ISSN No. 0976-5697

Volume 3, No. 3, May-June 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Security in Location Based Services: A Survey

Gaurav Gupta*
Assistant Professor in Computer Science,
Shoolini University, Solan, India
solan.gaurav@gmail.com

Deepika Goel Gupta
Faculty in Computer Science,
Green Hills Polytechnic College, Solan, India
deepikasolan.goel@gmail.com

Abstract — As the mobile networks are springing up, mobile devices have become a must gadget in our daily life. People can easily access Internet application services anytime and anywhere via the hand-carried mobile devices. Most of modern mobile devices are equipped with a GPS module, which can help get the real-time location of the mobile device. Location based services (LBS) aim at delivering point of need information. Personalization and customization of such services, based on the profiles of mobile users, would significantly increase the value of these services. The term Location Based Services (LBS) refers to mobile services in which the user location information is used in order to add value to the service as a whole. The user location information in that case consists of X-Y coordinates generated by any given Location Determination Technology **(LDT), such as Cell-ID, A-GPS, EOTD**, etc. Since profiles may include sensitive information of mobile users and moreover can help identify a person, customization is allowed only when the security and privacy policies dictated by them are respected. Systems which provide location based services have always been vulnerable to numerous privacy threats. The more we aim at safe usage of location based services, the more we feel the necessity of a secure location privacy system. In this paper I present the privacy and security issues, along with the threat of location cheating attacks, find the root cause of the vulnerability, and outline the possible defending mechanisms. Design and implementation of solution for these issues.

Keywords— LBS, GPS, EOTD, LDT, Cell-ID

I. INTRODUCTION

Given the recent advancement of mobile telecommunications technology and rapid diffusion of mobile devices, the importance of wired and wireless Internet services utilizing the past and present location information of users carrying mobile terminals with location tracking function is growing. LBS refer to value added services that detect the location of the users using location detection technology and related applications. LBS is expected to play an essential role in creating value-added that utilizes wire and wireless Internet applications and location information, since these are very useful in various fields.

The use of Location Based Services (LBS) has become ubiquitous with the growth of handheld devices, PDAs smart phones and GPS enabled cars. LBSs will flourish even more with the surge of new genre of information systems. While requesting for a location based service, a user can easily mask his identity using unlikable pseudonyms but he needs to provide his location information, even if with less precision. The location service provider (LSP) or an adversary, who secretly listens to the communication channel between a user and the LSP, builds his own chronological record of location data over the period of time.

There is a growing concern that such personal information are leaked for purposes other than what has been originally intended. Such concern is even more serious since location information on customers and possibility of tracking their movements can constitute a direct encroachment of other people's privacy by themselves. Hence, there is a growing need to conduct research on LBS security to prevent disclosure of personal information of individuals especially in the areas of authentication and security. Furthermore, an open LBS service infrastructure will extend the use of the LBS technology or services to business areas using web service technology. Therefore, differential resource access is a necessary operation for users to enable them to share their resources securely and willingly.

The goal of this paper is to investigate how well the most limited wireless devices can make use of LBS security services. This paper describes a novel security approach on fast LBS services. The objective of this paper is carry out a survey of the significance of security and privacy problems that are present in most existing mobile network systems. Because these systems have not been designed with security and privacy in mind, these issues are unsurprising. There are few main contributions in this paper, these are

a. There is identification of three classes of privacy and security problems associated with mobile social network systems:
   i. Direct anonymity issues,
   ii. Indirect or K-anonymity issues, and
   iii. Eavesdropping, spoofing, replay, wormhole and location cheating attacks.
b. In this paper I discus a novel authentication scheme which exploits volatile passwords –One-Time Passwords (OTPs) based on the time and location information of the mobile device to transparently and securely authenticate users while accessing Internet services, such as online banking services and e-commerce transactions. Compared to a permanent password base scheme, an OTP based one can prevent users from being eavesdropped. In addition to a memory less feature, the scheme restricts the validness of the OTP password not only in a certain time period but also in a tolerant geometric region to increase the security protection, and the identity server, to address the security and privacy problems

II. BACKGROUND AND RELATED WORK

In this section there is a short introduction of mobile social networking and the technologies that have made it possible.

A. Mobile Computing:

Smart phones now allow millions of people to be connected to the Internet all the time and support mature development environments for third-party application developers. This has put personal computing power in the pockets of users and at the same time, given them ubiquitous access to rich online social network information. In certain areas (such as college campuses) there are now high concentrations of active social network users with smart phones.

Recently there has been a dramatic rise in usage of smart phones, those phones capable of Internet access, wireless communication, and supporting development of third-party applications. This rise has been due largely to the iPhone and iPod Touch. In fact, according to Net Applications, Apple's handheld status symbol accounted for nearly two-thirds of all mobile web browsing traffic in April of 2009, almost eight times more than the nearest competitors. This is amazing considering that less than a year before this the iPhone was not even the leading platform for mobile web traffic.

B. Social Networks:

The growth of social networks has exploded over the last year. In particular, usage of Facebook has spread internationally and to users of a wide age range. According to Facebook.com's statistics page, the site has over 200 million active users of which over 100 million log on every day. To compare this with ComScore's global Internet usage statistics, this would imply that nearly 1 in 10 of all Internet users log on to Facebook every day and that the active Facebook Internet population is larger than any single country's Internet population (China is the largest with 179.7 million Internet users). Mobile users in particular are active Facebook users. According to Facebook statistics [3] (March 2009) there are currently over 30 million active mobile users of Facebook, and those users are almost 50% more active on Facebook than non-mobile users.

C. Privacy and Security:

Some previous Privacy research in both location-based services and social networks [4, 6, 7]. Previous work at Duke University has dealt with privacy and anonymity questions as they apply to sharing presence information with other users and matching

Users with a shared location and time. For instance, SmokeScreenpresents a protocol by which devices may broadcast identifiers that can be resolved to an identity through a trusted broker system. This identity could then be used to access personal information to drive third party applications.

III. SECURITY AND PRIVACY PROBLEMS

Peer-to-peer mobile social network systems and a mobile device in client-server mobile social network systems, such as Brightkite and Loopt, notify a centralized server about the current location of the device (available via GPS, cell-tower identification, or other mechanisms). By querying the server, mobile devices in these client-server systems can find nearby users, information about these nearby users, and other items of interest.

The following will discuss security and privacy problems associated with peer-to-peer and client-server mobile social network systems. Since there are differences between the peer-to-peer and client-server architectures.Table I summarizes the issues for each architecture.

Table 1 Summary Of Security And Privacy Issues For Peer-To-Peer And Client-Server Mobile Social Network Systems

Security and privacy issue	Applies to peer-to-peer systems	Applies to client-server systems
Direct anonymity	Yes	Yes
Indirect or K-anonymity	Yes	Yes
Eavesdropping, spoofing, replay, and wormhole attacks	Yes	No

A. Direct Anonymity Issues:

In a peer-to-peer context-aware mobile social network system such as Social Aware, we can track a user by logging the date and time that each mobile or stationary device detects the user's social network ID. By collecting such logs, we can construct a history of the locations that a user has visited and the times of each visit, compromising the user's privacy. Finally, given access to a user's social network ID, someone else could access that user's public information in a way that the user may not have intended by simply viewing that user's public profile on a social network Web site. Due to this process the clear text exchange of social networking IDs in systems such as WhozThat and Social Aware leads to unacceptable security and privacy risks, and allows the user's anonymity to be easily compromised. Such problems are directly compromise a user's anonymity direct anonymity attacks.

Direct anonymity attacks are also possible in client-server mobile social network systems. While users' social network

IDs are generally not directly exchanged between mobile devices in such systems, mobile or stationary devices can still track a user by logging the date and time that each device finds the user nearby. Since each device in these systems can find the social network user names and often full names of nearby users, the privacy of these users can be compromised. Thus, we have a direct anonymity issue - exposure of user names and locations in client-server systems allows the user's anonymity to be compromised.

B. The Indirect or K-Anonymity Problem:

Even if the user does not directly provide his/her identification information, the user's provided social network information (such as preferences) may be mapped back to the user's identity through the social network site or information cached within mobile and stationary devices in the environment. The indirect anonymity problem exists when a piece of information indirectly compromises a user's identity. An example of this is when a piece of information unique to a user is given out, such as a list of the user's favourite movies, this information might then be easily mapped back to the user. The K-anonymity problem occurs when n pieces of information or n sets of related information

can be used together to uniquely map back to a user's identity. Furthermore, if a set of information can only be mapped to a set of k or fewer sets of users, the user's anonymity is still compromised to a degree related to k. The challenge is to design an algorithm that can decide what information should and should not be given out in order to guarantee the anonymity of associated users. The abundance and diversity of social network information makes this privacy guarantee more complicated than it may initially appear. More formally, the particular problem is to find what personal information can be shared such that this information cannot be used to associate the user's identity with a specific context.

C. Eavesdropping, Spoofing, Replay, and Wormhole and location cheating Attacks:

Once a user's social network ID has been intercepted in a peer-to-peer mobile social network system, it can be used to mount a replay and spoofing attack. In a spoofing attack, a malicious user can masquerade as the user whose ID was intercepted (the compromised user) by simply sending (replaying) the intercepted ID to mobile or stationary devices that request the user's social network ID. Thus, the replay attack, where the compromised user's ID is maliciously repeated, is used to perform the spoofing attack. Another specific type of replay attack is known as a wormhole attack [13] where wireless transmissions are captured on one end of the network and replayed on another end of the network. In a system such as WhozThat or Social Aware [1], a malicious user could use a wormhole attack to capture a user's ID and masquerade as that user in a different, perhaps distant, location. Since these systems are vulnerable to such replay and spoofing attacks, we can no longer trust that each user who participates in these systems is really who they claim to be. Therefore, the value of such systems is substantially diminished. Furthermore, these attacks could be used for a variety of nefarious purposes. For example, a malicious user could masquerade as the compromised user at a specific time and place while committing a crime. Clearly, spoofing attacks in mobile social networking systems present serious security risks.

In addition to intercepting a user's social network ID via eavesdropping of the wireless network, a malicious user could eavesdrop on information transmitted when a device requests a user's social network profile information from a social network server.

Eavesdropping, spoofing, replay, and wormhole attacks are generally not major threats to client-server mobile social network systems. These attacks can be defended against with the appropriate use of a robust security protocol such as HTTPS, in conjunction with client authentication using user names and passwords or client certificates. If a user's social network login credentials (user name and password, or certificate) have not been stolen by a malicious user and the user has chosen an appropriately strong password, then it is nearly impossible for the malicious user to masquerade as that user.

a. Location cheating attack* [8]*: The objective of the attacks is to automatically check into as many businesses as possible and as frequently as possible to maximize benefits through location cheating. A more sophisticated attack is automated cheating. To make automated cheating easier, the cheaters may use venue profile analysis to identify victims, which can be the venues who provide discounts or users who aim to get mayor ship in specific venues.

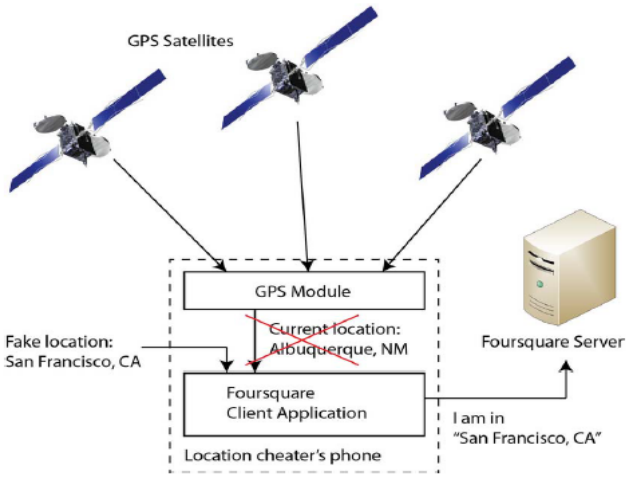

Figure 1 Illustration of location cheating.

IV. SECURITY AND PRIVACY SOLUTIONS

A. Anonymous IDs ,Identity Server and One Time Password:

For security and privacy of mobile network system various designed and implemented a system are there these are, the identity server, to address the security and privacy problems described previously and One-Time Passwords (OTPs) [5, 12] based on the time and location information of the mobile device to transparently and securely authenticate users while accessing Internet services, such as online banking services and e-commerce transactions. Compared to a permanent password base scheme, an OTP based one can prevent users from being eavesdropped**.** Mobile device has reasonably reliable Internet access through a wireless wide area network (WWAN) cell data connection or through a WiFi connection. Mobile devices that lack such an Internet connection will not be able to participate in system. Furthermore, we assume that each participating mobile device has a short-range wireless network interface, such as either Bluetooth or WiFi, for ad-hoc communication with nearby mobile and/or stationary devices.

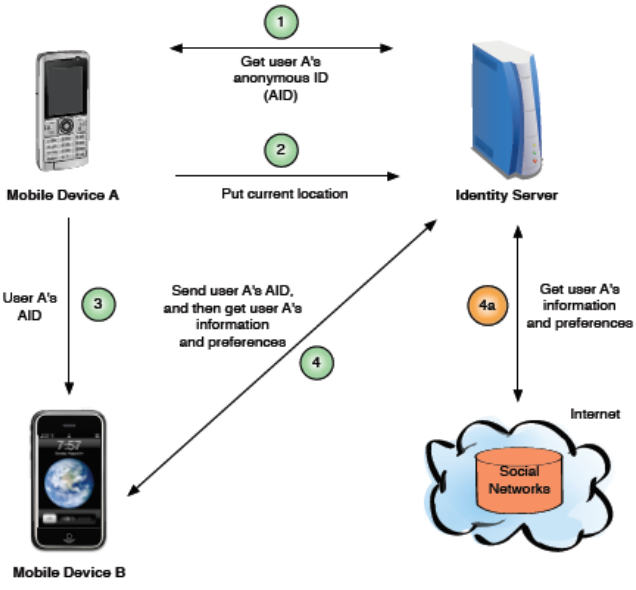

Figure 2 Anonymous IDs and the Identity Server.

Anonymous identifier or AID. The AID is a nonce that is generated by a trusted server, called the identity server (IS). Before a user's mobile device advertises the user's presence to other nearby mobile and stationary devices, it securely contacts the IS to obtain the AID. The IS generates a new AID for this mobile device using a cryptographic hash function such as SHA 1, with a random salt value. The IS associates the newly generated AID with the mobile device that requested the AID, and then returns the new AID to the mobile device. The user's mobile device then proceeds to share this AID with a nearby mobile and/or stationary device by launching a Bluetooth AID sharing service. After a near by mobile or stationary device (device B) discovers this AID sharing service on the user's mobile device (device A), device B establishes a connection to the user's mobile device to obtain the shared AID. After the AID has been obtained by device B, device A requests another AID from the IS. This new AID will be shared with the next mobile or stationary device that connects to the AID sharing service on device A. After the device B obtains the shared AID from device A, device B then proceeds to query the IS for the social network profile information for the user that is associated with this AID. Figure 2 shows the role of the IS in generating AIDs and processing requests for a user's social network information. Once the social network information for an AID has been retrieved by the IS, the IS removes this AID from the list of AIDs associated with the mobile user. Before the user's mobile device next advertises the user's presence using the Bluetooth AID sharing service, it will obtain a new AID from the IS as described above.

B. Eavesdropping, Spoofing, Replay, and Wormhole Attacks:

Our security and privacy solutions provide several security features that address the security threats. The use of AIDs prevents spoofing and replay attacks. Since AIDs, instead of social network IDs (such as Facebook IDs) [2, 3], are shared by the mobile device, a malicious user cannot spoof the social network identity of another user. By using a cryptographic hash function with a random salt value to generate AIDs for each mobile user, and continuously generating new AIDs upon request as AIDs timeout or are consumed by other devices, we prevent replay attacks whereby a malicious user may attempt to capture and reuse a sequence of AID values previously shared by a mobile device. Using OTP the security improvement are shown in the following table II

Table 2

Protocol	KERBEROS	S/KEY OTP	Our Protocol
Replay Attack	√	√	√
Eavesdropping Attack	⌂	√	√
Dictionary Attack	×	√	√
Brute Force Attack	×	⌂	√
Man – in – the – Middle Attack	×	×	√
User Impersonation Attack	⌂	√	√
# Notation: √ Satisfied ⌂ Partially Satisfied × Not Satisfied			

V. RELATED WORK ON SECURITY AND PRIVACY

As the technology of GPS grows mature, many location-based encryption schemes have been proposed recently. D. E. Denning's "Geo-encryption" takes advantage of GPS technology to conduct GPS-based encryption that integrates the location and time into the process. The decryption is processed in a limited area as well as time. Hsien- Chou Liao's location-dependent data encryption algorithm (LDEA) incorporates a latitude/longitude coordinate with a random key to encrypt data [9]. The encrypted message can only be decrypted when the receiver is in the region centred by the target coordinate within a Toleration Distance (TD).

About the location prediction, an algorithm based on mobility characteristic can effectively predict the future location of a mobile node in an ad hoc network where nodes use directional antennas to communicate with each other. Son, Helmy and Krishnamachari [14] identify two problems about location errors, the lost link (LLNK) problem and the loop in packet delivery (LOOP) problem. And then they propose two mobility prediction schemes to mitigate these problems. Neighbour Location Prediction (NLP) can solve LLNK and Destination Location Prediction (DLP) can solve the LOOP respectively.

In the study about the location-based authentication, Jarusombat and Kittitornkun propose a Geo-encryption scheme to generate Digital Signature [10, 11]. In this model, a sign server is used to assist the mobile device in creating a digital signature and receive mobility parameters from mobile devices. It provides authentication, data integrity and non-repudiation services. The author identifies two aspects ─ location-based key distribution and run-time location verification ─ to improve the network access control and proposes Location-Enforced Network Access (LENA) which eliminates the dependence on expensive hardware devices in order to locate the mobile devices. Authors propose a comprehensive definition of location authentication, a review of its threats and possible solutions to help provide a better understanding of this young security requirement.

VI. CONCLUSIONS

Even though mobile applications are all the rage, the security issue is still a major concern for most of users. In this survey I identified several important privacy and security issues associated with mobile network systems, along different security and privacy issues. This survey support anonymous exchange of social network information with real-world location-based systems, enabling context-aware systems that do not compromise users' security and privacy.

VII. REFERENCES

[1] Beach, M. Gartrell, S. Akkala, J. Elston, J. Kelley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan, B. Surendar, M. Terada, and R. Han, "Whozthat? evolving an ecosystem for context-aware mobile social networks," IEEE Network, vol. 22, no. 4, pp. 50–55, July-August 2008.

[2] N. Eagle and A. Pentland, "Social serendipity: Mobilizing social software," IEEE Pervasive Computing, vol. 4, no. 2, April-June 2005.

[3] "Mobile browsing by platform market share," http://marketshare.hitslink.com/mobile phones.aspx? qprid=55&sample=31.

[4] Aaron Beach, Mike Gartrell, and Richard Han "Solutions to Security and Privacy Issues in Mobile Social Networking" 2009 International Conference on Computational Science and Engineering

[5] "One Time Password" http://us.zyxel.com/

[6] Chowdhury S. Hasan, Sheikh I. Ahamed and Mohammad Tanviruzzaman MSCS Department, Marquette University Milwaukee, WI, USA," A Privacy Enhancing Approach for Identity Inference Protection in Location-Based Services" 2009 33rd Annual IEEE International Computer Software and Applications Conference

[7] Lingyan Wang Computer Science and Software Engineering Department Auburn University Shelby Center for Engineering Technology, Suite 3101 Auburn University, AL, 36849-5347, USA," Protecting Location Privacy through Identity Diffusion"

[8] Wenbo He, Electrical Engineering Department University of Nebraska-Lincoln Email: wenbohe@engr.unl.edu , Xue Liu School of Computer Science McGill University Email: xueliu@cs.mcgill.ca , Mai Ren Computer Science and Engineering University of Nebraska-Lincoln Email: mren@cse.unl.edu," Location Cheating: A Security Challenge to Location-based Social Network Services"2011 31st International Conference on Distributed Computing Systems

[9] Hsien-Chou Liao, Yun-Hsiang Chao, "A New Data Encryption Algorithm Based on the Location of Mobile Users," Information Technology Journal, Vol. 7, Issue 1, pp. 63-69, 2008.

[10] Jarusombat, SantiKittitornkun, Surin, "Digital Signature on Mobile Devices based on Location," International Symposium on Communications and Information Technologies, pp. 866-870, 2006.

[11] LichunBao, "Location Authentication Methods for Wireless Network Access Control," Performance, Computing and Communications Conference, pp. 160-167, 2008.

[12] Wen-Bin Hsieh Department of Electronic Engineering National Taiwan University of Science and Technology Taipei, Taiwand9802106@mail.ntust.edu.tw, Jenq-ShiouLeu Department of Electronic Engineering National Taiwan University of Science and Technology Taipei, Taiwanjsleu@mail.ntust.edu.tw," Design of a Time and Location Based One-Time Password Authentication Scheme"

[13] R. Maheshwari, J. Gao, and S. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in 26th IEEE Conference on Computer Communications (INFOCOM 2007), May 2007.

[14] D. Son, A. Helmy, B. Krishnamachari, "The Effect of Mobility-induced Location Errors on Geographic Routing in Ad Hoc and Sensor Networks: Analysis and Improvement using Mobility Prediction," IEEE Transactions on Mobile Computing, Vol. 3, Issue 3, pp. 233-245, July2004.