Pervasive and Mobile Computing 10 (2014) 22–33

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Secure interaction with piggybacked key-exchange

Wolfgang Apolinarski *, Marcus Handte, Muhammad Umer Iqbal, Pedro José Marrón

Networked Embedded Systems, University of Duisburg–Essen, Duisburg, Germany

ARTICLE INFO

Article history:
Available online 4 November 2013

Keywords:
Key-exchange
Online services
Smart phones

ABSTRACT

Online collaboration tools are a ubiquitous mediator of many human interactions. In the virtual world, they enable secure interaction by controlling access to shared resources. Yet relying on them to support face-to-face collaboration might be suboptimal as they require Internet connectivity. A more efficient way of co-located resource sharing is the use of local communications. Yet setting up the necessary security mechanisms can be cumbersome. In this article we present PIKE and its variant P2PIKE, key-exchange protocols that minimize this configuration effort. Both piggyback the exchange of keys on top of an existing service and exchange keys proactively—before the interaction takes place. In addition to an implementation, we outline two applications and present a thorough evaluation to show the benefits and limitations of our approach.

1. Introduction

Online collaboration tools such as Google+, Facebook or Dropbox have become an important and ubiquitous mediator of many human interactions. In the virtual world, they enable secure remote interaction by supporting restricted sharing of resources such as documents, photos or calendars between users. Users are typically identified with a unique identifier and they authenticate themselves by means of passwords or similar mechanisms.[1] The shared resources can then be tied to different sets of identifiers such as friend lists in Facebook or circles in Google+. To control access to resources, online collaboration tools typically use encrypted communication such as TLS and require authentication upon resource access. Using web-based interfaces, users can access their information from different machines. In addition, many services also provide mobile applications to support access on-the-go and an API for third-party tools to access their resources. Besides providing optimized visualizations, most mobile applications and third-party tools make use of local caching and synchronization to enable disconnected operation.

The success of these collaboration tools indicates that this mediation model can effectively support secure remote interaction. Yet, using them for face-to-face collaboration[2] that takes place in the physical world can be suboptimal. The main reason for this is that such collaboration involves multiple partners that interact with each other *at the same time and place*. In such a setting, the various issues arising from a remote connection – such as higher response times or intermittent connectivity – cannot be hidden by caching and synchronization. A much more efficient way to support online collaboration between co-located partners would be to support their online collaboration by means of short-range wireless communication. However, to provide a similar level of security, this would require encryption and the configuration of

* Corresponding author. Tel.: +49 201 183 2427.
E-mail addresses: wolfgang.apolinarski@uni-due.de (W. Apolinarski), marcus.handte@uni-due.de (M. Handte), umer.iqbal@uni-due.de (U. Iqbal), pjmarron@uni-due.de (P.J. Marrón).

1 Examples are two-factor authentication or client-specific certificates.

2 Here, collaboration is not restricted to work context.

1574-1192/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.pmcj.2013.10.013

corresponding authentication mechanisms. Without a mediating online tool, the co-located interaction partners would have to manually exchange authentication or encryption keys which so far has been too cumbersome to be used in practice.

To avoid this problem, we have designed PIKE, a key-exchange protocol that aims at seamlessly extending the support provided by online collaboration tools to enable wireless collaboration among face-to-face collaborators. The basic idea behind PIKE is to piggyback the exchange of keys on top of the existing service infrastructure of an online collaboration tool in a proactive manner. Thereby, we eliminate the need for manual configuration as well as Internet connectivity when the interaction takes place locally.

A prototype application scenario for PIKE is a business meeting for which invitations are shared over a secure connection using Google Calendar. When detecting the invitations, PIKE automatically exchanges keys over the Internet using the Google infrastructure and stores them locally on each partner's device. When the meeting takes place, the keys can be used to establish secure wireless LAN communication among the participants' devices or to authenticate participants without requiring any Internet connectivity. A second scenario envisions two friends that meet spontaneously in the city. Using their smart phones, they want to interact and transfer data (e.g., pictures) securely. A variant of PIKE, P2PIKE enables them to use automatically exchanged peer-to-peer keys to set-up a secure communication.

The contribution of this article is threefold. First, we introduce PIKE and its peer-to-peer variant P2PIKE as approaches for enabling non-mediated, secure and configuration-free face-to-face collaboration. Second, we describe the implementation of PIKE and P2PIKE as an extensible Android library that integrates with wireless tethering to enable the fully automatic establishment of a secure wireless LAN. Third, we present several applications and an analytical as well as an experimental evaluation indicating that both PIKE and P2PIKE are broadly applicable and (at least) as secure as the underlying online service.

2. Approach

Our goal with PIKE is to support local collaboration in a configuration-free and secure manner that does not require Internet connectivity during the time the interaction takes place. To achieve this, PIKE exchanges keys piggybacked on an existing service infrastructure before the interaction takes place. This key-exchange is typically triggered by a virtual representation of the upcoming interaction such as a meeting entry in a calendar. Additionally, it can be performed with all known users of an online service that use PIKE (e.g., Facebook friends running the PIKE app). The exchanged keys can then be used by applications to secure a wireless LAN communication, e.g., by means of encryption or message authentication.

2.1. System model and assumptions

The technical basis for PIKE are mobile *devices*, such as phones, tablets or laptops that share *resources* with each other remotely through a *network*, mediated by a *service*. Regarding these four building blocks we assume:

- *Services:* The service enables secure restricted sharing of resources. This means that the service authenticates its users, models relationships between different users with respect to resource usage and enables the specification and enforcement of access rights. The service performs its access control to resources properly, meaning that (a) it protects the resources from being accessed by illegitimate users and (b) it allows access from legitimate users. Yet, beyond proper service operation, we do not assume that the service is necessarily trustworthy. Examples may be Facebook, Google+or Dropbox.
- *Network:* A network such as the Internet enables devices to access the service regularly. The network may be insecure and, occasionally, it may be unreliable or unavailable, e.g., due to a network outage, an incomplete coverage or unaffordable roaming fees.
- *Devices:* The user's device is able to access the service regularly through the network. For this, the service uses a mobile application that synchronizes the changes to a shared resource or provides an API that can be used for resource synchronization.
- *Resources:* Some of the resources shared between users can be read and edited not only by the creator but also by the interaction partners. For PIKE, we assume that some of the shared resources are used to plan a face-to-face collaboration and thus provide time information. Examples for such resources are a calendar entry or a message indicating an upcoming meeting. Using P2PIKE, this assumption can be dropped. In Section 2.3.2, we describe the necessary changes to PIKE.

2.2. Design rationale and goals

Besides achieving the functional goal of exchanging keys, the desire to maximize PIKE's and P2PIKE's applicability for various types of face-to-face collaboration defines the following design goals.

- *Full automation:* To minimize the time required by interaction partners to set up secure communication, PIKE should not require manual configuration. Instead, the key-exchange performed by PIKE should be fully automated such that it becomes transparent to them.
- *High security*: In order to truly protect the interactions between the devices, key-exchange with PIKE must be secure. Given that the collaboration partners are already using an online collaboration service through remote interaction in