Lightweight Distance Bounding Protocol against Relay Attacks

Jin Seok KIM†, Kookrave CHO††, Dae Hyun YUM†††, Sung Je HONG†, Nonmembers, and Pil Joong LEE†, Member

SUMMARY Traditional authentication protocols are based on cryptographic techniques to achieve identity verification. Distance bounding protocols are an enhanced type of authentication protocol built upon both signal traversal time measurement and cryptographic techniques to accomplish distance verification as well as identity verification. A distance bounding protocol is usually designed to defend against the relay attack and the distance fraud attack. As there are applications to which the distance fraud attack is not a serious threat, we propose a streamlined distance bounding protocol that focuses on the relay attack. The proposed protocol is more efficient than previous protocols and has a low false acceptance rate under the relay attack.

key words: security, authentication, relay attack, mafia fraud attack, distance bounding protocol

1. Introduction

Authentication protocols are used to corroborate that an entity (or a prover) is the one that is claimed. Traditional authentication protocols are based on cryptographic techniques where a prover demonstrates its identity to a verifier by showing its knowledge of a secret. For example, the international standard ISO/IEC 9798 specifies entity authentication protocols based on symmetric encipherment algorithms, digital signatures, cryptographic check functions, and zero-knowledge techniques [1]. If a verifier V and a prover P share a secret K, a two-pass unilateral authentication protocol of ISO/IEC 9798-4 [2] that is depicted in Fig. 1 can be used; for simplicity, identifiers and text fields are omitted. The verifier V first sends a random number C to the prover P. Then, P responds with R = f(K, C) where f(·) is a cryptographic check function or a message authentication code algorithm. The authentication protocol of Fig. 1 is simple and efficient in that it is stateless, has only two passes, and does not need time synchronization.

Distance bounding protocols enable a verifier to determine an upper bound on the distance to a prover. The distance d is computed by measuring the (one-way) signal propagation time τp and multiplying it by the signal propagation speed c as d = c · Δt/2 with Δt = 2τp + τd where Δt is the measured total round-trip time and τd is the processing delay time [3]. To extract the signal propagation time, the processing delay time τd during signal exchanges must be as short and invariant as possible. A distance bounding protocol usually consists of n rounds of a single-bit challenge and rapid single-bit response, which is often called a fast bit exchange phase [4].

Distance bounding protocols are an effective countermeasure against location-related attacks. In the relay attack, a.k.a., the mafia fraud attack [5], both the verifier V and the prover P are honest, but malicious verifier V′ and prover P′ launch a man-in-the-middle attack, where V′ interacts with P and P′ interacts with V. The goal of P′ is to identify itself as being P, without either V or P noticing the fraud. Whereas the relay attack is executed by outsiders, the distance fraud attack is launched by insiders who try to cheat on the distance; a dishonest prover P who knows the secret K claims that it is closer to V than it really is. As the relay attack is executed by outsiders, the relay attack is always a threat; we cannot assume that we are able to control all unknown outsiders. However, the distance fraud attack is a matter of concern only when V does not trust P. In other words, the distance fraud attack is not a threat if insiders are assumed to be honest or if insiders gain nothing from the distance fraud attack. For example, when P runs an authentication protocol to access its own property (e.g., cars), P has no reason to launch the distance fraud attack; even if P cheats on the distance, it is not an “attack” or “threat” because P is the owner of the property.

Although Brands and Chaum [4] introduced the first distance bounding protocol in 1993, it was only when Hancke and Kuhn [3] proposed a distance bounding protocol in 2005 that distance bounding protocols attracted the attention of researchers. Hancke and Kuhn’s protocol (HKP), which is depicted in Fig. 2, consists of a slow phase of exchanging random numbers (Nv and Np) and a fast phase of exchanging challenge bits Ci and response bits Ri for i = 1, 2, . . . , n. In the slow exchange phase, V and P compute two n-bit sequences K0 and K1 with a pseudo-random function g(·). In the i-th round of the fast bit exchange phase, V sends a random challenge bit Ci ∈ {0, 1} and P sends back...
Verifier \(V\)  
(secret \(K\))  
Prover \(P\)  
(secret \(K\))

Choose \(C\)  

\[ C \rightarrow R \]

Check \(R\)

Fig. 1 ISO/IEC 9798-4 two-pass unilateral authentication protocol.

Verifier \(V\)  

Choose \(N_{V}\)  

\[ N_{V} \rightarrow N_{P} \]

Choose \(N_{P}\)

\[ R^{0}||R^{1} = g(K, N_{V}, N_{P}) \]

where \(R^{0} = R_{0}^{0}||R_{0}^{1}||\cdots||R_{0}^{n}\)

\(R^{1} = R_{1}^{0}||R_{1}^{1}||\cdots||R_{1}^{n}\)

Start of fast bit exchange phase

for \(i = 1\) to \(n\)

Choose \(C_{i} \in \{0, 1\}\)

Start timer: \(t_{i}\)

\[ C_{i} \rightarrow R_{i} \]

Stop timer: \(t'_{i}\)

\[ R_{i} = \begin{cases} R_{0}^{i} & \text{if } C_{i} = 0 \\ R_{1}^{i} & \text{if } C_{i} = 1 \end{cases} \]

end for

End of fast bit exchange phase

Check \(\Delta_{t} = t'_{i} - t_{i}\) and \(R_{i}\)

Fig. 2 Hancke and Kuhn’s distance bounding protocol.

**Table 1** Comparison of distance bounding protocols.

|      | Commun. | Comp. | \(\text{FAR}_{\text{relay}}\) | \(t_{d}\)      |
|------|---------|-------|----------------|----------------|
| Proposed | 0       | 1     | \(O(1/2^{n})\) | \(0\)           |
| HKP [3]  | 1       | 1     | \(O(3/4^{n})\) | \(\text{if-else}\) |
| KAP [7]  | 1       | 2n    | \(2n\)         | \(O(n(1/2)^{n})\) |
| SKP [8]  | 1       | 3n    | \(3n\)         | \(O(1/2^{n})\) |

Remark 1. We make the weakest assumptions; (1) the prover is a resource-scarce device such as an RFID tag without a battery, (2) the communication system is half-duplex, and (3) binary symbols are used. If more strong assumptions are made, \(\text{FAR}_{\text{relay}}\) can be reduced below \(O(1/2^{n})\); e.g., the bi-directional challenges can be used for full-duplex channels [6].

2. **Proposed Distance Bounding Protocol**

2.1 Protocol

We propose a lightweight distance bounding protocol that is depicted in Fig. 3, where the verifier \(V\) and the prover \(P\) share a secret \(K\). Before starting the fast bit exchange phase, the verifier \(V\) chooses an \(n\)-bit random number \(C^{0} = \)
C₀∥⋯∥C₀^n and the prover ℙ chooses C₁ = C₁|₀⋯∥C₁|^ₙ. Whereas random numbers C₀ and C₁ can be generated during the fast bit exchange phase, precomputation eliminates any additional computation during the fast bit exchange phase and minimizes the processing delay time t_d. The fast bit exchange phase of the proposed protocol is the simplest form one can imagine. In the i-th round, ℱ sends C₀ᵢ and ℙ responds with C₁ᵢ. After the fast bit exchange phase, the prover ℙ validates the conversation by sending R = h(K, C₀⟩⟨C₁) where h : {0, 1}^n → {0, 1}^n is a pseudorandom function and C₀ is composed of the bits C₀ᵢ (i = 1, . . . , n) that ℙ received from ℱ during the fast bit exchange phase. The token R plays the role of a message authentication code.

Conceptually, the proposed distance bounding protocol can be summarized as “talk freely and authenticate the conversation.” During the fast bit exchange phase, each entity just talks whatever it wants and then the prover authenticates the conversation by generating a message authentication code on the conversation. Compared with the ISO/IEC 9798-4 two-pass unilateral authentication protocol, the verifier’s challenge C in Fig. 1 is replaced by the fast bit exchange of C₀ and C₁ in Fig. 3.

Remark 2. Interestingly, the proposed distance bounding protocol is very similar to a scheme that was discussed (but declined) by Brands and Chaum [4]. They abandoned the scheme because they pursued resilience against both the relay attack and the distance fraud attack.

2.2 Analysis

We calculate the false acceptance rate of the proposed distance bounding protocol under relay attacks.

**Theorem 1:** The false acceptance rate of the proposed distance bounding protocol under relay attacks is \( \text{FAR}_{\text{relay}} = O\left(\left(\frac{1}{2}\right)^n\right) \), where n is the number of rounds.

**Proof.** Let ℱ and ℙ be an honest verifier and an honest prover who share a secret K. Let ℬ be an adversary modeled as {ℙ', ℱ'}. The adversary ℬ launches a man-in-the-middle attack that consists of two stages, which can be run sequentially or concurrently. In stage 1, the adversary ℬ acts as a verifier ℱ running the distance bounding protocol with ℙ. In stage 2, ℬ acts as a prover ℙ and runs the protocol with ℱ. The goal of ℬ is to impersonate ℙ in stage 2 by using information obtained in stage 1.

Let α be the event that ℬ succeeds in the relay attack (i.e., ℙ' passes the protocol in stage 2). Let C₀ be the value chosen by ℱ and C₀ is the adversary’s guess of C₀ in stage 1. Let β be the event that ℬ (acting as ℱ') correctly guesses at C₀ (i.e., C₀ = C₀). \( \text{FAR}_{\text{relay}} = \text{Pr}[α] \) is computed as follows.

\[
\text{Pr}[α] = \text{Pr}[α \land β] + \text{Pr}[α \land \overline{β}]
= \text{Pr}[α|β] \text{Pr}[β] + \text{Pr}[α|\overline{β}] \text{Pr}[\overline{β}]
= 1 \cdot \left(\frac{1}{2}\right)^n + \left(\frac{1}{2}\right)^n \left(1 - \left(\frac{1}{2}\right)^n\right)
= 2 \cdot \left(\frac{1}{2}\right)^n - \left(\frac{1}{4}\right)^n = O\left(\left(\frac{1}{2}\right)^n\right)
\]

where \( \text{Pr}[α|β] \) is the success probability of guessing an n-bit output of a pseudorandom function, which is \( \left(\frac{1}{2}\right)^n \). \( \square \)

2.3 Comparison

Table 1 compares the proposed protocol with the state-of-the-art protocols. The column of communication indicates the number of passes in the slow exchange phase. The column of computation means the total bit length of random numbers generated by pseudorandom functions. The col-
umn of \( t_d \) explains the portion of computation delay in \( t_d \); the processing delay time \( t_d \) consists of transmitter delay and computation delay where the latter is usually due to conditional branch (e.g., if-else statement) or binary bit operation (e.g., XOR).

The performance of KAP [7] depends on a security parameter \( p_d \) where \( 0 \leq p_d \leq 1 \). As we do not consider distance fraud attacks, \( p_d = 1 \) gives the lowest value of \( \text{FAR}_{\text{relay}} = \left( \frac{n}{2} + 1 \right) \left( \frac{1}{2} \right)^n = O \left( n \left( \frac{1}{2} \right)^n \right) \) and the computational cost of \( 2n \); the original analysis of KAP [7] has mistakes and a corrected analysis is given in [9]. For SKP (Swiss-Knife Protocol) [8], the costs for mutual authentication and privacy of identifiers, which we do not address, are excluded in Table 1. Finally, the proposed protocol has no computation delay during the fast bit exchange phase.

Remark 3. To achieve \( \text{FAR}_{\text{relay}} = O \left( \left( \frac{1}{2} \right)^n \right) \), previous works require at least three passes in the slow exchange phase; two passes are required to exchange random numbers between \( V \) and \( P \), and one pass is required to send a message authentication code. The message authentication code should have random numbers (or other kinds of fresh nonces) as input, which can be exchanged in slow or fast exchange phases. However, the message authentication code cannot be computed during the fast exchange phase because its computation time is not very short. Therefore, at least one pass seems unavoidable in the slow phase to achieve \( \text{FAR}_{\text{relay}} = O \left( \left( \frac{1}{2} \right)^n \right) \). In this sense, we think that the proposed scheme is lightweight.

3. Conclusion

By focusing on the relay attack, we build a distance bounding protocol with a high efficiency and a low false acceptance rate. It is an open problem to design an efficient and secure distance bounding protocol that is composed of the fast bit exchange phase only (i.e., no communication is required in the slow exchange phase).

Acknowledgement

Jin Seok Kim would like to thank Yu Kyeong Kim for her helpful comments.

References

[1] ISO/IEC 9798-1:2010, “Information technology – Security techniques – Entity authentication – Part 1: General,” 2010.
[2] ISO/IEC 9798-4:1999, “Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function,” 1999.
[3] G.P. Hancke and M.G. Kuhn, “An RFID distance bounding protocol,” SECURECOMM, pp.67–73, IEEE Computer Society, 2005.
[4] S. Brands and D. Chaum, “Distance-bounding protocols,” EUROCRYPT, Lect. Notes Comput. Sci., vol.765, pp.344–359, Springer, 1993.
[5] Y. Desmedt, C. Goutier, and S. Bengio, “Special uses and abuses of the Fiat-Shamir passport protocol,” CRYPTO, Lect. Notes Comput. Sci., vol.293, pp.21–39, Springer, 1987.
[6] D.H. Yum, J.S. Kim, S.J. Hong, and P.J. Lee, “Distance bounding protocol for mutual authentication,” IEEE Trans. Wireless Commun., vol.10, no.2, pp.592–601, 2011.
[7] C.H. Kim and G. Avoine, “RFID distance bounding protocol with mixed challenges to prevent relay attacks,” CANS, Lect. Notes Comput. Sci., vol.5888, pp.119–133, Springer, 2009.
[8] C.H. Kim, G. Avoine, F. Koeune, F.X. Standaert, and O. Pereira, “The swiss-knife RFID distance bounding protocol,” ICISC, Lect. Notes Comput. Sci., vol.5461, pp.98–115, Springer, 2008.
[9] R. Trujillo-Rasua, B. Martin, and G. Avoine, “The Poulidor distance-bounding protocol,” Workshop on RFID Security – RFIDSec’10, 2010.