1. Introduction

1.1 The Hierarchical Access Control Problem

With the rapid growth and pervasive deployment of information systems, sharing resources among multiple users over an open channel has become widespread. Access control on user permissions is a fundamental issue in any system that manages distributed resources. In this paper, we consider a multilevel security scenario, where users and data of an information system are organized into a hierarchy composed of disjoint security classes. Such a hierarchical structure arises from the fact that users in a distributed system may have distinct rights to access different parts or depths of the resources in the system, and some users may have higher privileges (in other terms, security levels or clearances) than others. In the real world there are many examples of this kind of hierarchy, such as in business administration, government departments, diplomatic corps, and the military. A hierarchical key assignment (KA) is to assign a distinct cryptographic key to each class so that users attached to any "base" class can also derive the keys of "lower" classes. As confidential data are classified into such security classes, they can be protected with respective encryption keys using a symmetric cipher, where the decryption operation asks a user for the same encryption key so as to recover the data.

Let there be \( m \) security classes \( C_i, 1 \leq i \leq m \) in the hierarchy partially ordered according to a binary relation \( \preceq \). In this partial-order hierarchy \( (C, \preceq) \), \( C_j \preceq C_i \) means the security level of class \( C_j \) is lower than that of class \( C_i \) (or, \( C_i \) dominates \( C_j \)), and \( C_j \preceq C_i \) allows for the additional case of \( j = i \). Formally, the hierarchical KA problem is to assign a key \( K_j \) to each class \( C_j \), so that a user assigned to her base class \( C_i \) can use the issued \( K_j \) to derive any \( K_j \) (thus to recover the data in \( C_j \)), if and only if \( C_j \preceq C_i \).

The partial-order hierarchy \( (C, \preceq) \) can be mapped to a directed acyclic graph (DAG), where each class corresponds to a vertex and there is a directed edge from \( C_i \) to \( C_j \) if and only if \( C_j \preceq C_i \). This graph can be simplified by eliminating all self-loops and edges which can be implied by the property of the transitive closure. Hence for such a refined DAG, an edge from \( C_i \) to \( C_j \) implies that \( C_j \preceq C_i \) and there is no \( C_k \) such that \( C_i \preceq C_k \preceq C_j \). In this case, we say \( C_j \) is an immediate descendant of \( C_i \), and \( C_i \) is an immediate ancestor of \( C_j \). Accordingly, if \( C_j < C_i \), but \( C_j \) is not an immediate descendant of \( C_i \), there must be a directed path from \( C_i \) to class \( C_j \) connected by two or more directed edges. A class may have multiple immediate ancestors (e.g., in Fig. 1, \( C_6 \) has two immediate ancestors \( C_2 \) and \( C_3 \)).

1.2 From Class Keys to Session Keys

In many commercial applications, there is an explicit temporal restriction so that a user is attached to her base class for only a limited period of time consisting of a contiguous set of time slots. Let the time dimension be discretized into even units (i.e., time slots or intervals) \( t = 0, 1, \ldots, z \). Here the maximum index \( z \) should not be considered as a limitation of the access control, as the system lifetime may be arbitrarily large. For instance, if each time slot represents a second, \( z = 3.156 \times 10^7 \) denotes roughly 1 year; if each slot represents a week, \( z = 5217 \) denotes roughly 100 years.

Now, instead of with the previous \( K_i \), let the class be assigned to a user at time \( t \) be encrypted with a volatile key \( k_{ij} \). Such periodical update of the encryption key (i.e., employing a dynamic key instead of a static one) implies enhanced security against cryptanalysis, and thus is also beneficial to applications where there are no explicit temporal con-
strains. Incorporating the temporal feature, we say the class key $K_i$ is instantiated with a series of session keys $\{k_{ij}\}$, by specifying:

- The static $K_i$ for $C_i$ is only used for generating session keys $\{k_{ij}\}$ as well as deriving the time-invariant class key $K_j$ of any lower class $C_j < C_i$, but never for actual data encryption.

- Only the time-based $k_{ij}$ is employed by the aforementioned symmetric cipher for real data protection with respect to security class $C_j$, from session to session indexed by the time slot $t$.

A typical application of such time-bound hierarchical KA scheme is the digital pay TV system, where the service provider organizes the channels into several possible subscription packages for users’ choices [1]. For example in Fig. 1 there are four independent TV channels $C_5$, $C_6$, $C_7$, and $C_8$, and subscription to package $C_5$ allows for the access to two of them ($C_6$ and $C_8$), while subscription to package $C_1$ allows for all. Another example is the electronic journal subscription system, where a user can subscribe to any combination of the available journals within a chosen period of time [2].

Assume a trusted central authority (CA) manages the key assignment. Upon registration, a user authorized to her combination of the available journals within a chosen period of subscription system, where a user can subscribe to any combination of the available journals within a chosen period of time [2].

In this paper, we refer interchangeably to time-based, time-bound, time-dependent, and time-variant. The rest of remarks are in Sect. 5.

2. Time-Bound Hierarchical KA: A Survey

In the literature, the hierarchical cryptographic KA problem was first studied by Akl and Taylor [3] in 1983, where the temporal consideration was yet unavailable. A recent modification of the Akl-Taylor scheme [3] can be found in [1], where a technique termed “merging” is introduced so that a solution more efficient than the original one [3] is possible; even the multilevel security hierarchy itself may not need to be constructed.

In 2002, Tzeng proposed a time-dependent hierarchical KA scheme [4] as an extension of the Akl-Taylor approach [3] with an additional access control on the temporal dimension technically enabled with the Lucas sequence [5], which is similar to the RSA public-key cryptosystem [6]. The scheme has some interesting applications such as secure broadcasting and cryptographic key backup [4]. Bertino et al. immediately adopted Tzeng’s scheme and showed that the scheme [4] is readily applicable to secure broadcasting of XML documents [7]. However, this first time-bound hierarchical KA scheme [4] was soon found to be vulnerable to the collusion attack. In [8], Yi and Ye showed that three users can conspire to infer some session keys that even a combination of them is not entitled to, but no security fix was proposed. We note that the identified security breach is irrelevant to the Lucas sequence [5] featured in Tzeng’s scheme [4], although there are certain known weaknesses associated with the sequence [9].

In 2004, Chien proposed the second time-bound hierarchical KA scheme employing a tamper-resistant device [10], which is a direct extension to the time-invariant hierarchical KA scheme earlier proposed by him and Jan [11]. The time-dependent scheme [10] is quite different from Tzeng’s [4] and greatly improves the computational performance. Interestingly, later Yi again showed that Chien’s scheme is subject to the collusion attack, where again three users can conspire to acquire some unauthorized session keys [12], but in a manner not as sophisticated as in his previous collusion attack [8] against Tzeng’s scheme [4]. Again Yi did not propose any security fix, though several very lightweight remedies are possible [13]. Although this time Bertino et al. took into consideration Yi’s three-party collusion attack [12] and proposed in [14] a security fix, their approach requires that the tamper-resistant device additionally support elliptic-curve cryptography, and thus is far more complex and cost-expensive than straightforward improvements on Chien’s scheme [10] such as those demonstrated by De Santis et al. [13]. Moreover, a complex solution does not always make for security [15], and the heavyweight security fix presented by Bertino et al. [14] was recently found to be still vulnerable to the collusion attack [16], where even only two conspirers are sufficient to break the fix.

In 2005, Yeh proposed a new time-bound hierarchical KA scheme [2] based on the RSA public-key cryptosystem [6], which is claimed to be resilient to collusion attacks. Unfortunately, Atieniese et al. soon identified that the scheme [2] is insecure against a two-party collusion attack [17], and the attack even affects a later work by Yeh published in 2008 [18]. There is also a scheme [19] very similar to Yeh’s [2], and is found to be vulnerable to a two-party collusion attack [20] as well.

In 2006, Wang and Laih proposed an alternative implementation of the Akl-Taylor scheme [3] employing the so-called merging technique [1]. The technique not only is applicable to the spatial dimension (i.e., the partial-order hierarchy) but also can be extended to construct a time-bound KA scheme based on a two-dimensional “global hierarchy”, which is the Cartesian product [4] of the security class hierarchy and the virtual time hierarchy. At the same
time, Tzeng proposed a secure data access system [21] based on an anonymous authentication scheme and his new time-based hierarchical KA scheme, the latter among which appears immune to collusion attacks. In the same year, the first result that provides a formal framework for time-bound hierarchical KA schemes was given by Ateniese et al. [17], where the notion of security for such KA schemes is formalized and two provably secure solutions are also proposed. It is worth noting that, both Tzeng’s new time-bound KA scheme [21] and Ateniese et al.’s provably secure solutions [17] consider the spatial hierarchy and the temporal dimension in an integrated, transformed view like the “global hierarchy” [1]. Therefore, the underlying ideas of these three works [1], [17], [21] in 2006 bear certain similarities.

The study on time-dependent hierarchical key assignment originated from the time-invariant KA problem in a partial-order hierarchy [3], but recently the research on purely time-based KA has become a topic of interest, where the notion of security classes is absent, i.e., the considered multilevel security reduces to a setting with only a universal class. For example, Atallah et al. presented in 2007 a provably secure approach that can incorporate time-dependent capabilities to existent key management schemes [22]. If the time is regarded as a single dimension, their solution can be extended to higher dimensions, and a proof of concept with respect to two dimensions is presented in [23] in the geospatial setting. In 2008, Srivatsa et al. followed the same idea, and applied Briscoe’s time-dependent KA scheme [24] to three dimensions, in a similar context of location-based broadcast services [25].

The topic of time-bound hierarchical KA has been widely discussed since 2002 [4]. A major problem observed is that, a proposed scheme may soon be found subject to certain collusion attacks (e.g., [8] against [4], both [12] and [13] against [10], [20] against [17], [19] against both [2] and [18], and the recent [16] against [14]), though sometimes a corresponding remedy may be available. Another problem is as follows. Typically, these schemes either involve public-key operations (modular exponentiations following the Akl-Taylor style [3]) or alike computations (the Lucas sequence in [4], and even bilinear maps in [17]), or require the protection by a tamper-resistant device (sometimes even both, as in Bertino et al.’s heavyweight security fix [14]). However, public-key (i.e., asymmetric) operations can be about a thousand times slower than symmetric ones [6], and commodity (particularly, low-cost) devices usually are not equipped with tamper-resistant casings. Hence, existent time-bound hierarchical KA schemes in general may not be very practical, and more research effort is needed before this security technique can be adopted in pervasive and emerging applications.

More recently proposed schemes [1], [17], [21] are believed to be resilient to collusion attacks, and may even achieve provable security. However, understanding the underlying constructions needs a heavy research background in cryptography, and they may not be easily implemented due to their intrinsic complexity (hence they are not topic of interest in the following sections). For example, in [1] the Akl-Taylor style [3] modular exponentiation is applied to the so termed “global hierarchy”, which is the Cartesian product [4] of the original partial-order hierarchy and the conceived time hierarchy. Similar approach is adopted in [21]. These two schemes not only are computation-intensive, but also ask for a significant amount of public storage. In [17], two provably-secure time-bound hierarchical KA schemes were proposed, one based on symmetric encryption and the other based on bilinear maps. While the former scheme seems preferable in terms of processing cost, it asks for a prohibitively large public storage space scaling as \(O(m^2 z^3)\), where \(m\) is the number of security classes in the partial-order hierarchy and \(z\) denotes the system lifetime. Note that \(z^3\) may be enormous (recall the examples in Sect. 1.2). In [22], Atallah et al. showed that it is possible to create a full-fledged hierarchical access control scheme with time-bound capabilities, but the proposed scheme also requires a formidable amount of public information.

We summarize the literature survey in Table 1. Next, we review two time-bound hierarchical KA schemes of interest proposed by Tzeng [4] and Chien [10], respectively. We provide a didactic viewpoint concerning not only their security but also pragmatic issues like practicality. We also present technical challenges and indicate possible directions for future research.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Security</th>
<th>Related</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bertino et al.  [14]</td>
<td>compromised[16]</td>
<td>[18]</td>
<td>fix with security proof available in full version of [16]</td>
</tr>
<tr>
<td>Huang-Chang [19]</td>
<td>compromised[20]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wang-Laib [1]</td>
<td>no formal proof</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tzeng [21]</td>
<td>no formal proof</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ateniese et al. [17]</td>
<td>provable</td>
<td></td>
<td>(e_1)'s become pairwise relatively prime (thus slightly different from [3], [4])</td>
</tr>
<tr>
<td>Atallah et al.  [22]</td>
<td>provable</td>
<td>[23]</td>
<td>contributes the first formal framework and two provably secure schemes</td>
</tr>
<tr>
<td>Briscoe [24]</td>
<td>no formal proof</td>
<td></td>
<td>incorporates time-dependent capabilities to existent key management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>purely time-based, no security hierarchy</td>
</tr>
</tbody>
</table>

Table 1 Brief summary of time-bound hierarchical KA schemes in the literature.
3. Tzeng’s Scheme

3.1 Review of the Scheme

In 2002, Tzeng proposed the first time-bound hierarchical KA scheme [4] by introducing a time-based dimension to the Akl-Taylor scheme [3]. Following our notation, Tzeng’s scheme can be considered as a generalization of previous ones where the private primitive $I(i, t_1, t_2)$ assigned by the CA to a user simply reduces to a single $K_{i}$, the time-invariant class key of his base class. Intuitively, the time-variant extension can be made by requiring each user to memorize $(t_2 - t_1 + 1)$ instances of each class key assigned to his base class $C_i$ and all the classes lower down in the partial-order hierarchy. However, storing $O(t_2 - t_1)$ keys is not realistic as $z$ may be arbitrarily large. Tzeng not only introduced the time-bound concept, but also showed that it is possible to find a solution far more elegant than the straightforward extension whose storage expense may be on the order of $mz$ in the worst case. In Tzeng’s scheme [4] the user private primitive $I(i, t_1, t_2)$ only consists of a very small quantity of information, whose size is independent of either the number of classes that the user can access (i.e., $|\{C_j \mid C_j \subset C_i\}$) or the number of authorized time slots (i.e., $(t_2 - t_1 + 1)$). However, the price is that, the derivation of the session key is very costly. Next, we look into its mathematical details.

**Initialization.** Assume that a partial-order hierarchy consists of $m$ disjoint classes $C_i$, $1 \leq i \leq m$ ordered by the binary relation “$\preceq$”, for a lifetime numbered as slots 0 throughout $Z$. The CA chooses two pairs of large strong primes $(p_1, q_1)$ and $(p_2, q_2)$, and computes $n_1 = p_1q_1$ and $n_2 = p_2q_2$. The CA also selects two random numbers $a$ and $b$, $1 < a < n_1$ and $1 < b < n_2$. Numbers $p_1, q_1, a$, and $b$ are for the partial-order hierarchy, while numbers $p_2, q_2, n_2$, and $b$ are for the Lucas sequence [5] implementing the time-bound attribute.

- For the partial-order hierarchy, the CA randomly chooses $g_1, g_2, e_1, e_2, \ldots, e_m \in (Z_{n_1})^*$, and computes $h_1, h_2, d_1, d_2, \ldots, d_m$ such that $g_1h_1 \equiv g_2h_2 \equiv e_id_i \equiv 1 \pmod{\phi(n_1)}$ for $1 \leq i \leq m$.
- Concerning the time dimension, the CA randomly chooses $f_1$ and $f_2$, and associates with each $t \in [0 \ldots z]$ a $w_t = V_{f_1-1}f_2(b)$, which we call the instance secret. The Lucas sequence $(V_{\ell}(x))_{\ell=0}^{\infty}$ regarding $x \in Z^*$, is defined over $Z_{n_2}$ as $V_{\ell}(x) = V_{\ell-1}(x) - V_{\ell-2}(x) \pmod{n_2}$ for $\ell \geq 2$, with the initial conditions $V_0(x) = 2$ and $V_1(x) = x \pmod{n_2}$. One of its properties is $V_{\ell}(V_{\ell}(x)) = V_{2\ell}(x)$. 

**Public information.** A one-way hash function $H$ and parameters $(n_1, g_1, g_2, e_1, e_2, \ldots, e_m, (a, f_1, f_2))$.

**Class key.** The CA computes $K_0 = a^{d_1d_2-\ldots-d_m} \pmod{n_1}$, and for $1 \leq i \leq m$, the class key of $C_i$ is defined as $K_i = K_0^{\prod_{j \in C_i} e_j} \pmod{n_1}$. Figure 1 illustrates the class key assignment for a possible partial-order hierarchy.

**Session key.** The encryption key for class $C_i$ (i.e., the instance of $K_i$) at time $t \in [0 \ldots z]$ is:

$$k_{i,t} = H(\gamma(i, t), w_t), \text{ where } \gamma(i, t) = K_i^{H(\gamma(i, t), w_t)} \pmod{n_1}. \quad (1)$$

**Private primitive.** When a user is to be attached to the base class $C_i$ for the period of time $[t_1 \ldots t_2]$, he is given $I(i, t_1, t_2) = (K_i^{H(\gamma(i, t), w_t)} \pmod{n_1}, V_{f_1-1}f_2(b)) = (I_K, I_V)$, which is always of a constant size $(n_1 + n_2)$.

**Key derivation.** Given $I(i, t_1, t_2) = (I_K, I_V)$, the user can derive any $k(j, t)$ if $C_j \subset C_i$ and $t_1 \leq t \leq t_2$. To do so, he first computes (including inferring $K_j$ from $K_i$):

$$I_K^{f_1-1}f_2^{i-1} \prod_{C_j \subset C_i} e_j \pmod{n_1} = (K_i^{\prod_{C_j \subset C_i} e_j} \pmod{n_1}, V_{f_1-1}f_2^{i-1} \pmod{n_1}) = K_j^{H(\gamma(i, t), w_t)} \pmod{n_1}$$

$$V_{f_1-1}f_2^{i-1}(I_V) = V_{f_1-1}f_2^{i-1}(I_V) \pmod{n_1}.$$ 

Then, following (1) he can derive $k_{i,t} = H(\gamma(j, t), w_t)$.

3.2 Yi and Ye’s Attack against the Scheme

In [8], Yi and Ye demonstrated a sophisticated collusion attack essentially against the time-bound property of Tzeng’s scheme [4], while the partial-order property inherited from the Akl-Taylor scheme [3] is not challenged. The affected element in the user private primitive $I(i, t_1, t_2) = (I_K, I_V)$ is $I_K$, while $I_V$ based on the Lucas sequence [5] appears to be not responsible for the identified security breach. Although cryptologists have warned against certain applications of the Lucas sequence [9], so far there is no reported weakness concerning its adoption in the time-bound KA scheme [4].

**The collusion attack.** Assume there are three users $A$ with $I(a, t_1, t_2)$, $B$ with $I(b, t_1, t_2)$, and $C$ with $I(c, t_3, t_5)$, where $t_5 \leq t_2 \leq t_3 \leq t_5$. The security class of concern is any $C_j$ satisfying $C_j \subset C_i$, $C_j \subset C_0$, but $C_j \not\subset C_i$. Following [4], $A$ can compute $\gamma(j, t_2)$ and $B$ can compute $\gamma(j, t_3)$ (recall formula (1)). The point is that, it is feasible to infer $\gamma(j, t)$ for any $t \in [t_2 \ldots t_3]$, from $\gamma(j, t_2)$ and $\gamma(j, t_3)$ [8]. Therefore, with such $\gamma(j, t)$ offered by $A$ and $B$, and the instance secret $w_t$ computed by $C$ (note that $[t_2 \ldots t_3] \subset [t_5 \ldots t_6]$), the three inner attackers can follow formula (1) to infer $k(j, t)$ for $t_2 \leq t \leq t_3$, which even a combination of them is not entitled to.

![Fig. 1](image_url)
3.3 Discussions

Bertino et al. directly adopted Tzeng’s scheme to build an access control mechanism for XML documents [7], and thus their mechanism is also subject to the above collusion attack. However, in [8] Yi and Ye did not provide any remedy to Tzeng’s scheme. We note for the user private primitive $I(k, t_1, t_2) = (I_k, I_v)$, both $I_k$ and $I_v$ are time-bound, which seems unnecessary; actually, sometimes complexity impairs security [15]. Hence, a possible fix is to remove from the vulnerable $I_k$ the time-dependent ingredient (the exponent $h_k^2h_2^{-1}$), resulting in $I_k = K_i \mod n_1$. This way $I_k$ and $I_v$, the two building blocks respectively addressing spatial class designation and temporal restrictions, are decoupled, which corresponds to clear separation of duty. In a nutshell, for forwarding two building blocks respectively addressing spatial class keys are computed in the RSA setting [6], with the modulus $n_1 = p_1q_1$ and the random exponents $e_i \in \mathbb{Z}_{\phi(n_1)}^*$, $e_d \equiv 1 \mod \phi(n_1)$ for $1 \leq i \leq m$. Consequently, in [4] $K_0 = d_0i^{d_0-e_0} \mod n_1$, and $K_j = K_0^{\prod_{i \in C_i} e_i} \mod n_1$ for $1 \leq i \leq m$. In the Akl-Taylor scheme [3], however, $K_0$ is randomly chosen (i.e., information-theoretic), while each class $C_i$ is associated with a distinct prime $e_i$. Although $K_i$ is computed from $K_0$ in the same manner, Tzeng’s modification complicates the generation of $K_0$, as all the $d_i$’s in [4] are actually unnecessary. Moreover, a subtle security breach may arise regarding the selection of $e_i$’s. Next, we discuss this problem separately.

We begin with a very simple partial-order hierarchy containing only three security classes $C_1$, $C_2$, and $C_3$, where $C_2$ and $C_3$ are both immediate descendants of $C_1$ (hence $C_2$ and $C_3$ are independent of each other). Since $C_2 \leq C_1$ and $C_3 \leq C_1$, we have $K_2 = K_0^{e_2} \mod n_1$ and $K_3 = K_0^{e_3} \mod n_1$. In most cases, randomly selecting $e_1 \in \mathbb{Z}^*_n$ as in [4] does not lead to a problem. However, if one of $e_2$ and $e_3$ happens to be a divisor of the other (which can be easily checked as all $e_i$’s are public), say $e_2 | e_3$, then users in $C_3$ can trivially compute the class key of an irrelevant security class $C_2$ by $K_2 = K_0^{e_2} \mod n_1$. The problem may also occur in a more complicated (and possibly more realistic) hierarchy. One can take Fig. 1 for example, where $K_5$, $K_6$, $K_7$, and $K_8$ are four independent class keys; there might be a similar security breach if the exponents $e_5$, $e_6$, $e_7$, and $e_8$ are chosen without care. Therefore, although $e_i$’s do not necessarily need to be primes (but specified in the original Akl-Taylor scheme [3] and derivatives like [1]), any of them should not be a divisor of any else. This observation can be attributed to Tang and Mitchell [20], though the actual target of their attack is Huang and Chang’s scheme [19].

It is also worth noting that, later in Tzeng’s new time-bound hierarchical KA scheme [21], $K_0$ becomes information-theoretic (thus no $d_i$’s), while (according to a footnote in [21] but without any explanation) $e_i$’s should be pairwise relatively prime; the rest remains the same, say $K_i = K_0^{\prod_{j \in C_i} e_j} \mod n_1$, and thus $K_j = K_0^{\prod_{j \in C_j} e_j} \mod n_1$ for $C_j \leq C_i$; Although looser than originally specified by Akl and Taylor [3], the unexplained requirement on $e_i$’s may still seem to be an overkill; that any of them is not a divisor of any else seems sufficient for security. However, we show the requirement is necessary by again considering the example in Fig. 1. Suppose gcd($e_6, e_4 + e_8$) = 1. Then a user in $C_4$ knowing $K_4 = K_0^{\prod_{j \in C_4} e_j} \mod n_1$, and a user in $C_6$ knowing $K_6 = K_0^{\prod_{j \in C_6} e_j} \mod n_1$, can conspire to infer $K_0^{\prod_{j \in C_7} e_j} \mod n_1$ following the merging idea [1], essentially by employing the common modulus attack [6]. Assume $e_7 | e_8$, say $e_7 = 15$, $e_4 = 9$, and $e_8 = 25$. Then, $K_3 = K_0^{\prod_{j \in C_3} e_j} \mod n_1$ can be easily derived from $K_0^{\prod_{j \in C_6} e_j} \mod n_1$, which is the class key of $C_3$ but not intended for even the coalition of $C_4$ and $C_6$. It is enough to
deter such collusion attack by requiring the $e_i$’s to be pair-wise relatively prime.

4. Chien’s Scheme

4.1 Review of the Scheme

In 2004, Chien proposed the second time-bound hierarchical KA scheme [10] involving no expensive operations like modular exponentiation or Lucas sequence. It actually extends his time-invariant KA protocol [11] featuring a reference table instead of following the Akl-Taylor style [3] with a tamper-resistant device performing mainly one-way hash functions. From [11] to [10], the introduced instance secret $w_i$ is computed by the tamper-resistant device with a technique that can be termed as the dual directional hash chains, which serves as the building block for the temporal restrictions.

Let $H^t(x)$ be the result of applying a one-way hash function $H$ for $t$ times to $x$. Then $x, H(x), H^2(x), \cdots$ forms a forward hash chain. Chien’s scheme [10] employs two hash chains (a forward one and a reverse one), and is far more efficient than Tzeng’s scheme [4]. However, the computation of the instance secret $w_i$ needs the protection by a tamper-resistant device. Otherwise, two users may conspire to share the “earlier” one of their forward chains and the “later” one of their reverse chains to infer unauthorized instance secrets. Note the Lucas sequence in [4] is not subject to such a collusion. Therefore, compared with Tzeng’s scheme, Chien additionally introduced a tamper-resistant device.

Next, we look into the nuts and bolts of Chien’s scheme [10]. We follow the previous notation.

Initialization. The CA randomly selects a server secret key $X$, two secret values $a$ and $b$, and $m$ keys $K_i$, $1 \leq i \leq m$. The security class $C_i$, identified by ID$_i$, is assigned the class key $K_i$, $1 \leq i \leq m$.

Public information. For each directed edge $C_j \prec C_i$ in the hierarchy, the CA publishes a reference $r_{ij} = H(X||ID_i||ID_j)||K_i)$ on a public board, resulting in the public reference table $r_{ij}$ for $C_j \prec C_i$, $1 \leq i, j \leq m$.

Session key. Compute $w_i$ with the dual hash chains. Then the data in class $C_i$ at time $t$ is encrypted with:

$$k_{ij} = H(K_i \oplus w_i), \text{ where } w_i = H^t(a) \oplus H^{t-i}(b).$$

Private primitive. When a user is assigned to his base class $C_i$ for a period of time $[t_1 \cdots t_2]$, the CA distributes $K_i$ to the user through a secure channel. The CA also issues the user a tamper-resistant device, in which $X, H^t(a)$, and $H^{t-i}(b)$ are secretly stored (even inaccessibly to the device owner). The device also contains non-confidential (but readily) information ID$_i$ and $H$. Therefore, $I(i, t_1, t_2) = (K_i, H^t(a), H^{t-i}(b))$ is the user-specific private primitive (of a constant size, similar to Tzeng’s scheme [4]).

Key derivation. With the tamper-resistant device, the user entitled to $I(i, t_1, t_2)$ can derive any $k(j, t)$ for $C_j \leq C_i$ and $t_1 \leq t \leq t_2$. For example, if $C_j = C_i$, the user simply enters $K_i$ into the device, which yields $k_{ij} = H(K_i \oplus H^{t-i}(a)) \oplus H^{t-i}(H^{t-i}(b))$ complying with (2). Generally, assume the path from $C_i (\equiv C_{t_o}, \theta \geq 2)$ to $C_j (\equiv C_{t_z})$ is $C_{t_{1+1}} \prec C_{t_2} \prec \cdots \prec C_{t_0}$, where $C_{t_0}$ is an immediate descendant of $C_{t_{i+1}}, 1 \leq d \leq \theta - 1$. The user enters $r_{i(t_{d+1}), t_{d+1}, t_d, \cdots, t_1}$, $ID_{t_0} \equiv ID_j, ID_{t_d}, \cdots, ID_{t_1}, ID_{t_z} \equiv ID_j$, and $K_{t_0} = K_i$ into the device, which sequentially computes:

$$K_{t_{d+1}} = r_{i(t_{d+1}), t_{d+1}, t_d, \cdots, t_1} \oplus H(X||ID_{t_0}||ID_{t_1}||K_i),$$

$$K_{t_d} = r_{i(t_{d+1}), t_{d+1}, t_d, \cdots, t_1} \oplus H(X||ID_{t_0}||ID_{t_1}||K_i),$$

$$K_j = K_{t_z} = r_{i(t_{z+1}), t_{z+1}, \cdots, t_1} \oplus H(X||ID_{t_0}||ID_{t_1}||K_i),$$

$$w_i = H^{t-i}(H^t(a)) \oplus H^{t-2i}(H^{t-2i}(b)),$$

and $k_{ij} = H(K_j \oplus w_i)$ following (2).

4.2 Yi’s Attack against the Scheme

In [12], Yi again demonstrated a three-party collusion attack, which is against Chien’s scheme [10] and is general-ized as follows. Assume there are three users $A$ with $I(a, t_1, t_2), B$ with $I(b, t_1, t_2)$, and $C$ with $I(c, t_1, t_2)$, where $C$ is an immediate descendant of $B$, and $C \not\prec B$. At first, with the public reference $r_{bc} = H(X||ID_a||ID_b||K_b) \oplus K_c$, $C$ knowing $K_c$ can infer $H(X||ID_a||ID_b||K_b) = r_{bc} \oplus K_c$ and forward it to $B$. Suppose $A$ also forwards $K_a$ to $B$. Then, as if going to derive $k_{a,t}$ for $t_3 \leq t \leq t_4$, can enter into his tamper-resistant device the correct class identifier $ID_a$, its base class key $K_a$, but a crafted $r_{bc} = H(X||ID_a||ID_b||K_b) \oplus K_a$. The device is then misled into computing $K_b' = r_{bc}' \oplus H(X||ID_a||ID_b||K_b) = H(X||ID_a||ID_b||K_b) \oplus K_a) \oplus H(X||ID_a||ID_b||K_b) = K_a$, which appears to be still within the combined knowledge of the three conspiring users $A, B, and C$. However, the point is that, $B$’s device can also compute $w_i$ for $t_3 \leq t \leq t_4$, and thus can yield corresponding $k_{a,t}$ following (2). Obviously, such collusion violates the intended security policy (unless $[t_1 \cdots t_2] \subseteq [t_1 \cdots t_2]$). In other words, it is easy for the three users to acquire $K_a$’s instances beyond $A$’s authorized time period $[t_1 \cdots t_2]$.

4.3 Discussions

This time, different from the previous one [8], Yi’s attack [12] against Chien’s scheme [10] actually targets the partial-order property, while the time-bound property based on the dual hash chains is not challenged. Note that without the protection of the tamper-resistant device, a user with $I(i, 0, t_1)$ and another user with $I(i, t_2, z)$ can collude to acquire $w_i$ for any $t$ in the entire system lifetime (and thus any $k_{ij}$ for $0 \leq t \leq z$). This explains why the dual hash chains should only be employed in a tamper-resistant device so as to compose a secure solution to time-bound key management. On the other hand, interestingly, Yi’s attack does not affect the time-invariant version [11] of Chien’s KA scheme, as in that case the conspiring users cannot gain any more than the combination of their respective privileges. However, when another dimension is introduced, as from [11] to
[10]. Yi exploited the partial-order property to launch an interweaving attack (recall Sect. 3.3). Therefore, it seems that, the combination of respectively secure building blocks does not always result in an integration that is overall secure. This is the lesson we learn from Chien’s scheme [10].

In Sect. 3.3 when proposing a possible security fix to Tzeng’s scheme [4], we have pointed out that, the decoupled structure \( k_{ij} = H(K_i \mod n_1, w_j) \) should be implemented in a tamper-resistant device such that \( K_i = K_i \mod n_1 \) will not be revealed even to the device owner. In Chien’s scheme [10], \( k_{ij} = H(K_i \oplus w_j) \) follows the decoupled structure and the tamper-resistant device is also assumed, but \( K_i \) is distributed in the clear to the user upon registration. This observation helps understand Yi’s attack. Although in [12] Yi again did not propose any remedy, a security fix can be made in a straightforward manner, also based on the above observation. That is, during the registration of a user entitled to \( I(i, t_1, t_2) \), \( K_i \) should also be securely embedded in the issued tamper-resistant device, just like the way \( X, H^0(a) \), or \( H^{t_2-t_1}(b) \) is stored. Such a slight modification to distributing the base class key makes the security difference, as this way \( K_i \) and \( w_j \) in (2) are fully decoupled. It also makes the time-bound hierarchical KA scheme more user-friendly, as the device owner no longer needs to input \( K_i \) for session key derivation. Note that it is prohibitively difficult for human beings to bear in mind a cryptographic key (randomly generated by the CA according to [10]).

Essentially, Yi’s collusion attack [12] lies in the misuse of the tamper-resistant device, which is deceived into believing that the derived class key is always of a lower security class than the device owner’s base class. Hence alternatively, Chien’s scheme [10] can be repaired by preventing users from entering crafted references like the \( r_{bc} \) in Sect. 4.2. For example, if \( r_{ij} \) on the public board is changed to an encrypted form, say \( E_X(r_{ij}||ID_o) \), the tamper-resistant device can employ the server secret key \( X \) and the readily public identifier \( ID_o \) to reliably retrieve an authenticated \( r_{ij} \). Three similar lightweight remedies have been presented in [13]. However, securely embedding \( K_i \) (along with other secrets) into the tamper-resistant device should be the most convenient, as it incurs the slightest modification and user-friendliness as a bonus.

Recently, a heavyweight remedy to Chien’s scheme [10] was proposed by Bertino et al. [14], where the tamper-resistant device is additionally required to support elliptic-curve cryptography so as to defend against Yi’s three-party collusion attack [12]. Essentially, the scheme by Bertino et al. [14] is a rewritten (the elliptic-curve edition) of Chien’s scheme [10], where each of the public references \( r_{ij} \) is generated and then employed using the elliptic-curve public-key cryptography instead of the cost-efficient one-way hash function. Unfortunately, recently Sun et al. [16] showed that, aside from the increased computational overhead, the rewritten scheme [14] appears to be even more vulnerable than the original one [10]; merely two conspirators are enough to misuse the tamper-resistant device to infer unauthorized session keys. Simple fix to the rewritten scheme is also suggested in [16], which still reduces to the authentication on \( r_{ij} \) and thus directly applies to the original Chien’s scheme [10] (without necessarily involving the expensive elliptic-curve cryptography).

Finally, compared with Tzeng’s scheme [4], Chien’s scheme [10] seems more promising, as expensive computations like modular exponentiation and the Lucas sequence have both been replaced with cost-efficient operations (mainly one-way hash functions). Chien’s scheme is also efficient in terms of storage and communication; the user private primitive incurs constant storage cost, and the needed public parameters \{\( r_{ij} \)\} are of the same size with the number of direct edges in the DAG representing the partial-order hierarchy. Note that such \( ||r_{ij}|| \) usually scales as \( O(m) \) (e.g., \( ||r_{ij}|| = 10 \) in Fig. 1, where \( m = 8 \)), and thus is comparable to Tzeng’s scheme [4]. In case \( m \) is not large, it is possible to store all these public parameters on the user’s device. The only issue seems to be that, Chien’s scheme is based on a tamper-resistant device (in which the user base class key \( K_i \) should be securely embedded). However, note that the remedy for Tzeng’s scheme [4] to thwart the collusion attack [8] also asks for the protection by a tamper-resistant device (recall Sect. 3.3). Therefore, for real adoption, Chien’s scheme [10] is more promising than Tzeng’s [4].

5. Conclusions

In this paper the topic of time-bound hierarchical key assignment is concerned. We surveyed the recent literature and looked into two representative schemes by Tzeng [4] and Chien [10] as case studies. Collusion attacks have shown to be a major threat to time-bound hierarchical KA schemes. Secure building blocks do not always lead to an integration that is overall secure, and complexity may not necessarily help with security.

Both schemes [4], [10] can be remedied to withstand known collusion attacks. The point is to follow a decoupled structure \( k_{ij} = H(K_i, w_j) \) on a tamper-resistant user device, where \( K_i \) and \( w_j \) should be inaccessible to even the device owner so as to prevent interweaving attacks. Moreover, in Tzeng’s [4] and other schemes that follow the Akl-Taylor style key assignment [3], the assigned exponents do not necessarily need to be primes, but they should be pairwise relatively prime.

Due to cost considerations, existent time-bound hierarchical KA schemes may not be readily applicable to commodity (particularly, low-cost) devices that neither afford heavy computation nor have tamper-resistant casing. More studies are needed in order to find efficient and practical KA solutions.

References


Wen Tao Zhu received his BS and PhD degrees both from Department of Electronic Engineering and Information Science at University of Science and Technology of China. He has since 2004 been with the Singapore Management University in 2006.

Robert H. Deng received his Bachelor from National University of Defense Technology, China, his MSc and PhD from the Illinois Institute of Technology, USA. He has been with the Singapore Management University since 2004, and is currently Professor. Associate Dean for Faculty & Research, School of Information Systems. Prior to this, he was Principal Scientist and Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. He has 26 patents and more than 200 technical publications in international conferences and journals in the areas of computer networks, network security and information security. He is an Associate Editor of the IEEE Transactions on Information Forensics and Security, Associate Editor of Security and Communication Networks Journal (John Wiley), and member of Editorial Board of Journal of Computer Science and Technology (the Chinese Academy of Sciences). He received the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006.
Jianying Zhou received PhD in Information Security from University of London in 1997, MSc in Computer Science from Chinese Academy of Sciences in 1989, and BSc in Computer Science from University of Science and Technology of China in 1986. Currently he is Senior Scientist in Institute for Infocomm Research. His research interests are in computer and network security, mobile and wireless communications security, and secure electronic commerce. He has published over 130 referred papers at international conferences and journals, of which the top 10 publications received over 1000 citations.

Feng Bao received his BS in mathematics, MS in computer science from Peking University and his PhD in computer science from Gunma University in 1984, 1986 and 1996 respectively. Currently he is the Principal Scientist and the Department Head of the Cryptography & Security Department of the Institute for Infocomm Research, Singapore. His research areas include algorithm, automata theory, complexity, cryptography, distributed computing, fault tolerance and information security. He has published more than 190 international journal and conference papers and owned 16 patents.