Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Location leakage in distance bounding: Why location privacy does not work

Aikaterini Mitrokotsa [a,*], Cristina Onete [b], Serge Vaudenay [c]

[a] Chalmers University of Technology, Gothenburg, Sweden
[b] IRISA/INRIA, Univ. Rennes 1, Rennes, France
[c] EPFL Lausanne, Switzerland

ARTICLE INFO

Article history:
Received 27 July 2013
Received in revised form
24 February 2014
Accepted 2 June 2014
Available online 12 June 2014

Keywords:
Location privacy
Distance-bounding
Authentication
Location indistinguishability
Relay attacks

ABSTRACT

In many cases, we can only have access to a service by proving we are sufficiently close to a particular location (e.g. in automobile or building access control). In these cases, proximity can be guaranteed through signal attenuation. However, by using additional transmitters an attacker can relay signals between the prover and the verifier. Distance-bounding protocols are the main countermeasure against such attacks; however, such protocols may leak information regarding the location of the prover and/or the verifier who run the distance-bounding protocol.

In this paper, we consider a formal model for location privacy in the context of distance-bounding. In particular, our contributions are threefold: we first define a security game for location privacy in distance bounding; secondly, we define an adversarial model for this game, with two adversary classes; finally, we assess the feasibility of attaining location privacy for distance-bounding protocols. Concretely, we prove that for protocols with a beginning or a termination, it is theoretically impossible to achieve location privacy for either of the two adversary classes, in the sense that there always exists a polynomially-bounded adversary winning the security game. However, for so-called limited adversaries, who cannot see the location of arbitrary provers, carefully chosen parameters do, in practice, enable computational location privacy.

1. Introduction

Often, our location is critical in order to gain access to places and/or services. For instance, in applications such as automobile access control the key (prover) needs to be close enough to the car lock (verifier) in order to unlock it (Ford, 2011). In some cases, unlocking the car may in fact also start the car (in passive keyless entry and start (PKES) systems (Francillon et al., 2010)). If the proximity check is performed through signal attenuation, an adversary may easily perform man-in-the-middle attacks by relaying messages between the communicating parties (provers and verifiers), while these parties are situated far from each other. Thus, in the automobile example, an adversary may unlock the car even if the car key (the prover) is located very far. This type of attack (called mafia fraud (Desmedt, 1988)) can also be mounted against bankcards (Drimer and Murdoch, 2007), mobile

* *Corresponding author.*
E-mail addresses: aikaterini.mitrokotsa@chalmers.se (A. Mitrokotsa), maria-cristina.onete@irisa.fr (C. Onete), serge.vaudenay@epfl.ch (S. Vaudenay).
http://dx.doi.org/10.1016/j.cose.2014.06.001
0167-4048/

phones (Francis et al., 2010), proximity cards (Hancke et al., October 2009), and wireless ad-hoc networks (Hu et al., 2006; Poturalski et al., 2008).

Distance-bounding (DB) protocols are meant to counteract man-in-the-middle relay attacks in authentication schemes. They are challenge-response authentication protocols, that allow the verifier, by measuring the time-of-flight of the messages exchanged, to calculate an upper bound on the prover's distance (as well as checking the validity of the responses which usually ensure authentication). DB protocols were first introduced by Brands and Chaum (Brands and Chaum, 1993) to preclude relay attacks in ATM systems. Subsequently, numerous DB protocols were proposed (Kim et al., 2008; Reid et al., 2007; Bussard and Bagga, 2004) and many attacks against them have been published (Bay et al., 2012; Boureanu et al., 2012; Fischlin and Onete, 2013a; Boureanu et al., 2013c, 2013a). DB protocols have also been analysed for the case of noisy channels (Mitrokotsa et al., 2010) and the optimal setting of security parameters (Dimitrakakis et al., 2012; Mitrokotsa et al., 2013). To the best of our knowledge (Boureanu et al., 2013b; Boureanu et al., 2013) describes the latest most secure distance-bounding protocol against all known attack modes. Another provably-secure protocol attaining quite strong terrorist-fraud resistance requirements has been recently published in Fischlin and Onete (2013b).

Location privacy was introduced in the context of distance bounding by Rasmussen and Čapkun (2008), who noted that distance-bounding protocols may leak further location-related information than just the fact that the prover is within the maximum allowed distance from the verifier. This information leakage follows from the measurement of the messages' arrival times.

To combat this, Rasmussen and Čapkun (2008) proposed a privacy-preserving distance-bounding protocol (denoted here as the RČ protocol). Though the protocol in Rasmussen and Čapkun (2008) claims to preserve location privacy, we note that location privacy has never been formalized in the literature. Additionally, the RČ protocol has been shown to be susceptible to a non-polynomial dictionary attack which may reveal the prover's and verifier's locations (Aumasson et al., 2011) as well as to a *mafia fraud* attack (Mitrokotsa et al., 2012). Mitrokotsa et al. (2012) have proposed a new distance-bounding protocol called *Location-Private Distance Bounding* (LPDB) that improves the basic construction of the RČ protocol and renders it secure against the latter attack.

Distance bounding can also be extended to location verification (Singelée and Preneel, 2005) (also known as secure positioning (Sastry et al., 2003)), where multiple verifiers interact with a single prover. In that case the location of the prover can be determined using the intersection of the bounding spheres surrounding each verifier. This approach is also taken under consideration in the recent work regarding position-based cryptography (Chandran et al., 2009). Our approach here is different as we consider a single verifier and many provers, and we thus only achieve distance bounding, and not secure positioning. Moreover, in position-based cryptography all the adversaries have the same knowledge as the prover, including the secret key. However, in our model, we do not allow the adversary knowledge of the secret key, as that would allow it to trivially distinguish between the two provers in the location privacy game, without actually requiring any location data.

We also mention the recent work on localisation privacy by Burmester (Burmester, 2011; Burmester and Naccache, 2012), where location is used in a steganographic sense (such that provers are convinced that verifier-generated challenges are honest, and they do not reveal their presence to adversaries). However, very notably the constructions in Burmester and Naccache (2012) require provers to be aware of their position/location, which is a strong assumption in generic authentication/distance-bounding scenarios. In this case, location is used as a part of the verifier's challenge, and the prover verifies that the location is sufficiently close to its own location.

1.1. *Contributions*

In this paper, we address precisely the topics of location privacy in distance-bounding. Our contributions are threefold:

1. We first define a classical left-or-right *indistinguishability* game for location privacy in distance-bounding protocols. In this game, the adversary knows its distance to the verifier $\mathcal{V}$ and can create provers $\mathcal{P}$ at arbitrary distances from itself and $\mathcal{V}$.
2. For this location privacy game, we consider two main adversarial classes: *omniscient* and *limited* adversaries. *Omniscient* adversaries capture an adversary that can measure the signal strength of the transmitted messages and is aware, for all transmissions along the timed channel, when the message is sent and when it arrives at its own interface. Unsurprisingly, no location privacy is feasible for omniscient adversaries. *Limited* adversaries, on the other hand, are only aware of the time at which they receive messages from other participants.
3. Finally, we show that achieving location privacy with respect to limited adversaries is impossible for protocols with a beginning or a termination, and which run in polynomial time. We prove that location privacy against limited adversaries minimally requires the prover and the verifier to introduce exponential delays between receiving and sending messages, and we give a lower bound for these delays. Since the transmission speed is high (e.g. the speed of light in the case of RFID transmissions), the delay can be implemented in practice. Finally, we show how to specify these delays in the LPDB protocol proposed in Mitrokotsa et al. (2012).

1.2. *Organization*

This paper is organized as follows. We begin by defining distance-bounding protocols and location privacy in Section 2, outlining also our adversarial classes. We then assess the feasibility of achieving location privacy for distance-bounding protocols in Section 3, for both *omniscient* and *limited* adversaries, giving a lower bound for the delays that each party must have between receiving a message and sending a response message. We apply our results and the obtained