Protocol for Simultaneous Ownership Transfer of Multiple RFID Tags with TTP

Wei Zhou\textsuperscript{1,2} and Selwyn Piramuthu\textsuperscript{2,3}

\textsuperscript{1} Information & Operations Management, ESCP Europe, Paris, France
\textsuperscript{2} RFID European Lab, Paris, France
\textsuperscript{3} Information Systems and Operations Management, University of Florida Gainesville, Florida 32611-7169, USA
wzhou@escpeurope.eu, selwyn@ufl.edu

Abstract. Ownership transfer of items that are RFID-tagged require more than physical means to accomplish the process. Their inherent ability to communicate with entities that are not necessarily in their close proximity necessitates supplementary ownership transfer measures that complement the transfer of the physical item. Over the past few years, several ownership transfer protocols have been developed with the explicit purpose of transferring ownership of a tag from one owner to another. While it generally suffices to transfer ownership of tags one by one, sometimes it is necessary to simultaneously transfer ownership of multiple tags from one owner to another. This is especially true when multiple items are required to belong together during and outside of the ownership transfer process. Extant literature on RFID ownership transfer protocol, however, does not consider this scenario. We propose a protocol that attempts to address this gap in the literature.

Keywords: RFID, ownership transfer, multiple tags.

1 Introduction

Over the past five years, several ownership transfer protocols for RFID tags have been proposed and studied (e.g., \cite{1, 2, 3, 6, 8, 9}). A majority of these have been found to have vulnerabilities that can readily be taken advantage of by a resourceful active adversary (e.g., \cite{6}). A majority of these ownership transfer protocols deal with the common single tag - single owner scenario. A few (e.g., \cite{5}) consider variations of this scenario such as the single tag - multiple owners, multiple tag - single owner, and inclusion/exclusion scenarios where tags move in and out of the system.

Another stream of research related to RFID authentication protocols include published literature that followed as a direct result of the ‘yoking proof’ (\cite{4}) protocol, ‘grouping proof’ (\cite{7}) protocol and their variants. Essentially, these protocols purport to simultaneously authenticate the presence of multiple tags in the field of the reader. Such a scenario may include, for instance in the example presented in \cite{4}, the necessity of simultaneous presence of a given pharmaceutical
item along with its instructions. Although the intention is to authenticate the presence of multiple tags simultaneously, these protocols and a majority of their variants accomplish this in a sequential manner whereby the authentication of the first tag is immediately followed by the authentication of the next tag, and so on. Since these authentications are done sequentially as a compact batch, the process is almost similar to comparable simultaneous authentication of these tags.

To our knowledge, extant published literature does not include the scenario where tags that need to be simultaneously present together change ownership together from the same previous owner to the same new owner. Given the need for ‘yoking proof’ protocol and its variants and the need for ownership transfer protocols, it is not hard to envision the need for protocols that incorporate the dynamic present in both these scenarios. We purport to fill this gap in extant literature by proposing a protocol for verifying the simultaneous presence of multiple tags in the field of the reader while ownership transfer involving these tags takes place.

We consider the scenario where two tags that need to be simultaneously present in the field of the reader change ownership in the presence of a trusted third party (TTP). We do not consider the case where a TTP is absent. Without the presence of a TTP, it is extremely difficult to transfer ownership of items between two entities even if these two entities share a common secret that is not known to any other entity. In this case, the protocol becomes an ownership sharing one and not an ownership transfer protocol since the previous owner may continue to maintain RF access to the tag. Since this paper is not about ownership sharing, we do not consider the case where a TTP is absent. The proposed protocol is an extension of the single owner - single tag ownership protocol presented in ([6]) with appropriate and necessary modifications to incorporate verification of the simultaneous presence of multiple tags.

This paper is organized as follows: The next section provides a sketch of the proposed protocol for two tags transferring ownership between two owners in the presence of a TTP. Section 3 provides a brief security analysis of the proposed protocol. Section 4 concludes the paper with a brief discussion.

2 Simultaneous Ownership Transfer Protocol with TTP

Notation

The following notations are used in this paper:

- \( N_J \): random \( l \)-bit nonce generated by entity \( J \)
- \( R_i, T_i \): reader/owner \( i \), Tag \( i \)
- \( s_{ij} \): shared keys between/among entities (including tags)
- \( H \): one-way hash function \( \{0, 1\}^* \rightarrow \{0, 1\}^l \)
- \( f'_k, f_k \): keyed (with key \( k \)) encryption function
- \( t_i \): shared secret between tag \( i \) and TTP
- \( r_i \): shared secret between reader \( R_i \) and TTP