Resisting Relay Attacks on Vehicular Passive Keyless Entry and Start Systems

Tao Yang, Lingbo Kong[§], Wei Xin, Jianbin Hu[*], Zhong Chen
Institute of Software, EECS, Peking University, Beijing, China
MoE Key Lab of Network and Software Assurance, Peking University, Beijing, China
MoE Key Lab of High Confidence Software Technologies, Peking University, Beijing, China
[§] School of Software Engineering, Beijing Jiaotong University, Beijing, China
Email: {ytao,xinwei,hjbin,chen}@infosec.pku.edu.cn
[*] *Jianbin Hu is the corresponding author.*

***Abstract*—Passive Keyless Entry and Start (PKES) systems are popularly embed in modern cars, which allow users to open and start their cars while having their car keys' in their pockets. They bring convenience to users but are vulnerable to relay attacks. A relay attack to PKES is a widely known attack against the challenge- response technique used in the passive keyless vehicle system, which allows to open and start the car while the true distance between the key and car remained large. The main countermeasure against relay attacks is the use of distance bounding protocols measuring the round-trip time between the car and the key. However, most schemes tend to a more complex design to decrease adversary's success probability. In this paper, we propose a novel distance bounding protocol to resist relay attacks in PKES systems, using only $2n$ bits of memory, which, to our best knowledge, is equal to Hancke and Kuhn's protocol and less than any existing protocols. In addition, by using our protocol, the key is able to detect adversary's malicious queries. We also make a comparison with typical previous distance bounding protocols in both memory and mafia fraud success probability.**

***Keywords*-Secure PKES, relay attack, distance bounding, keyless system**

I. Introduction

Complex electronic systems are embed in modern cars to improve driver safety and convenience. Recently, car manufacturers have introduced Passive Keyless Entry and Start (PKES) systems that allow users to open and start their cars while having their car keys' in their pockets. This feature is very convenient for the users since they don't have to search for their keys when approaching or preparing to start the car.

[1], [2], [3] analyzed the security of PKES systems and show that they are vulnerable to relay attacks. Relay attack is a widely known attack against the challenge- response technique used in the passive keyless vehicle system. It allowed to open and start the car while the true distance between the key and car remained large. It worked without physically compromising the key or raising any suspicion of the owner. To deploy a relay attack, an attacker needs a key agent ($\overline{K}$) and a car agent ($\overline{C}$), which not only have regular functions of the key and the car, but also with the ability of relaying communications. The relay channel between $\overline{K}$ and $\overline{C}$ usually has a long distance in order to relay information without being detected. The relay attack setup is shown in Fig. 1. A relay module in the dashed rectangular is made up of three parts, the key agent, the car agent and the relay channel. The car agent and the key agent are placed respectively near the real key and car. Any information transmitted from the real car to the real key is relayed by the key agent and the car agent to the real key. The key mistakes the car agent as the real car and responds. The response is then relayed back passing through the car agent and the key agent to the real car. The real car is unable to distinguish between the real key and the key agent and will therefore assume that the real key is in the near field and associated with the owner. This corresponds to the scenario where the key is e.g., in the owner's pocket in the supermarket, and the car is at the supermarket parking lot.

We note that the main reason why relay attacks are possible on PKES systems is that, to open and start the car, instead of verifying that the correct key is in its physical proximity, the car verifies if it can communicate with the correct key, assuming that the ability to communicate (i.e., communication neighborhood) implies proximity (i.e., physical neighborhood). This is only true for non-adversarial settings. In adversarial settings communication neighborhood cannot be taken as a proof of physical proximity. Given this, any secure PKES system needs to enable the car and the key to securely verify their physical proximity. This is only natural since the car should open only when the legitimate user (holding the key) is physically close to the car. We outline a new PKES system, based on distance bounding, that achieves this goal, and preserves user convenience for which PKES systems were initially introduced.

[3] tested 10 recent car models from 8 manufacturers and show that their PKES systems are vulnerable to certain types of relay attacks.

In this paper, we propose a novel low memory-cost distance bounding protocol to resist relay attack in PKES systems. Our protocol uses only $2n$ bits of memory, which, to our best knowledge, is equal to Hancke and Kuhn's protocol [4], and less than any other existing protocols. In addition, in our protocol, a key is able to detect malicious queries.

The rest of the paper is organized as follows. Section II presents the problems of existed relay attack countermeasures and our scheme. Section III introduces our novel protocol.

978-1-4673-0024-7/10/$26.00 ©2012 IEEE

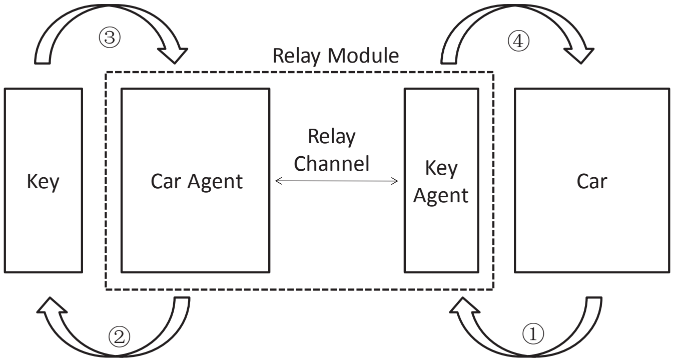

Fig. 1. Relay attack on a PKES system

Sections IV compares performances of our proposed protocol with other distance bounding protocols. In Section V, we describe related work on PKES attacks and distance bounding protocols. Finally, section VI concludes.

II. System Design

A. Problems of Relay Attack Countermeasures

We list several countermeasures proposed against relay attacks.

- **To rely on the signal strength:** The first one is to rely on the signal strength to indicate the proximity between the devices. In the countermeasure, the car transmits a short range LF signal such that only if the key is in its close proximity ($\sim$ 1m) will it hear the signal. Similarly, the car could measure the strength of the signal that the key transmits in order to infer the distance to the key. This countermeasure is very weak and can be simply defeated since the attacker can fully mimic the car and the key by relaying signals using expected signal levels.
- **To rely on the signal properties:** Other countermeasure that rely on the measurements of signal properties, like those using complex modulation schemes, measure group delay times or measure intermodulation products suffer from similar shortcomings. Namely, an attacker equipped with a good antenna and waveform generator can mimic expected signal features or can simply relay the observed signals without demodulating them.
- **To rely on the signal corruption:** In [6] signal corruption is also reported as a possible countermeasure against relay attacks. However, the authors note that this countermeasure can be overcome by an attacker using a good amplifier.
- **To rely on multi-channel communication:** Relay attacks can also be prevented using multi-channel communication, where typically out-of-band channels are used to verify if the relay occurred [19]. However, these approaches require human involvement, and as such are not well suited for PKES systems.

B. Distance Bounding

The main purpose of PKES is to allow access to the car and authorization to drive to the user that is at the time of entry and start physically close to the car. By being close to the car, the user indicates its intention to open the car and by being in the car, to drive the car. The car therefore needs to be able to securely verify if the user is close to the car to open the car and if the user is in the car to start the car. Given this, a natural way that can be used to realize secure PKES systems is by using **distance bounding**. Distance bounding denotes a class of protocols in which the verifier measures an upper-bound on its distance to the prover, where the prover can be trusted or untrusted. This means that given that the verifier and the prover are mutually trusted, the attacker cannot convince them that they are closer than they really are, just further.

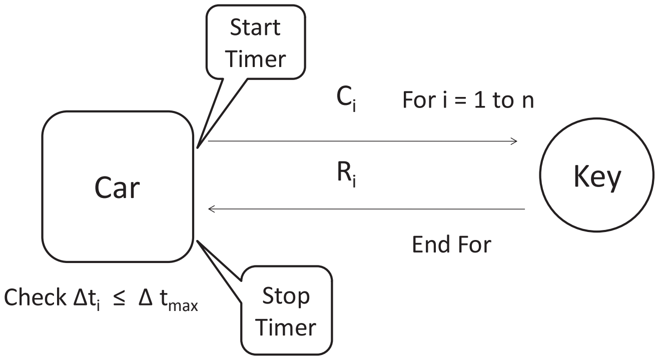

Fig. 2. Round Trip Time Measurement

A PKES system based on RF distance bounding would work in the following way. When the user approaches the car, the key and the car perform a secure distance bounding protocol. If the key is verified to be within a appropriate distance (e.g., 2m), the car would unlock and allow the user to enter. In order to start the car, the car will verify if the key is in the car. This can be done using a verifiable multilateration protocol proposed in [5], which allows the car to securely compute the location of a trusted key. In the following sections, we will introduce our distance bounding protocol for PKES systems.

III. Protocol Design

A. Problems in Existed Distance Bounding Protocols

We first review some existed protocols and examine them here and analyze their effectiveness and appropriateness for PKES systems.

- **Extra memory was required:** In 2005, Hancke and Kuhn [6], [4] first introduced a distance bounding protocol (HKP) and soon has been chosen as a reference-point since many schemes were based on the protocol. HKP was later modified by Munilla et al. with "void challenges" [7]. The main idea of [7] is to add another n-bits string p in each execution, if $p_i = 1$ car sends challenge (full-challenge) and $p_i = 0$ she does not(void-challenge). These void-challenges, will allow the key to detect whether she is communicating with an adversary or a legitimate car. Assume that the probability of being full challenges is p_f, in [8], author recommended, the optimal value of p_f is 4/5. Since p_f = 3/4 is close to 4/5 and easy to generate, the author proposed to use $2n$

bits to generate the vector p combining bits two by two, if $H_{2i-1}H_{2i}$ are '00','01' or '10', it means that $p_i = 1$, and if they are '11' it means $p_i = 0$. It is an exquisite design, however, it needs extra n bits to generate p.

- **Memory was wasted:** Another problem in existing distance bounding protocols is that only n bits of v^0 and v^1 have been used, leaving remaining n bits wasted. The author also suggested that using two directions of $n+1$ bits of v instead of $2n$ bits of v^0 and v^1. If a challenge $c_i = 0$, the key responds with the most significant bit of v, then discards this bit; If the challenge $c_i = 1$, the key will respond with the least significant bit of v, then discards this bit. This design seems possible, yet it brings a serious threat. If an adversary sends all 1-bit zero challenges to the key in advance, she will obtain the first n bits of v. As a result, the adversary will be able to answer most of the challenges except for the first '1' challenge from the car. Moreover, there is a concealed defect in this method, if the car sends c_i to the key, the key receives a wrong challenge bit for some reason such as noisy circumstances. The car and the key will lose synchronization which leads to disastrous consequences in the later rounds.

B. Our Scheme

Our proposed scheme aims to address aforementioned issues. The basic idea is described as follows: we use a Hash function $H(x, N_a, N_b)$ to generate a $2n$ bits string which is split into n bits of p and v respectively. If $p_i = 1$, the car sends a 1-bit random challenge; if $p_i = 0$, the car performs a XOR operation between p_i and v_i, if $p_i \bigoplus v_i = 1$, then car still sends a 1 bit random challenge, and if $p_i \bigoplus v_i = 0$, she does not. In this way, the probability of being full challenges can be achieved to 3/4. Since the car still has 1/4 probability to send void challenge, and adversary can not get both p_i and v_i in advance, the malicious queries to the key can be detected . In order to save memory, we use an expression of $(\neg p_i) \bigoplus (c_i \wedge v_i)$ instead of v_i^0 and v_i^1 as a response. The expression satisfies that c_i and $\neg c_i$ have the same chance to generate 0 or 1, an adversary can hardly finds any useful message when her pre-ask challenge (c_i^*) is different from the car's challenge (c_i), so she will unable to answer the challenge correctly in the fast phase.

Now we describe our protocol in detail.

Initialization. The Car (C) and the Key (K) share a secret x and agree on a security parameter n and a public pseudo random function H whose output size is $2n$. C sets a timing bound Δt_{max}.

Slow Phase. C generates a random nonce N_a and sends it to K. In response, K generates N_b and sends it to C. C and K then both compute $H^{2n} := H(x, N_a, N_b)$. Let $H_i (1 \le i \le 2n)$ be the i^{th} bit of H^{2n}, C and K split H_{2n} into two registers of length n: $p = H_1...H_n$ and $v = H_{n+1}...H_{2n}$.

Fast Phase. (for all i = 1, . . . , n)(a)At the car's side. C generates a random bit $c_i \in 0,1$, if $p_i = 1$, C sends c_i to K, if $p_i = 0$, C makes a further judgement, if $p_i \oplus v_i = 1$, C sends c_i to K, if $p_i \oplus v_i = 0$, she does not send.(b)At the key's side. Upon reception of a challenge c_i from C, if $p_i \oplus v_i = 0$, K responds with a random bit (error detected); else, K responds with $(\neg p_i) \bigoplus (c_i \wedge v_i)$ to C. The procedures of C and K are shown in Algorithm 1 and Algorithm 2.

Algorithm 1 The Procedure for C to Generate a Challenge

```
C generates a random bit $c_i \in$ (0,1)
if $p_i = 1$ then
    C sends $c_i$ to K
else
    if $p_i \oplus v_i = 1$ then
        C sends $c_i$ to K
    else
        C does not send challenge
    end if
end if
```

Algorithm 2 The Procedure for K to Respond a Challenge

```
K receives of a challenge $c_i$
if $p_i \oplus v_i = 0$ then
    K responds with a random bit
else
    K responds with $(\neg p_i) \bigoplus (c_i \wedge v_i)$
end if
```

Verification. The authentication succeeds if the received r_i from the key equal to $(\neg p_i) \bigoplus (c_i \wedge v_i)$ and $\Delta t_i \le \Delta t_{max}$ in each round.

IV. Security Analysis

As stated in [9], there are four types of frauds in distance bounding protocols: impersonation fraud, distance fraud, mafia fraud and terrorist fraud. Mafia fraud is regarded as the most serious attack among them since it can be mounted without the approvement or notice of both the car and the key. In [9], Mafia fraud is defined as an attack where an adversary defeats a distance bounding protocol using a MITM attack between the car and an honest key located outside the neighborhood. In this section, we mainly analyze the mafia fraud success probability. Generally, the adversary has two attack strategies. One is that she responds to the car without asking in advance to key (no-ask strategy). Another is that she can ask in advance to the key (pre-ask strategy). We denote the adversary's probability of success without asking as P_{no-ask} and that with asking as P_{ask}. Let p_f be the probability of being full challenges, n be the total number of intervals, and $p(i)$ be the probability that exactly i full-challenges occur. In no-ask case, adversary's strategy is as follows: (a) if a challenge is void, the adversary knows the right answer is also void, therefore, sends nothing; (b) if a challenge is full, the adversary replies with an random bit of 0 or 1. P_{no-ask} can be calculated as:

$$P_{no-ask} = (1 - \frac{p_f}{2})^n \tag{1}$$

In our protocol, $p_f = 3/4$, thus the adversary's probability of the success without asking i.e., P_{no-ask}, is $(5/8)^n$.

1) Asking in Advance: We use c_i^* to denote the challenge that the adversary asks to the key in advance, c_i to denote the challenge that the car sends to the key.

TABLE I
TRUTH TABLE OF $(\neg p_i) \bigoplus (c_i \wedge v_i)$

p_i	c_i	v_i	$\neg(p_i) \bigoplus (c_i \wedge v_i)$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

If $c_i^* = c_i$ or the car does not send a challenge bit, the adversary can correctly answer the response. If $c_i^* \neq c_i$, from the TableI, we can draw a conclusion: c_i and $\neg c_i$ have the same probability making $(\neg p_i) \bigoplus (c_i \wedge v_i)$ be 0 or 1. Therefore, the adversary could not distinguish the result of $(p_i \vee c_i) \bigoplus (c_i \wedge v_i)$ when $c_i^* \neq c_i$. Therefore, the adversary has a chance of 1/2 of giving a correct response. Therefore, the adversary's probability of success is as same as Munilla et al's protocol when $p_f = 3/4$. In [8], P_{ask} is regarded as the probability that no void-challenge occurs and also she guesses correctly all of the responses: $P_{ask} = (p_f \cdot \frac{3}{4})^n$. Actually, this result is not accurate, later Avoine gave a more precise result in [9] which is as follows:

$$P_{ask} = \begin{cases} (1-p_f)^n & if \quad 0 \leq p_f < 4/7 \\ (p_f \cdot \frac{3}{4})^n & if \quad 4/7 < p_f \leq 1 \end{cases} \tag{2}$$

Given that $p_f = 3/4$ in our protocol, the adversary's probability of success when asking in advance, $P_{ask} = (9/16)^n$. Therefore it is better for the adversary to choose the no-ask attack strategy in our protocol.

TABLE II
MEMORY AND SUCCESS PROBABILITY IN COMPARISON

	Memory	P_{no-ask}	P_{ask}
HKP	2n	$(\frac{1}{2})^n$	$(\frac{3}{4})^n$
MP	3n	$(\frac{3}{4})^n$	$(\frac{1}{2})^n$
KAP	4n	$(\frac{1}{2})^n$	$P_{kap-ask}$
ATP	$2^{n+1}-2$	$(\frac{1}{2})^n$	$(\frac{1}{2})^n(\frac{n}{2}+1)$
OURS	2n	$(\frac{5}{8})^n$	$(\frac{9}{16})^n$

2) Comparison: In this paper, we compare our protocol with a number of famous previous proposed distance bounding protocols as a comparison, including Hancke and Kuhn's protocol(HKP), Munilla et al's protocol(MP), Kim and Avoine's protocol (KAP), Avoine and Tchamkerten's Protocol (ATP). In MP, we assume $p_f = 1/2$, so $P_{no-ask} = (3/4)^n$ and $P_{ask} = (1/2)^n$ from Equation 1 and Equation 2. We also use some results from [10]. In KAP, $P_{ask} = \frac{p_d}{2} \sum_{i=1}^{i=n} (\frac{3-p_d}{4})^{i-1} (\frac{1}{2})^{n-i+1} + (\frac{3-p_d}{4})^n$, we assume $p_d = 1/2$, and use $P_{kap-ask}$ to substitute for it. TableII depicts the values of three parameters (memory, mafia fraud success probability of no asking (P_{no-ask}) and success probability of asking in advance (P_{ask}). From the table, we can see that our protocol consumes less memory and has a good security performance.

V. RELATED WORK

A. Attacks on Keyless Systems

The closest work to our investigation can be found in [1], [2]. The authors perform security analysis of Keyless Car Entry systems including relay attacks. While the performed analysis identifies the relay problem, the proposed relay attack consists of two separate UHF relay links to relay messages in both directions. The proposed abstract setup has the problem of creating a feedback loop as the car will also receive the relayed signal from the second link. We show that such a realization is not needed in modern PKES systems and demonstrate it experimentally. Moreover, the authors do not provide neither hardware design, nor practical implementation of the attack. Finally, no adequate countermeasures are proposed. Some practical attacks on PKES systems have been recently reported [11]. However, no detailed information is available and it is not possible to understand the details of the attack. It is unclear if the attack relies on a modulation/ demodulation relay or on a physical-layer relay attack. Moreover, it is impossible to verify the reported claims and if the attack is indeed real.

B. Relay attacks

Brands and Chaum [12] designed the first distance bounding protocol based on RTT to hinder relay attacks. In 2005, Hancke and Kuhn [6], [4] first introduced a distance bounding protocol (HKP) into RFID systems. HKP has been chosen as a reference-point since many schemes were based on the protocol. In 2006, Munilla et al. modified HKP by applying "void challenges" [7]. Reid et al. [13] eliminated HKP's vulnerability to the terrorist fraud attack. In 2009, Avoine et al. [14] extended the void challenges to p-symbols. Avoine et al. [15] and Trujillo-Rasua et al. [10] respectively brought tree-based and graph-based methods into distance bounding protocols. Kim et al. [16] provided a protocol based on binary mixed challenges that converges toward the expected and optimal $(1/2)^n$ bound on the success probability of the adversary. Singelée and Preneel [17] proposed a protocol using Error Correcting Code (ECC) to cope with bit errors during the rapid bit exchanges.

Recently, two RF distance bounding implementations appeared, showing the feasibility of implementing distance bounding protocols. One implemented XOR resulting in a processing time at the prover of approx. 50 ns [18] and the other implemented concatenation with the provers processing time of less than 1 ns [19].

VI. CONCLUSION

In this paper, we propose a novel distance bounding protocol to resist relay attacks in PKES systems, using only $2n$ bits of memory, which, to our best knowledge, is equal to Hancke and Kuhn's protocol and less than any existing protocols.

In addition, by using our protocol, the key is able to detect adversary's malicious queries. We also make a comparison with typical previous distance bounding protocols in both memory and mafia fraud success probability.

Acknowledgement

This work was supported in part by the NSFC under grant No. 61170263 and No. 61003230.

References

[1] S. M. M. Ansaf Ibrahem Alrabady, "Some attacks against vehicles passive entry security systems and their solutions," in *IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY VOL. 52, NO. 2*, 2003.

[2] ——, "Alrabady a. i., and mahmud s. m. 2005. analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs." in *IEEE Trans. Vehicular Technology, 54, 1, 41–50.*, 2005.

[3] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *NDSS*, 2011.

[4] G. Hancke and M. Kuhn, "An RFID Distance Bounding Protocol," in *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, IEEE. Athens, Greece: IEEE Computer Society, September 2005, pp. 67–73.

[5] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[6] G. Hancke, "A practical relay attack on iso 14443 proximity cards," Tech. Rep., 2005.

[7] J. Munilla, A. Ortiz, and A. Peinado, "Distance Bounding Protocols with Void-Challenges for RFID," in *Workshop on RFID Security – RFIDSec'06*. Graz, Austria: Ecrypt, July 2006.

[8] J. Munilla and A. Peinado, "Distance Bounding Protocols for RFID Enhanced by using Void-Challenges and Analysis in Noisy Channels," *Wireless Communications and Mobile Computing*, vol. 8, no. 9, pp. 1227–1232, January 2008.

[9] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, "A Framework for Analyzing RFID Distance Bounding Protocols," *Journal of Computer Security – Special Issue on RFID System Security*, 2010.

[10] R. Trujillo Rasua, B. Martin, and G. Avoine, "The Poulidor Distance-Bounding Protocol," in *Workshop on RFID Security – RFIDSec'10*, Istanbul, Turkey, June 2010.

[11] "Ettus research llc." http://www.ettus.com/.

[12] S. Brands and D. Chaum, "Distance-bounding protocols (extended abstract)," in *EUROCRYPT*, 1993, pp. 344–359.

[13] J. Reid, J. M. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, 2007, pp. 204–213.

[14] G. Avoine, C. Floerkemeier, and B. Martin, "RFID Distance Bounding Multistate Enhancement," in *Proceedings of the 10th International Conference on Cryptology in India – Indocrypt 2009*, ser. Lecture Notes in Computer Science, B. K. Roy and N. Sendrier, Eds., vol. 5922. New Delhi, India: Springer, December 2009, pp. 290–307.

[15] G. Avoine and A. Tchamkerten, "An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement," in *Information Security Conference – ISC'09*, ser. Lecture Notes in Computer Science, P. Samarati, M. Yung, F. Martinelli, and C. A. Ardagna, Eds., vol. 5735. Pisa, Italy: Springer, September 2009, pp. 250–261.

[16] C. H. Kim and G. Avoine, "RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks," in *8th International Conference on Cryptology And Network Security – CANS'09*, ser. Lecture Notes in Computer Science, J. A. Garay, A. Miyaji, and A. Otsuka, Eds., vol. 5888. Kanazawa, Ishikawa, Japan: Springer, December 2009, pp. 119–133.

[17] D. Singelée and B. Preneel, "Key establishment using secure distance bounding protocols," in *MobiQuitous*, 2007, pp. 1–6.

[18] M. Kuhn, H. Luecken, and N. O. Tippenhauer, "UWB impulse radio based distance bounding," in *7th Workshop on Positioning, Navigation and Communication, WPNC 2010*, Mar. 2010, pp. 28–37.

[19] K. B. Rasmussen and S. Čapkun, "Realization of rf distance bounding," in *Proceedings of the 19th USENIX conference on Security*, ser. USENIX Security'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 25–25.