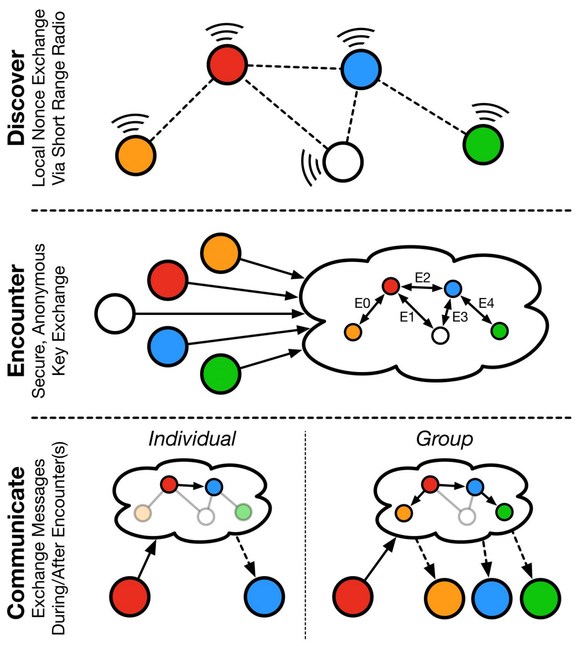
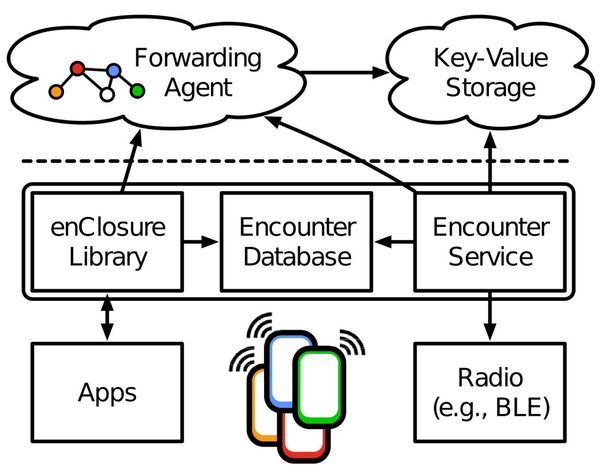
enClosure: Group Communication via Encounter Closures

Lillian Tsai, Roberta De Viti, Matthew Lentz, Peter Druschel, Stefan Saroiu, Bobby Bhattacharjee

MIT, Max Planck Institute for Software Systems (MPI-SWS), University of Maryland, Microsoft Research

Overview & Design





Prototype

- **enClosure Android library** for encounter formation + messaging
- **Microsoft's Embedded Social Platform** as the kvs
- **C++ application running in an SGX enclave** as the Forwarding Agent

Practical: A dedicated, fully charged smartphone lasts 4 days while forming 3000+ encounters

Messaging Properties

Completeness
Confidentiality
Authenticity

Challenges & Future Work

- **Usability**: DoS, unwanted communication, application UI
- **Security**: Encounter graph mining attacks, encounter database protection
- **Strengthen the threat model**: Cryptographically secure agent, hash chain encounter histories

What does enClosure enable?

1. **Contextual, spontaneous, secure, and privacy-preserving group communication among devices connected by paths in the encounter graph**

2. **Powerful new group communication applications by addressing communication partners using encounter closures subject to causal, spatial, and temporal constraints**
   - Messaging among users **sharing an experience**
   - **Virtual guest book, context-based recommendation**
   - **Lost-and-found**
   - Targeted dissemination of **health risk warnings**
   - **Investigation of missing person cases**
   - …

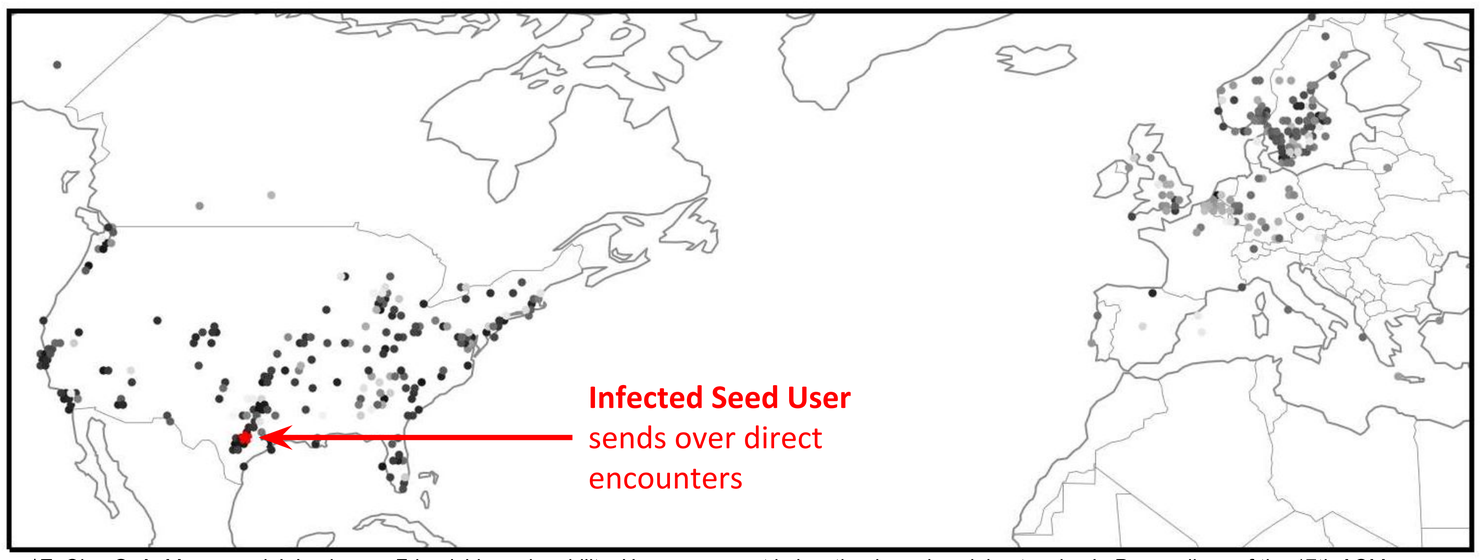
Example: Health Risk Warning

enClosure can target audiences over large geographic areas. This allows a health risk warning to anonymously identify potential patients and affected areas.

Message Address = Forwarding Constraints

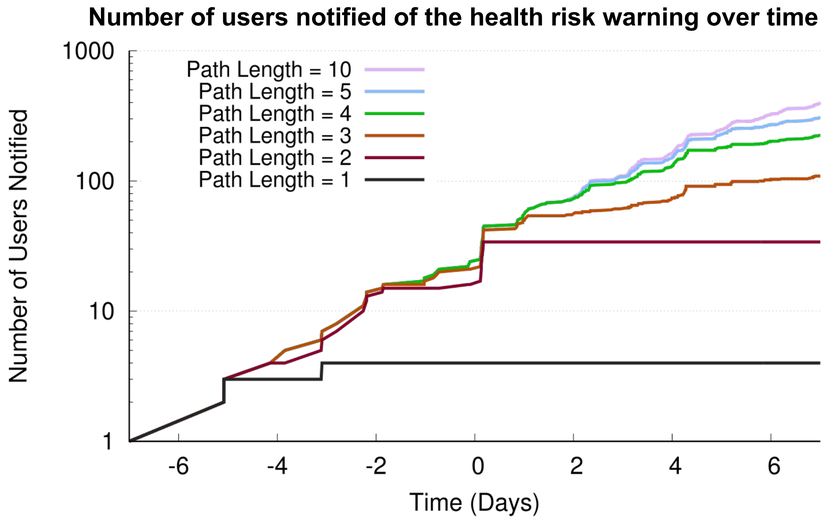
- **Causal=True** (mimics contagious disease propagation)
- **Time=7 days** (mimics disease recovery/potential infection period)

Simulation on Gowalla Location Traces*



E. Cho, S. A. Myers, and J. Leskovec. Friendship and mobility: User movement in location-based social networks. In Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD '11, pages 1082–1090, New York, NY, USA, 2011. ACM.

Number of users notified of the health risk warning over time



Furthest distance traveled by the heath-risk warning over time