isn't in the collection, establishment is denied even if the components are in the same application [30].

This label oriented framework enables an ease of use and deployment. However, it can lead to poor security practices as shown from the number of privacy breaches previously reviewed. In addition, management of permissions becomes almost impossible when there are a large number of applications involved. It became hard to follow which application, service provider, or company behind to which component has access to. Fig. 2 shows how granting of permissions is being kept tracked. Moreover, users are not aware of the date, time or how their personal information are collected. There are no ways to revoke, change or limit the access permissions granted to applications.

C. The Inherited Privacy Issues in the IoT

The seamless interconnectivity of objects, envisioned in the IoT, highlights the complexity of realizing location privacy in this environment. It is clearly evident that it is almost impossible to achieve perfect privacy as long as seamless communication is taking place. When location based systems, powered by the autonomity of the Internet of Things, track users automatically on an ongoing basis, they generate an enormous amount of potentially sensitive information, especially when the location information are tangled with identity information.

The main location privacy concern with regards to the IoT is that many new automated attack vectors become possible [31]. The literature shows that if an effective public record of people's locations is created through automations, discriminations based on race and religious, for example, are most likely to occur. Things, referred to as objects that log data about their use, location, history and others private information present an interesting challenge.

With the current schema of permissions used on mobile devices, the amount of personal data that would be occasionally collected in an IoT environment will be extremely larger than what we have experienced before. In facts, the ways in which data collection, mining and provisini-

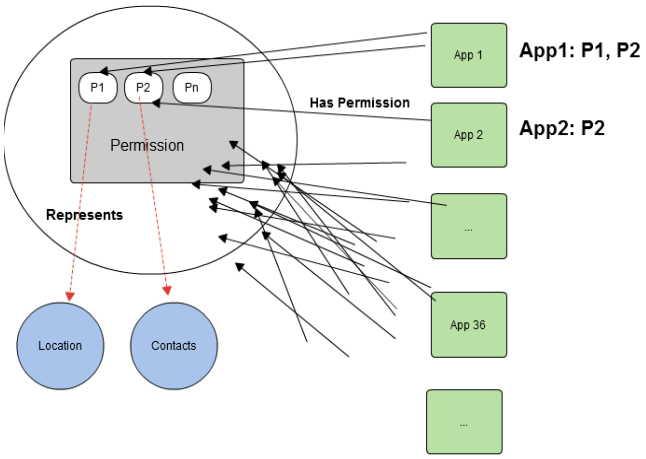

Figure 2. Inability to keep Track of Applications' Permission on Android

-ing will be performed in the IoT environment can become arbitrary as more objects and applications obtain accesses to a user's personal information. Fig. 3 shows how a snail trail track of personal information and location can be generated from the use of typical IoT services, including LBS.

V. CONCLUSIONS

Privacy is one of the major implications as the Internet of Things develops. Privacy no longer means anonymity in the IoT. Profiling and data mining within any IoT scenario can form a potential harm to individuals due to the automatic process of data collection, their storage and the way personal data can be easily shared and analyzed.

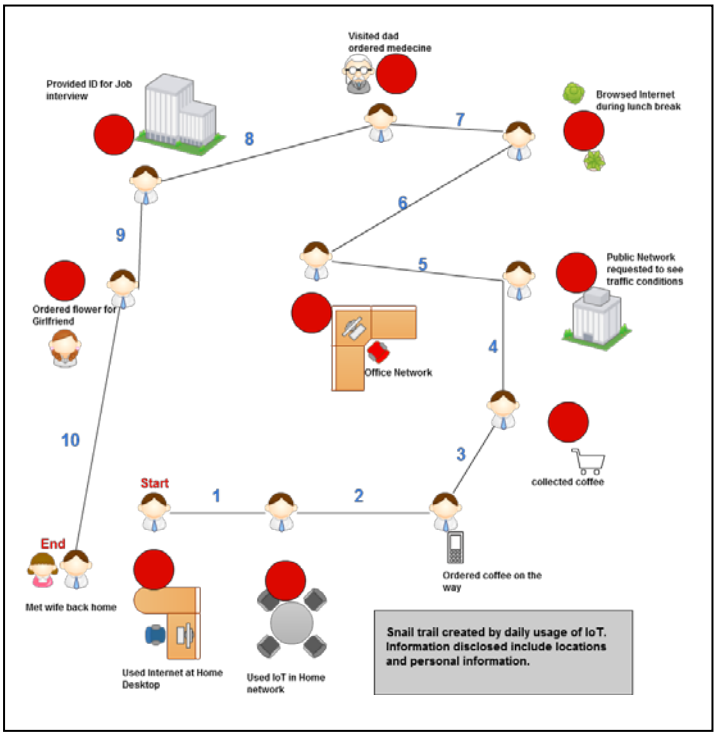

Figure 3. Snail Trail Track

In addition, the foundations and regulations for digital privacy were established some years ago when the Internet was centralized. These regulations deal with the collection of data and access rights, and ensure their correct handling. That's no longer the case today. At its simplest definition, privacy means, giving users the option to control how their collected personal information might be used; specifically for secondary usage and third party access. As an example, in the online environment, privacy choices can be exercised by simply clicking a box on the browser screen that indicates a user's decision with respect to the use of the information being collected. The concept remained the same in the evolution of social networking, where users in Facebook indicate to whom and to witch extent their information can be revealed. These are known as the principles of notice and choice.

Collection of personal information without the individual's knowledge or consent is possible and more luckily to occur within this new environment. What if your new sunglasses start sharing information about your location every time you cross the harbor bridge? This can easily be made if the sunglasses are equipped with a tiny RFID. The vision of IoT is that overall interconnectivity would allow individuals to locate and monitor everything, everywhere and at any time. But what if users don't want to share their location information? Do they have control over that? What are the principles that should govern the deployment of such technology? And who determine that fine line between tracing and surveillance, security and privacy, and to what extent collection of personal information and tracking of people locations are accepted?

Obviously, in the literature, there exist several traditional approaches to protect the location information of a user. Some approaches try to prevent disclosure of unnecessary information, some other approaches use anonymization techniques, such as mix zone, and other relies on access control. Each of these approaches has some benefits to the problem but also suffers from certain limitations. Therefore, given the particular characteristics of the IoT and its heterogeneity, there is a need to study these solutions in order to investigate their suitability of adoption in typical IoT scenarios. It is important that research into privacy protection techniques to bear in mind the heterogeneity of access in the IoT and the fact that the user should be considered as a non-expert user of technology.

REFERENCES

[1] M. CLENDENIN. (2010, *CHINA'S 'INTERNET OF THINGS' OVERBLOWN, SAYS EXEC*. AVAILABLE: HTTP://WWW.INFORMATIONWEEK.COM/NEWS/STORAGE/VIRTUALIZATION/225700966?SUBSECTION=NEWS

[2] Y. DONG AND W. QINGXIAN, "THE STUDY ON THE APPLICATION OF RFID- BASED MOBILE PAYMENT TO THE INTERNET OF THINGS," IN *MULTIMEDIA TECHNOLOGY (ICMT), 2011 INTERNATIONAL CONFERENCE ON*, 2011, PP. 908-911.

[3] Y. WEI, "DESIGN AND REALIZATION OF MOBILE INFORMATION COLLECTION MODULE IN LOGISTIC INTERNET OF THINGS UNIFIED INFORMATION SYSTEM," IN *BUSINESS MANAGEMENT AND ELECTRONIC INFORMATION (BMEI), 2011 INTERNATIONAL CONFERENCE ON*, 2011, PP. 36-39.

[4] R. LING, "THE SOCIOLINGUISTICS OF SMS: AN ANALYSIS OF SMS USE BY A RANDOM SAMPLE OF NORWEGIANSMOBILE COMMUNICATIONS." VOL. 31, ED: SPRINGER LONDON, 2005, PP. 335-349.

[5] I. SMITH, *ET AL.*, "SOCIAL DISCLOSURE OF PLACE: FROM LOCATION TECHNOLOGY TO COMMUNICATION PRACTICES PERVASIVE COMPUTING," IN *PERVASIVE COMPUTING*. VOL. 3468, H. GELLERSEN, *ET AL.*, EDS., ED: SPRINGER BERLIN / HEIDELBERG, 2005, PP. 151-164.

[6] A. LEONHARDI AND K. ROTHERMEL, "ARCHITECTURE OF A LARGE-SCALE LOCATION SERVICE," IN *DISTRIBUTED COMPUTING SYSTEMS, 2002. PROCEEDINGS. 22ND INTERNATIONAL CONFERENCE ON*, 2002, PP. 465-466.

[7] A. HOPPER, "THE CLIFFORD PATERSON LECTURE, 1999. SENTIENT COMPUTING," *PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY OF LONDON. SERIES A: MATHEMATICAL, PHYSICAL AND ENGINEERING SCIENCES*, VOL. 358, PP. 2349-2358, 2000.

[8] K. ELGETHUN, M. G. YOST, C. T. E. FITZPATRICK, T. L. NYERGES, AND R. A. FENSKE, "COMPARISON OF GLOBAL POSITIONING SYSTEM (GPS) TRACKING AND PARENT-REPORT DIARIES TO CHARACTERIZE CHILDREN'S TIME-LOCATION PATTERNS," *J EXPOS SCI ENVIRON EPIDEMIOL*, VOL. 17, PP. 196-206, 2006.

[9] K. KAEMARUNGSI AND P. KRISHNAMURTHY, "PROPERTIES OF INDOOR RECEIVED SIGNAL STRENGTH FOR WLAN LOCATION FINGERPRINTING," IN *MOBILE AND UBIQUITOUS SYSTEMS: NETWORKING AND SERVICES, 2004. MOBIQUITOUS 2004. THE FIRST ANNUAL INTERNATIONAL CONFERENCE ON*, 2004, PP. 14-23.

[10] V. HONKAVIRTA, T. PERALA, S. ALI-LOYTTY, AND R. PICHÉ, "A COMPARATIVE SURVEY OF WLAN LOCATION FINGERPRINTING METHODS," 2009, PP. 243-251.

[11] H. LIU, H. DARABI, P. BANERJEE, AND J. LIU, "SURVEY OF WIRELESS INDOOR POSITIONING TECHNIQUES AND SYSTEMS," *SYSTEMS, MAN, AND CYBERNETICS, PART C: APPLICATIONS AND REVIEWS, IEEE TRANSACTIONS ON*, VOL. 37, PP. 1067-1080, 2007.

[12] M. RAHNEMA, "OVERVIEW OF THE GSM SYSTEM AND PROTOCOL ARCHITECTURE," *COMMUNICATIONS MAGAZINE, IEEE*, VOL. 31, PP. 92-100, 1993.

[13] Y. LIU, Z. YANG, X. WANG, AND L. JIAN, "LOCATION, LOCALIZATION, AND LOCALIZABILITY," *JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY*, VOL. 25, PP. 274-297, 2010.

[14] B. HOH, M. GRUTESER, H. XIONG, AND A. ALRABADY, "ENHANCING SECURITY AND PRIVACY IN TRAFFIC-MONITORING SYSTEMS," *PERVASIVE COMPUTING, IEEE*, VOL. 5, PP. 38-46, 2006.

[15] K. MICHAEL, A. MCNAMEE, AND M. MICHAEL, "THE EMERGING ETHICS OF HUMANCENTRIC GPS TRACKING AND MONITORING," PRESENTED AT THE PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON MOBILE BUSINESS, 2006.

[16] D. ASHBROOK AND T. STARNER, "USING GPS TO LEARN SIGNIFICANT LOCATIONS AND PREDICT MOVEMENT ACROSS MULTIPLE USERS," *PERSONAL AND UBIQUITOUS COMPUTING*, VOL. 7, PP. 275-286, 2003/10/01 2003.

[17] J. KRUMM, "INFERENCE ATTACKS ON LOCATION TRACKS," PRESENTED AT THE PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING, TORONTO, CANADA, 2007.

[18] (2012, *18 FIRMS SUED FOR USING PRIVACY-INVADING MOBILE APPS*. AVAILABLE: HTTP://WWW.COMPUTERWORLD.COM/S/ARTICLE/9225219/18_FIRMS_SUED_FOR_USING_PRIVACY_INVADING_MOBILE_APPS

[19] (2011, *APP GENOME PROJECT*. AVAILABLE: HTTPS://WWW.MYLOOKOUT.COM/APPGENOME

[20] "MCAFEE THREATS REPORT: FIRST QUARTER 2012," MCAFEE LABS2012.

[21] "MOBILE THREATS REPORT," F-SECURE2012.

[22] W. ENCK, *ET AL.*, "TAINTDROID: AN INFORMATION-FLOW TRACKING SYSTEM FOR REALTIME PRIVACY MONITORING ON SMARTPHONES," PRESENTED AT THE PROCEEDINGS OF THE 9TH USENIX CONFERENCE ON OPERATING SYSTEMS DESIGN AND IMPLEMENTATION, VANCOUVER, BC, CANADA, 2010.

[23] C. MULLINER AND C. MILLER, "FUZZING THE PHONE IN YOUR PHONE," IN *BLACKHAT USA 2009*, LAS VEGAS, NV, USA, 2009.

[24] (2011, *GOOGLE MOVES TO DELETE 'RUFRAUD' SCAM ANDROID APPS*. AVAILABLE: HTTP://WWW.BBC.COM/NEWS/TECHNOLOGY-16177013

[25] M. La Polla, F. Martinelli, and D. Sgandurra, "A Survey on Security for Mobile Devices," *Communications Surveys & Tutorials, IEEE*, vol. PP, pp. 1-26, 2012.

[26] N. Seriot, "iPhone Privacy," in *Black Ha*, Virginia, USA, 2010.

[27] S. THURM and Y. I. KANE. (2010, Your Apps Are Watching You. Available: http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html

[28] P. Gupta, "Metro Interface Improves Windows 8 While Increasing Some Risks," ed: McAfee, 2012.

[29] H. Fredrik, "System Integrity for Smartphones: A security evaluation of iOS and BlackBerry OS," Master, Department of Electrical Engineering, Information Coding, Linkoping University, 2011.

[30] W. Enck, M. Ongtang, and P. McDaniel, "Understanding Android Security," *Security & Privacy, IEEE*, vol. 7, pp. 50-57, 2009.

[31] A. Görlach, A. Heinemann, and W. Terpstra, "Survey on Location Privacy in Pervasive Computing

Privacy, Security and Trust within the Context of Pervasive Computing." vol. 780, P. Robinson, *et al.*, Eds., ed: Springer US, 2005, pp. 23-34.