Computer Communications 67 (2015) 92–102

Contents lists available at ScienceDirect

Computer Communications

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

Comparing distance bounding protocols: A critical mission supported by decision theory

Gildas Avoine[a,b], Sjouke Mauw[c], Rolando Trujillo-Rasua[c,*]

[a] INSA Rennes, IRISA UMR 6074, Institut Universitaire de France, France
[b] Université Catholique de Louvain, Belgium
[c] CSC, Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg

ARTICLE INFO

Article history:
Received 3 March 2015
Accepted 12 June 2015
Available online 19 June 2015

Keywords:
Authentication
Distance bounding
Comparison
Decision making
Relay attack

ABSTRACT

Distance bounding protocols are security countermeasures designed to thwart relay attacks. Such attacks consist in relaying messages exchanged between two parties, making them believe they communicate directly with each other. Although distance bounding protocols have existed since the early 1990s, this research topic resurrected with the deployment of contactless systems, against which relay attacks are particularly impactful. Given the impressive number of distance bounding protocols that are designed every year, it becomes urgent to provide researchers and engineers with a methodology to fairly compare the protocols in spite of their various properties. This paper introduces such a methodology based on concepts from the decision making field. The methodology allows for a multi-criteria comparison of distance bounding protocols, thereby identifying the most appropriate protocols once the context is provided. As a side effect, this paper clearly identifies the protocols that should no longer be considered, regardless of the considered scenario.

1. Introduction

Distance bounding protocols are the most popular countermeasures against relay attacks. In a relay attack on an authentication protocol, an adversary aims to convince the verifier that he directly communicates with the genuine prover, while the adversary is actually in the middle and relays the messages exchanged between the two parties. Typically, a relay attack makes the verifier believe the prover is located within his neighborhood while he is far away.

1.1. Relay attacks

Conway [15] introduced in 1976 the concept of a relay attack through the *Chess Grandmaster problem* where a little girl is challenged to defeat a Chess Grandmaster in correspondence chess. The solution suggested by Conway to allow the little girl to be successful is to perform a relay attack between two Chess Grandmasters: the attack consequently consists in relaying the moves received between the two Chess Grandmasters, which results for the little girl in either a won or two draws.

Relay attacks also apply to authentication protocols as originally proposed by Desmedt, Goutier, and Bengio at Crypto 87 [17], whose work was later extended by Brassard and Quisquater in [7]. In their papers, the authors refuted Shamir's claims about the Fiat–Shamir protocol [18] when he says that the protocol is secure even when being executed one million times in a Mafia-owned store [21]. Desmedt et al. indeed raised that a relay attack is still possible, and they consequently named the suggested relay attack *mafia fraud*. Since then, both terms, relay attack and mafia fraud, are used interchangeably in the literature. Note however that Avoine et al. [1] distinguish mafia fraud from relay attacks by considering that the adversary cannot modify the forwarded messages in a relay attack. This distinction allows for representing an adversary who does not know the specifications of the considered protocol.

Although mafia fraud was suggested late in the 1980s, practical implementations of this type of fraud appeared much later. Mafia fraud actually became a real threat with the ubiquity of contactless technologies. For example, practical attacks were developed against Radio Frequency IDentification (RFID) [22,23], Near Field Communication (NFC) [20], and Passive Keyless Entry and Start Systems (PKES) in modern cars [19]. For example, off-the-shelves devices to perform relay attacks against PKES can be bought on Internet [12].

1.2. Distance bounding protocols

Mafia fraud does not rely on exploiting security protocol vulnerabilities. Conventional security mechanisms are thus ineffective against it. Based on an idea from Beth and Desmedt [8], Brands and

* Corresponding author. Tel.: +352 466 644 5458; fax: 466 644 3 5458.
E-mail address: rolando.trujillo@uni.lu, rolando.trujillo@gmail.com (R. Trujillo-Rasua).

http://dx.doi.org/10.1016/j.comcom.2015.06.007
0140-3664/

Chaum suggested a countermeasure to mafia fraud that consists in measuring the Round-Trip-Time (RTT) of 1-bit messages exchanged between the parties, using a dedicated communication channel [10]. In their solution, the verifier measures the round-trip time t_m between the moment he sends a challenge and the moment he receives the response from the prover. The verifier can consequently estimate a tight upper-bound on the distance between the prover and the verifier by computing $d = c \cdot (t_m - t_d)/2$, where c is the speed of light and t_d is the delay induced by the prover to compute the response, given the challenge.

Note that distance bounding protocols do not detect relay attacks in a strict sense. Instead, they detect unexpected delays, and conclude in such a case that a mafia fraud attack might have occurred. As a consequence, neither the communication channel, nor the calculation should introduce flexible timing during the protocol execution, since that could be exploited by an adversary. For example, requiring the prover to perform heavy computations in passive contactless systems may allow an adversary to significantly reduce t_d by overclocking the prover's device, which in turn may allow the adversary to increase t_m without making d above the expected upper-bound. Since Desmedt et al.'s seminal work [8], a conservative assumption for designing distance bounding protocols consists in considering minimally sized messages (typically 1-bit messages) and lightweight computations during the time-measurement phase.

1.3. Protocol evaluation

Avoine et al. introduced in [1] a *Framework* for analyzing distance bounding protocols. This widely used Framework defines four types of fraud that should be considered in the security evaluation of distance bounding protocols. For the sake of accuracy, the fraud definitions from [1] are provided *in-extenso* below.

- Given a distance bounding protocol, an *impersonation fraud* attack is an attack where a lonely prover purports to be another one.
- A *mafia fraud* attack is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle (MITM) between the reader and an honest tag located outside the neighborhood.
- Given a distance bounding protocol, a *distance fraud* attack is an attack where a dishonest and lonely prover purports to be in the neighborhood of the verifier.
- A *terrorist fraud* attack is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle (MITM) between the reader and a dishonest tag located outside of the neighborhood, such that the latter actively helps the adversary to maximize her attack success probability, without giving to her any advantage for future attacks.

The security evaluation of a distance bounding protocol then consists in computing the resistance of the protocol for every type of fraud, which is done by computing the probability for an adversary to successfully perform the considered fraud.

Since Brands and Chaum's breakthrough, many distance-bounding protocols have been proposed,[1] which deliver improvements in terms of security (see Section 2). These proposals also introduce new requirements on the protocols, e.g., to be usable on noisy channels, and properties, e.g., to be more computationally efficient or to require less memory. Given the various requirements and properties, a fair methodology to compare distance bounding protocols is strongly needed.

[1] http://www.avoine.net/rfid/.

Table 1
List of protocols and their acronyms.

Authors	Reference	Year	Acronym
Brands and Chaum	[10]	1993	BC
Čapkun, Buttyán,and Hubaux	[13]	2003	MAD
Bussard and Bagga	[11]	2005	BB
Hancke and Kuhn	[24]	2005	HK
Munilla and Peinado	[28]	2006	MP
Kim, Avoine, Koeune, Standaert, and Pereira	[27]	2008	Swiss-Knife
Avoine and Tchamkerten	[5]	2009	Tree-based
Trujillo-Rasua, Martin, and Avoine	[33]	2010	Poulidor
Rasmussen and Čapkun	[29]	2010	RC
Yum, Kim, Hong and Lee	[34]	2010	YKHL
Kim and Avoine	[26]	2011	KA
Boureanu, Mitrokotsa, and Vaudenay	[9]	2013	SKI
Trujillo-Rasua, Martin, and Avoine	[31]	2014	TMA

1.4. Contribution

This paper introduces a methodology based on concepts from the decision making field to perform a multi-criteria comparison of distance bounding protocols. The methodology identifies the most desirable protocols, given a set of required properties, and disqualifies protocols that are dominated by better solutions whatever the considered properties. Even though the methodology can be understood without difficulty, applying it on a large set of distance bounding protocols may be time-consuming. As a consequence, an open-source computer tool was released in order to easily include into the comparison future distance bounding protocols and new criteria.

2. Background

Distance bounding protocols are authentication protocols that, in addition, compute an upper bound on the distance between the prover and the verifier. Since we focus on the distance bounding properties of such protocols, we ignore any such protocol that does not even achieve authentication, e.g., due to impersonation attacks or key-recovery attacks [30]. The considered protocols are briefly introduced and classified according to their main features, which are the features that occur most frequently in literature and that should be taken into account to compare the protocols. The protocols are listed in Table 1.

2.1. Compared protocols

2.1.1. Resistance to mafia and distance fraud

The earliest distance bounding protocol, introduced by Brands and Chaum in 1993 [10], consists of an initial commitment phase, followed by n rounds where the verifier sends a single-bit challenge and receives a single-bit response from the prover. The protocol is then completed with a final phase where the commitment is opened and a signature of the exchanged messages is provided by the prover. The phase during which the round trip time (RTT) is measured is known as being the *fast phase* while the other ones are known as the *slow phases*. The BC protocol, provided in Algorithm 1, reaches the optimal security bound $(1/2)^n$ against both mafia and distance fraud, where n is the number of rounds.[2] The authors, however, left as an open problem the design of a distance-bounding protocol that resists to terrorist fraud as well.

2.1.2. Resistance to terrorist fraud

The challenge of designing a protocol resistant to terrorist fraud was taken up later in 2005 by Bussard and Bagga [11], who proposed

[2] For every distance bounding protocol with a single fast phase consisting of n rounds of 1-bit exchanges, an adversary who answers randomly during the fast phase and relays all the other messages succeeds with probability $(1/2)^n$ [1].