Pervasive and Mobile Computing 16 (2015) 205–219

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

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

Commitment-based device-pairing protocol with synchronized drawings and comparison metrics☆

Markku Antikainen [a,*], Mohit Sethi [a,b], Sinisa Matetic [a], Tuomas Aura [a]

[a] Aalto University, Finland

[b] Nomadiclab, Ericsson Research, Finland

ARTICLE INFO

Article history:
Available online 31 October 2014

Keywords:
Security
Device pairing
Commitment protocol
Edit distance

ABSTRACT

This article presents a new method for pairing devices securely. The commitment-based authentication uses a fuzzy secret that the devices only know approximately. Its novel feature is time-based opening of commitments in a single round. We also introduce a new source for the fuzzy secret: synchronized drawing with two fingers of the same hand on two touch screens or surfaces. The drawings are encoded as strings and compared with an edit-distance metric. A prototype implementation of this surprisingly simple and natural pairing mechanism shows that it accurately differentiates between true positives and man-in-the-middle attackers.

1. Introduction

Secure device pairing, which enables easy creation of long-term associations as well as ad-hoc transactions between personal computing devices, is an important and widely studied area [1]. The key challenge in device pairing is to allow two devices to securely identify and authenticate each other without having any a-priori shared information. Several communication technologies, such as Bluetooth [2], WiFi [3], and ZigBee [4], require the user to enter the same key string or authentication code to both devices or to compare and approve codes displayed by the devices. While these methods can provide reasonable security, they require user interaction that is relatively unnatural and often considered a nuisance. Thus, there is an ongoing quest in pervasive computing research for more natural ways of pairing devices. The method proposed in this paper, synchronized drawing with two fingers on touch-sensitive surfaces, continues this work in a world where touch screens and surfaces have become increasingly ubiquitous.

To reduce the amount of user interaction required in the pairing process, several proposals use contextual or location-dependent information, or natural user input such as sound or movement, for the authentication. The proposed protocols perform pairing by utilizing a shared *fuzzy* secret that the devices only know approximately. This shared secret may be extracted, for example, from ambient audio or radio signals [5–7] or from simultaneous sensing of user actions. As an example, Mayrhofer [8] as well as Kirovski et al. [9] derive a shared fuzzy secret from the user shaking or moving the two devices together. In such protocols, a major challenge is to establish an exact shared cryptographic key starting from two noisy and, thus, slightly differing measurements of sensor data. In this paper, we overview the existing methods for establishing a shared secret from noisy input and propose a new protocol, which is a single-round, time-based variant of the existing commitment protocols.

☆ This is an extended version of a paper that appeared in PerCom 2014 (Sethi et al. (2014)).

* Corresponding author.

E-mail addresses: markku.antikainen@aalto.fi (M. Antikainen), mohit.sethi@aalto.fi (M. Sethi), sinisa.matetic@aalto.fi (S. Matetic), tuomas.aura@aalto.fi (T. Aura).

http://dx.doi.org/10.1016/j.pmcj.2014.10.006

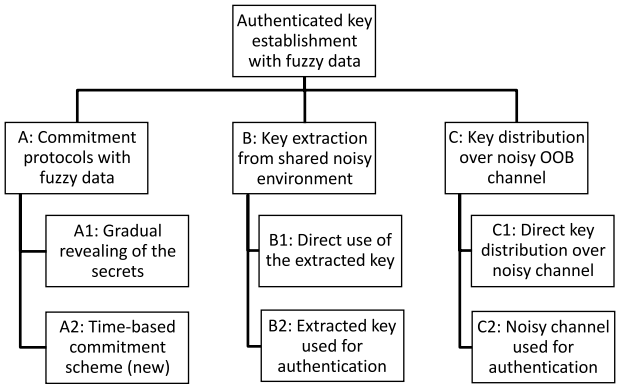

Fig. 1. Taxonomy of key-establishment with fuzzy data.

We start in Section 2 by providing an overview and taxonomy of existing key-establishment methods that use fuzzy shared secrets for authentication. In Section 3, we derive a new time-based variant of the commitment-based key establishment. Section 4 presents the novel human-assisted pairing mechanism that uses synchronized drawings as the fuzzy shared secret. We implement a prototype and evaluate the security of this pairing mechanism. In particular, we evaluate various metrics for comparing the drawings and find an efficient metric based on string edit distance. Section 5 discusses the security of the proposed scheme. Finally, Section 6 concludes the paper.

2. Background

This section explains the threat model used throughout the paper (Section 2.1) and provides a survey and taxonomy of existing solutions for *authenticated key-establishment with fuzzy data* (Section 2.2). We consider protocols that tolerate errors in the data from which they derive a shared secret key.

2.1. Threat model

The use case for authenticated key-establishment with fuzzy data is relatively simple: two devices that communicate over an insecure network, such as a wireless link, need to establish a shared secret key. The devices also have access to an out-of-band (OOB) channel, which has a high error rate. The errors may be caused, for example, by external noise on the channel or by differences in the sensory inputs of the two devices. The noisy channel may be used either to send messages between the devices or to receive the same external signal. A wide range of key-establishment protocols have been proposed based on different types of noisy channels such as ambient sound or radio signals [5,10,11].

The goal of a pairing mechanism is to establish a shared secret key that can be used to secure subsequent communication over the insecure network. The security analysis of this paper assumes a powerful Dolev–Yao type attacker on the insecure network [12]. The noisy OOB channel, on the other hand, is assumed to provide some inherent protection for the confidentiality and integrity of data. This may be, for example, because the channel is location limited and under the direct supervision of the user. The attacker aims to subvert the authentication and access the subsequent communication over the insecure network either by passively eavesdropping it or by actively impersonating one or both of the devices.

2.2. Related work

In the following, we divide the related work into the categories illustrated in Fig. 1.

2.2.1. Commitment-based protocols

Commitment-based protocols (category A in Fig. 1) are the closest equivalent to the new protocol proposed in this paper. The earliest protocol to use commitment for protecting the integrity of communication against man-in-the-middle attacks was the interlock protocol by Rivest and Shamir [13]. While it makes use of encryption rather than hash functions, the principle is similar to the modern protocols. Later, commitment-based protocols were developed for authentication with a short one-time secret. As we will see, these can be modified to work equally well with a fuzzy (i.e. noisy) secret.

These protocols begin with an unauthenticated key exchange, such as Diffie–Hellman or public-key encryption without certificates. The resulting strong, fresh (but initially unauthenticated) shared key k is then authenticated to prevent spoofing and man-in-the-middle (MitM) attacks. For this purpose, the devices share a short secret p, such as a 6-digit number, distributed over an out of band channel. In the *commitment phase* of the authentication, the devices exchange cryptographic commitments to the values of the short secret and the fresh shared key. A commitment is a cryptographic hash $H(k, p, r)$, where r is a fresh random number needed for blinding the secrets. In the *opening phase*, both sides reveal their random numbers r and verify that hash sent by the other party in the first phase is correct.