Information Processing Letters 113 (2013) 151–155

Contents lists available at SciVerse ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

A note on time-bound hierarchical key assignment schemes

Giuseppe Ateniese[a], Alfredo De Santis[b], Anna Lisa Ferrara[c], Barbara Masucci[b,*]

[a] *The Johns Hopkins University, Baltimore, MD 21218, USA*
[b] *Università di Salerno, 84084 Fisciano (SA), Italy*
[c] *Bristol University, Bristol, BS8 1UB, UK*

ARTICLE INFO

Article history:
Received 15 September 2010
Received in revised form 10 May 2012
Accepted 5 January 2013
Available online 10 January 2013
Communicated by A. Tarlecki

Keywords:
Cryptography
Distributed systems
Safety/security in digital systems
Access control

ABSTRACT

A *time-bound hierarchical key assignment scheme* is a method to assign time-dependent encryption keys to a set of classes in a partially ordered hierarchy, in such a way that each class can compute the keys of all classes lower down in the hierarchy, according to temporal constraints.

In this paper we consider the *unconditionally secure* setting for time-bound hierarchical key assignment schemes and distinguish between two different goals: security with respect to *key indistinguishability* and against *key recovery*. We first present definitions of security with respect to both goals; then, we prove a tight lower bound on the size of the private information distributed to each class; finally, we show an optimal construction for time-bound hierarchical key assignment schemes.

1. Introduction

A *time-bound hierarchical key assignment scheme* is a method to assign time-dependent encryption keys to a set of classes in a partially ordered hierarchy, in such a way that each class can compute the keys of all classes lower down in the hierarchy, according to temporal constraints. Specifically, we consider a scenario where the users of a computer system are organized in a certain number of disjoint classes, called security classes. The life-time of the system is divided into a sequence of time periods. Each user in a class is authorized to access the data of a class lower down in the hierarchy at a certain time period, provided that she has the credentials to compute the key corresponding to that class and for that time period.

There are several applications which may be implemented by using a time-bound hierarchical key assignment scheme. As an example, consider a web-based electronic newspaper company which offers several types of subscription packages, covering different topics. Each user may decide to subscribe to a package for a certain period of time (e.g., a week, a month, or a year). Subscription packages could be structured to form a partially ordered hierarchy where leaf nodes represent different topics and an internal node represents a package covering all topics associated to the leaf classes which can be reached by that node. For each time period, an encryption key is then assigned to each node in the hierarchy. The key corresponding to a leaf class can be computed by each user that subscribes to a package which includes the topic associated to that leaf class and for that period of time. A similar solution was employed by Bertino et al. [4], who showed how to control access to an XML document according to temporal constraints.

In this paper, we consider two different security goals: security with respect to *key indistinguishability* and security against *key recovery*. Security with respect to key indistinguishability formalizes the requirement that the adversary is not able *to learn any information* about a key that it should not have access to, i.e., it is not able to distinguish it from a random string having the same length. On the

[*] Corresponding author.
E-mail addresses: ateniese@cs.jhu.edu (G. Ateniese), ads@dia.unisa.it (A. De Santis), anna.lisa.ferrara@bristol.ac.uk (A.L. Ferrara), masucci@dia.unisa.it (B. Masucci).

0020-0190/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ipl.2013.01.006

other hand, security against key recovery corresponds to the requirement that an adversary is not able to *compute* a key that it should not have access to.

The most used approach to time-bound key assignment schemes is based on unproven specific assumptions (e.g., [1,2,9,5,7,16,11,15,14,12,13,3]). In this paper we focus on an information-theoretic approach which differs from the above computational approach since it does not depend on any unproven assumption. In [8] an information-theoretic approach to hierarchical key assignment schemes has been considered. A hierarchical key assignment scheme controls the accesses among the classes with respect to the structure of the hierarchy but does not consider time-dependent constraints.

In the information-theoretic setting, the key assigned to each class at a certain time period is *unconditionally secure*, with respect to one of the above security goals, against an adversary with unlimited computing power, controlling any coalition of classes not allowed to compute such a key. We present definitions of security with respect to each goal in the unconditionally secure setting and then we prove a tight lower bound on the size of the private information distributed to each class.

2. The model

Consider a set of users divided into a number of disjoint classes, called *security classes*. A security class can represent a person, a department, or a user group in an organization. A binary relation $\preccurlyeq$ that partially orders the set of classes V is defined in accordance with authority, position, or power of each class in V. The poset $(V, \preccurlyeq)$ is called a *partially ordered hierarchy*. For any two classes u and v, the notation $u \preccurlyeq v$ is used to indicate that the users in v can access u's data. We denote by A_v the set $\{u \in V\colon\ u \preccurlyeq v\}$, for any $v \in V$. The partially ordered hierarchy $(V, \preccurlyeq)$ can be represented by a directed graph where each class corresponds to a vertex in the graph and there is an edge from class v to class u if and only if $u \preccurlyeq v$. Further, this graph can be simplified by eliminating all self-loops and edges which can be implied by the property of the transitive closure. We denote by $G = (V, E)$ the resulting directed acyclic graph.

In this paper we consider the case where a user may be in a class for only a period of time. We consider a sequence $T = (t_1, \ldots, t_n)$ composed of n distinct time periods. Each user may belong to a class for a certain non-empty contiguous subsequence λ of T. Let $\mathcal{P} = \{(t_i, \ldots, t_j) | 1 \leqslant i \leqslant j \leqslant n\}$ be the set of all non-empty contiguous subsequences of T. Such a set is called the *interval-set* over T. In the following, given a time sequence $\lambda \in \mathcal{P}$, we denote by $t \in \lambda$ the fact that the time period t belongs to the sequence λ. Moreover, we abuse notation by using t to denote a time period $t \in T$ as well as the time sequence $(t) \in \mathcal{P}$.

A *time-bound hierarchical key assignment scheme* for a partially ordered hierarchy represented by a directed acyclic graph $G = (V, E)$ and a time sequence T is a method to assign a private information $s_{v,\lambda}$ to each class $v \in V$ for each time sequence $\lambda \in \mathcal{P}$ and an encryption key $k_{u,t}$ to each class $u \in V$ for each time period $t \in T$. The generation and distribution of the private information and keys is carried out by a trusted third party, the TA, which is connected to each class by means of a secure channel. The encryption key $k_{u,t}$ can be used by users belonging to class u in time period t to protect their sensitive data by means of a symmetric cryptosystem, whereas, the private information $s_{v,\lambda}$ can be used by users belonging to class v for the time sequence λ to compute the key $k_{u,t}$ for any class $u \in A_v$ and each time period $t \in \lambda$. For each class $u \in V$, each time sequence $\lambda \in \mathcal{P}$, and each time period $t \in T$, we denote by $S_{u,\lambda}$ and $K_{u,t}$ the sets of all possible values that $s_{u,\lambda}$ and $k_{u,t}$ can assume, respectively.

We formally define time-bound hierarchical key assignment schemes by using the entropy function (we refer the reader to the Appendix A for some proprieties of the entropy function and to [6] for a complete treatment of Information Theory), mainly because this leads to a compact and simple description of the schemes and because the entropy approach takes into account all probability distributions on the keys assigned to the classes. In the following, with a boldface capital letter, say $\mathbf{Y}$, we denote a random variable taking values on a set, denoted by the corresponding capital letter Y, according to some probability distribution $\{Pr_{\mathbf{Y}}(y)\}_{y \in Y}$. The values such a random variable can take are denoted by the corresponding lower case letter. Given a random variable $\mathbf{Y}$, we denote by $H(\mathbf{Y})$ the Shannon entropy of $\{Pr_{\mathbf{Y}}(y)\}_{y \in Y}$.

Now we are ready to describe the *correctness* and *security* requirements that a time-bound hierarchical key assignment scheme has to satisfy.

Correctness. *Each user can compute the key held by any class lower down in the hierarchy for each time period in which it belongs to its class.*
Formally, for each class $v \in V$, each class $u \in A_v$, each time sequence $\lambda \in \mathcal{P}$, and each time period $t \in \lambda$, it holds that $H(\mathbf{K}_{u,t} | \mathbf{S}_{v,\lambda}) = 0$.

Notice that the correctness requirement is equivalent to saying that the values of the private information $s_{v,\lambda}$ held by each user belonging to a class $v \in V$ for a time sequence $\lambda \in \mathcal{P}$ correspond to a unique value of the key $k_{u,t}$, for each class $u \in A_v$ and each time period $t \in \lambda$.

As regards as the security requirement, for each class $u \in V$ and each time period $t \in T$, the key $k_{u,t}$ should be protected against a coalition of users belonging to each class v such that $u \notin A_v$ in all time periods, and users belonging to each class w such that $u \in A_w$ in all time periods but t. We denote by $F_{u,t}$ the set of all pairs (class, time-sequence) whose credentials do not allow to compute the key $k_{u,t}$. Formally, $F_{u,t} = \{(v, \lambda) \in V \times \mathcal{P}\colon\ u \notin A_v$ or $t \notin \lambda\}$. Given a set $X = \{(v_1, \lambda_1), \ldots, (v_\ell, \lambda_\ell)\} \subseteq F_{u,t}$, we denote by S_X the set $S_{v_1,\lambda_1} \times \cdots \times S_{v_\ell,\lambda_\ell}$. We consider two different security goals: security with respect to *key indistinguishability* and security against *key recovery*. Security with respect to key indistinguishability formalizes the requirement that the adversary coalition is not able *to learn any information* about a key that it should not have access to, i.e., it is not able to distinguish it from a random string having the same length. On the other hand, security against key recovery corresponds to the requirement