Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.508 – 512

RESEARCH ARTICLE

Design of Encounter-Based Social Network in Mobile Application

S.Niranjani[1], A.Rathna[2]

[1]PG Student, M.E Computer and Communication & Anna University
[2]Assistant Professor, Electronics and Communication &Anna University
Ganadipathy Tulsi's Jain Engineering College, Vellore, TamilNadu
[1] nniran@gmail.com; [2] hrathna201@gmail.com

Abstract— ***The mobile social networks are likely to a large extent enhance interaction with mobile users and shared the information in encounter-based social network. In this encounter traditional social network as opposed users abuse the information's. So this new approach challenges network basically different by previous social network designs. In this paper, we propose design for encounter-based mobile social network using security for location and encounter privacy. Here also we explore different requirements for these new systems. We present a system by which devices who shared a physical location and time can be matched by a central server. To highlight of these challenges network it was designed for specifically secure centralized server. Centralized servers cannot always be relied upon to protect data confidentially. So we describes the design of SMILE, is secure for a privacy-protection "missed-connections" service for mobile users. It also provides services using mobile devices without relying on trusted coordinating server. Here SMILE design using key exchange protocols. We develop cryptography hash technique for protect the information through the mobile application. This paper presents a design of secure encounter-based social network by implementing in android application called MeetUp.***

Keywords— Social networks; Location-based services; Privacy

I. Introduction

In Mobile social networks (MSNs) are increased social networking platforms over which one or more person are able to communicate with one another using handheld wireless Communication mobile devices such as laptops, PDAs, and cellular phones, have been widely used. In the last decade, the number of users of online social networking sites and of mobile phone services has skyrocketed. For example, the most popular online social networking site, Face book, MySpace Google+2 and Twitter social life by facilitating interaction with old friends, sharing of events, distribution of data and various other aspects of social life. Face book has more than 500 million active users, and more than 50% of its active users log on to Face book at least once per day. Mobile social networking brings these two fast-growing phone services, there were 4.1billion mobile cellular subscribers in total in March 2009[3]. Mobile based social networks like GyPSii, Brightkite, Loopt provide some exclusive features like short messaging notification, maps and location based services etc On social networking sites, other than communicating with existing friends, person can find and make friends with other user who have similar interests, are from the same school or company, work colleagues, family members etc. mobile social networks are most popular websites are transforming into mobile domain. It also used application and games provide the mobile users. While mobile social networks hold great promise for enabling many exciting new applications, they also create serious privacy and security concerns. There have appeared many of such applications provided limited versions of their services on mobile phones. Users of these mobile social network sites interested in accessing the social networking applications can use their mobile devices while on the sites (the servers) are treated as a central authority with which the user can trust.

In these conservative networks support only a subset of social networking: persons will only be able to found a relationship in the social network if they know of, or are introduced to each other. On the other, in an encounter based social network, the only requirement for establishing a connection is to be in the same position at the same point in time similar to conspicuous up a conversation at an open place. Encounter-based social networks would provide computing communications to allow for creation of varied services such as a "missed connections" (business card exchange), or real-time in-person key distribution to secure communication in other systems.

The existing encounter-based mobile social network systems pay little heed to the security and privacy concerns revealing one's personal social networking preferences and friendship information to the everywhere computing environment. In particular, in mobile social networks, the mobile users may face the risk of leaking of their personal information and their location privacy. Security guarantees that are slight secure in encounter existing system. In this no security terms involved in encounter based social networks. Here authentication users connect encryption and decryption so only abuse personal data [1]. In this paper we consider basic requirements for encounter-based social networks in addition to basic functionality like high availability, scalability, privacy security. We propose specific design architecture for encounter-based social network. In this architecture suggest two possible implementation, each conspicuous a balance between performance and security. To highlights of challenges it was designed for specifically secure centralized server. We also described SMILE design of secure centralized services provides missed connection for strong location and encounter privacy. Design shows the benefits and tradeoffs offs of specific security

II. REQUIREMENTS AND ANALYSIS

We have used some of the specific desired security features of encounter based social networks design. We look at some requirements for secure encounter based networks. We proposed the design of SMILE. The design involves basic principles used in security and functional requirements are authentication, availability, scalability, confidentiality. Our involvement in this work is as follows,

- By first outlining security and functional requirements that are ideally desired for encounter-based social network in security and privacy.
- We examine SMILE, design of secure encounter-based social network, and meet these requirements, showing that it is vulnerable to many attacks.
- We proposed a new design for secure encounter based social networks.
- We show the practicability of our designs by implementing a proof-of-concept system including an android application called MeetUp. Here also its performance in real world settings using mobile devices.

.

III. OVERVIEW OF SMILE

SMILE enlarges ideas from and uses cryptographic construction to found trust between persons who shared an encounter. We verified design for encounter-based social network showing attacks such as impersonation, privacy breaching, and users' collusion for protect this attacks in network. SMILE try to allow users equipped with mobile devices to build such trust relationships while protection their privacy against potential attackers [2]. In SMILE, users who want to communicate with each other must prove that an encounter occurred. To do this, an attracted person generates and passively broadcasts the "encounter key" to others within his communication range, and posts a hash of the encounter key, along with a message encrypted using the encounter key, to a centralized server. Other users in SMILE with the same encounter key may claim the encounter by simply looking up the hash of the key, which is used for indexing the encrypted message at the centralized server. Only the user with the correct key will be able to decrypt the message left by the first encounter party at the server.

This paper describe SMILE, a mobile social service in which trust is recognized only on the basis of shared encounters the service provider is not trusted to access users location information and assume no pre-established trust relationships among users of the service is the notion of an encounter, which is defined as a short period of co location between people. The benefit of our approach is that it provides a specific view of design. An encounter is defined as two users being in close physical nearness to each other for a period of time. The analysis providing a privacy protection missed- connections service with strong location-privacy and encounter-privacy guarantees. Based on this analysis, we have found that SMILE provides users with both location and encounter privacy from adversarial service providers and peers, and that our passive key-exchange protocol is practicability using a widely-deployed, range wireless technology, such as Wi-Fi.

We present the design of SMILE, Secure Missed connections through Logged Encounters. SMILE aim to secure, centralized missed-connections service using mobile devices [6]. The basic framework of SMILE's messaging procedure is as follows: (1) mobile users passively exchange cryptographic keys with nearby peers; (2) users periodically upload lot of key hashes to a central, matching server; (3) a user sends a message to the server encrypted with one such key and identify it with the related key hash; (4) the server frontward the encrypted message to all users that have transfer the same key hash; (5) only encounter members are able to decrypt the message. SMILE offers protection against malicious agents endeavour to determine or reveal a user's location history, encounter history, or private messages.

IV. DESIG OF ENCOUNTER-BASED SOCIAL NETWORKS

We design new specific encounter-based social networks that greatly differ from pervious social networks design. Here also discuss two generic designs for different benefits and tradeoffs [1]. The functional design of a usual encounter-based social network consists of three major mechanism located at three different architectural layers, shown in Fig. 1: the user layer, the plug-in layer, and the "cloud." The encounter refer to a storage location of the encounters and private messages (e.g. a central rendezvous/meeting point server or distributed) which is used by different encounter people in the post-encounter point. However, the design can be somewhat flexible, allowing storage mechanism to be with passion chosen using a plug-in architecture: the support centralized servers, distributed hash tables [13] or even Tor hidden service [7].

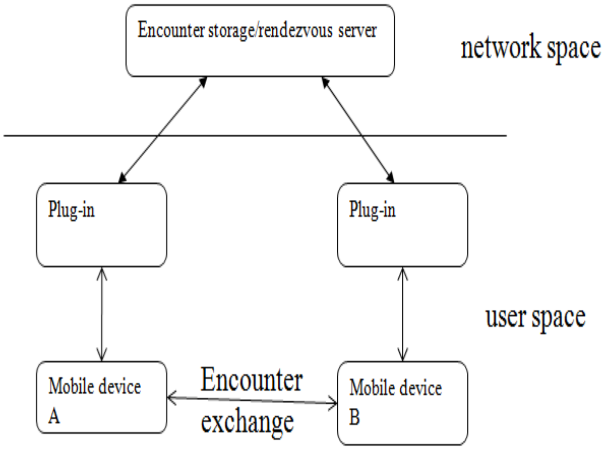

Fig 1: Architecture for encounter-based social networks

Simple unauthenticated key contract during the encounter is vulnerable to a MitM attack. In that the peoples involved in the encounter are already awake of each other visually, the only way to avoid this vulnerability is to enforce a visual authentication scheme where users can identify that they are communicating with the desired people simply by looking at a photo of that user. Digital certificate signed by a trusted power with sufficient information to identify users, including a photo of the user. Since cryptographic signatures make them more secure against malicious alter than their physical counterparts. Our certification and visual authentication schemes are very simple. First, a user Alice generates a pair of public and secret keys (PK, SK), computes the hash value of her own image and other applicable information, including a Tor hidden service URI, which is a unique identifier that is used later by Bob to communicate with Alice over Tor hidden service.

V. IMPLEMENTATION

We implemented the system on the Android platform and tested it on multiple devices under ideal conditions, as well as conditions that users are likely to encounter in urban settings.

Google has collected an enormous catalog of words derived from the regular entries in the Google search engines. The record contains more than 230 billion words. If we utilize this type of speech identifier, it is likely that our voice is stored on Google servers. This circumstance stipulates constant increase of information used for training, improving accuracy of the technique. The working of speech recognition systems is usually estimated in terms of accuracy and speed. Speech is deformed by contextual sound and reverberation. Both aural modelling and speech modelling are essential parts of current mathematical based speech recognition procedures. Hidden Markov models (HMMs) are extensively used in many systems.

A. Implementing Wireless Communication

Inter-device communication was applied using Bluetooth. The limited range of Bluetooth devices ensures that users are within close physical nearness to exchange certificates. So only our design executed in Wi-Fi this makes it more likely that users are within visual range and can identify each other [5]. For the delayed key exchange, that has been seen before when we present multiple devices that have been observed previously, along with photos related to the vendors. We connected a laptop to the local Wi-Fi network at our chosen location and listened for to ensure that we were limited to the target location, area coverage 5000m. We had a user with a known device name connect to the same network, but at different location, and verified to exchange data in encounter-based social network.

B. Effective Range

Our trial indicates that under those conditions, the devices can find out each other and exchange information at a range up to 24 meters. Transfer times improved as we increased the distance between the two devices, but all were faster than 400ms.We calculate the time required to transfer 20KB of data over our Bluetooth channel from a user holding a device in a particular manner. Measurements were taken at 45◦ increment by a request device moving around a responding device. The test was repeated for radii of 1, 2, 3 and 4 meters around the responding device.

C. Key Distribution

We visualize SMILE running on mobile phones and laptops. Thus, compatibility with currently-deployed technology is a mobile social network. Fortunately, convenient-available wireless communication platforms can be used for key distribution. Wi-Fi (802.11) is another widely-available option. Wi-Fi's relatively larger range, and increased ability to go through walls, provides a type of co-location security. SMILE trusted on cryptography only to prove that an encounter occurred with any co-located peer. The problem becomes simpler if we assume that nearby members associate to the same Wi-Fi access point, in which case broadcast packets can be used slightly. The primary drawbacks of this approach are the high power draw of 802.11-beacon scanning and the loss of Internet connectivity over Wi-Fi. Advanced techniques exist for establishing a shared key over a wireless channel. Using Bluetooth as a key-distribution mechanism prevents SMILE from detecting extremely brief encounters because of its relatively slow service-scan speed (_30s). As a result, clients will record at most two entries per minute, per encounter. Only a malicious server colluding with a user in the encounter space would be able to extract any information from the rendezvous key the server acting alone gets no useful information.

D. Visual Authentication schemas

Certificates signed by the right include hashes of photos and Tor hidden service URI unique to the user. The file containing the certificate, the photo, the hidden service URI, and the signature are the deployed to each device in the system. The credential name authority is responsible for confirm that only one instance of such files arrange per user We note that 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 services may make these attacks very visual authentication scheme where users can identify that they are communicating with the desired user 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 name by a trusted authority with sufficient information to identify users, including a photo of the user. Since cryptographic signatures make them more secure against malicious alert than their physical matching part.

E. Measurements in urban settings

We tested MeetUp in a densely-populated urban setting, in a bus station populated by students equipped with mobile phones, with this being as the only difference from the range and obstacles experiments above. The data collected from this experiment used in android phone. Only two users members We observe that it takes less than a second in all cases to do the encounter, and at average it takes approximately 600ms.

F. Tor Hidden Service

We present Tor, a circuit-based low-latency secret communication design for location-hidden services via rendezvous point's service [7]. Each user's runs local software specific called an onion proxy (OP) to fetch directories, establish circuits across the network, and handle connections from user applications. These onion proxies accept TCP streams and multiple across the circuits. Location-hidden services allow Bob to offer a TCP service, We transferred a 40KB data bundle that only the planned recipient will be able to decrypt such as a web server, without revealing his IP address. The timings tend to be very consistent per circuit but very different between circuits (ranging from 1.5 to about 8.5 seconds). Tor hidden service does not increase the attack surface, but rather hides the users' additional network information, such as IP address, while enabling the rendezvous in a decentralized fashion.

VI. CONCLUSION

In this paper, we have showed a design for secure encounter-based social networks to fulfil security guarantees. We design network using more fulfil requirements and introduce a specific structure for constructing encounter-based social networks. We than use our design several security and functional requirements for these mobile devices such as availability, privacy, security, integrity, scalability. Based on our proposed design for encounter-based social networks and also describe a SMILE design providing with strong location and encounter privacy security guarantees in the social network. In our design using key exchange protocols and implementing in mobile. Our result shows that feasibility of secure social network through android application. These design supports in android smartphones are protecting personal information exchange through users.

REFERENCES

[1] Abedelaziz Mohaien, Denis Foo Kune, Eugene Y. Vasserman, Myungsun Kim, Yongdae Kim, "Secure Encounter-Based Mobile Social Networks: Requirements, Designs, and Tradeoffs," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 6, pp. 380-393, Nov.-Dec. 2013, doi:10.1109/TDSC.2013.19

[2] J. Manweiler, R. Scudellari, and L. P. Cox "SMILE: Encounter-based Trust for mobile social services In E.A1shaer S.Jha editors ACM conference on computer and communication security pages 246-255 ACM 2009.

[3] J. Clark, E. Zasoski, J. Olson, M. H. Ammar, and E. W. Zegura Dbook: A Mobile social networking application for delay tolerant networks. In Challenged Networks, pages 113–116, 2008.

[4] CMS Wire. Android dominates burgeoning us Smartphone market. http://goo.gl/WZ4tZ, August 2012.

[5] A. Acquisti, R. Gross, and F. Stutzman. Faces of facebook: Privacy in the age of augmented reality. In *BlackHat*, 2011," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys 08), PP.239-252, 2008.

[6] Miroslav kneˇzevi'c Dbook: Efficient Hardware Implementa Cryptographic Primitives March 2011.

[7] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second generation onion router. In *Proceedings of the USENIX* Security Symposium, 2004.

[8] M. Farb, M. Burman, G. Chandok, J. McCune, and A. Perrig. Safeslinger: An easy-to-use and secure approach for human Trust establishment. Technical Report CMU-CyLab-11-021,Carnegie Mello University, 2011.

[9] P. Hancock, A. Burton, and V. Bruce. Face processing: Human perception and principal components analysis. *Memory and Cognition, 24:26*–40, 1996.

[10] J. Lenhard, K. Loesing, and G. Wirtz. Performance measurements of Tor hidden services in low-bandwidth access networks. In M. Abdalla, D. Pointcheval, P.-A. Fouque, and D. Vergnaud, editors, *ACNS*, volume 5536 of *Lecture Notes I* Computer Science, pages 324–341, 2009.

[11] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari and S. V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments In Mobicom, 2009.

[12] T.Ristenpart, G.Maganis, A.Krishnamurthy and T.Kohno, "Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs", in USENIX Security, 2008.

[13] P.Maymounkov and D.Mazieres, "A peer-to-peer information System based on the XOR metric" in I.P of the 1st international Workshop on Peer-to-Peer Systems (IPTPS02), editor, IPTPS, 2002.