# A class of precomputation-based distance-bounding protocols

Sjouke Mauw CSC/SnT, University of Luxembourg sjouke.mauw@uni.lu Jorge Toro-Pozo
CSC, University of Luxembourg
jorge.toro@uni.lu

Rolando Trujillo-Rasua SnT, University of Luxembourg rolando.trujillo@uni.lu

Abstract—Distance-bounding protocols serve to thwart various types of proximity-based attacks, such as relay attacks. A particular class of distance-bounding protocols measures round trip times of a series of one-bit challenge-response cycles, during which the proving party must have minimal computational overhead. This can be achieved by precomputing the responses to the various possible challenges. We formalize this class of precomputation-based distance-bounding protocols. By designing an abstract model for these protocols, we can study their generic properties, such as security lower bounds in relation to space complexity. Further, we present a novel family of protocols in this class that resists well to mafia fraud attacks.

#### I. Introduction

Contactless technologies such as RFID, have become the *de facto* solution for many identification/authentication applications, e.g. access control, ticketing, e-passports. Some access control mechanisms have been designed in such a way that physical proximity is enforced easily, e.g., mechanical locks or biometric identification. However, due to the open nature of wireless channels, providing the same kind of guarantee in wireless systems is far from trivial.

Simple proximity enforcing techniques, such as setting up small communication timeouts or short-range communication channels, can be easily circumvented in practice by a variety of attacks [1]. Perhaps, the most popular and devastating of such attacks is *mafia fraud* [2], also known as *relay attack* [3].

The most reliable countermeasure against these type of attacks is *distance-bounding* (DB) which typically consists in measuring the Round Trip Time (RTT) of a message exchange. Amongst more than 30 DB protocols proposed<sup>1</sup> so far, we can find a large class (e.g., [4], [5], [6], [7], [8]) whose members follow two core principles raised by Hancke and Kuhn in [3]:

- RTT measurements should exchange single-bit messages.
- Each RTT measurement ought to be based on a challengeresponse authentication scheme so that, even if the protocol stops after a few RTT measurements, some guarantees of proximity can be provided.

Distance-bounding protocols adhering to these principles normally consist of two phases. The first phase is called the *slow phase*, where the verifier and the prover exchange nonces and use a shared key to secretly *precompute* a lookup table with potential responses for the next phase. The second phase, known as *fast phase*, consists of *n* RTT measurements (often

1http://www.avoine.net/rfid/index.php

called *rounds*). At the *i*th round, the verifier sends a random bit-challenge  $c_i$  to the prover and starts a clock. The prover replies instantly to the challenge  $c_i$  by using the precomputed lookup table. Upon reception of the prover's reply, the verifier stops the clock and computes the RTT. The protocol finishes correctly if all responses are correct and all RTTs are lower than a predefined threshold.

Because all protocols based on these principles have a similar shape, it would be natural and useful to consider them as instantiations of the same protocol scheme, with slight variations. That would provide us with a mathematical model, allowing us to study theoretical properties that hold for a large class of protocols. We have called them *precomputation-based distance-bounding protocols*.

## II. PRECOMPUTATION-BASED DISTANCE-BOUNDING PROTOCOLS

In [3] the authors explain the advantage of avoiding a final slow phase, even at the cost of an apparent decrease in the resistance to mafia fraud. In terms of execution time and computational complexity, the cost of executing a couple of additional rounds during the fast phase is significantly lower than the cost of performing expensive cryptographic operations and message exchanges over a traditional communication channel.

Precomputation-based protocols are distance-bounding protocols without a final slow phase where all possible responses to the verifier's challenges are precomputed in the initial slow phase. These responses are stored in memory such that query time should be minimum. The authentication is carried on during the fast phase. Because of the time measurement, the operations have to be as low cost as possible, e.g., accessing to random access memory, simple bit operations.

We sketch a simple model that captures a prominent class of DB protocols based on precomputation. The approach uses a particular class of Deterministic Finite Automata (DFA) with labels attached to states. We consider a protocol as a set of DFA, where each automaton describes the protocol's behaviour in the fast phase. The structure and labeling of such automaton follows from the calculations in the slow phase, in which, e.g., the nonces are chosen. Consequently, every possible outcome of the slow phase results in an automaton.

The execution of a protocol therefore consists of the (random) selection of one automaton (in the slow phase) and a run (fast phase) consisting of a n-steps walk through the automaton, i.e. an alternation of input and output symbols, that represent challenges and responses, respectively. We remind that n stands for the number of rounds.

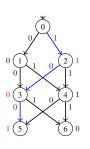


Fig. 1. An automaton example

In Figure 1 we depict an automaton example for the HK protocol [3] for 3 rounds. The states  $\{0,1,\ldots,6\}$  are linked by transitions represented by the arrows. The states have binary labels attached, shown to their left and right. We have shown also an execution with the challenges 100—in blue—whose corresponding responses—in red—are 101.

The proposed model captures

several state-of-the-art DB protocols, such as [3], [4], [5], [8]. The virtue of this model is that it supports generic analysis of members of this protocol class. For instance, we can analyze the security limits of a protocol in relation to the number of rounds.

#### III. PROPERTIES AND SECURITY ANALYSIS

In 2009, Avoine and Tchamakerten proposed the tree-based protocol [5], whose security against mafia fraud is  $\frac{1}{2^n}(1+\frac{n}{2})$ , where n is the number time measurements. Since then, that value has become a *de facto* lower bound on the resistance to this type of attacks.

Supported in our model, we have proved that, for any precomputation-based distance-bounding protocol, there exists an attack that succeeds with such a probability. This demonstrates that  $\frac{1}{2^n}(1+\frac{n}{2})$  is a tight lower bound on the security of this type of protocols against mafia fraud. Based on this result, we introduce the concept of *optimality* that stands for a precomputation-based distance-bounding protocol for which, there does not exist a mafia fraud attack whose probability of success is higher than the above-mentioned value.

In that sense, the model allows to analyze the relation memory-optimality given that the required memory is *measurable* according to the number of states of the largest possible automaton in the protocol. It is worth remarking tree-based approach is the only optimal protocol proposed so far. However, it requires an exponential amount of states and consequently the memory complexity becomes exponential.

We also describe a subclass within the precomputationbased distance-bounding protocols, whose members are *layered* and *random-labeled*. A brief description of these two properties is as follows:

- A protocol is layered if for every automaton, two input sequences of different length reach different states.
- A protocol is random-labeled if for a random automaton and a random state in it, the probability of being labeled with any input symbol is the same.

To evaluate the resistance of a DB protocol against mafia fraud usually two strategies are considered: *pre-ask* and *post-ask* [9], although the latter is not relevant in protocols without

a final slow phase [9]. A pre-ask strategy can be summarized as follows: the adversary relays the first slow phase between the verifier and the prover. Then –before the verifier starts the fast phase– it executes the fast phase with the prover, retrieving some information on possible responses (often called *pre-ask session*). Afterward, the attacker performs the fast phase with the legitimate verifier.

In the context of layered and random-labeled protocols, we proved that the best pre-ask strategy for the adversary is simply to reply to the verifier with the responses obtained from the prover in the pre-ask session. We state that HK and tree-based protocols are both within this subclass whereas the Poulidor protocol [4] is not.

Finally, we propose a family of layered and random-labeled protocols, called *uniform protocols*, whose members have a security level arbitrarily close to the optimal value  $\frac{1}{2^n}(1+\frac{n}{2})$ . The use of memory of these protocols are considerable lower than the exponential one required by the tree-based approach.

#### IV. FUTURE WORK

As future work, we will study security of precomputation-based distance-bounding protocols against other types of attack, e.g. distance fraud and terrorist fraud. We will also analyze deeply the relation optimality-memory. Our hypothesis is that optimality implies exponential amount of states. Further, for a given upper-bound on the number of states (i.e. available memory), we want to find the best precomputation-based distance-bounding protocol. In addition, we will study the security in non-layered precomputation-based distance-bounding protocols, e.g. Poulidor protocol [4].

### REFERENCES

- G. P. Hancke, K. Mayes, and K. Markantonakis, "Confidence in smart token proximity: Relay attacks revisited," *Computers & Security*, vol. 28, no. 7, pp. 615–627, 2009.
- [2] Y. Desmedt, C. Goutier, and S. Bengio, "Special uses and abuses of the Fiat-Shamir passport protocol," in *Proc. Advances in Cryptology* (CRYPTO'87), ser. LNCS, vol. 293. Springer, 1988, pp. 21–39.
- [3] G. Hancke and M. Kuhn, "An RFID distance bounding protocol," in Proc. First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm'05). IEEE, 2005, pp. 67–73.
- [4] R. Trujillo-Rasua, B. Martin, and G. Avoine, "The Poulidor distance-bounding protocol," in *Proc. 6th International Conference on Radio Frequency Identification: Security and Privacy Issues (RFIDSec'10)*, ser. LNCS, vol. 6370. Springer, 2010, pp. 239–257.
- [5] G. Avoine and A. Tchamkerten, "An efficient distance bounding RFID authentication protocol: Balancing false-acceptance rate and memory requirement," in *Proc. 12th International Conference on Information Security (ISC'09)*, ser. LNCS, vol. 5735. Springer, 2009, pp. 250–261.
- [6] R. Trujillo-Rasua, B. Martin, and G. Avoine, "Distance bounding facing both mafia and distance frauds," *IEEE Transactions on Wireless Commu*nications, vol. 13, no. 10, pp. 5690–5698, 2014.
- [7] C. Kim and G. Avoine, "RFID distance bounding protocols with mixed challenges," *IEEE Transactions on Wireless Communications*, vol. 10, no. 5, pp. 1618–1626, 2011.
- [8] S. Kardas, M. S. Kiraz, M. A. Bingöl, and H. Demirci, "A novel RFID distance bounding protocol based on physically unclonable functions," in *Proc. 7th International Conference on Radio Frequency Identification: Security and Privacy Issues (RFIDSec'11)*, ser. LNCS, vol. 7055. Springer, 2012, pp. 78–93.
- [9] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, "A framework for analyzing RFID distance bounding protocols," *J. Comput. Secur.*, vol. 19, no. 2, pp. 289–317, Apr. 2011.