International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 3 –SEPTEMBER 2014.

Generic Framework for Encounter Based Mobile Social Networks

G. Raghavendra[*1], and K. Janardhan[#2]

[*]*Student, Dept of CSE, Intell Engineering College, Affiliated to JNTUA University, ANANTAPURAMU, AP, India*

[#] *Asst Professor, Dept of CSE, Intell Engineering College, Affiliated to JNTUA University, ANANTAPURAMU, AP, India*

[1]graghava9999@gmail.com

[2]jkradhan7@gmail.com

***Abstract*— The protection of information from unauthorized disclosure is increasingly scarce on the Internet. The concern for the lack of privacy is particularly true for popular peer-to-peer data sharing applications, where public rendezvous and dynamic membership mean that the user behavior can be easily monitored. On the other hand, anonymization systems where the second pary is likely to be not known like Tor and Freenet emphasize privacy but at the cost of poor performance and robustness, especially in case of misaligned incentives and inefficient protocol choices such as single path routing A new approach Encounter based social networks This new approach presents challenges that are fundamentally different from those tackled by previous social network designs.**

In this paper, we look at the efficient and protection requirements for these new systems, such as availability, security, and privacy, and present several design options for building secure encounter-based social networks.

Keywords: Encounter based networks, location privacy, mobile communication, Social networks .

I. INTRODUCTION

Encounter-based social networks provides a computing infrastructure which allows for creation of varied services such as a "missed connections" virtual bulletin board, on-the-fly introductions , or real-time in-person key distribution to bootstrap secure communication in other systems. Though, Encounter-based systems [1] appear very similar to existing communal networks, they present a vividly like chalk and cheese set of challenges which includes security and privacy of users and authenticity of the other party in a conversation. Since people do not automatically place their trust in others simply based on presence in the similar locality, it is also enviable to expose the minimum amount of information required for future secure communication. Restricting the concept of location sharing to pre-established social relations makes a large class of compelling mobile social services impossible.

In this work, we provide a fine-grained separation between the encounter event and the eventual connection and communication: Authentication and Communication provides unlink ability between the two paired users whereas the delay between the authentication and communication increases convenience and flexibility at the cost of somewhat degraded unlink ability. Both of the said 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.

II. EXISTING SYSTEM

The existing systems such as SMILE, GAnGS [2] and SPATE succeed in meeting some of the functional requirements; they do not resistt against a number of common security vulnerabilities. SMILE uses a centralized online entity. In SMILE system, though the confidentiality of encounter-related information is safeguarded by encryption, the privacy of users can be breached. Since no authentication or key agreemnet is required, it is vulnerable to impersonation attack. Also SMILE is prone to user collusion. A gang allows users to indicate which two devices should communicate at a time. This scheme is efficient for communication among the groups involving device-pairing. SPATE [4] involves streamlining of cryptographic operations to make the system more securely usable on mobile devices. Neither of the above discussed existing works considers privacy or anonymity of participants, since authentication and collaboration are done at the same phase.

Many encounter-based designs do not consider even basic security and privacy requirements along with functionality and performance. Since location plays a crucial role for encounter based systems there are so many services designed for short-range communication such as Brightkite and Loopt WhozThat, Serendipity, SocialAware, Veneta , D-book, and

Bump. All the services refer to involves locality based communication [5], but not suggest the idea of setting privacy.

III. PROPOSED SYSTEM

In this proposed work, we assume that other users at the encounter time and location are probably malicious, and may collect information, conspire with other parties, and otherwise make it difficult for two people to establish a secure private connection. In this we design a visual authentication scheme that provides authenticity guarantees for users involved in an encounter. This scheme is ensured to capitalize on that people are good at remembering faces but worse at remembering names.

The preliminary security requirements which we consider in this work include i) Privacy or unlinkability ii) Authenticity iii) Confidentiality. 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 system allows storage components to be dynamically chosen using plugin architecture: at the same time supports centralized servers, distributed hash tables, or even or hidden services.

From the design mentioned in Fig 1.a 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. This design can easily scale to a large number of simultaneous users, and is resilient to failure.

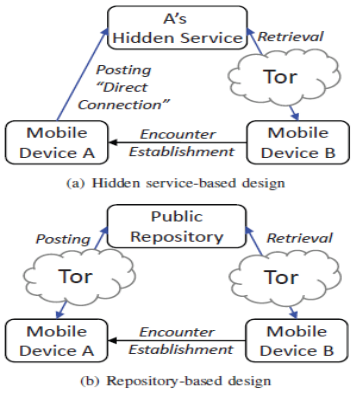

Fig. 1. Two specific designs. Fig. (a) illustrates the first design using Tor hidden services as encounter storage place. Fig. (b) illustrates the second design where users store encounter information on a public replica and gain anonymity to their access using a normal Tor operation.

The design referred in Fig 1.b assumes a public repository to which users involved in the encounter can post encounter information. The latter design 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. The design uses 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.

The implementation on an iPhone platform 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. When an adversary captures the certificate exchanged between two honest participants, gets 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 that are sent via the hidden service.

Our iPhone application, "MeetUp," permit users to find other users of the system within Bluetooth range, decide with whom they wish to communicate, and send and receive private messages. A certificate signed by an authenticated authority includes hashes of photos and Tor hidden service URI unique to the user. In our system, the file containing the certificate, the photo, the hidden service URI, and the signature are the deployed to each device in the system.

Our design assumes the availability of smart phones for users and their willingness to use their phones to participate in the system. Implementing our MeetUp application on smart phones, the study indicated that 25% of the questioned subjects did not respond, implying the likelihood of not having smart phones or not willing to use their phones for social networks for such applications as MeetUp.

Up on the implementation of Meetup on wireless gadgets, the protocol is a Multicast DNS query on the local network to check for name collisions. Of an experimental study, to ensure that we were limited to the target location, we had a user with a known device name connect to the same network, but at different location, and verified our inability to observe his/her device's DNS messages, around an area of 5000m2 Multicast DNS messages tells us when an iOS device joins the network, but we don't know how long it stays.

The overhead required in MeetUp is in the form of communication, computation, and memory.

Communication resources- required for transferring and receiving encounter information,

Computations - required for establishing Tor circuits

Memory - required for storing the encounter information in the mobile device and later on a desktop machine that is used for running the hidden service.

The overhead for performing online computations in our design includes signature verification in order to verify the authenticity of certificates issued by the certificate authority.

IV. CONCLUSION

In this paper, we explore the functional and security requirements for secure encounter-based social networks, such as availability, security, and privacy. Also, we explore the basic functional requirements like high availability, scalability, and robustness to failure. We developed a prototype of our design, called MeetUp, that uses visual authentication for encounter information exchange and verification that guarantees authentication for information exchange and verification. The advantage of this design is that the visual authentication is effective at remembering faces rather than the names.

V. 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, Secure Encounter-based Mobile Social Networks: Requirements, Designs, and Tradeoffs.

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

[3] A. Mohaisen, E. Y. Vasserman, M. Schuchard, D. F. Kune, and Y. Kim, "Secure encounter-based social networks:requirements, challenges, and designs," in ACM Conference on Computer and Communications Security, E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, Eds. ACM, 2010, pp. 717–719.

[4] Y.-H. Lin, A. Studer, H.-C. Hsiao, J. M. McCune, K.-H. Wang, M. Krohn, P.-L. Lin, A. Perrig, H.-M. Sun, and B.-Y. Yang, "SPATE:small-group PKI-less authenticated trust establishment,"in MobiSys, 2009, pp. 1–14.

[5] 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.