Towards More Security Distance Bounding Protocol to prevent relay attacks

Jingxian zhou[1, a], Feng Xiao[2, b] , Zhaojun Gu[1, c]

[1]*Information Security Evaluation Center, Civil aviation university of china, Tianjin, China*

[2]*School of mathematics and computer science, Jianghan University, Wuhan, China*

[a]*jxzhou@cauc.edu.cn,* [b]*xfstone1985@163.com,* [c]*zjgu@cauc.edu.cn*

Abstract.

Many distance bounding protocols have been proposed recently, with encouraging results. However, there is no distance bounding protocol without final signature that provides success probability of attacker smaller than (3/4)^n in the presence of all frauds. In this paper, we propose a novel distance bounding protocol without a confirmation message based on two bits mixed challenges. It is prove that our protocol provides a reduced false acceptance rate under all those frauds, remarkably the terrorist fraud.

Keywords: Distance bounding protocol, Relay attacks, Terrorist fraud attacks, False acceptance rate, Secrecy.

Introduction

Distance bounding protocol was first suggested by Desmedt [1] by introducing the distance bounding concept based on the measurement of the round trip time of exchanged messages. A number of distance bounding protocols were proposed in current years [2]-[4], [6], [7]. They are classified into two classes depending on whether a final signature is involved. Their security was so far mainly evaluated by analyzing their resilience to three types of attacks: Distance Fraud, Mafia Fraud and Terrorist Fraud.

In Distance Fraud attacks, a sole dishonest prover convinces the verifier that he is at a different distance than he really is. A distance fraud attack is possible when there is no relationship between the challenge bits and the response bits exchanged during the distance verification. In Mafia Fraud attacks, the prover is honest, but an attacker tries to modify the distance that the verifier establishes by interfering with their communication. Terrorist Fraud is similar to Mafia Fraud. In this attack scenario, the legitimate prover P is dishonest and helps a illegal prover $\tilde{P}$ to convince the verifier V of a wrong distance without giving its private key. In some protocols, the terrorist fraud is always achieved with probability equal to one (i.e. [3]). And Terrorist Fraud attack is not discussed in another protocols (i.e. [6],

[7]).

Contribution. Defeating three attacks simultaneously is quite a difficult challenge and an ongoing research topic. We proposed a new distance bounding protocol without final signature. Our protocol is different in following sense. A new rule of fast exchange has been used to guarantee the randomness of binary responses. That is, the adversary can not predict the challenges and send the corresponding responses earlier. In this way, our protocol can against three fraud attacks simultaneously, and achieve a strong security level.

Proposed Distance Bounding Protocol

Description of Protocol

The protocol described in the section consists of identification phase, nonce delivery phase and fast bit exchange phase. As shown in Fig.1, verifier V and prover P share two secret information k_1 and k_2. The length of k_1 is $3n$ bits, while k_2 is n bits long. The implementation of the security protocol includes three parts, which are presented as follows.

Identification phase:

In order to carry out the verify process, V must identify the prover P to access its key information.

(1) V first announces its presence by broadcasting a $Hello$ message.

(2) P responds to the $Hello$ message by sending its $index$. V looks up the database for the key k_1 and k_2 corresponding to P's $index$.

If $index$ is not recognized as a valid value, P is rejected.

Nonce delivery phase:

In this phase, V delivers a nonce v to P in a secret manner as follow.

(3) V generates a $3n$-bit random nonce, v, drawn uniformly from the multiplicative group Z_q^*. Where n is a security parameter, q is a $3n$-bit prime integer. With k_1, k_2 and v, V computes: $A \equiv v + k_1 \bmod q$, $B \equiv v \times k_2 \bmod q$. Then V broadcasts A and B.

Upon receiving A and B, P extracts v from message A and verifies its integrity using message B as follow: $(A - k_1) \times k_2 \equiv B \bmod q$. If the equation is false, P will abort the protocol. The value v is divided into three registers v_1, v_2, v_3, where: $|v_1| = |v_2| = |v_3| = n$, $v_j = v_j^1 \| v_j^2 \| \ldots \| v_j^n, j = 1, 2, 3$.

Fast bit exchange phase:

The fast bit exchange phase consists of n rounds. In the i-th round, the verifier V measures the challenge-response delay time.

(4) If $v_1^i \oplus v_2^i = 0$ the verifier V sends a random challenge $c_i \in \{0,1\}$, while if $v_1^i \oplus v_2^i = 1$ V sends challenge $c_i \in \{2,3\}$, where c_i is encoded to two bits c_i^0 and c_i^1, the rules as: $0 \to 00, 1 \to 01, 2 \to 10, 3 \to 11$.

(5) Upon reception of a challenge c_i, the prover P first verifies c_i by the value of $v_1^i \oplus v_2^i$. If c_i is right, then P sends back the bit $r_i = v_1^i \oplus v_3^i \oplus c_i^1$ if $c_i \in \{0,1\}$; P sends back the bit $r_i = v_2^i \oplus v_3^i \oplus k_2^i \oplus c_i^1$ if $c_i \in \{2,3\}$. If c_i is wrong, P detects an error, it always replies a random value to all the subsequent challenges sent by the verifier V. By doing this, both V and P fight the adversary.

Verification: When the fast phase is finished, V verifies that the responses from P are correct and checks whether $\Delta t_i \le \Delta t_{max}$, $\forall i = 0,1,\dots n$, where Δt_{max} is a timing bound.

Security Analysis

In this section, we will analyze the false acceptance rate of the proposed distance bounding protocol against the distance fraud attack, the mafia fraud attack and the terrorist fraud attack.

Theorem 1. The probability of accepting a modified nonce v' by P is at most $1/(q-1)$.

Proof Assume that message A has been modified so that the extracted nonce becomes $v' \equiv v + \varepsilon \mod q$; for some $\varepsilon \in Z_q$. Also assume that message B has been modified to $B' \equiv B + \delta \mod q$ for some $\delta \in Z_q$. The integrity of the extracted v' is verified using the received B' as follows:

$$B + \delta \equiv B' \equiv v' \times k_2 \equiv B + (\varepsilon \times k_2)\ modq \qquad (1)$$

Equivalently, the false A' is accepted only if $\delta \equiv \varepsilon \times k_2 \mod q$. If $\delta = 0$, then $\varepsilon \times k_2 \equiv 0 \mod q$. Since q is a prime integer, so $\varepsilon = 0$. It is mean that both A and B not been changed. If $\varepsilon \ne 0$, the congruence of Eq. 1 can never be satisfied. That is, any modification of message A alone will be detected with probability one by P;

If $\delta \ne 0$, since k_2 is unknown to the adversary, for any fixed δ, there exists a unique $\varepsilon \in Z_q^*$ that satisfies Eq. 1. Therefore, the probability of modifying both

A and B in a way undetected by P is at most $1/(q-1)$ (equivalently, guessing the value of k_2).

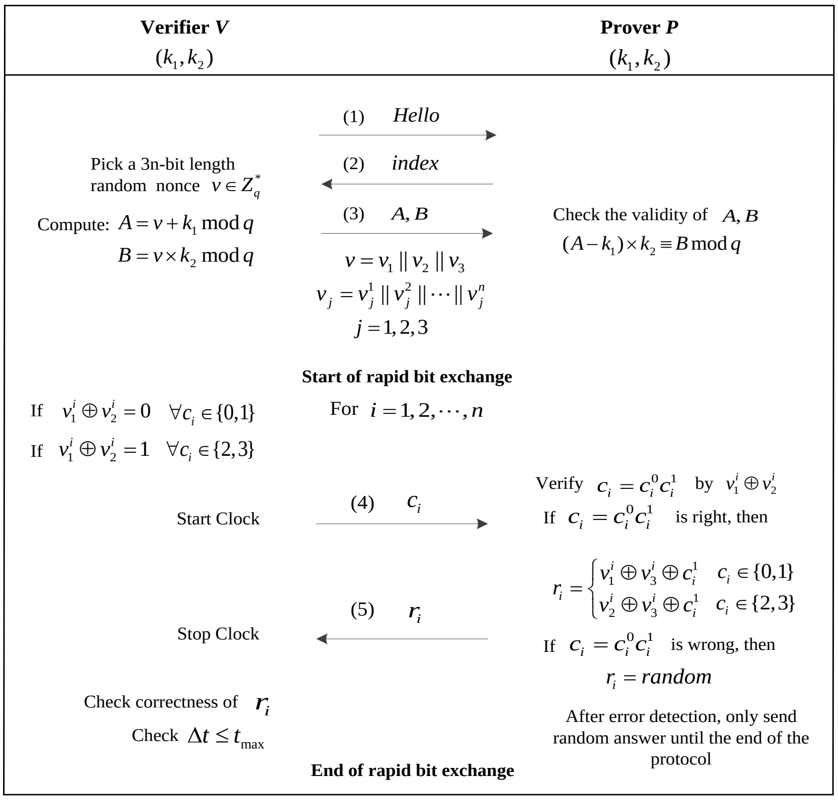
Verifier *V*
(k_1, k_2)
Prover *P*
(k_1, k_2)
(1) *Hello*
Pick a 3n-bit length random nonce $v \in Z_q^*$
(2) *index*
Compute: $A = v + k_1 \bmod q$
$B = v \times k_2 \bmod q$
(3) A, B
Check the validity of A, B
$(A - k_1) \times k_2 \equiv B \bmod q$
$v = v_1 \| v_2 \| v_3$
$v_j = v_j^1 \| v_j^2 \| \cdots \| v_j^n$
$j = 1, 2, 3$
Start of rapid bit exchange
For $i = 1, 2, \cdots, n$
If $v_1^i \oplus v_2^i = 0 \quad \forall c_i \in \{0,1\}$
If $v_1^i \oplus v_2^i = 1 \quad \forall c_i \in \{2,3\}$
Verify $c_i = c_i^0 c_i^1$ by $v_1^i \oplus v_2^i$
Start Clock
(4) c_i
If $c_i = c_i^0 c_i^1$ is right, then
$r_i = \begin{cases} v_1^i \oplus v_3^i \oplus c_i^1 & c_i \in \{0,1\} \\ v_2^i \oplus v_3^i \oplus c_i^1 & c_i \in \{2,3\} \end{cases}$
(5) r_i
Stop Clock
If $c_i = c_i^0 c_i^1$ is wrong, then
$r_i = random$
Check correctness of r_i
Check $\Delta t \le t_{\max}$
After error detection, only send random answer until the end of the protocol
End of rapid bit exchange

Fig.1. Our proposed distance bounding protocol

Theorem 2. The false acceptance rate of the proposed distance bounding protocol against distance fraud attacks is given by $FAR_D = (1/2)^n$.

Proof In distance fraud attack scenario, a user who knows all the secret information tries to cheat on the distance. That is, a legitimate (but dishonest or malicious) insider tries to cheat on the distance while he or she is actually located at a distance. We show that the FAR of the proposed protocol under distance fraud attacks is $(1/2)^n$. Let ξ_i be the event that a dishonest tag succeeds in the i-th round. Let Ξ_i be the event defined by $\Xi_i = \xi_i$ and $\Xi_i = \xi_i \mid \xi_1 \wedge \cdots \wedge_{i-1}$ for $i > 1$. When $v_1^i \oplus v_2^i = 0$, to cheat on the distance, the dishonest P should send the right response $r_i = v_1^i \oplus v_3^i \oplus c_i^1$ before receiving the challenge c_i from V. Because $c_i^1 = 0$ or 1, P succeeds with probability $1/2$;

$$Pr[\Xi_i \mid v_1^i \oplus v_2^i = 0]Pr[v_1^i \oplus v_2^i = 0] = \frac{1}{2}.\frac{1}{2} = \frac{1}{4} \tag{2}$$

Similarly,

$$Pr[\Xi_i \mid v_1^i \oplus v_2^i = 1]Pr[v_1^i \oplus v_2^i = 1] = \frac{1}{2}.\frac{1}{2} = \frac{1}{4} \tag{3}$$

From the law of total probability, $P[\Xi_i]$ is easily obtained

$$\begin{aligned} Pr[\Xi_i] &= Pr[\Xi_i \mid v_1^i \oplus v_2^i = 0]Pr[v_1^i \oplus v_2^i = 0] \\ &\quad + Pr[\Xi_i \mid v_1^i \oplus v_2^i = 1]Pr[v_1^i \oplus v_2^i = 1] \\ &= \frac{1}{4} + \frac{1}{4} = \frac{1}{2} \end{aligned} \tag{4}$$

Finally, the success probability of a distance fraud attack is given by

$$\begin{aligned} Pr[\xi_1 \wedge \xi_2 \wedge \cdots \wedge \xi_n] &= Pr[\xi_1]Pr[\xi_2 \mid \xi_1] \cdots Pr[\xi_n \mid \wedge_{i=1}^{n-1} \xi_i] \\ &= Pr[\Xi_1]Pr[\Xi_2] \cdots Pr[\Xi_n] \\ &= (\frac{1}{2})^n \end{aligned} \tag{5}$$

Theorem 3. The false acceptance rate of the proposed distance bounding protocol against mafia fraud attacks is given by $FAR_M = (1/2)^n (n/2+1)$.

Proof In order for malicious prover $\hat{P}$ to masquerade as P to V, $\hat{P}$ must be reply to V 's challenges correctly in each round. To compute FAR_M, we assume that $\hat{P}$ queries P in advance. $\hat{P}$ sends predicted challenges $c_i^* = c_i^{0*} c_i^{1*}$ to P and gets the responses $r_{i'}$ corresponding to her challenges. Afterward, $\hat{P}$ executes the fast phase with V and receives the challenges c_i s. There are two equal likely cases, (i) if $c_i^{0*} = c_i^0$, $\hat{P}$ sends the correct response with probability of 1; (ii) if $c_i^{0*} \neq c_i^0$, $\hat{P}$ guesses the response with probability of $1/2$.

The probability of not being detected by V until the i-th round, $Pr(i)$, depends whether the attack is detected by P in the previous rounds or not. We define the following events:

- $\overline{a}_i$: the event that the attack is not detected at the i-th round by V ,
- b_i : the event that the attack is detected at the i-th round by P ,
- $\overline{b}_i$: the event that the attack is not detected at the i-th round by P ,
- $\overline{A}_i$: the event that the attack is not detected **until the i-th round** by V ,
- B_i : the event that the attack is detected at the i-th round by P **for the first time**,
- $\overline{B}_i$: the event that the attack is not detected **until the i-th round** by P .

We can define the success probability of the mafia fraud attack as follows:

$$Pr[FAR_M] = Pr[\overline{A}_n \mid \overline{B}_n]Pr[\overline{B}_n] + \sum_{i=1}^{n} Pr[\overline{A}_n \mid B_i]Pr[B_i] \tag{6}$$

The probability of being detected by P in the i-th round for the first time is: $Pr[B_i] = (1/2)^i$; and the probability of not being detected by P until i-th round is: $Pr[\overline{B}_i] = (1/2)^i$.

We can compute

$$Pr[\overline{A}_n \mid B_i] = \prod_{j=1}^{i-1} Pr[\overline{a}_j \mid \overline{b}_j].\prod_{j=i}^{n} Pr[\overline{a}_j \mid b_i] \tag{7}$$

where $Pr[\overline{a}_j \mid b_i] = 1/2$, $j > i$, and there are two cases of being detected by P in the i-th round: 1) $(v_1^i \oplus v_2^i = 0) \wedge (c_i = 0$ or $1)$, 2) $(v_1^i \oplus v_2^i = 1) \wedge (c_i = 2$ or $3)$. The probability of each case is $1/2$ and V cannot detect an attack. Hence, the probability that the attack is not detected by V when it is not detected by P in the same round is

$$Pr[\overline{a}_j \mid \overline{b}_j] = \frac{Pr[\overline{a}_j \wedge \overline{b}_j]}{Pr[\overline{b}_j]} = \frac{1/2}{1/2} = 1 \tag{8}$$

Therefore, we have that

$$Pr[\overline{A}_n \mid B_i] = \prod_{j=i}^{n} Pr[\overline{a}_j \mid b_i] = (\frac{1}{2})^{n-i+1} \tag{9}$$

$$Pr[\overline{A}_n \mid \overline{B}_i] = \prod_{j=1}^{i} Pr[\overline{a}_j \mid \overline{b}_j] = 1. \tag{10}$$

We can finally compute

$$\begin{aligned} Pr[FAR_M] &= Pr[\overline{A}_n \mid \overline{B}_n]Pr[\overline{B}_n] + \sum_{i=1}^{n} Pr[\overline{A}_n \mid B_i]Pr[B_i] \\ &= 1.(\frac{1}{2})^n + \sum_{i=1}^{n}(\frac{1}{2})^{n-i+1}.(\frac{1}{2})^i \\ &= (\frac{1}{2})^n(\frac{n}{2}+1) \end{aligned} \tag{11}$$

Theorem 4 The false acceptance rate of the proposed distance bounding protoco l against terrorist fraud attacks is given by $FAR_T = (1/2)^n(n/2+1)$.

Proof In our protocol, the random nonce v which generated by V plays a very important role. If v is provided to the adversary by the malicious prover, then the long term key k_1 and k_2 will be computed according to the public message A and B. The malicious prover also can provide to the adversary the two following values: $v_1^i \oplus v_3^i$ and $v_2^i \oplus v_3^i \oplus k_2^i$. Using the verifier challenges, the adversary computes the correct answers with probability 1. However, the adversary is able to retrieve k_2^i from the three values $v_1^i \oplus v_3^i$, $v_2^i \oplus v_3^i \oplus k_2^i$ and $v_1^i \oplus v_2^i$, where the value $v_1^i \oplus v_2^i$ can be known by the challenge c_i. Furthermore, k_1 can be obtained from the message A and B.

Therefore, in terrorist fraud attacks, we can assume v is secret. Under this condition, the capability of terrorist fraud is equivalent to the mafia fraud. Thus, by theorem 3, the success probability of terrorist fraud is shown as follows:

$$FAR_T = FAR_M = (1/2)^n(n/2+1) \tag{12}$$

Conclusions

Distance bounding protocols combine cryptographic techniques with physical characteristics of signals to fight against location-related attacks. In this paper, we presented a new secure distance bounding protocol that significantly enhances the proposed ones. New fast exchange rule had been used to promise the random of binary responses. The advantage of the proposed protocol was efficiency and the lower FAR under distance, mafia, and terrorist fraud attack. The most important contribution of this paper was that our protocol achieve the ideal security level $(1/2)^n$ against for distance fraud.

Acknowledgements

This work was supported by National Natural Science Foundation of China (Grant No. 61303232), the fundamental research funds for the central universities (Grant No. 3122013C004) and the scientific research foundation of CAUC (Grant No. 2013QD24X).

References

[1] T. Beth, Y. Desmedt. Identification tokens – or: Solving the chess grandmaster problem. In CRYPTO'90, Santa Barbara, California, USA, Lecture Notes in Computer Science, Springer, Vol. 537(1991), p. 290-307.

[2] C. H. Kim, G. Avoine, F. Koeune, F. X. Standaert, O. Pereira. The Swiss-Knife RFID Distance Bounding Protocol. LNCS, vol. 5461 (2009), p. 98-115.

[3] C. H. Kim, G. Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. LNCS, Springer, Vol. 5888(2009), p. 119-133.

[4] B. Alomair, L. Lazos, R. Poovendran. Securing low-cost RFID systems: An unconditionally secure approach. Journal of Computer Security, 2011, 19(2), p. 229-257.

[5] G. Avoine, C. H. Kim. Mutual distance bounding protocols. IEEE Transactions on mobile computing, vol. 99(2012), p. 1-11.

[6] W. Xin, H. P. Sun and Z. Chen. Analysis and design of distance-bounding protocols for RFID. Journal of Computer Research and Development, 2013, 50(11), p. 2358-2366.

[7] H. Dowon . Authenticated Distance Bounding Protocol with Improved FAR: Beyond the Minimal Bound of FAR. IEICE Transactions on Communications, 2014, 97(5), p. 930-935.