RFID Distance-Bounding: What is Wrong and How to Fix it

Abstract. Radio Frequency Identification (RFID), the technology for contactless transmission of data between small devices and readers, penetrates more and more our daily life. The technology is nowadays used in passports, transponder keys, or logistics, usually as a mean to identify the tag to the reader. Security solutions for such devices are often vulnerable to so-called man-in-the-middle (MITM) attacks where an adversary tries to impersonate as the device by communicating with the actual RFID tag while talking to the reader, relaying the tag's data to the reader. Such attacks have been reported in practice, e.g., for the HB protocol, for smartcards, and even for Passive Keyless Entry and Start (PKES) systems in cars [14]. Distance-bounding protocols aim at impeding such attacks by measuring response times: MITM attacks are supposed to take larger response times than executions with the actual tag. So far, many proposed protocols have later been broken, which we attribute to a lack of profound models and formal security claims. In this work we thus give an overview of distance-bounding RFID modeling and design issues. More concretely, we compare the two prominent models in [2,13], assessing how far the definitions capture the intuition behind them. Finally, we describe how to achieve distance bounding security, giving an overview of the techniques most often used in practice.

1 Introduction

Man-in-the-middle attacks (MITM) are powerful strategies against authentication and identification schemes. Authentication protocols are run between a prover and a verifier, where the prover attempts to prove its legitimacy to the verifier. Security is achieved if an illegitimate prover (or adversary) is unable to impersonate a legitimate one. However, as [10] observed, all authentication protocols are vulnerable to man-in-the-middle attacks where the adversary that simply relays transmissions between an honest prover and an honest verifier. This adversary always succeeds in impersonation attempts; pure relaying of messages is called mafia fraud following [10]. Mafia fraud is particularly relevant for environments with no certificates or trusted third parties, such as, e.g., Radio Frequency Identification (RFID) as defined in [18,8,11,17,14].

Though resource constrained, RFID tags are cost-efficient, widely used in logistics, public transport, club membership cards, and even personal

identification. They are also more vulnerable to attacks, however, as shown by [14], who mounted two separate attacks on the Passive Keyless Entry and Start (PKES) systems in cars; both attacks are based on inexpensive relaying of messages to and from honest provers. In fact, these attacks form only the tip of a very large iceberg: we mention, amongst other implementations, the attacks on the HB protocol: [22,16,12,5,31,27]. For an overview of RFID security see [23].

As a potential remedy against MITM attacks (especially mafia fraud), [4] introduced distance-bounding protocols. The crucial idea is that pure relaying produces a processing delay inside the MITM adversary, which can be detected by measuring the prover's response time to a verifier's challenge on the clock. If the measured time exceeds a predetermined threshold, then the verifier suspects a MITM attack and rejects the authentication attempt.

Distance-bounding protocols as introduced by Brands and Chaum are a succession of fast (time-critical) rounds, using the clock, and a slow (lazy) phase without the clock. Some recent constructions, such as the Swiss-knife protocol [26], have two lazy phases, one before, and one after the time-critical phases. Since its introduction, distance bounding, especially for RFID, has incited numerous publications, e.g., [1,2,**?**] [3,4,6]; [36,7,8]; [10,11,13,17,18]; [20,25,33,34,35], also identifying different attack types and desirable security properties in this context.

The classical security of RFID distance-bounding protocols consists of four properties, resp. attacks: (1) mafia fraud, where MITM adversaries must authenticate to the verifier in the presence of an honest prover (however, pure relaying strategies are prevented by the use of the clock); (2) terrorist fraud, where provers help the adversary offline (but do not forward critical data e.g. the secret key); (3) distance fraud, where provers claim to be closer than they actually are; and (4) impersonation resistance, where the adversary attempts to impersonate the prover in the lazy rounds, without relaying.

Attacks (1)–(3) above are described by the following example in [13]. Let Alice hold the unique key (an RFID transponder) to a gym locker (with an RFID reader). One evening, Alice is not at the gym, but at a party. For *mafia fraud*, the MITM consists of two parties: Bob and Bobette. Bob is at the gym, by the locker; Bobette is at the party with Alice. Now Bob and Bobette relay messages between the locker and Alice's tag, trying to open the locker for Bob (without Alice's consent). If, however, Alice and Bob are friends, she may *allow* Bob to use her locker that evening. This is *terrorist fraud*: Alice helps Bob authenticate, but wants to ensure that Bob cannot authenticate *without* her help, this or any other time. Bobette is not needed here, as Alice volunteers information herself. Finally, if Alice parked her car in a bad spot, she might want to "prove" that she was at the gym instead

(she has a unique key token, thus if the locker is opened, she must have been there). Alice's goal now is to pretend she is closer to the reader than she actually is. This is *distance fraud*.

A timeline of distance-bounding developments. There are two general aspects related to distance bounding: protocol development and formal modelling. After the initial, informal definition of mafia fraud by [10], there followed the constructions by [4], which laid the groundwork of distance-bounding protocol design. As a side-branch, we mention the HB authentication (not distance-bounding protocol) published by [22]. This lightweight authentication protocol can be used in resource-constrained devices, and it fuelled research into RFID authentication. [20] next published a distance-bounding protocol which claimed to achieve mafia and distance fraud resistant. However, without a formal model, both properties are proved according to an informal understanding of mafia and distance fraud, by using a metric called the false acceptance rate (FAR). This metric indicates the rate at which an adversary is accepted by the verifier as legitimate and within distance. The same metric is used in subsequent protocols by [6], [33], [3], [25], and by [26].

Initially, no distance-bounding protocol had offline authentication as in property (4) above; this idea was introduced by [3]. Also, terrorist fraud resistance appears in much fewer constructions than mafia and distance fraud resistance; this rare property is achieved in e.g.[6,33,26] by relating impersonation attempts, such that the tag's offline help also leaks (information about) a long-term secret key. Thus, the dishonest tag that provides offline assistance to the adversary cannot control the adversary's access, contrary to terrorist fraud requirements. Terrorist fraud resistance is also proved by using the FAR and an informal description of the notion. Using such notions, Reid et al. claim that terrorist fraud resistance implies distance fraud resistance.

Despite extensive research in distance-bounding protocols, however, allegedly secure protocols are still proved vulnerable to attacks. Indeed, in 2011, [1] showed attacks against the Hitomi and NUS protocols. It is a matter of some concern that such attacks are still possible, even when constructions are proved secure by using the FAR.

The first formal model defining the four threats above is due to [2], and it aims to enforce a formal treatment of distance-bounding threats and ensure provable security and uniform proofs. The framework introduces both a black- and a white-box model for the four attacks, depending on whether the prover may access the algorithm's implementation or not. Amongst other results, Avoine et al. prove that terrorist fraud resistance implies distance fraud resistance in both the black and the white box model. However, the

recent model of [13], also formalizing the four properties, proves that they are independent.

We stress that the two results do not contradict each other *as the frameworks are different*. The apparent contradiction stems from the assumptions of the two frameworks. Notably, Avoine et al. specifically aim to provide a *generic* model, including only the more popular and best known adversary strategies, and providing *minimum* requirements from distance-bounding protocols. By contrast, Dürholz et al. show a much more formal treatment, and the security notions are defined exactly, quantifying the adversary's interactions with the RFID system (by eavesdropping on sessions between the reader and the tag, or by interacting with either of the two). The formalization of terrorist fraud resistance in [13] is in particular stronger than that informally used in distance-bounding protocols.

Thus, the different results proved by the parallel frameworks of [2] and [13] reflect the approaches they take to defining mafia, terrorist, and distance fraud. However, it is crucial for distance-bounding protocol design to understand the limitations of the respective security frameworks and compare the provable security properties of different schemes.

In fact, many distance-bounding protocols aim to resist one (or more) of the above threats, e.g. the mafia and distant fraud resistant constructions by [4,20,3,25], and the terrorist fraud resistant constructions of [33,26,6]. We also note that mafia fraud has been implemented in many flavours in the literature – [11,14,15,21,18,19,24,28,30]; of particular importance to RFID authentication are the implementations against RFID systems and the ISO 14443 standard [14,15,21,18,19,30].

Contributions. In this work we survey recent achievements in RFID distance-bounding. In particular, we show how the notions are formalized in the two recent models by [2] and [13], comparing how far they capture intuition. Noting that Avoine et al. have considered both a black and a white box security model, we also describe the differences between the two models and how the work of [13] fits into this division. We also discuss how to achieve the notions in general.

2 Preliminaries

The general scenario in distance-bounding usually considers a single prover (e.g. an RFID tag) and a single verifier (e.g. an RFID reader) – as in authentication protocols. Recently [9] also considered scenarios with two provers, one honest and one dishonest; here, however, we focus on classical distance-bounding scenarios, with one reader and one tag, sharing a secret key sk generated by a key generation algorithm Kg. Following the idea of [4], the

reader is equipped with a clock that can measure the time-of-flight between the sending-time of the reader's challenge and the receiving-time of the response. Most distance-bounding protocols are round based, where the rounds are fast (time-critical) if the verifier clocks the roundtrip time, or slow (lazy) if the clock is not used; still, a round-based description is not comprehensive, as some distance-bounding protocols, e.g. the one in [32], are not round based.

[2] define distance-bounding as authentication plus distance checking. Authentication as in [29] is a process by which the verifier is assured of both the identity of the prover and of the fact that the prover has participated in the process. This definition thus excludes replay attempts (when the prover does not actively participate). We note that this definition is not sufficient to describe distance bounding, as mafia fraud is a man-in-the-middle attack where the adversary relays information between a legitimate prover and a legitimate verifier and can thus authenticate (i.e. the prover does that active part in the authentication, although it is not aware of it). Distance checking is defined in [2] as a process by which the verifier may compute a function of the distance between itself and the prover at the end of the protocol. Thus, distance-bounding protocols are run between a single prover and a single verifier and at the end the verifier: (i) is convinced of the prover's identity; (ii) is convinced that the prover actively participated in the protocol; and (iii) can compute the upper-bound of the distance between itself and the prover. The security notions for distance-bounding protocols are called *correctness* (i.e. when no attack occurs, the verifier accepts if the legitimate prover is within an agreed-upon distance) and *soundness* (i.e. the verifier rejects both a legitimate prover that is out of range and an illegitimate prover, whether it is within or out of range).

[13] more formally define *identification schemes for a set of timing parameters* as protocols run between a reader $\mathcal{R}$ and a tag $\mathcal{T}$ with the aid of a key generation algorithm Kg, such that: (i) the three algorithms are efficient; (ii) the key generation generates a secret key (stored by reader and tag as described above); (iii) running the reader and tag interaction yields an accept/reject bit depending on the timing parameters. [13] also requires completeness, i.e. if the key is honestly generated and the tag is within range defined by the parameters, the reader should accept the tag. The main parameters considered by [13] are the number of time-critical rounds N_c, and the maximal allowed roundtrip time $t_{\max}$.

References

1. Abyneh, M.R.S.: Security analysis of two distance-bounding protocols. In: Proceedings of RFIDSec 2011. Lecture Notes in Computer Science, Springer

(2011)
2. Avoine, G., Bingol, M.A., Karda, S., Lauradoux, C., Martin, B.: A formal framework for analyzing RFID distance bounding protocols. In: Journal of Computer Security - Special Issue on RFID System Security, 2010 (2010)
3. Avoine, G., Tchamkerten, A.: An efficient distance bounding RFID authentication protocol: Balancing false-acceptance rate and memory requirement. In: Information Security. Lecture Notes in Computer Science, vol. 5735, pp. 250–261. Springer-Verlag (2009)
4. Brands, S., Chaum, D.: Distance-bounding protocols. In: Advances in Cryptology — Eurocrypt'93. pp. 344–359. Lecture Notes in Computer Science, Springer-Verlag (1993)
5. Bringer, J., Chabanne, H.: Trusted-HB: A low-cost version of hb $^{+}$ secure against man-in-the-middle attacks. Transactions on Information Theory 54(9), 4339–4342 (2008)
6. Bussard, L., Bagga, W.: Distance-bounding proof of knowledge to avoid real-time attacks. Security and Privacy in the Age of Ubiquitous Computing 181, 222–238 (2005)
7. Carluccio, D., Kasper, T., Paar, C.: Implementation details of a multi purpose ISO 14443 RFIDtool. In: Printed handout of Workshop on RFID Security - RFIDSec 06 (July 2006)
8. Clulow, J., Hancke, G.P., Kuhn, M.G., Moore, T.: So near and yet so far: Distance-bounding attacks in wireless networks. In: European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks. Lecture Notes in Computer Science, vol. 4357, pp. 83–97. Springer-Verlag (2006)
9. Cremers, C., Rasmussen, K.B., Čapkun, S.: Distance hijacking attacks on distance bounding protocols. Cryptology ePrint Archive, Report 2011/129 (2011), ePRINTURL
10. Desmedt, Y.: Major security problems with the 'unforgeable' (feige)-fiat-shamir proofs of identity and how to overcome them. In: SecuriCom. pp. 15–17. SEDEP Paris, France (1988)
11. Drimer, S., Murdoch, S.J.: Keep your enemies close: distance bounding against smartcard relay attacks. In: Proc. of the 16-th USENIX Security Symposium on USENIX Security Symposium, article no. 7. ACM Press (2007)
12. Duc, D., Kim, K.: Securing HB+ against GRS man-in-the-middle attack. In: Symposium on Cryptography and Information Security (SCIS). The Institute of Electronics, Information and Communication Engineers (2007)
13. Dürholz, U., Fischlin, M., Kasper, M., Onete, C.: A formal approach to distance bounding RFID protocols. In: Proceedings of the 14$^{\text{th}}$ Information Security Conference ISC 2011. pp. 35–49. Lecture Notes in Computer Science, Springer-Verlag (2011)
14. Francillon, A., Danev, B., Čapkun, S.: Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars (2010), ePRINTURL
15. Francis, L., Hancke, G., Mayes, K., Markantonakis, K.: Practical NFC peer-to-peer relay attack using mobile phones. In: RFIDSec'10 Proceedings of the 6$^{\text{th}}$ international conference on Radio frequency Identification: security and privacy issues. pp. 47–62. Springer-Verlag (2010)

16. Gilbert, H., Robshaw, M., Sibert, H.: An active attack against HB+ - a provably secure lightweight authentication protocol. Cryptology ePrint Archive, Report 2005/237 (2005), ePRINTURL
17. Haataja, K., Toivanen, P.: Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures. Transactions on Wireless Communications 9(1), 384–392 (2010)
18. Hancke, G.P.: A practical relay attack on ISO 14443 proximity cards (2005)
19. Hancke, G.P.: Practical Attacks on Proximity Identification Schemes (2006)
20. Hancke, G.P., Kuhn, M.G.: An RFID distance bounding protocol. In: SECURECOMM. pp. 67–73. ACM Press (2005)
21. Hlaváč, M., Rosa, T.: A Note on the Relay Attacks on e-Passports (2007), ePRINTURL
22. Hopper, N.J., Blum, M.: Secure human identification protocols. In: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security ADVCRYPTO. Lecture Notes in Computer Science, vol. 2248, pp. 52–66. Springer-Verlag (2001)
23. Juels, A.: RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications 24(2), 381–394 (2006)
24. Kfir, Z., Wool, A.: Picking virtual pockets using relay attacks on contactless smartcard systems. In: Conference on Security and Privacy for Emergency Areas in Communication Networks – SecureComm 2005. pp. 47 – 58. IEEE Computer Society Press (2005)
25. Kim, C.H., Avoine, G.: RFID distance bounding protocol with mixed challenges to prevent relay attacks. In: Proceedings of the 8th International Conference on Cryptology and Networks Security (CANS 2009). Lecture Notes in Computer Science, vol. 5888, pp. 119–131. Springer-Verlag (2009)
26. Kim, C.H., Avoine, G., Koeune, F., Standaert, F.X., Pereira, O.: The swissknife RFID distance bounding protocol. In: Proceedings of the 14$^{\text{th}}$ Information Security Conference ISC 2011. pp. 98–115. Lecture Notes in Computer Science, Springer-Verlag (2009)
27. Leng, X., Mayes, K., Markantonakis, K.: HB-MP+ protocol: An improvement on the HB-MP protocol. In: International Conference on RFID. pp. 118–124. IEEE Computer Society Press (2008)
28. Levi, A., Çetintas, E., Aydos, M., Koç, c.K., Çaglayan, M.U.: Relay attacks on bluetooth authentication and solutions. In: International Symposium Computer and Information Sciences – ISCIS 2004. Lecture Notes in Computer Science, vol. 3280, pp. 278 – 288. Springer-Verlag (2004)
29. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press (1996)
30. Oren, Y., Wool, A.: Relay attacks on RFID-based electronic voting systems. Cryptology ePrint Archive, Report 2009/442 (2009), ePRINTURL
31. Ouafi, K., Overbeck, R., Vaudenay, S.: On the security of hb# against a man-in-the-middle attack. In: Advances in Cryptology — Asiacrypt 2008. Lecture Notes in Computer Science, vol. 5350, pp. 108–124. Springer (2008)
32. Rasmussen, K.B., Čapkun, S.: Location privacy of distance bounding. In: Proceedings of the Annual Conference on Computer and Communications Security (CCS). ACM Press (2008)

33. Reid, J., Gonzalez Nieto, J.M., Tang, T., Senadji, B.: Detecting relay attacks with timing-based protocols. In: ASIACCS. pp. 204–213. ACM Press (2007)
34. Singelée, D., Preneel, B.: Distance bounding in noisy environments. In: European Workshop on Security in Ad-hoc and Sensor Networks – ESAS. Lecture Notes in Computer Science, vol. 4572, pp. 101 – 115. Springer-Verlag (2007)
35. Trujillo-Rasua, R., Martin, B., Avoine, G.: The poulidor distance-bounding protocol. In: RFIDSec 2010. pp. 239 – 257
36. Čapkun, S., Butty'an, L., Hubaux, J.P.: Sector: Secure tracking of node encounters in multi-hop wireless networks. In: ACM Workshop on Security of Ad Hoc and Sensor Networks - SASN. pp. 21 – 32. ACM Press (2003)