Poster-enClosure: Group Communication via Encounter Closures

Lillian Tsai*
MIT

Roberta De Viti
MPI-SWS

Matthew Lentz
University of Maryland

Stefan Saroiu
Microsoft Research

Bobby Bhattacharjee
University of Maryland

Peter Druschel
MPI-SWS

ABSTRACT

New applications enabled by personal smart devices and the Internet-of-Things (IoT) require communication in the context of an *encounter* (a period of spatial co-location). However, existing encounter-based communication (EbC) systems are limited to communication among participants that share a direct encounter. This work is inspired by two insights: (1) encounters also enable group communication among devices connected by *paths in the encounter graph* that is contextual, spontaneous, secure, and privacy-preserving; and (2) addressing communication partners using encounter closures subject to causal, spatial, and temporal constraints enables powerful new forms of group communication.

We present the design of *enClosure*, a service providing group communication based on encounter closures for mobile and IoT applications, and a prototype implementation for Android. We show that enClosure provides a privacy-preserving, secure platform for a wide range of group communication applications ranging from connecting attendees of an event to disseminating health risk warnings.

CCS CONCEPTS

• **Security and privacy** → *Pseudonymity, anonymity and untraceability; Privacy-preserving protocols; Social network security and privacy*; • **Human-centered computing** → *Ubiquitous and mobile computing systems and tools*.

KEYWORDS

mobile computing, privacy, group communication, encounter-based communication, Internet-of-Things (IoT)

ACM Reference Format:

Lillian Tsai, Roberta De Viti, Matthew Lentz, Stefan Saroiu, Bobby Bhattacharjee, and Peter Druschel. 2019. Poster-enClosure: Group Communication via Encounter Closures. In *The 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '19)*, June 17–21, 2019, Seoul, Republic of Korea.

*This research was performed at MPI-SWS on a Fulbright grant.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
MobiSys '19, June 17–21, 2019, Seoul, Republic of Korea
© 2019 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-6661-8/19/06.
<https://doi.org/10.1145/3307334.3328614>

Korea. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3307334.3328614>

1 INTRODUCTION

Personal smart devices and stationary IoT devices enable many context-aware applications and services. With their smart devices, people may interact with nearby people and resources, or follow up with others they have encountered, directly or indirectly, in the past, in the past..

Prior work has shown that *encounter-based communication (EbC)* [1–5] can meet these communication needs while providing strong security and privacy guarantees: (1) EbC enables communication during and after an encounter without the need to exchange contact details; (2) EbC is privacy-preserving because users need not disclose information to a third party; (3) EbC enables communicators partners to authenticate as devices encountered at a given time and place; and (4) EbC ensures message confidentiality and integrity.

Previous EbC systems have been limited to communication among devices that have directly encountered each other. Our work is based on two key insights. First, secure encounters can also enable communication among parties connected by paths in the graph of encounters, while retaining the same strong properties as direct EbC. Second, addressing communication partners using closures of the encounter graph subject to causal, spatial, and temporal constraints enables powerful new forms of group communication. We explore the opportunities and challenges associated with *group communication via encounter closures*, and present and evaluate enClosure, a library service for Android and Microsoft Embedded Social.

enClosure enables rich, powerful, contextually meaningful communication among devices and users. For instance, enClosure enables communication among users who occupied the same space but never met; users who crossed each others' trajectories at different times; and users connected by causal chains of encounters which may imply a flow of information or can be used to backtrack a spread of disease.

enClosure differs fundamentally from existing forms of group communication. Unlike in conventional address-based group communication, users need not exchange individual addresses or agree on a group address. Unlike in publish-subscribe services, users need not agree on a topic ontology or reveal their interests. Unlike in Web-based location services, users need not disclose their identities, whereabouts, social connections, and communication to a third party. With enClosure, users run the enClosure service and address intended

Figure 1: enClosure Overview: Users *discover* others, form *encounters*, and may *communicate* via encounter closures.

receivers via encounter closures with causal, temporal, and spatial constraints. This form of addressing gives enClosure unique expressive power to name communication partners without requiring users to reveal upfront their contact details or other linkable information.

2 ENCLOSURE APPLICATIONS

Figure 1 presents an overview of enClosure. As in direct EbC, communication proceeds in phases. Devices initially discover others using short-range broadcast, and establish encounters associated with location and time. During or after these encounters, devices connected in the encounter graph can communicate using an untrusted Cloud service, such as a third party key-value store.

This simple, three-phase model has broad reach, and enables many new forms of contextual group communication that go far beyond direct EbC while retaining the same spontaneity, security, and privacy properties. We demonstrate how enClosure facilitates communication among users who shared an experience; communication among users and stationary devices in their wider vicinity; virtual guest book and context-based recommendation services; lost-and-found services; and targeted dissemination of health risk warnings. Users retain the opportunity to participate merely by running the enClosure service in the background.

These applications all require that communication partners are selected based on the spatial, temporal, or causal relationship of their encounters. This is a drastic departure from existing platforms where communication is formed around names, roles, or interests, and this distinction is key to enClosure’s strong privacy and security guarantees.

3 DESIGN

Figure 2 shows the high-level architecture of enClosure. enClosure client devices run the *encounter service* continuously

Figure 2: enClosure’s high-level architecture, including components running locally on the users’ devices (bottom) along with the Cloud services (top).

in the background. The service forms secure encounters with nearby devices and adds them to the *encounter database*. Apps running on client devices who wish to use enClosure link the *enClosure library*, which provides a messaging API. The key-value store holds encrypted messages in transit, as well as Diffie-Hellman parameters advertised by enClosure devices. The forwarding agent forwards messages according to message header constraints and executes in a trusted execution environment (TEE).

We demonstrate how this design provides messaging completeness, confidentiality, and authenticity properties. Furthermore, we examine ways to extend our design to accommodate stronger threat models, such as mining of the encounter graph, mounting DOS attacks, and spamming others with unwanted communication.

We evaluate a prototype enClosure Android library—with Microsoft Embedded Social and Intel SGX for the key-value store and TEE respectively—to show that enClosure can easily be supported using current mobile hardware. Finally, using trace-based simulations, we show the utility of enClosure by modeling real-world application scenarios that benefit from enClosure’s messaging via encounter closures.

REFERENCES

- [1] P. Aditya, V. Erdélyi, M. Lentz, E. Shi, B. Bhattacharjee, and P. Druschel. Encore: Private, context-based communication for mobile social apps. In *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '14, pages 135–148, New York, NY, USA, 2014. ACM.
- [2] L. P. Cox, A. Dalton, and V. Marupadi. Smokescreen: Flexible privacy controls for presence-sharing. In *Proceedings of the 5th International Conference on Mobile Systems, Applications and Services*, MobiSys '07, pages 233–245, New York, NY, USA, 2007. ACM.
- [3] M. Lentz, V. Erdélyi, P. Aditya, E. Shi, B. Bhattacharjee, and P. Druschel. SDDR: Light-weight, secure mobile encounters. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC'14, pages 925–940, Berkeley, CA, USA, 2014. USENIX Association.
- [4] J. Manweiler, R. Scudellari, and L. P. Cox. Smile: Encounter-based trust for mobile social services. In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, pages 246–255, New York, NY, USA, 2009. ACM.
- [5] A. Mohaien, D. F. Kune, E. Y. Vasserman, M. Kim, and Y. Kim. Secure encounter-based mobile social networks: Requirements, designs, and tradeoffs. *IEEE Transactions on Dependable and Secure Computing*, 10(6):380–393, Nov 2013.