IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

SECURE ENCOUNTER USING DATA HIDING IN BROADCAST NETWORK

Prof. Harish Barapatre[1] *Mr.Roshan Mhatre* [2] *Miss. Anagha Vaidya* [3]
Mr. Amit Gupta [4] *Miss. Fatema Paradawala*[5]
Yadavrao Tasgaonkar College Of Engineering And Technology, Bhivpuri Road, Karjat.[1 2 3 4 5]

***Abstract*— Encounter-based social networks and encounter based systems link users who share a location at the same time, as opposed to the traditional social network paradigm of linking users who have an offline friendship. This new approach presents challenges that are fundamentally different from those tackled by previous social network designs. In this paper, we explore the functional and security requirements for these new systems, such as availability, security, and privacy, and present several design options for building secure encounter-based social networks. To highlight these challenges we examine one recently proposed encounter-based social network design and compare it to a set of idealized security and functionality requirements. We show that it is vulnerable to several attacks, including impersonation, collusion, and privacy breaching, even though it was designed specifically for security. Mindful of the possible pitfalls, we construct a flexible framework for secure encounter-based social networks, which can be used to construct networks that offer different security, privacy, and availability guarantees. We describe two example constructions derived from this framework, and consider each in terms of the ideal requirements. Some of our new designs fulfill more requirements in terms of system security, reliability, and privacy than previous work. We also evaluate real-world performance of one of our designs by implementing a proof-of-concept iPhone application called MeetUp. Experiments highlight the potential of our system and hint at the deploy ability of our designs on a large scale.**

Index Terms—Social networks, Location-based services, Privacy.

I. INTRODUCTION

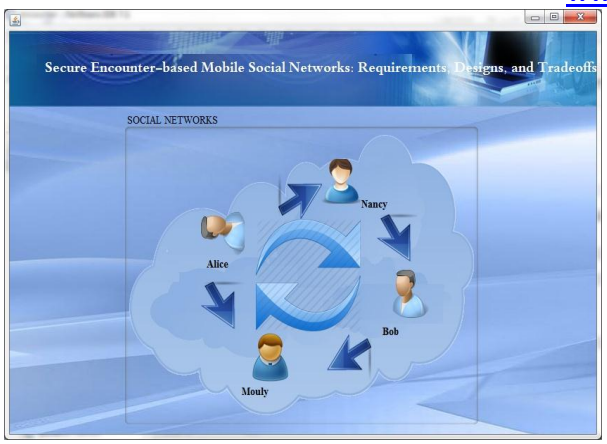
In the conventional model of social networks, users select their contacts from a set of off-line acquaintances. Despite their utility, these conventional networks support only a subset of social networking: two users will only be able to establish a relationship in the social network if they know of, or are introduced to each other. On the other hand, in an encounter- based social network, the only requirement for establishing a connection is to be in the same place at the same time—similar to striking up a conversation at a public place. 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. Additionally, requirements like anonymity a feature that is not needed in most traditional online social networks based on prior face-to-face contact need to be considered in encounter-based networks. This is desirable because users would expect information about people they happen to meet to stay private. Furthermore, 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. In this paper we consider fundamental requirements for encounter-based social networks. We note that 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. A recent state-of-the-art design, fails to meet a number of these requirements (even though it was built explicitly with security in mind). We propose a generic design that can be used to construct networks that provide different security guarantees. We then describe individual designs and show the benefits and trade-offs of specific security design decisions.

COPYRIGHT TO IJETIE

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org



Unlike prior work, we provide fine-grained separation between the encounter event and the eventual connection and communication: authentication and communication may hap- pen immediately, or may be delayed for an arbitrary period of time. The former provides unlink ability between the two paired users (a third party cannot determine that two users have made a connection), while the latter increases convenience and flexibility at the cost of somewhat degraded unlink ability. However, both schemes guarantee authentication—that once established, the connection is with the desired user. Both of these designs consist of an "online phase," where the encounter takes place and encounter instance information is exchanged, and an "offline" or delayed communication phase, where encounter information is used for the two parties to reconnect and communicate privately. It is worth noting that we assume that other users at the encounter time and location are potentially malicious, and may collect information, collude with other parties, and otherwise make it difficult for two people to establish a secure private connection. We developed a prototype of our design, called Meet Up [that] uses visual authentication for encounter information exchange and verification. At the core of our system is a visual authentication scheme that provides authenticity guarantees for users involved in an encounter. Our authentication scheme capitalizes on that people are good at remembering faces but worse at remembering names Encounter-based networks with visual authentication would play to people's strengths, allowing anyone who remembers a face to later connect with the "owner" of that face, without the need to remember additional information. Meet Up uses Tor hidden services to provide an anonymous communication channel for the second phase of our protocol. By performing preliminary real- world experiments using plausible deployment settings, and considering user feedback, we highlight the end-user usability of our system and its feasibility for deployment at larger scales. While the main contribution of this paper is an encounter- based social network design, our techniques can be employed for a wide range of applications, such as a drop-in replacement for a face-to-face key distribution service for future secure communication or for privacy-preserving file sharing systems, e.g. OneSwarm. In OneSwarm, untrusted users get their keys from an online key distribution center. Using our design, one may distribute keys to untrusted users based on some shared activity an encounter. Any application that requires key pre-distribution, such as storage services, private file-sharing systems, private collaboration groups, etc, would benefit from our design in the same way. Another ex- ample is a scientific meeting, where some researchers present their work, and others participate in discussions, and no one has time to introduce themselves to everyone. We can employ our encounter-based system for private on-the-fly name and business card distribution.

Our contributions in this work are as follows. (*i*) by first outlining security and functional requirements that are ide- ally desired for encounter-based social network and arguing that these are minimal requirements for many distributed system with reasonable security and privacy guarantees, we examine the extent to which SMILE, a recent state-of-the- art design of secure encounter-based social network, meets these requirements, showing that it is vulnerable to many attacks. (*ii*) We propose a new and generic architecture for encounter-based social networking that greatly differs from the architecture of previously proposed systems and suggest two possible implementations, each striking a balance between performance and security. (*iii*) we show the feasibility of our designs by implementing a proof-of-concept system— including an iPhone application called MeetUp—conforming to our requirements and evaluating its performance in real- world settings using mobile devices, and by bringing further evidence on the usability of our design and rationality of used assumptions based on several user studies.

The organization of this work is as follows. We describe idealized security and functional requirements expected in encounter-based networks. We discuss some of the related work in the literature, followed by a discussion of vulnerabilities of SMILE. We introduce the design of generic encounter-based social network and discuss two specific designs. We discuss the implementation of Meet Up, and details of some of the experiments that we performed to illustrate the usability of our design.

SMILE: encounter-based trust for mobile social Service

Conventional mobile social services such as Loopt and Google Latitude rely on two classes of trusted relationships: participants trust a centralized server to manage their location

COPYRIGHT TO IJETIE

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

information and trust between users is based on existing social relationships. Unfortunately, these assumptions are not secure or general enough for many mobile social scenarios: centralized servers cannot always be relied upon to preserve data confidentiality, and users may want to use mobile social services to establish new relationships. To address these shortcomings, this paper describes SMILE, a privacy-preserving "missed-connections" service in which the service provider is untrusted and users are not assumed to have pre-established social relationships with each other. At a high-level, SMILE uses short-range wireless communication and standard cryptographic primitives to mimic the behavior of users in existing missed-connections services such as Craigslist: trust is founded solely on anonymous users' ability to prove to each other that they shared an encounter in the past. We have evaluated SMILE using protocol analysis, an informal study of Craigslist usage, and experiments with a prototype implementation and found it to be both privacy preserving and feasible.

2 Requirements and Challengs

Many encounter-based designs do not consider even basic security and privacy requirements along with functionality and performance. Others fail to meet these requirements even though they were created with the explicit goal of satisfying them. Below, we explore some requirements for idealized secure encounter-based social net- works. While this list is by no means complete, it can be used as a preliminary guide for evaluating past and future designs.

2.1 Security Requirements

Here we outline some of the desired security features of encounter-based social networks. Note that these requirements are generic in the sense that they may apply to many distributed systems which combine human interaction, sensitive private information, and network communication. The security requirements we expect in these systems are as follows. (i) Privacy or unlink ability. The privacy of two parties sharing an encounter must be protected, even from others in the vicinity who may also participate in simultaneous encounters. In this case, privacy means that an external adversary (even one taking part in the encounter or colluding with a “bulletin board” or rendezvous server to be used in latter phase) who is not one of the two users of interest should not be able to conclusively determine that two users have made a connection. (ii) Authenticity, meaning that when two users decide to make a connection, they should be assured that messages indeed originate from each other. (iii) Confidentiality, meaning that information exchanged between two users should be accessible only to them.

2.2 Functional Requirements

The following are generic functional requirements in the con- text of large-scale distributed systems that are also desirable for an encounter-based social network. (i) Availability. As such, the infrastructure to exchange encounter information should be accessible most of the time. The unavailability of individual users should not affect the availability of other users. Since the time at which encounter parties check for potential encounters associated with their activities could be arbitrary, the encounter-based social network is more sensitive to availability than conventional social networks. (ii) Scalability. With typical social networks being large in size, any potential social network design, including those based on encounters, should scale to support a large number of simultaneous users. This requires minimizing dependence on a centralized entity.

3 DESIGNS AND DESIGN OPTINS

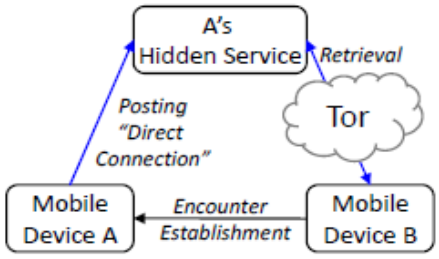
With requirements outlined earlier, we generalize the design of previous systems. Special attention has been given to the security and privacy requirements previous designs failed to achieve. We divide the design into functional blocks and describe potential attacks on various parts of the system. Then, we discuss two instantiations of the generic design; each with different benefits and trade-offs.

3.1 Functional Components

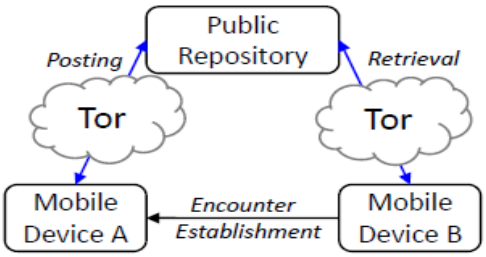
The functional design of a typical encounter-based social net- work consists of three major components located at three different architectural layers. The user layer, the plug-in layer, and the “cloud” The term cloud may refer to a storage location of the encounters and private messages (e.g. a central 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 explain. Furthermore, to establish a balance between the functional and security requirements, we also discuss two specific designs in the next subsection. Below, we elaborate on what requirements each designs meet.

COPYRIGHT TO IJETIE

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org



(a) Hidden service-based design



(b) Repository-based design

3.2 Design option

Immediate exchange

if a user is willing to manually select the picture of other users of interest while still at the encounter site, she can compose an encounter key, encrypt it to the selected user's public key, and broadcast the resulting message. Each user in the vicinity will detect the transmission and attempt to decrypt it. However, only the target user will be able to decrypt the message correctly, and thus recover the encounter key. This key will be used later to exchange private messages at the rendezvous point. This method prevents the rendezvous server and colluding adversaries from determining which two users are communicating. The advantage of this design option is enabling users to make decisions while at the encounter space while they remember well parties they encountered, enabling direct communication and utilization of the physical encounter, reasoning about some security guarantees in this scenario might not be as easy. Particularly, unconventional attacker capable of measuring signal strength and associating that to users might be able to breach the privacy of users by matching who meets whom by monitoring the encrypted traffic between them, thus violating the unlink ability requirement

Delayed Key Exchange

Devices will consistently broadcast their certificates, but will not require others users to immediately review the information. (As in the immediate pairing scheme, we can use timed-release encryption to enforce this constraint.) At a later time, the device user can look at the list of collected identities (and public keys) and select those with whom he wishes to communicate. As before, we will use non-malleable encryption to compose a message to the other user, but now the message must be stored "in the cloud" in such a way that it is linkable to the public key of the user for whom it is intended, and some encounter nonce passed at the time of the encounter. This may not be a significant problem, considering that only keys and faces are exposed, and not more personal components of users' identities. A sequence diagram showing the operation of the two key generation design options is shown in Fig. 2(b). While this scheme does not suffer from the shortcomings in the immediate pairing scheme, the capability of reconnecting to encounter parties depends entirely on the capability of encounter parties to recall such encounters. We believe remembering people is quite easy, given the limited number of encounters per time window

4 IMPLEMENTATION AND EXPERIMNTS

To validate our method and assess the practicality of our design, we implemented the system on the iPhone platform and tested it on multiple devices under ideal conditions, as well as conditions that users are likely to encounter in urban settings. In our implementation, we used the delayed rendezvous scheme where the user's device can collect simulated broadcast information during encounters and then use the decentralized Tor hidden service architecture for the second part of the encounter. Those require a hidden service URI (an address through which one can access services deployed by hidden servers to be part of the user's information and is thus linked with the certificate as a bundle in sent the transmissions. Notice that, even when an adversary captures the certificate exchanged between two honest participants, and get access to the URI, the honest participant running the hidden service will still have a full control over whether to respond to requests for communication sent via the hidden service. Accordingly, while the use of the hidden service would resolve the rendezvous problem and provide means for reconnection in the future based on the previous encounter, it will increase the attack surface by enabling means for the adversary to breach the Privacy of the users and their encounter.

Notice that our design is generic. We are not limited to any specific platform like Apple's iOS, which we chose for development, in any of our design ingredients. Our choice of development platform for our proof-of-concept application is only due to availability and ease of use for quick prototyping. Other platforms, such as Android, would work just as well. Consequently, any conclusions on the usability

COPYRIGHT TO IJETIE

of our design are independent of the platform, as we only require a smart phone with basic wireless capabilities.

5 APPLICATIONS

There are numerous applications of opportunistic mobile social networks, and more applications are evolving as the smart phone technology is advancing.

Opportunistic computing

Opportunistic computing utilize the shared resources, content, services, applications, and computing resources, by the devices connected in an opportunistic mobile social network, to provide a platform for the execution of distributed computing tasks. However, opportunistic computing requires middleware services to cope with the intermittent connectivity and delay of the opportunistic communication environments.

Recommender systems

A novel application area of opportunistic mobile social networks is the recommender systems. Such systems track the user activities, mobility patterns, and utilize the user's contextual information to provide recommendations on variety of items.

6 CONCLUSION

In this work we show that existing designs for secure encounter-based social networks fail to fulfill reasonable security guarantees. We outline several requirements that ideal encounter-based social networks need to satisfy, and introduce a generic framework for constructing encounter-based social networks. We then use our framework to showcase several designs, and demonstrate that our designs fulfill more requirements than SMILE, the design motivates our work. If the signature is valid, then the data transmission is occurring between the sender & receiver. In Immediate Key Exchange process, each user in the vicinity will detect the transmission and attempt to decrypt it & also it is time based process, when the user gives acknowledgement to the sender. However, only the target user will be able to decrypt the message correctly. In Delayed key exchange process is a time released process, the user public key & image are send to the user, here also only the target user will be able to decrypt the message correctly & there by providing better security in communication process.

ACKNOWLEDGEMENT

We thank Prof. HARISH K. BARAPATRE for knowledge, guidance & co-operation in the process of making this project.

REFERENCES:-

- M. Farb, M. Burman, G. Chandok, J. McCune, and A. Perrig, "Safeslinger: An easy-to-use and secure approach for human trust establishment," Carnegie Mellon University, Tech. Rep. CMU-CyLab-11-021, 2011.
- C. M. Gartrell, W. C. M. Gartrell, D. S. Mishra, S. Charles M. (m., and C. Science, "Socialaware: Context-aware multimedia presentation via mobile social networks," 2008.
- V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Locationbased trust for mobile user-generated content: applications, challenges and implementations," in HotMobile '08: Proceedings of the 9th workshop on Mobile computing systems and applications. New York, NY, USA: ACM, 2008, pp. 60–64.
- 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.
- A.-K. Pietil¨ainen, E. Oliver, J. LeBrun, G. Varghese, and C. Diot, "MobiClique: middleware for mobile social networking," in WOSN '09: Proceedings of the 2nd ACM workshop on Online social networks. New York, NY, USA: ACM, 2009, pp. 49–54.
- M. von Arb, M. Bader, M. K. 0002, and R. Wattenhofer, "Veneta: Serverless friend-of-friend detection in mobile social networking," in WiMob, 2008, pp. 184

COPYRIGHT TO IJETIE