ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Location Based Mobile Secure Social Networks

Roshan Sanu. Y[1], S. Uma Rani[2]

Department of Information Technology, Maharaja Engineering College, Avinashi, Tamilnadu, India[1]

Asst. prof, Department of Information Technology, Maharaja Engineering College, Avinashi, Tamilnadu, India[2]

Abstract: Location based systems allows users to share their location as soon as a link is established between the users. The system is a mobile social network developed on the android platform. The system enables high security and privacy for the users of the mobile network. The system uses advanced cryptographic methods to ensure the authenticity of users. Unlike the traditional social networking systems, the location based system uses a combination of public – private key cryptography which ensures maximum security and privacy. The location sharing mechanism is also enabled in the system with the help of GPS in the mobile phones. The system provides security that is relying on the user's wish. The location-based chat function in the system helps users to ensure that their friends and relatives are easily accessible within their circle. The security mechanism also prevents unauthorized access to chat even if hackers hack the username and password.

Keywords: Social networks, Privacy, Location sharing.

I. INTRODUCTION

Mobile social networking is social networking where individuals with similar interests converse and connect with one another through their mobile phone and/or tablet. Much like web-based social networking, mobile social networking occurs in virtual communities. A current trend for social networking websites, such as Facebook, is to create mobile apps to give their users instant and real-time access from their device. In turn, native mobile social networks have been created like Foursquare, Instagram, and Path, communities which are built around mobile functionality. More and more, the line between mobile and web is being blurred as mobile apps use existing social networks to create native communities and promote discovery, and web-based social networks take advantage of mobile features and accessibility. Mobile and web-based social networking systems often work symbiotically to spread content, increase accessibility and connect users from wherever they are. The evolution of social networking on mobile networks started in 1999 with basic chatting and texting services. With the introduction of various technologies in mobile networks, social networking has reached to an advance level over four generations.

First generation began in 1999 or early 2000. Technologies used in this generation are application based, pre-installed on mobile handsets. Features such as text only chat via chat rooms. Second generation began in 2004 through 2006. Introduction of 3G and camera phones added many features such as uploading photos, mobile search for person based on profile, contact / flirt with person anonymously etc. The services of this generation mobile social networks can be used by pay as you go or subscription to service.

The experiments for third generation mobile social networks started in 2006. The features include richer user experience, automatic publishing to web profile and status updates, some web 2.0 features, search by group / join by interests, alerts, location based services content sharing especially music etc.. Regional distributions of this generation of mobile social networks include Japan, Korea, Western Europe, and North America. Advertising and ad supported content become increasingly important. The services in this generation can be used by plans such as pay as you go; subscription based still popular networks gain scale to become content distribution platform.

Fourth generation began in 2008 and reached in 2010. All the features in third generation are advanced in this generation of social mobile networks. The features of this generation include the features of third generation, ability to hide/ mask presence, asynchronous video conversation, multi point audio chat conversation with one button, multiplayer mobile gaming etc. Technologies which made these features possible are web 2.0 widgets, Flash lite, open source, open handset alliance.

II. RELATED WORK

Abedelaziz Mohaien, Denis Foo Kune: Suggested encounter-based social networks would provide a computing infrastructure to allow for creation of varied services such as a “missed connections” virtual bulletin board, on-the-fly introductions (business card exchange), or real-time in-person key distribution to bootstrap secure communication in other systems. Although at first glance encounter-based systems appear very similar to existing social networks, they present a dramatically different set of challenges, not the least of which are security and privacy of users and authenticity of the other party in a conversation. Guarantees that are trivial in traditional social networks, such as authenticity (ensuring one is communicating with the desired person), become open problems in encounter-based networks. Since people do not automatically place their trust in others simply based on presence in the same location, it is also desirable to reveal the minimum amount of information required for future secure communication. Sharing detailed personal information is not the primary goal of encounter-based networks, but can of course be easily implemented if both users agree upon the successful verified encounter. This considers fundamental requirements for encounter-based social networks. In addition to basic functionality like high availability, scalability, and robustness to failure, these systems should provide several security guarantees, including privacy in the form of unlink ability of users sharing an encounter, confidentiality of data exchanged among encounter participants, and authentication of both users in a two-party conversation.

Alexandra-Mihaela Siriteanu, Adrian Iftene: Suggested a system that illustrates the social nature of a human being – the need to be always in touch with family and friends – taking into account facilities available on Android platform. The role of this application is to create a social network in which the users are being alerted when their friends are around. This gives them the possibility to set up a meeting or to avoid one. The users have the possibility to check in some locations and allow their friends to follow their activity. Taking into account the security of the users, the facilities of the application an option which allows close friends or family to check the user’s location based on a keyword text message. For this purpose, available Android location and messages services are used for finding an approximate location of a mobile phone running this program and then sharing it through MeetYou or via SMS. Information is being displayed using default components provided by Android platform and also more complex elements including heterogeneous lists CWAC, Google Maps and augmented reality using Mixare Library. Human need for socialization had been brought to light since ancient times, when Aristotle said: “Man is by nature a social animal” (Aristotle, Politics I), by this he meant to emphasize the fact that human being is destined to live in peers within organized community. As there is no society without communication, so there is no person without social interaction. Over time, forms of communication and understanding about this process have been expanded based on technology progress.

Earl Oliver, Jason LeBrun: Suggested a novel mobile social networking middleware named MobiClique. MobiClique forms and exploits ad hoc social networks to disseminate content using a store-carry-forward technique. The approach distinguishes itself from other mobile social software by removing the need for a central server to conduct exchanges, by leveraging existing social networks to bootstrap the system, and by taking advantage of the social network overlay to disseminate content. An open API to encourage third-party application development is proposed. The system architecture and three example applications are designed. Then it shows experimentally that MobiClique successfully builds and maintains an ad hoc social network leveraging contact opportunities between friends and people sharing interests for content exchanges. The experience also provides insight into some of the key challenges and short-comings that researchers face when designing and deploying similar systems. Applications in the virtual world such as online social networks and instant messaging have done much to remove the tyranny of geography. Beyond friendship and exchanges between two parties (which is referred to as dyadic communication), virtual groups have proliferated creating communities centered on interests varying from gaming to editing Wikipedia pages. Despite the increased power and reach of virtual communities, postulate says that the power of physical communities based on physical contact and closeness will continue to be an essential part of human relationships.

Charles M. Gartrell: Suggested, a system for answering the basic social question of Who's that?. WhozThat ties together online social networks with mobile smartphones, and provides an infrastructure for building a new class of context-aware applications that leverage social network information. Social networks provide access to an extensive collection of personal information about users, including name, gender, contact information, interests, music preferences, movie preferences, book preferences, and friendship connections with others, which represent but a few of the fields that users populate on their social network profiles. Once a computationally-enabled environment knows personal contextual information about its users, it can take a number of actions in response to this information. One class of such actions involves tailoring multimedia, such as music and video, for local presentation to one or more co-located users based on the preferences of those users. SocialAware is a framework for building social-networking-enabled context-aware services. To demonstrate the feasibility of this framework, prototypes of two context-aware multimedia presentation applications have been implemented. The first application, called SocialAwareTunes, plays music that reflects the preferences of one or more users residing in a common physical space such as a bar or restaurant. The second application, called SocialAwareFlicks, displays recommended movie trailers that match the movie preferences of one or more users jointly watching a common display. SocialAwareFlicks could be deployed in locations such as video-rental establishments for marketing purposes, to make customers aware of new video rentals that match their interests.

III. ANDRIOD OS

Android is an open source and Linux-based Operating System for mobile devices such as smartphones and tablet computers. Android was developed by the Open Handset Alliance, led by Google, and other companies. Android offers a unified approach to application development for mobile devices which means developers need only develop for Android, and their applications should be able to run on different devices powered by Android. The first beta version of the Android Software Development Kit (SDK) was released by Google in 2007. The source code for Android is available under free and open source software licenses. Google publishes most of the code under the Apache License version 2.0 and the rest, Linux kernel changes, under the GNU General Public License version 2.

IV. FUNCTIONAL COMPONENTS

The functional design of a typical encounter-based social network consists of three major components located at three different architectural layers: user layer, plug-in layer, and "cloud." The term cloud may refer to a storage location of the encounters and private messages (e.g. a central rendezvous server or distributed "mini-servers") which is used by different encounter parties in the post-encounter phase. However, the design can be quite flexible, allowing storage components to be dynamically chosen using a plug-in architecture: the system may support centralized servers, distributed hash tables, or even Tor hidden services. Notice that each of the different layers provides functionalities used to realize one or more functional or security requirement among these. Furthermore, to establish a balance between the functional and security requirements, there are two specific designs as follows:

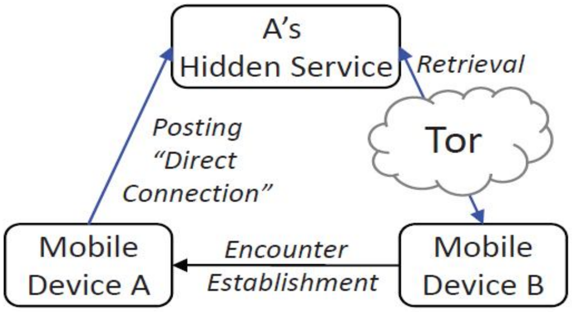

Fig 5.1 Hidden Service Design

A hidden service needs to advertise its existence in the Tor network before clients will be able to contact it. Therefore, the service randomly picks some relays, builds circuits to them, and asks them to act as introduction points by telling them its public key. By using a full Tor circuit, it's hard for anyone to associate an introduction point with the hidden server's IP address. While the introduction points and others are told the hidden service's identity (public key), there is no need to learn about the hidden server's location (IP address).

Tor makes it possible for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server. Using Tor "rendezvous points," other Tor users can connect to these hidden services, each without knowing the other's network identity.

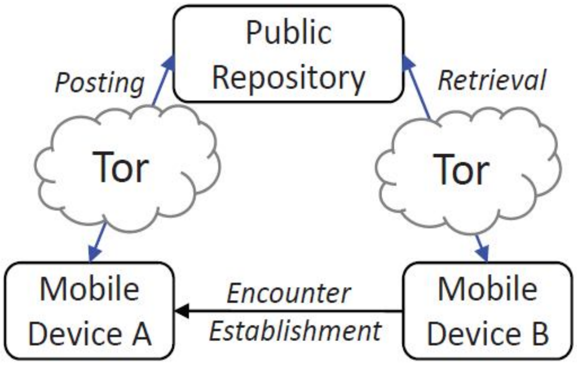

Fig 5.2 Repository Based Design

4.1 NEED FOR STRONG AUTHENTICATION

Unauthenticated key agreement during the encounter is vulnerable to a man-in-the-middle attack. Given that the parties involved in the encounter are already aware of each other visually, the only way to avoid this vulnerability is to enforce a visual authentication scheme where users can recognize that they are communicating with the desired party simply by looking at a picture of that user.

In other settings such as a professional conference, a company logo and other information, this could be viewed as a reduced digital version of a business card (though, in many cases, the same scenario of using a personal photo on a personal business card still applies). To provide user authentication, we assume each user to have a digital certificate signed by a trusted authority with sufficient information to identify users, including a photo of the user. The signing authority's public key would be known to all other nodes that use this social network. It is not far-fetched to assume that future authentication tokens such as passports and driver licenses will be issued digitally. Since cryptographic signatures make them more secure against malicious tampering than their physical counterparts. Though, we do not use such certificate but a limited one. With that assumption, a user of a location-based system broadcasts a certificate with his or her picture and public key which is received by other people in the encounter space including the intended destination. Such information is then used for reconnection according to one of the design options.

The facial recognition algorithms exist, which might reduce the privacy of the user, when an attacker collects photos from certificates being exchanged and compare them to photos associated with names and obtained from other sources such as other online social networks. Although these attacks are computationally expensive, one may argue that the use of cheap cloud services may make these attacks very feasible. This concern is answered by pointing out three issues. First, even when using such cloud service, the attack, unless targeted towards a particular user, would be infeasible with a substantial cost that the attacker has to pay in order to breach the privacy of users who use the system.

Second, the attacker does not need to collect broadcast certificates in order to apply the attack, but may simply take pictures of the encounter space and achieve a similar result to prove the presence of an individual at a certain place at a certain time. Finally, all prior work of facial recognition depends greatly on features extracted from original photos, but not from cartoon versions of them, which could be used to remedy the privacy breach associated with using a photo for visual authentication. The user study considers cartoon version of photos instead of the original photos indeed hints on improved usability of the design.

V. EXPERIMENTAL RESULTS

The application relies on the key distribution among the users in order to perform the networking functionalities apart from their passwords. This mechanism ensures maximum security. The location sharing features establishes a confidence among the users in the sense that they can make their friends and relatives know their exact locations as the current social scenarios suggests. The users can travel according to their wish and can share their location with their guardians and parents such that they become aware of the user's geographical location.

Key distribution was a challenging problem in the context of distributed computing systems. One obstacle for key distribution is the fact that it is hard to make an authority always online to take care of the distribution of keys, as well as the scalability issue of key distribution for larger networks. The proposed design can be utilized for key distribution, and can be used as a plug-and-play service for this purpose. There are two classes of users, trusted and untrusted users, and both are used for different purposes and differ in the way they get keys based on their function. While the trusted users get their keys from those who trust them directly in an offline fashion, untrusted users get their keys from a key distribution center, which should be online all the time. Using our design, one may distribute keys to untrusted users based on activity shared with them—such as an encounter. One even may consider the scenario of establishing trust based on the encounters. Other key distribution applications that may benefit from our design include storage services, file-sharing, etc.

VI. CONCLUSION

In this paper, we notice that the first party—referred to as the encounter source—uses a broadcast communication channel that makes the second party of the encounter—which is referred to as the encounter destination—unlinkable to the source.

Since encounter information is deposited on the central server by the destination and is based on the source's information, this information might be used to breach the privacy of users — any entity may check the source's mailbox to see if there is a message. This is a necessary piece of information, and a potential attacker might learn it from several other sources, apart from this application. The goal is to ensure that we are indeed sending messages to the appropriate party. The design assumes the availability of smart phones for users and their willingness to use their phones to participate in the network.

REFERENCES

[1] A. Acquisti, R. Gross, and F. Stutzman, "Faces of facebook: Privacy in the age of augmented reality," in BlackHat, 2011.

[2] J. Manweiler, R. Scudellari, and L. P. Cox, "SMILE: encounter-based trust for mobile social services," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 246–255.

[3]A. 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, 2008.

[4] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer, A. Perrig, B.-Y. Yang, and T.-C. Wu, "GAnGS: gather, authenticate 'n group securely," in MOBICOM, 2008, pp. 92–103.

[5] R. J. Clark, E. Zasoski, J. Olson, M. H. Ammar, and E. W. Zegura, "D-book: a mobile social networking application for delay tolerant networks," in Challenged Networks, 2008, pp. 113–116.

[6] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (IETF RFC 5280)," Internet Engineering Task Force, Request For Comments, 2008.

[7] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The secondgeneration onion router," in Proceedings of the USENIX Security Symposium, 2004.

[8] N. Eagle and A. Pentland, "Social serendipity: Mobilizing social software," IEEE Pervasive Computing, vol. 4, no. 2, pp. 28–34, 2005.