Future Generation Computer Systems 31 (2014) 169–181

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Private aggregation for presence streams

Eleanor G. Rieffel [a,*], Jacob T. Biehl [a], Adam J. Lee [b], William van Melle [a]

[a] FX Palo Alto Laboratory, United States
[b] University of Pittsburgh, United States

HIGHLIGHTS

- Examines role that privacy-preserving aggregation can play in presence systems.
- Defined and implemented new privacy-preserving aggregation protocols.
- User studies and user feedback motivating privacy-preserving aggregation.

ARTICLE INFO

Article history:
Received 9 January 2012
Received in revised form
7 May 2013
Accepted 17 May 2013
Available online 28 May 2013

Keywords:
Privacy
Presence systems
Awareness
Access control
Cloud computing
Homomorphic encryption

ABSTRACT

Collaboration technologies must support information sharing between collaborators, but must also take care not to share too much information or share information too widely. Systems that share information without requiring an explicit action by a user to initiate the sharing must be particularly cautious in this respect. Presence systems are an emerging class of applications that support collaboration. Through the use of pervasive sensors, these systems estimate user location, activities, and available communication channels. Because such presence data are sensitive, to achieve wide-spread adoption, sharing models must reflect the privacy and sharing preferences of their users. This paper looks at the role that privacy-preserving aggregation can play in addressing certain user sharing and privacy concerns with respect to presence data.

We define conditions to achieve CollaPSE (*Colla*boration *P*resence *S*haring *E*ncryption) security, in which (i) an individual has full access to her own data, (ii) a third party performs computation on the data without learning anything about the data values, and (iii) people with special privileges called "analysts" can learn statistical information about groups of individuals, but nothing about the individual values contributing to the statistic other than what can be deduced from the statistic. More specifically, analysts can decrypt aggregates without being able to decrypt the individual values contributing to the aggregate. Based in part on studies we carried out that illustrate the need for the conditions encapsulated by CollaPSE security, we designed and implemented a family of CollaPSE protocols. We analyze their security, discuss efficiency tradeoffs, describe extensions, and review more recent privacy-preserving aggregation work.

Published by Elsevier B.V.

1. Introduction

Successful collaboration requires information sharing. Myriad communication and collaboration tools enable users to share information anywhere and anytime from a variety of devices. Many of these devices contain sensors that can be leveraged to provide information about a person to their colleagues without the need for the user to take explicit action, improving communication and awareness between colleagues. Modern communication and collaboration tools face a significant challenge: to achieve a delicate balance between sharing enough information to support effective communication and awareness between colleagues while not sharing information that is inappropriate, invasive, or simply not desired. This challenge is particularly salient for systems that share information without requiring an explicit action by a user to initiate the sharing. In this paper, we take a system level approach to addressing this design challenge. We focus on presence systems, but many of our results are more broadly applicable.

Presence systems are an emerging class of applications that support collaboration in both business and social life. They fuse physical sensing capabilities with social and communication software, leveraging pervasive sensors to estimate user location, activities, and available communication channels. Because such presence data are sensitive, to achieve wide-spread adoption, the sharing models underpinning the design of presence systems must reflect the privacy and sharing preferences of the users, especially for the highly charged issue of stored data.

To understand the expectations and preferences of potential users of such systems with respect to how presence data are

* Corresponding author. Tel.: +1 650 367 7145.
E-mail addresses: rieffel@fxpal.com (E.G. Rieffel), biehl@fxpal.com (J.T. Biehl), adamlee@cs.pitt.edu (A.J. Lee), billvm@fxpal.com (W. van Melle).

0167-739X/$ – see front matter. Published by Elsevier B.V.
http://dx.doi.org/10.1016/j.future.2013.05.009

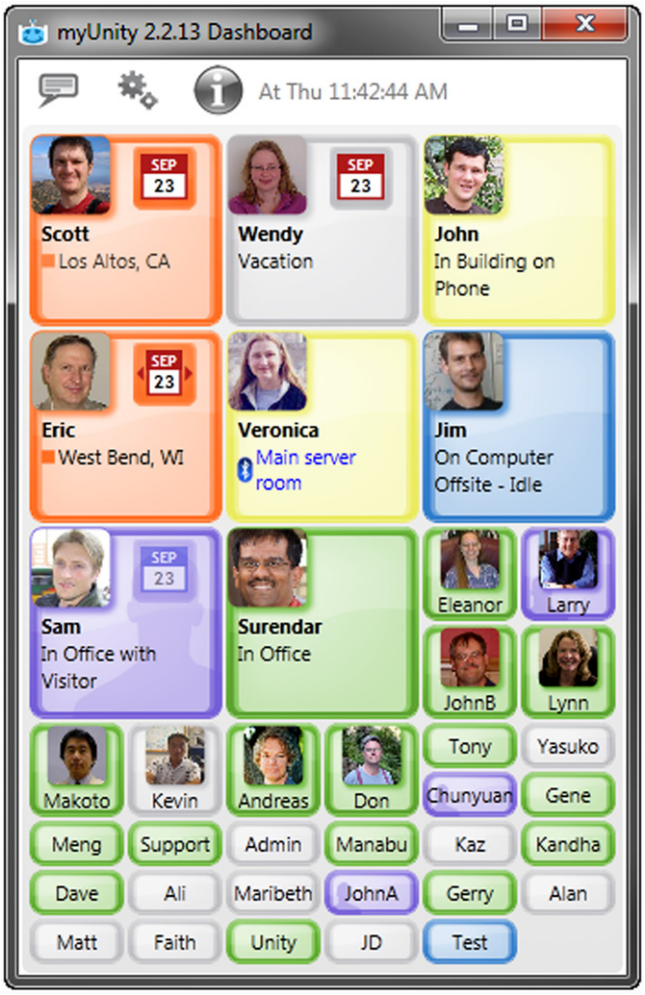

Fig. 1. The myUnity dashboard provides users a quick overview of their colleagues' presence.

shared and used, we conducted a broad survey [1]. One key finding showed that participants were significantly more concerned about long-term retention of presence data than its collection and moment-to-moment sharing. To delve into preferences specifically with respect to stored data, we conducted a second survey, published here for the first time. In this survey, we asked the opinion of longtime users of myUnity [2], a presence system that had been in use by more than 30 users for over two years, on issues related to long-term retention of presence data. At the time, myUnity did not store data, but its users were interested in seeing personal trends, activity patterns of coworkers, and presence patterns of groups of users. MyUnity's designers were also interested in retaining data to analyze usage of the system. We asked myUnity users to rate various possibilities for how presence data could be protected, aggregated, accessed, and shared. These studies suggest that users want full access to their own data, are more comfortable contributing their values to a statistical analysis if they do not have to reveal the individual values even to the analysts, and do not want to reveal their data to entities that they perceive as not having a reason to need their data.

These studies motivate the development of CollaPSE (*Colla*boration *P*resence *S*haring *E*ncryption) security, in which (i) an individual has full access to her own data, (ii) a third party performs computation on the data without learning anything about the data values, and (iii) people with special privileges whom we call *analysts* can learn statistical information about groups of individuals, but nothing about the individual values contributing to the statistic other than what can be deduced from the statistic. More specifically, analysts can decrypt aggregates without being able to decrypt the individual values contributing to the aggregate. This paper is an extended version of [3], which first introduced the conditions for CollaPSE security. That paper described simple, non-interactive, privacy-preserving aggregation schemes that efficiently realize all conditions for CollaPSE security for time-series data, and an implementation, using readily-available cryptographic functions, integrated with the myUnity presence system. While the current implementation does not involve an external third party, its structure would allow commodity cloud services to be used, enabling these solutions to scale to large, distributed organizations.

We begin by providing an overview of the myUnity presence system, and then describe the two studies that motivate the CollaPSE protocols that support privacy-preserving aggregation. The design criteria stemming from these surveys are then crystallized into a problem definition that captures the desired properties of CollaPSE protocols. The architecture and encryption background are reviewed prior to presenting the protocols. Benchmarking results from a prototype implementation are described. The main contributions of this paper beyond that of Rieffel et al. [3] are

- an extended discussion section, which includes a security analysis and a discussion of issues such as efficiency tradeoffs, robustness against missing values, extensions that support differential privacy and more complex structures, as well as
- descriptions of the studies that illustrate the need for and motivate the design of our protocols, and
- a review of recent related work, including further privacy-preserving aggregation protocols and their applications, particularly to the smart meter domain.

Prior to launching into a discussion of the studies that motivate the design of our protocols and the details of the protocols and implementation, we describe the myUnity presence system, which they are designed to enhance.

2. Overview of MyUnity

The past few years have seen a rapid expansion of technologies that fuse physical sensing capabilities with social and communication software. One such system is myUnity [4], a presence system for the workplace that supports collaboration by increasing workers' awareness of their colleagues' physical presence, activities, and preferred communication channels.

MyUnity was designed to expand collaboration opportunities by building group awareness. MyUnity collects data from cameras, Bluetooth device sensors, mouse and keyboard activity, network connectivity, IM availability, and the employee calendar (Fig. 2). At regular intervals, the data are aggregated and summarized into one of five presence states. A sixth state indicates there is insufficient data on the user. Users run clients that display presence states for colleagues as photo tiles within an awareness dashboard (Fig. 1). Each tile's color indicates the user's presence state:

- *purple*: the person *has visitors* in her office.
- *green*: the person is *in her office*.
- *yellow*: the person is *in the building*.
- *blue*: the person is *actively connected remotely*.
- *orange*: the person is *connected via mobile* client.

The system represents each presence state as a five-bit string, in which each bit corresponds to one of the five positive presence states. The six legal presence values are 10000, 01000, 00100, 00010, 00001, and 00000, corresponding to *in office*, *has visitor*, *in building*, *active online remotely*, *connected via mobile client*, and *insufficient information*. The interface displays presence information

Download English Version:

https://daneshyari.com/en/article/425685

Download Persian Version:

https://daneshyari.com/article/425685

Daneshyari.com