Distance Bounding based on PUF

Mathilde Igier and Serge Vaudenay

EPFL
CH-1015 Lausanne, Switzerland
http://lasec.epfl.ch

Abstract. Distance Bounding (DB) is designed to mitigate relay attacks. This paper provides a complete study of the DB protocol of Kleber et al. based on Physical Unclonable Functions (PUFs). We contradict the claim that it resists to Terrorist Fraud (TF). We propose some slight modifications to increase the security of the protocol and formally prove TF-resistance, as well as resistance to Distance Fraud (DF), and Man-In-the-Middle attacks (MiM) which include relay attacks.

1 Introduction

Wireless devices are subject to relay attacks. It is problematic because these devices are at the basis for authentication in many domains like payment with credit cards, building access control, or biometric passports. To ensure the security of wireless devices against relay attacks, Brands and Chaum [5] introduced the notion of *Distance Bounding* (DB) protocols in 1993. The idea is that a prover P must prove that he is close to a verifier V. Several attack models exist to make the verifier accept with a prover too far away from the verifier. The attacks described in the literature are: 1. *Distance Fraud attacks (DF)* [5]: A far away prover P tries to make V accept. No participant is close to V. 2. *Mafia Fraud attacks (MF)* [6]: A malicious actor A who does not hold the secret tries to make V accept using an honest but far away prover P. 3. *Terrorist Fraud (TF)* [6]: A malicious actor A who does not hold the secret tries to make V accept by colluding with a malicious far away prover P who holds the secret.

We use the formal security model which was proposed by Boureanu et al. [1]. Most of the proposed protocols are vulnerable to TF attacks but a few protocols provide security against all types of threats. However, all these proofs are made on the assumption that in TF, the prover does not want to give his credential to the adversary for further application. This assumption is weak and does not correspond to reality. None of the DB protocols in the plain model can provide TF security without this assumption, so, we should consider alternate models. DF and TF security are easier to provide using tamper resistant hardware on the prover side because the prover cannot access his secret. Kılınç and Vaudenay [11] provide a new model for distance bounding protocols with secure hardware. In this model, the game consists of several verifier instances including a distinguished one V, hardware with their instances, instances of provers and actors. There is one distinguished hardware h with instances far away from V. The winning condition of this game is that V accepts.

- The DB protocol is DF-secure if the winning probability is negligible whenever there is no instance close to V.
- The DB protocol is MiM-secure if the winning probability is negligible whenever an honest prover is holding h.
- The DB protocol is TF-secure if the winning probability is negligible.

PUFs are tamper resistant hardware used in counterfeiting detection and authentication protocols. A PUF is a physical component which maps a challenge to a response. By definition, a PUF, as it is described in [13], has the following properties: non clonable, non emulable, a response R_i gives negligible information on a response R_j with $R_i \neq R_j$ and a PUF cannot be distinguished from a random oracle. For simplicity reasons, we will treat PUFs as random oracles with access limited to their holder. The aim of our work is to provide a provably secure protocol using PUF in DB protocols. A TF-secure DB protocol based on PUF was proposed in [10]. Nevertheless, this protocol assumes that provers implement their protocol while using a PUF. In the model of Kleber et al. [12], the prover can implement any malicious protocol while accessing to the PUF, the protocol in [10] is trivially TF-insecure in this stronger model.[1] Kleber et al. design a protocol in [12] which is claimed to be secure in their model. However we contradict that fact in this paper and propose to modify it in order to improve the security.

Our contribution in this paper is as follows: 1. We show that the protocol proposed by Kleber et al. [12] is not secure against *Terrorist Fraud* which contradicts the claims from their authors; 2. We provide some slight modifications of this protocol which we call pufDB to improve its security; 3. We provide proofs of security for this pufDB protocol for the following attacks: *Distance Fraud* and *Mafia Fraud*; 4. We prove the security of pufDB protocol against *Terrorist Fraud* when the prover is limited in the amount of bits per round he can send. The security strengthens when the distance from the prover to the verifier increases.

[1] In this protocol, the PUF is not used during the fast phase, so the malicious prover can give whatever is needed to complete the protocol to a close-by adversary.

To the best of our knowledge, pufDB is the first protocol which provides TF security even when the prover is allowed to leak his secret.

Due to limited space, proofs of our results are deferred to the full version of this paper [9]. The full version also includes the analysis for two other threat models: impersonation fraud and distance hijacking.

2 The Kleber et al. Protocol

2.1 Details of the Protocol

The verifier is called V and the prover P. The main idea of the protocol proposed by Kleber et al. [12] is to replace the PRF in P of conventional Distance Bounding protocols by a PUF. In this protocol, it is possible to use both Challenge-response PUF or PublicPUF.[2] The protocol is made of two distinct phases: the preparation phase and the time critical phase.

Prior to the protocol, it is assumed that V can query the PUF and store a number of challenge-response pairs (CRP), at a round i such that $r_i = PUF(C_i)$. A CRP is defined as $(C_i, r_i), 0 \leq i < n$ with n the number of rounds. There is always a set of CRPs corresponding to PC to complete the run. A set of CRPs shall not be used in protocols more than once.

In the time critical phase, only one bit can be sent from V to P in a round. However the PUF needs a big space of challenges to be secure. Therefore V transmits a pre-challenge PC to P during the preparation phase. Then, in the time critical phase, the pre-challenge is combined with the challenges c_i received by P to generate a challenge $C_i = \text{PC}_0 ... PC_{n-2-i} || c_0 c_1 \ldots c_i$ for the PUF. It is assumed that the hardware is such that the PUF can precompute C_i and when the prover receives the last bit of C_i he can return the response r_i in almost no time. The time critical phase consists of n transmission rounds. The verifier V starts the clock when he sends a challenge c_i and stops the clock when he receives the response r_i. In the paper, T_{max} and E_{max} are defined. T_{max} is the maximal number of responses which can arrive too late. E_{max} is the maximal number of errors admitted in the responses. A response which arrives late is not checked.

[2] Normally, a PUF is non emulable so the verifier should first borrow the PUF to get input-output pairs. To avoid it, we can use Public-PUF also called SIMPL system (SIMulation Possible but Laborious). SIMPL systems guarantee that the response to a challenge cannot be computed faster with a simulator of the PUF than with the real PUF. Anyone can compute the right response but it takes much more time with the simulator of the PUF.

We note that if one c_i is incorrectly received by P, then all subsequent PUF computations will produce random outputs, independently from the expected r_i. This is an important problem in this protocol: it is not tolerant to reception errors by P.

The protocol is claimed to be provably secure for all types of Fraud by Kleber et al. [12]. They prove the security of their protocol using the model of Dürholz et al. [7]. They only give a proof of security against Terrorist Fraud attacks. In fact, in the model defined by Kılınç et al. [11], when the protocol uses hardware, the proof that the protocol is secure against Terrorist Fraud attacks gives a proof of security against all the other types of attacks. However, when there is no additional restriction in the protocol, this protocol is insecure against Terrorist Fraud attack as we show in the section 2.2. To prove the security against Terrorist Fraud, Kleber et al. assume that the probability for the adversary to win the game is equal to $\left(\frac{1}{2}\right)^{n-E_{max}-T_{max}}$. We contradict this assumption.

2.2 A Terrorist Fraud Attack

Notations. d_{VP} is the distance between V and the far away prover P, t_{VP} is the signal propagation time between V and P (it is assume that $\frac{d_{VP}}{t_{VP}}$ is a constant such as the speed of light); Similarly, d_{AP} is the distance between A and the far away prover P, t_{AP} is the signal propagation time between A and P; B is the maximal distance allowed by the protocol, t_B is the maximal signal propagation time over the distance B; Finally, T is the time between sending two consecutive challenges c_i and c_{i+1}.

In this scenario a malicious far away prover colludes with an adversary close to the verifier. In the protocol of Kleber et al. the adversary receives PC from the verifier. He can send it to the malicious prover who holds the PUF. There is no information concerning the distance d_{AP} between P and A nor about the time T in between rounds. A forwards every message from V to P. To answer a challenge c_i on time, P is missing m bits. He computes 2^m PUF values and sends them to A so that A will always be able to respond on time. For instance, if t_m denotes the time it takes for P to compute the 2^m values and to transmit them to A (without time of flight), the attack works if

$$t_{AP} + t_{VA} \leq t_B + \frac{(mT - t_m)}{2} \tag{1}$$

More concretely, we assume $m = 1$, $B = 3$m and $t_B = 10$ns. We consider V running at 1GHz and have one clock cycle between rounds, so $T = 1\mu$s. We consider a faster malicious prover P running at 10GHz so that he can evaluate two challenges with the PUF (corresponding to the possible challenges for m =1) in t_m = 200ns. With $d_{VA} = B$, the attack succeeds for t_{AP} = 400ns i.e d_{VP} = 120m. The attack is possible because there is a huge amount of time between the reception of r_i and the emission of c_{i+1}, but our figures show this is a quite realistic scenario.

2.3 Slight Modifications of the Protocol

We choose to slightly modify the protocol of Kleber et al. [12] to improve its security. We call pufDB the new protocol. First, we impose a regular rhythm for sending the challenges, second, the $(n-1)$ bits of PC are sent with the same rhythm as if there were challenges in the time critical phase but expecting no answer. The prover begins to send responses when he receives the first bit of challenge c_0. With this slight change, we make sure there is no more time left for attacks in between the transmission of PC and c_0 than there is in between the transmission of each c_i and this time is bounded. Moreover, we assume that P cannot accept consecutive challenges separated by time lower than $\frac{T}{2}$, so, we cannot speed up P by sending challenges too fast.[3] Finally, another modification is that we concatenate PC with the challenges without dropping any bit. So, $C_i = PC||c_0...c_i$ is of $n+i$ bits. This guarantees domain separation for the functions computing the responses. So, to summarize, we use the three following requirements: 1. The elapsed time between sending each bit of $PC||c_0...c_{n-1}$ by V is exactly T; 2. The elapsed time in between receiving two consecutive bits by P is at least $\frac{T}{2}$; 3. PC is concatenated to $c_0...c_i$ without dropping any bit.

We denote by t_0 the time when the verifier sends c_0 to the prover. So c_i is sent at time $t_0 + iT$ and PC_i is sent at time $t_0 + (i - n + 1)T$.

Lemma 1 (Number of missing bits). *For each round i, the number of challenges which did not arrive yet to the far away prover P when it becomes critical to send the response r_i is $m = \lceil 2(\frac{t_{VP}-t_B}{T}) \rceil$. The number of possible C_i is 2^m.*

3 Distance Fraud Analysis of pufDB

To prove resistance against Distance Fraud attacks, it is necessary to prove that a far away prover P who holds the PUF has a negligible probability to win the game presented in section 2. The idea of a Distance

[3] We allow challenges to arrive faster than a period T to capture the Doppler effect when P moves towards V. With $\frac{T}{2}$ as a limit, P can move at the light speed!???check

Fraud attack is to find a way for the far away prover P to send r_i such that it arrives on time to V. To arrive on time, the response r_i should be sent before receiving the challenge c_i. So, there are chances for the response to be wrong.

Theorem 1. *We use m from Lemma 1. We define $q_m = \prod_{l=1}^{m} {p_l}^{\frac{1}{m}}$ for $p_l = \frac{1}{2} + \frac{1}{2} \times \frac{1}{2^{2^l}} \binom{2^l}{2^{l-1}}$, in a DF-attack, we have that*

$$\Pr(\textit{win the game}) \leq \sum_{i=0}^{E_{max}+T_{max}} \binom{n}{i} {q_m}^n$$

For $2(E_{max} + T_{max}) \leq n$ any DF-attack is bounded by

$$\Pr(\textit{win the game}) \leq e^{-n \times \left(2\left(\frac{1}{2} - \frac{E_{max}+T_{max}}{n}\right)^2 - \ln(2q_m)\right)} = \textit{bound}_{DF}$$

If there exist $\alpha, \beta \in \mathbb{R}$ such that $E_{max} \leq \alpha n$, $T_{max} \leq \beta n$ and $\alpha + \beta < 0.049$ then, $\textit{bound}_{DF}$ is negligible.

Here is the table of the first values of q_m:

m	1	2	3	4	5	6	7	8	9
q_m	0.75	0.7181	0.6899	0.6657	0.6454	0.6283	0.6141	0.6022	0.5921

So depending on m, q_m smoothly goes from $\frac{3}{4}$ to $\frac{1}{2}$ as m grows. p_l decreases and tends towards $\frac{1}{2}$, so q_m decreases and tends towards $\frac{1}{2}$ as well.

For $m \geq 2n - 1$, we can have a better bound. The adversary has no bit to compute the PUF (not even the bits of PC), so we can redo the analysis and obtain

$$\Pr(\text{win the game}) \leq \sum_{i=0}^{E_{max}+T_{max}} \binom{n}{i} {p_n}^n \leq e^{-n \times \left(2\left(\frac{1}{2} - \frac{E_{max}+T_{max}}{n}\right)^2 - \ln(2p_n)\right)}$$

These results are unchanged when using a public PUF.

4 Mafia Fraud Analysis of pufDB

To prove resistance against Mafia Fraud attacks it is necessary to prove that if an honest far away prover P holds the PUF, an adversary close to V has a negligible probability to win the game presented in section 2.

We prove security against Man-in-the-Middle (MiM) attacks. We first informally describe what is the best possible attack. A is a malicious actor.

Before receiving a challenge c_i from the verifier V, he sends a guessed challenge c'_i to a far away prover P. He receives r'_i from the prover. If $c'_i = c_i$ then the adversary sends r'_i to the verifier. In this case, the adversary wins the round with probability 1.

Pre-asking gives an extra chance to pass a round. But if one c_i is incorrectly guessed, any subsequent pre-asking request will return some useless random bits. So the best strategy is to start pre-asking until there exists a round i such that $c'_i \neq c_i$, then to continue with the impersonation attack strategy.

We have not considered replay attacks because A has no time to begin any other instance of the protocol if P does not answer at frequency larger than $\frac{T}{2}$. Actually, let V be the distinguisher verifier in a MiM attack and PC the value that he sends. As the PUF is held by a single participant, there are no concurrent sessions for P. Sending c_i to P takes at least $\frac{(n+1)T}{2}$ time but during this time, the session for V terminates. So, only one session of P receives c_i, for each i.

Theorem 2. *In any MiM attack, we have*

$$\Pr(\textit{win the game}) \leq \left(\frac{1}{2}\right)^{n+1-T_{max}} \times \sum_{i=0}^{E_{max}+1} \binom{n+1-T_{max}}{i}$$

This is bounded by $e^{-2(n+1-T_{max})\times\left(\frac{1}{2}-\frac{E_{max}+1}{n+1-T_{max}}\right)^2}$ *when* $2E_{max} + T_{max} \leq n+1$. *For* $E_{max} \leq \alpha n$, $T_{max} \leq \beta n$, *and* $2\alpha + \beta < 1$, *this is negligible.*

Using a public PUF just adds a negligible term in the bound.

5 Terrorist Fraud Analysis of pufDB

In Terrorist Fraud attacks, an adversary A colludes with a far away malicious prover P to make V accept. Without any limitation on the power of the verifier the protocol is insecure against TF. In our model, the prover is limited on the communication complexity. With this limitation, the prover can compute all the challenges but he has a limitation on the amount of bits he can send to A. He can compress the 2^m bits of the table of responses for each round into s bits and send to A the compressed version. From the s bits received and the challenge sent by V, A can try to recover the response.

Lemma 2. *Let s and l be two positive integers and $N = 2^l$. We define $p_{l,s} = 1-\frac{1}{N}E(\min_C d(f,C))$ where f is a random boolean function of l-bit input and the minimum is over sets C of up to 2^s elements. We define*

$$p^*_{l,s} = 1-\frac{1}{2^N}\sum_{i=0}^{R+1}\frac{i}{N}N'_i \quad , \quad \bar{p}_{l,s} = \frac{1}{2}+\frac{1}{\sqrt{N}}\times\left(\sqrt{\frac{s\ln 2}{2}}+\sqrt{\frac{2}{2^s}+\frac{1}{N}}\right)+\frac{1}{N}$$

where R is the maximum value such that $\sum_{i=0}^{R}2^s\binom{N}{i} \leq 2^N$ and $N'_i = 2^s\binom{N}{i}$ for $0 \leq i \leq R$, $N'_i = 0$ for $i > R+1$, and $N'_{R+1} = 2^N - 2^s\sum_{i=0}^{R}\binom{N}{i}$. We have $p_{l,s} \leq p^*_{l,s}$. For $s \leq \frac{2^l}{2}$, we also have $p^*_{l,s} \leq \bar{p}_{l,s}$.

Theorem 3. *We use m as defined in Lemma 1. We assume that the malicious prover is limited to s bits of transmission per round to the adversary in a TF-attack. We use $q_{m,s} = \prod_{l=1}^{m} p_{l,s}{}^{\frac{1}{m}}$ and we have*

$$\Pr(\textit{win the game}) \leq \sum_{i=0}^{E_{max}+T_{max}}\binom{n}{i}q_{m,s}{}^{n}$$

where $p_{l,s}$ is defined in Lemma 2. For $2(E_{max}+T_{max}) \leq n$ a TF-attack has a success probability bounded by

$$\Pr(\textit{win the game}) \leq e^{-n\times\left(2\left(\frac{1}{2}-\frac{E_{max}+T_{max}}{n}\right)^2-\ln(2q_{m,s})\right)} = \textit{bound}_{TF}$$

If there exist $\alpha, \beta \in \mathbb{R}$ such that $E_{max} \leq \alpha n$, $T_{max} \leq \beta n$ then the protocol is secure when $\alpha+\beta < \frac{1}{2}-\sqrt{\frac{\ln(2q_m)}{2}}$.

Using a public PUF just adds a negligible term in the bound.

We have the following relation:

$$\text{Packet transmission time} = \frac{\text{Packet size}}{\text{Bit rate}}$$

The adversary succeeds to send s bits when $\frac{d_{AP}}{c}+\frac{s}{\text{Bit rate}} \leq T$ with $\frac{d_{AP}}{c}$ the packet traveling time is in ns, this is negligible compared to T in μs. So, we get the relation $s \leq \text{Bit rate}\times T$. For wireless communication, the maximal bit rate is of order 1Gbps and we define $T = 1\mu$s. So the prover can send maximum $s = 1000$ bits to the adversary. So the maximal s is $s = 2^{10}$.

For a noisy communication such that $E_{max} = 5\%n$ and $T_{max} = 0$ with $s = 2^{10}$, if the prover is close to the verifier ($m \leq 18$), pufDB cannot be proven secure against TF-attacks.

If the prover is close to the verifier then he can help the adversary in doing the authentication himself or in giving directly the device to the adversary. So, we can assume that the prover is quite far from the adversary proportionally to the distance allowed. For instance, if we consider that $d_{VP} = 3000\text{m}$, $B = 3\text{m}$, $T = 1\mu\text{s}$ and the speed of the light $c = 3.10^8\text{m.s}^{-1}$ we get $t_B = 10\text{ns}$ and $m = 20$. For $s = 2^{10}$, we obtain $q_{m,s} = 0.7917$ so the protocol achieves a security level of 2^{-10} in 110 rounds, and 2^{-20} in 307 rounds.

If we can lower T to $T = 100\text{ns}$ and $t_B = 10\text{ns}$ then the prover can send at most $s = 2^7$ bits to the adversary and we have security for a noisy communication with $E_{max} = 5\%n$ and $T_{max} = 0$ for $m \geq 15$ which corresponds to $t_{VP} > 71t_B$.

6 Conclusion

Until pufDB, none of the existing protocol has provided Terrorist Fraud resistance in the plain model without assuming that the adversary would not share his secret, which is not a realistic assumption. The protocol of Kleber et al. is not secure against Terrorist Fraud attacks. pufDB is an improvement of this protocol. We prove security against Distance Fraud and Mafia Fraud. We further prove the security against TF using a reasonable limitations on the number of transmission per round.

We compare with other distance bounding protocols. The parameters in pufDB, SKI [2, 3], FO [8, 14] and DBopt [4] are taken such that the protocols achieve 99% completeness with a noise of 5% as it is described in [4]. If we take the worst case for pufDB (i.e. $m = 1$), pufDB needs more rounds than the previous protocols to achieve the same security level. However, for m large, pufBD is more efficient than SKI and FO to achieve security against DF and MF and it almost reaches the optimal bounds of DBopt.

Protocol	n (security level of 2^{-10})	n (security level of 2^{-20})
SKI	48	91
FO	84	151
DBopt (DB2,DB3)	24	43
pufDB ($m = 1$)	345	474
pufDB ($m > 2n - 1$)	26	45

Table 1: Efficiency of the protocols against DFand MF for completeness 99% under noise 5% ($T_{max} = 0$)

Acknowledgement. The authors thank Negar Kiyvash and Daniel Cullina for their valuable help in the proof of Th. 3.

References

1. I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Practical & Provably Secure Distance-Bounding. *The 16th Information Security Conference, Dallas, Texas, USA*, pages 13–15, November 2013.
2. I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Secure & Lightweight Distance-Bounding. *Proceedings of LIGHT- SEC 2013, volume 8162 of LNCS*, pages 97-113, 2013.
3. I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Towards Secure Distance Bounding. *20th anniversary annual Fast Software Encryption (FSE 2013), LNCS*, 2013.
4. I. Boureanu and S. Vaudenay. Optimal Proximity Proofs. *10th International Conference on Information Security and Cryptology (INSCRYPT 2014)*, pages 13-15, December 2014.
5. S. Brands and D. Chaum. Distance-bounding protocols. in: Advances in Cryptology. *Eurocrypt'93*, pages 344-359, 1993.
6. Y. Desmedt. Major security problems with the 'unforgeable' (Feige)-Fiat- Shamir proofs of identity and how to overcome them. *In Proceedings of the 6th worldwide congress on computer and communications security and protection (SecuriCom)*, pages 147-159, March 1988.
7. U. Dürholz, M. Fischlin, M. Kasper, and C. Onete. A formal approach to distance bounding RFID protocols. *Proceedings of the 14th Information Security Conference ISC 2011, LNCS*, pages 47-62, 2011.
8. M. Fischlin and C. Onete. Terrorism in distance bounding: Modelling terrorist-fraud resistance. *Proceedings of ACNS 2013, Lecture Notes in Computer Science*, pages 414-431, 2013.
9. M. Igier and S. Vaudenay. Distance Bounding based on PUF. *Cryptology ePrint Archive, Report 2016/???*, 2016.
10. S. Kardaş, M.S. Kiraz, M.A. Bingöl, , and H. Demirci. A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions. *7th International Workshop, RFIDSec 2011*, pages 78-93, 2011.
11. H. Kılınç and S. Vaudenay. Optimal Distance Bounding with Secure Harware. under submission.
12. S. Kleber, R.W. Van Der Heijden, H. Kopp, and F. Kargl. Terrorist Fraud Resistance of Distance Bounding Protocols Employing Physical Unclonable Functions. *IEEE International Conference and Workshops on Networked Systems (NetSys)*, 2015.
13. U. Rührmair, Sölter. J., and F. Sehnke. On the Foundations of Physical Unclonable Functions. *Cryptology ePrint Archive, Report 2009/277*, 2009.
14. S. Vaudenay. On modeling Terrorist Frauds. *Provsec'13, Lecture Notes in Computer Science 8209*, pages 1-20, 2013.