Secure Encounter-based Social Networks

Abedelaziz Mohaisen[†], Eugene Y. Vasserman[‡], Max Schuchard[†], Denis Foo Kune[†] and Yongdae Kim[†]

[†]CSE Department, University of Minnesota.
{mohaisen, ,schuch,foo,kyd}@cs.umn.edu

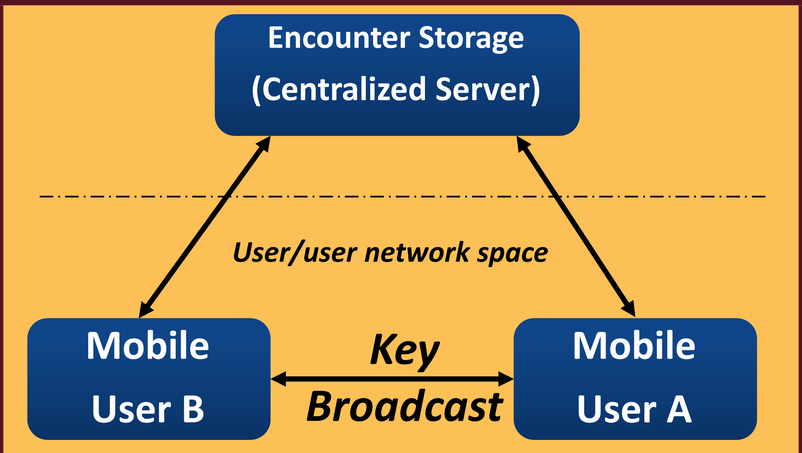
[‡]Department of CIS, Kansas State University
eyv@ksu.edu

University of Minnesota

Motivation

Modern social networks only allow users to form relationships with either no offline interactions (strangers) or after offline meetings (acquaintances). New "encounter-based" networks allow relationships between people who are less than acquaintances but more than strangers—users can connect to others with whom they have shared a physical space. Encounter-based social networks have unique security and functionality requirements that were not met in some of the recent work. This work analyzes these requirements, demonstrates the shortcomings of SMILE, a recent security-focused encounter-based scheme, and proposes a flexible generic framework for constructing secure social encounter-based networks. We demonstrate the usefulness of this framework with two candidate designs.

Overview of SMILE



- Passive wireless key exchange
- Truncated, hashed encounter keys sent to a centralized server with timestamps
- Encrypted messages with encounter keys are indexed by the truncated hash
- Only users with the corresponding key retrieve the encrypted message
- Key truncation provides $k-$anonymity

Vulnerabilities of SMILE

- **Impersonation attack:** no authentication is performed for passively-exchanged keys, so an attacker may impersonate any user whose key it records
- **Traceability attack:** unauthenticated user can trace activities of legitimated users in the encounter space; the location where encounters take place
- **Collusion attack:** users colluding with the central server may collect enough information (timestamps, location, encounter keys) of legitimate users to unmask encounters
- **Unmasking attack:** SMILE's anonymity properties depend on its widespread use, and an estimate of the number of other users in close proximity; an adversary can easily misrepresent the latter using a Sybil Attack

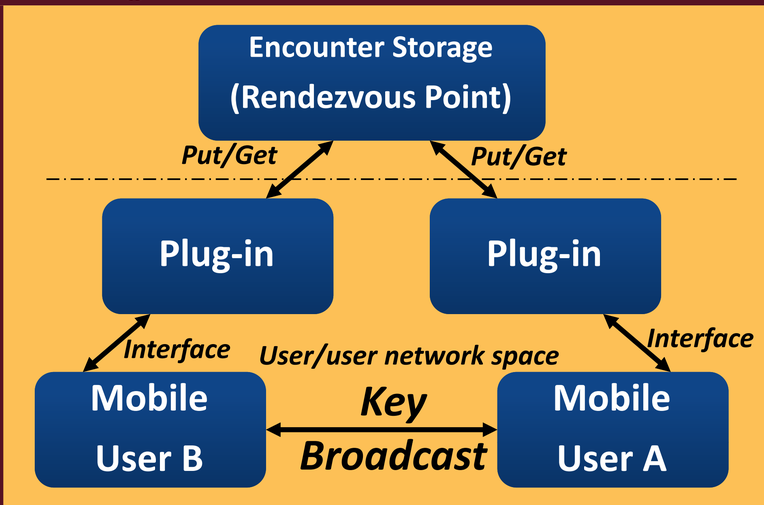
Contributions

- We outline requirements, challenges, and designs for encounter-based mobile social networks, where relationships are based on a temporarily shared location.
- We examine a recent design, SMILE, against a set of functional and security requirements. Despite SMILE's explicit security-focused design, it is vulnerable to several attacks such as impersonation, collusion, and privacy breaching.
- We describe ideal security requirements for mobile social networks, and suggest a flexible design framework from which we construct several schemes offering different security properties. We further show that our systems offer better security than previous work.

Idealized Requirements

- **Privacy:** an adversary should not be able to conclusively determine that two users have made a connection (associated)
- **Authenticity:** when two users associate, they should be certain that private messages indeed come from each other
- **Confidentiality:** after associating, private messages exchanged between connected users should only be readable by them
- **Availability:** the infrastructure to exchange encounter information should be accessible to users *most of the time* — the connection infrastructure must resist disruption (denial of service attacks) by misbehaving users
- **Scalability:** the design must support a large number of simultaneous users, minimizing reliance on a centralized server

Designs for Secure Encounter-based Social Networks



Functional components:

- *User layer:* a user's mobile device silently exchanges encounter information with any other compatible device in its vicinity
- *Plug-in layer:* an interface between the user and the "encounter storage"
- *Rendezvous layer:* used for storing and retrieving encounters; can be a public server or a distributed service (e.g. P2P DHT)

Security components:

- *Visual authentication:* users recognize that they are communicating with the desired party by looking at their pictures
  - We use a digital certificate, signed by trusted authority, matching a user's picture to his or her public key — sufficient information to visually "authenticate" key owners (passports already store biometric information digitally)
  - Key agreement can proceed immediately (at encounter time) or after an enforced delay
- *Immediate key agreement:*
  - A user selects another person within visual range and generates an encounter key
  - The user's device broadcasts the encounter key, encrypted to the user of interest, whose public key is authenticated by their broadcast key/picture certificate
  - All users try to decrypt, but only person of interest succeed
  - Encounter key is later used for secure and unlinkable after-encounter communication
- *Delayed rendezvous:*
  - As in immediate key generation, devices periodically broadcast their certificates, but prevent immediate access to them using time-lock puzzles
  - At a later time, the device user can review collected certificates and visually select persons of interest
  - The user may compose a message and post it at a rendezvous point, in such a way that it is linkable to its intended recipient
- *Security guarantees:*
  - Encounters are unlinkable when using immediate key generation; only linkable to pictures when using delayed rendezvous
  - Users post or look up encounter information using the Tor network to gain anonymity
  - Our design is immune to impersonation since this is equivalent to certificate forgery
- *Getting rid of centralized severs:*
  - Each user operates his own Tor hidden-service, which is indexed by his public key
  - Each user maintains encounter information and respond to requests by others who had encounter with him.

References

[1] J. Manweiler, R. Scudellari, L.P. Cox. SMILE: Encounter-based trust for mobile social services. In *ACM CCS*, 2009: 246-255.

[2] J. Douceur. The Sybil attack. In *IPTPS*, 2002.

[3] R. Dingledine, N. Mathewson, P. Syverson. Tor: The second-generation onion router. In *USENIX Security Symposium* 2004.

[4] A. Mohaisen, E. Vasserman, M. Schuchard, D. Kune, Y. Kim. Secure encounter-based social networks: requirements, challenges, and designs. *UMN Technical Report*, 2010.

Funding

This research was supported by the NSF grant CNS-0917154 and a grant from KAIST.