Revisiting DoS Attacks and Privacy in RFID-Enabled Networks

Paolo D’Arco, Alessandra Scafuro, and Ivan Visconti
University of Salerno, Italy
{paodar,visconti}@dia.unisa.it, alescafu@gmail.com

Abstract. Vaudenay presented in [ASIACRYPT 2007] a general RFID security and privacy model that abstracts some previous works in a single, concise, and much more understandable framework. He introduced eight distinct notions of privacy, corresponding to adversaries of different strength, and proved some possibility and impossibility results for such privacy notions. However, some interesting problems as: 1) achieving stronger privacy using low-cost tags (i.e., tags that usually can not perform public-key cryptography), 2) achieving stronger privacy in presence of side-channel attacks (e.g., DoS attacks, detection of the outputs of identification protocols), and 3) achieving stronger privacy under standard complexity-theoretic assumptions, are still left open.

In this paper, we address the above problems and give two contributions. First of all we show that Vaudenay’s privacy notions are impossible to achieve in presence of DoS attacks. Therefore, we extend the model to better reflect the real-world scenario, where these attacks are easy to mount (e.g., by physically destroying/making inactive tags). More precisely, we refine Vaudenay’s privacy model to deal with DoS and DoS-like attacks, and introduce an additional privacy notion, referred to as semi-destructive privacy, which takes into account hardware features of some real-world tags. Then, we show an efficient RFID protocol that, by only using symmetric-key cryptography, satisfies the notion of semi-destructive privacy, under standard complexity-theoretic assumptions.

1 Introduction

RFID technology. Radio frequency identification (RFID) enables readers to perform wireless identification of objects labeled with RFID tags. It is well known that the pervasive use of this technology introduces various privacy threats (e.g., tracking of users, profiling, linking activities). Unfortunately, RFID tags have often very restricted computational and storage capabilities. Therefore, privacy so far has been addressed with lower priority with respect to other critical requirements as authentication (which prevents an adversary from impersonating tags) and efficiency (e.g., suitability for low-cost tags).

Privacy models. The design of a secure and privacy-preserving RFID system requires an appropriate security and privacy model to enable a careful analysis of the system. However, existing security and privacy models for RFID
(e.g., [1,2,3,4]) suffer from various shortcomings. Indeed, they do not consider important aspects like adversaries with access to side-channel information (e.g., information on whether the identification of a tag was successful or not) or the privacy of corrupted tags (i.e., whose secrets have been disclosed).

Vaudenay’s model. Given the various and in some cases incomparable privacy models defined before, Vaudenay presented in [5] a general model that abstracts some previous works in a single, concise and more understandable framework. Indeed, he introduced eight privacy notions which correspond to adversaries of different strength (the security definition is equivalent to the one given in [3]). In [6] the eight privacy classes of [5] have been reduced to three privacy classes, under some restrictions on the power of the adversary. According to [5], the first four notions (i.e., weak, forward, destructive, and strong privacy) allow the adversary to obtain, as side-channel information, the result of an interaction between tag and reader. The other four notions (narrow-weak, narrow-forward, narrow-destructive and narrow-strong privacy) instead do not consider the side-channel information about the successful identification of a tag with a reader. Unfortunately the only non-narrow privacy notions achieved in [5] are forward and weak privacy. Moreover, forward privacy is obtained by using public-key cryptography (not implemented yet in currently available low-cost tags). On the other hand, concerning with the narrow privacy notions, narrow-strong privacy is obtained by using public-key cryptography and narrow-destructive privacy is obtained in the controversial random oracle model [7]. In a recent work [8] following up some ideas discussed in [9], narrow-forward privacy has been obtained with symmetric-key operations only on the tags, but extending the model with anonymizers.

DoS attacks and privacy in RFID systems. In [5] a narrow-destructive RFID protocol, secure in the random oracle model, was proposed. Moreover, it was showed how a DoS attack can be mounted by the adversary to desynchronize a tag from a reader. This attack has the consequence that the tag is not able to succeed anymore in the identification with the reader. It was also pointed out how the adversary can use the desynchronization attack, along with side channel information, to succeed in the *privacy experiment*, which is used to model the privacy notion. More specifically, the desynchronization attack is turned into a privacy attack. Finally, building on that, it was shown that the narrow-destructive scheme does not even enjoy weak privacy.

Our results. In this paper, we give two contributions. First of all, we revisit Vaudenay’s model by considering DoS attacks. We show that an adversary that is able to stop the activities of a tag is *always successful* in winning the privacy experiment, regardless of the privacy level considered (i.e., even achieving narrow-weak privacy would be impossible). DoS attacks are not included in Vaudenay’s model and we show that, unfortunately, the model results to be inadequate in measuring privacy notions when such attacks can occur. However, since in the real world a DoS attack is *semantically different from a privacy violation*, we consider the possibility of refining the adversarial model, so that privacy notions