Information Sciences 209 (2012) 80–92

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem

Ashok Kumar Das [a,*], Nayan Ranjan Paul [b], Laxminath Tripathy [c]

[a] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[b] Department of Computer Science, KMBB College of Engineering and Technology, Khurda 752 056, India
[c] Department of Information Technology, Eastern Academy of Science and Technology, Bhubaneswar 754 001, India

ARTICLE INFO

Article history:
Received 20 November 2010
Received in revised form 28 December 2011
Accepted 25 April 2012
Available online 9 May 2012

Keywords:
Key management
Elliptic curve
Hierarchical access control
Polynomial interpolation
Security
Exterior root finding attacks

ABSTRACT

In a key management scheme for hierarchy based access control, each security class having higher clearance can derive the cryptographic secret keys of its other security classes having lower clearances. In 2008, Chung et al. proposed an efficient scheme on access control in user hierarchy based on elliptic curve cryptosystem [Information Sciences 178 (1) (2008) 230–243]. Their scheme provides solution of key management efficiently for dynamic access problems. However, in this paper, we propose an attack on Chung et al.'s scheme to show that Chung et al.'s scheme is insecure against the exterior root finding attack. We show that under this attack, an attacker (adversary) who is not a user in any security class in a user hierarchy attempts to derive the secret key of a security class by using the root finding algorithm. In order to remedy this attack, we further propose a simple improvement on Chung et al.'s scheme. Overall, the main theme of this paper is very simple: a security flaw is presented on Chung et al.'s scheme and then a fix is provided in order to remedy the security flaw found in Chung et al.'s scheme.

1. Introduction

Hierarchical access control is a fundamental problem in computer and network systems. In a hierarchical access control, a user of higher security level class has the ability to access information items (such as message, data, and files) of other users of lower security classes. A user hierarchy consists of a number n of disjoint security classes, say, $SC_1, SC_2, \ldots, SC_n$. Let this set be $SC = \{SC_1, SC_2, \ldots, SC_n\}$. A binary partially ordered relation $\geqslant$ is defined in SC as $SC_i \geqslant SC_j$, which means that the security class SC_i has a security clearance higher than or equal to the security class SC_j. In addition the relation $\geqslant$ satisfies the following properties:

(a) [Reflexive property] $SC_i \geqslant SC_i, \forall SC_i \in SC$.
(b) [Anti-symmetric property] If $SC_i, SC_j \in SC$ such that $SC_i \geqslant SC_j$ and $SC_j \geqslant SC_i$, then $SC_i = SC_j$.
(c) [Transitive property] If $SC_i, SC_j, SC_k \in SC$ such that $SC_i \geqslant SC_j$ and $SC_j \geqslant SC_k$, then $SC_i \geqslant SC_k$.

If $SC_i \geqslant SC_j$, we call SC_i as the predecessor of SC_j and SC_j as the successor of SC_i. If $SC_i \geqslant SC_k \geqslant SC_j$, then SC_k is an intermediate security class. In this case SC_k is the predecessor of SC_j and SC_i is the predecessor of SC_k. In a user hierarchy, the encrypted message by a successor security class is only decrypted by that successor class as well as its all predecessor security classes in that hierarchy.

* Corresponding author. Tel.: +91 40 6653 1506; fax: +91 40 6653 1413.
E-mail addresses: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (A.K. Das), nayan.p@kmbb.in (N.R. Paul), laxmintripathy@gmail.com (L. Tripathy).

0020-0255/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2012.04.036

Akl and Taylor [1] first developed the cryptographic key assignment scheme in an arbitrary partial order set (poset) hierarchy. MacKinnon et al. [2] presented an optimal algorithm, called the canonical assignment, to reduce the value of public parameters. Harn and Lin [3] then proposed a bottom up key generating scheme, instead of using a top-down approach as in the Akl and Taylor scheme and MacKinnon et al.'s scheme.

In order to solve dynamic access control problems, many schemes have been proposed in the literature [4–13]. Chang et al. [8] proposed a key assignment scheme based on Lagrange's interpolation method and one-way hash function. In their scheme, a user with higher security clearance must iteratively perform the key derivation process for deriving the secret key of a user who is not an immediate successor. Other proposed schemes [7,10] enhance Akl and Taylor's scheme [1], and explore other possible approaches that can enable a user in a hierarchy to modify the secret key as and when necessary. Thus, a predecessor can directly and efficiently derive the secret keys of its successor(s). Kuo et al. later developed a method [6] that employs the public key to encrypt the secret key. Their scheme has a straightforward key assignment algorithm, small storage space requirement, and uses a one-way hash function.

Shen and Chen proposed a novel key management scheme based on discrete logarithms and polynomial interpolations in a user hierarchy [9]. However, Hsu and Wu [12] presented an attack, called the exterior root finding attack, on Shen-Chen's scheme [9] so that an attacker can derive the encryption key of a user in the hierarchy. In [12], authors showed that some malicious insider, for example a user in a security class, can have access to the information items held by those who are not his/her subordinates. They further proposed an improvement to amend the flaws in Shen-Chen's scheme.

Chen and Huang proposed an efficient novel key management scheme for dynamic access control in a user hierarchy [13]. Their scheme is based on the efficiencies of one-way hash function and symmetric-key encryptions and decryptions. Further, their scheme supports dynamic access control including adding new security classes in the hierarchy, deleting existing security classes from the hierarchy, adding new relationships in the hierarchy, deleting existing relationships from the hierachchy as well as changing secret keys of security classes in the hierarchy. The performance of their scheme is also efficient compared to Akl-Taylor's scheme [1], Kuo et al.'s scheme [6], and Lin's scheme [4].

In 2008, Chung et al. [11] proposed an efficient key management and derivation scheme based on the elliptic curve cryptosystem. In their scheme, the secret key of each security class can be determined by a trusted centralized authority (CA). An attractive advantage of their scheme is that it solves dynamic key management efficiently and flexibly. However, we show that their scheme is vulnerable to exterior root finding attacks.

In this paper, we propose an exterior root finding attack on Chung et al.'s scheme [11] to show that their scheme is vulnerable under this proposed attack. Our attack on Chung et al.'s scheme is similar to Hsu-Wu's exterior root finding attack on Shen-Chen's novel key management scheme. In our exterior root finding attack on Chung et al.'s scheme, an attacker (adversary) who is not a user in any security class in a user hierarchy can derive the secret key of a security class by using the root finding algorithm. In order to eliminate this security flaw in their scheme, we further propose a simple improvement on their scheme. Hence, the theme of this paper is very simple: a security flaw is presented on Chung et al.'s scheme and then a fix is provided to remedy the security flaw found in Chung et al.'s scheme.

The rest of this paper is sketched as follows. In Section 2, we review some mathematical background which are useful to review Chung et al.'s scheme. We then give briefly an overview of Chung et al. scheme [11] in Section 3. In Section 4, we describe our proposed exterior root finding attack on Chung et al.'s scheme [11]. In Section 5, we propose a simple improvement on Chung et al.'s scheme to remedy the attack proposed in Section 4 and discuss security of our improved scheme. We provide performance comparison of our improved scheme with Chung et al.'s scheme and Chen-Haung's scheme in Section 6. Finally, we conclude the paper in Section 7.

2. Mathematical background

In this section, we discuss the elliptic curve and its properties. We then discuss the rules for adding points on elliptic curve and the elliptic curve discrete logarithm problem. We, finally, discuss the properties of a one-way hash function and M. Ben-or's method [14] for root finding and factorization of polynomials in finite field.

2.1. Elliptic curve over finite field

Let a and $b \in Z_p$, where $Z_p = \{0, 1, \ldots, p-1\}$ and $p > 3$ be a prime, such that $4a^3 + 27b^2 \neq 0 \pmod p$. A non-singular elliptic curve $y^2 = x^3 + ax + b$ over the finite field $GF(p)$ is the set $E_p(a, b)$ of solutions $(x, y) \in Z_p \times Z_p$ to the congruence

$$y^2 = x^3 + ax + b \pmod p,$$

where a and $b \in Z_p$ are constants such that $4a^3 + 27b^2 \neq 0 \pmod p$, together with a special point $\mathcal{O}$ called the point at infinity or zero point.

The condition $4a^3 + 27b^2 \neq 0 \pmod p$ is the necessary and sufficient to ensure that the equation $x^3 + ax + b = 0$ has a non-singular solution [15]. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be points in $E_p(a, b)$, then $P + Q = \mathcal{O}$ implies that $x_Q = x_P$ and $y_Q = -y_P$. Also, $P + \mathcal{O} = \mathcal{O} + P = P$, for all $P \in E_p(a, b)$. Moreover, an elliptic curve $E_p(a, b)$ over Z_p has roughly p points on it. More precisely, a well-known theorem due to Hasse asserts that the number of points on $E_p(a, b)$, which is denoted by $\#E$, satisfies the following inequality [16]: