Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
July 2014, 21(Suppl. 1): 88–93
www.sciencedirect.com/science/journal/10058885
The Journal of China Universities of Posts and Telecommunications
http://jcupt.xsw.bupt.cn

CPK-based login authentication for electricity operation information system

ZOU Xiao-jia, YOU Xiang-dong (✉), PAN Hao, ZHANG Zhi-yuan, WANG Xiao-lei

School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract

Login authentication security is indispensable to applications of client/server (C/S) structure. Although some security technology in login authentication is relatively mature after years of development, it cannot meet high security requirements for the system in the case of limited resources. To deal with it, this paper proposes a new login authentication solution and applies it in electricity operation information system (EOIS), an application aiming at electrical equipment overhaul and report. The authors firstly discuss the reason why combined public key (CPK) is adopted as the key technology instead of the common one public key infrastructure (PKI). Secondly, they expatiate on CPK generation mechanism and the realizing process of login authentication, including local authentication using CPK-based digital signature and remote authentication using web service. Then, some results from three encryption methods (message-digest algorithm 5(MD5), secure hash algorithm (SHA-1) and CPK-based digital signature) to test EOIS are given, which show that the new solution builds its security on Hash function chosen and protection of combined private key. Finally, the security analysis reveals that CPK-based login authentication is safer to ensure the certainty of user identity, the integrality and non-repudiation of messages, and the confidentiality of transmission.

Keywords CPK, login authentication, digital signature, web service, electricity operation information system

1 Introduction

With the prosperity of mobile network and smart phones, the power industry is facing great opportunities and challenges in information operation and management. A traditional method is to send staff for equipments maintenance and manual records to the company, which is supposed to be complicated and inefficient. Applications of C/S mode offer a train of thought in information operation and management. Meanwhile, the issue of C/S communication security, which should be taken into account, is based on login authentication.

A typical login authentication method is based on user-name/MD5-digest-password. A client sends its user-name and password to a server. The server verifies the identity of the client by checking MD5 digest password. This will bring potential security problems, and one of which is that the server may suffer forgery attacks, tamper attacks and resend attacks since the message can be sniffed and easily hijacked.

CPK-based authentication technology, first proposed by professor Nan in Ref. [1], builds its security upon the difficulty of solving discrete logarithm. It satisfies three conditions in identity authentication, namely certification of scale, validation of simplicity and management of efficiency [2]. Compared to current popular PKI [3] technology, CPK technology has more advantages. One is lower key storage and higher efficiency, the other is without trusted third party certificate authority (CA) involved and certificate library online supported [2]. As a result, it can easily manage to store private keys in memory chips and realize user ID authentication, digital signature and data encryption. To ensure login authentication security, the paper primarily introduces CPK-based login authentication solution with web service

Received date: 24-03-2014
Corresponding author: YOU Xiang-dong, E-mail: youxiangdong@bupt.edu.cn
DOI: 10.1016/S1005-8885(14)60507-0

technology, and implements it in EOIS.

2 Key generation principle based on CPK

CPK key management system can be built on either normal discrete logarithm problem or elliptic curve discrete logarithm problem [4]. Under similar secure conditions, the latter has an advantage of smaller storage in cryptographic applications. We briefly describe the process of key pair generation referring to CPK standards V6.0 [5], taking elliptic curve cryptography (ECC) [6] as an example. We use the following symbols to express things in the rest of the paper.

$\boldsymbol{A}_{m\times32}$, $\boldsymbol{B}_{h\times2}\rightarrow$ combined matrix
$(a,b,\boldsymbol{G},n,p)\rightarrow$ parameters of ECC
$\boldsymbol{G}\rightarrow$ base point of S
$E_p(a,b)\rightarrow$ elliptic curve group
$S\rightarrow$ a child group of $E_p(a,b)$
$n\rightarrow$ rank of S
$F_p\rightarrow$ the finite field
$u_{id}\rightarrow$ user's identity
$H(*)\rightarrow$ a hash operation
$(r_{\mathrm{IPK}},\boldsymbol{R}_{\mathrm{IPK}})\rightarrow$ identity-key
$r_{\mathrm{IPK}}\rightarrow$identity-private-key
$\boldsymbol{R}_{\mathrm{IPK}}\rightarrow$identity-public-key
$(q_{SPK},\boldsymbol{Q}_{SPK})\rightarrow$ separating-key
$q_{SPK}\rightarrow$ separating-private-key
$\boldsymbol{Q}_{SPK}\rightarrow$separating-public-key
$(k_{CPK},\boldsymbol{K}_{CPK})\rightarrow$ combined-key
$k_{CPK}\rightarrow$ combined-private-key
$\boldsymbol{K}_{CPK}\rightarrow$ combined-public-key
$A\rightarrow$a client $B\rightarrow$ the server
$N_{\mathrm{user}}\rightarrow$user name
$P_{\mathrm{user}}\rightarrow$user password
$T_0\rightarrow$ network transfer time tolerated
$(s,c)\rightarrow$original digital signature
$F_{CSPK}(*)\rightarrow$ a mapping operation using a collection of seeded-public-key
$F_{k_{CPK}}(*)\rightarrow$a digital signature generation operation
$F_{\boldsymbol{K}_{CPK}}(*)\rightarrow$a digital signature verification operation

Combined-key is made up of identity-key and separating-key. Identity-key is generated by combined matrix $\boldsymbol{A}_{m\times32}$ and separating-key is created by combined matrix $\boldsymbol{B}_{h\times2}$. Also, $\boldsymbol{A}_{m\times32}$ and $\boldsymbol{B}_{h\times2}$ are defined in key management center (KMC).

2.1 ECC over F_p

CPK system adopts elliptic curve E over the finite field F_p, with parameters (a, b, G, n, p). E is defined as follows,

$$y^2=(x^3+ax+b)\bmod p \tag{1}$$

In Eq. (1), p is an odd prime (p>3), as a and b are parameters that satisfy $4a^2+27b^2\neq0$, $a,\ b\in F_p$ [6]. With l solutions of Eq. (1), namely the point set $\boldsymbol{M}=\{\boldsymbol{M}_1,\boldsymbol{M}_2,...,\boldsymbol{M}_l\}$ and a special point $\boldsymbol{O}=(x_o,y_o)$, an elliptic curve group $E_p(a,b)=\{\boldsymbol{M}_1,\boldsymbol{M}_2,...,\boldsymbol{M}_l,\boldsymbol{O}\}$ is formed [4]. A suitable point $\boldsymbol{G}=(x_G,y_G)$ from $E_p(a,b)$ can be chosen as the base point. With some linear displacement points $r\boldsymbol{G}$, $r\in\{1,2,...,n\}$, an additive group S can be worked out as Eq. (3) whose rank is n. Also, n is a prime number and the smallest positive integer that satisfies Eq. (2).

$$n\boldsymbol{G}=\boldsymbol{O}\rightarrow n(x_G,y_G)=(x_o,y_o) \tag{2}$$

$$S=\{\boldsymbol{G},2\boldsymbol{G},...,r\boldsymbol{G},...,n\boldsymbol{G}\}=\{(x_1,y_1),(x_2,y_2),...,(x_r,y_r),...,(x_n,y_n)\},r\in\{1,2,...,n\} \tag{3}$$

$$\boldsymbol{R}=r\boldsymbol{G}=(x_r,y_r)\rightarrow\boldsymbol{R}\in S \tag{4}$$

From Ref. [2], given an arbitrary integer r less than n as the private key, the corresponding public key $\boldsymbol{R}$ is as Eq. (4) above.

2.2 How to map user's identity u_{id} to a sequence M_{id}

An entity's identity, with a user's personal information included, can be mapped into coordinates of a matrix through hash operations. In Eq. (5), w_i indicates a row coordinate of an element in each column of matrix $\boldsymbol{A}_{m\times32}$, with a word size of s byte and v_i indicates that of matrix $\boldsymbol{B}_{h\times2}$, with a word length of t byte.

$$M_{id}=H(u_{id})=w_1,w_2,...,w_{32},v_1,v_2,m=2^s,h=2^t \tag{5}$$

2.3 How to get identity-key and separating-key by matrix $\boldsymbol{A}_{m\times32}$ and matrix $\boldsymbol{B}_{h\times2}$

As Eqs. (6–9) show, $\boldsymbol{A}_{m\times32}$ is used to generate identity-key, which is made up of public-key matrix $\{\boldsymbol{R}_{i,j}\}_{m\times32}$ and private-key matrix $\{r_{i,j}\}_{m\times32}$, where $i\in\{1,2,...,(m-1),m\}$, $j\in\{1,2,...,31,32\}$. From Eq. (4), $\{\boldsymbol{R}_{i,j}\}_{m\times32}$ can be derived from $\{r_{i,j}\}_{m\times32}$. According to Ref. [7], with a sum of any element taken from each column in $\{r_{i,j}\}_{m\times32}$, a new private key is produced. The generation method of public key is similar to that of private key when the suitable point $\boldsymbol{G}$ is chosen. That is to say, a combined matrix like $\boldsymbol{A}_{m\times32}$ with a size of $m\times32$ can generate m^{32} private-public key pairs. Hence, in CPK system, huge numbers of key-pairs can be