SECURE ENCOUNTER-BASED MOBILE SOCIAL NETWORKS: REQUIREMENTS, DESIGNS, AND TRADEOFFS

Unnati Dhavare [1], Prof. Umesh Kulkarni [2]

[1]A.R.M.I.E.T A.S.Rao Nagar, Sapgaon, Shahapur, Thane, Maharashtra 400708

[2]V.I.T. Vidyalankar campus, Vidyalankar College Marg, Wadala (East), Mumbai, Maharashtra 400037

ABSTRACT

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. 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. 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 also evaluate real-world performance of one of our designs by implementing a proof-of-concept iPhone application called meet up. Experiments highlight the potential of our system and hint at the deployability of our designs on a large scale.

KEYWORDS: SOCIAL NETWORKS, LOCATION-BASED SERVICES, PRIVACY.

1. INTRODUCTION

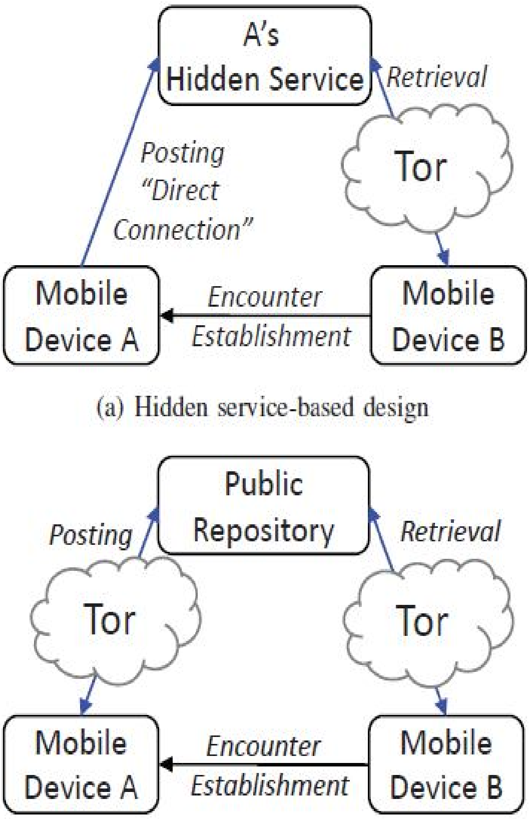
In the conventional model of social networks, users select their contacts from a set of off-line acquaintances. Despite their utility, these conventional networks support only a subset of social networking: two users will only be able to establish a relationship in the social network if they know of, 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. Early work assumed that the parties could communicate over a public but authenticated channel or, equivalently, assumed a passive adversary. This assumption was relaxed in later work, which considered an active adversary who could modify all messages sent between the two parties. In proposed system 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 unlinkability of users sharing an encounter, confidentiality of data exchanged among encounter participants, and authentication of both users in a two-party conversation. We show that SMILE, a recent state-of-the-art design, fails to meet a number of these requirements.

2. LITERATURE SURVEY

Wireless sensor network is a collection of large number of sensor nodes that are communicating using wireless medium. Secure Data Aggregation in Wireless Sensor Network: a survey Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto. [1]. Attack on Fully Homomorphic Encryption over the Integers this paper presents a heuristic attack on the fully homomorphic encryption over the integers by using lattice reduction algorithm. [2]. A Fully Homomorphic Encryption Scheme. Such a scheme allows one to compute arbitrary functions over encrypted data without the decryption key { i.e., given encryptions E(m1); : : : ;E(mt) of m1; : : : ;mt, one can e±ciently compute a compact ciphertext that encrypts f(m1; : : : ;mt) for any e±- ciently computable function f. This problem was posed by Rivest et al. in 1978 [3]. Computing Arbitrary Functions of Encrypted Data. [4].

3. SYSTEM ARCHITECTURE



(a) Hidden service-based design

Fig.1. Two specific designs. Fig. (a) Illustrates the first design using Tor hidden services as encounter storage place. Fig. (b) Illustrates the second design where users Store encounters information on a public replica and gain anonymity to their access using a normal Tor operation.

4. 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 Meet Up.

5. OVERVIEW OF SMILE

The main work in the literature that is similar to our work in goals and purpose is SMILE. SMILE extends ideas from [26] to establish trust between individuals who shared an encounter. It attempts to allow users equipped with mobile devices to build such trust relationships while preserving their privacy against potential attackers (e.g., the rendezvous server and other users in the encounter settings). In SMILE, users who want to communicate with each other must prove that an encounter occurred between them. To do this, the first device in the encounter generates and broadcasts the "encounter key" to other devices within its communication range. The same device then posts a cryptographically-secure hash of the encounter key, along with a message encrypted using the encounter key to a centralized server. Due to the pre-image resistance properties of the hash function, the centralized server cannot recover the encounter key without help, and thus cannot read the message. Other users of SMILE with the same encounter key may claim the encounter by looking up the hash of the key, which is used for indexing the encrypted message at the centralized server. Only users with the correct key will be able to decrypt the message left by the first encounter party at the server, and every user with the correct key can derive the retrieval hash value. The benefits of the basic design of SMILE as it is described here is that it reduces the misuse in the encounter system: only people who have been at the encounter place are those who know the encounter credentials and are able to claim the encounter.

6. 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.

7. MODULES

1. Trusted Certification Module
2. Strong Authentication for Immediate Pairing Module
3. Delayed assignation Module

4. Decentralization and Anonymity Module

7.1MODULES DESCRIPTION

Trusted Certification Module

In our design, we use the X.509 standard for certification without any modification to the structure of the certificate, but we limit the attributes available in the certificate used for encounters (discussed below) in order to preserve the privacy of our users. Indeed, the X.509 standard allows optional attributes for biometric information such as photos, which enables us to embed visual information into the certificate. The trusted authority mentioned previously is responsible for ensuring that the details provided by user for certification is an actual representative picture, and allows others to visually identify the user. So, even when issuing a certificate that combines multiple pieces of private information, such as the certificate owner name and address, the authority will issue a separate, limited certificate with reduced amounts of private information which fits our social encounters design (only user's public key). The ultimate signature by the trusted authority will sign all embedded attributes in the certificate.

Strong Authentication for Immediate Pairing:

In this module, we develop the module as, 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. We can go a step further and use time d release encryption to hide the contents of the message even from its intended recipient until the encounter is over, ensuring that users do not inadvertently give themselves away by using their devices at the same time.

Delayed Assignation:

Devices will consistently broadcast their certificates, but will not require others users to immediately review the information. 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.

Decentralization and Anonymity Module:

In this module, we use the generic design combined with Tor hidden services to provide communication anonymity. While Tor provides users with anonymity, Tor hidden services enable servers to conceal their identities as well. Each user runs his own Tor hidden service and uses it for two purposes: first, to hide his identity and gain anonymity as to his location and second, to serve follow-up requests relating to previously encounters. The other party must use the Tor client to access the hidden service, also gaining anonymity and hiding her location from the server. This design can easily scale to a large number of simultaneous users and is resilient to failure; since an attack on the entire social network built using this distributed design would require attacking many individual nodes simultaneously (i.e. the failure of one hidden service would not affect other hidden services)

Centralized Design with Anonymity Guarantees:

In this module, we assume a public repository to which users involved in the encounter can post encounter information. Suppose that Alice shares a public space with Bob, and therefore learns his public key from his certificate. At an arbitrary time after Alice and Bob share a location, Alice can go through all her collected identities, notice Bob's picture, and decide to strike up a conversation. She composes a message to Bob, encrypts it under Bob's public key, and posts the encrypted message on the centralized repository under Bob's public key. To gain anonymity as to her identity and location, Alice uses a Tor client, concealing her IP address from the central server. This is more efficient than the hidden services used in the previous protocol, which require one of the encounter parties to be online all the time to serve other parties involved in the encounter. In this design, on the other hand, Bob can get the messages left for him at the central repository at any time. He similarly accesses the repository through Tor to conceal his identity, and downloads all messages addressed to him. To identify such messages, we suggest using nonces as part of the indexing scheme. These random one-time values generated and exchanged at runtime of the encounter protocol, along with the public key of the encounter party that initiates the encounter, are hashed and used for indexing.

8. CONCLUSION

In this work we show that existing designs for secure encounter based social networks fail to fulfil 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 fulfil more requirements than SMILE, the design the motivates our work. We show the feasibility of our work through a demonstration of Meet Up, an iPhone application that uses our design. In the future, we will investigate further extensions to the current framework, alternative designs options, and additional pluggable components. We will also investigate developing Meet Up on other mobile platforms as well as a larger-scale deployment using multiple wireless communication protocols.

ACKNOWLEDGMENT

I would like to express my sincere gratitude towards my guide Prof.Umesh Kulkarni for the help, guidance an encouragement in the development of this methodology. They supported me with scientific guidance, advice and encouragement, and were always helpful and enthusiastic and this inspired me in my work. I have benefitted from numerous discussions with guide and other colleagues.

REFERENCES

[1] Abedelaziz Mohaien, Denis Foo Kune,Member, IEEE,Eugene Vasserman,Member, IEEE, Myungsun Kim, and Yongdae Kim, Member, IEEE “Secure Encounter-based Mobile Social Networks: Requirements, Designs, and Tradeoffs”- Ieee Transactions On Dependable And Secure Computing, Vol. 1, No. 8, August 2013.

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

[3] 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 in Computer Science, pages 324–341, 2009.

[4] M. Macy. Learning to cooperate: Stochastic and tacit collusion in social exchange. The American Journal of Sociology, 97(3):808–843, 1991.

[5] J. Manweiler, R. Scudellari, and L. P. Cox. SMILE: encounter-based trust for mobile social services. In E. Al-Shaer, S. Jha,and A D. Keromytis, editors, ACM Conference.