Secure Enterprise Information Systems: A Mutual Authentication Scheme for Roaming Users Using Memorable Information

Lin Yang, Xinghua Ruan, Jingdong Xu and Gongyi Wu

College of Information Technical Science, Nankai University, Tianjin 300071, P.R. China
cameling_yang@yahoo.com.cn {ruanxinghua, xujd, wgy}@nankai.edu.cn

Abstract. In enterprise information systems, personal mobility provides the ability for roaming users to access enterprise network services from anywhere at anytime. However, methods for mutual authentication between roaming user and servers are still far from satisfied. In this paper, we focus on such a mutual authentication scheme, by which users can only use memorable information to log in servers with confidence. The scheme is designed in a threshold fashion to improve system's availability and robustness. It can resist known attacks, such as replay attack, password guessing attack and verifier stolen attack. We believe this scheme is suitable for enterprise computing scenarios, in which network environments are confidential and closed.

Keywords: *Enterprise information systems, Security, Privacy, Trust, Password, Mutual authentication, Identity-based cryptography*

1. INTRODUCTION

Personal mobility provides the ability for roaming users to access proper network service at anytime, from anywhere. This problem is of growing importance as Internet-enabled computing devices become ever more prevalent and versatile. A common scenario in enterprise information systems is described as follows: a big enterprise with many departments possesses sufficient numbers and abundant variety of computing devices for its employees; each employee belongs to one particular department and has rights of accessing to dedicated services provided by that department; an employee can log in his or her department's network from any of these devices using one enterprise-wide unique interface.

One crucial issue of above scenario is mutual authentication between the employee and his or her department's network. This would be straightforward if users can only use memorable information, such as names and passwords, to complete mutual authentication. However, memorable passwords are very susceptible to exhaustive search or dictionary attacks [1-3].

In this paper, we propose a new threshold password-and-names-based mutual authentication scheme for roaming users. The proposed scheme is based on elliptic curve cryptography [4]. Password is used for authenticating user to servers in a threshold fashion [5], and identity-based cryptography techniques [6] is used to solve

the problem of authenticating servers to user. The roaming user can achieve mutual authentication with his or her department's networks by only keeping three pieces of information in mind. They are his or her user name, relative password and his or her department's name. We assume all these pieces of information are memorable, since two names are familiar to users, and password can be weak and short.

2. PROPOSED SCHEME

There are four kinds of entities in proposed scheme, namely the dealer, the server, the client and the user. The scheme consists of mainly three phases: the setup phase, the registration phase and the authentication phase. For reader's convenience, we first list the notations used in our scheme in Table 1.

Table 1. Notations

Symbol	Meaning
E	an Enterprise's dealer
D	a particular department
N_D	the department's name
(t,n)	the parameters of the department's threshold system
A	a collection of n servers in the department
B	a subset of A and $\|B\|$ equals to t
S_i	a server in the department, $i \in \{1,2,...,n\}$
(Sk_i, Pk_i)	the server S_i 's private/public key pair
C	a client terminal
nonce	a nonce selected by client in authentication phase
U	a roaming user
N_U	the user's username
P_U	the user's password
G_1	an additive cyclic group of order prime q
G_2	a multiplicative cyclic group of order prime q
P	a generator of G_1
$\hat{e}$	a bilinear map that maps $G_1 \times G_1$ to G_2
H_1	a hash function that maps $\{0,1\}^*$ to G_1
H_2	a hash function that maps $\{0,1\}^* \times G_1$ to $\mathbb{Z}_q^*$
H_3	a hash function that maps $\{0,1\}^* \times G_1 \times G_1$ to $\mathbb{Z}_q^*$
s	a secret held by dealer for the enterprise
r	a secret held by dealer for the department
r_i	the secret share of r stored in server S_i

Dealer has the responsibility for initializing enterprise-wide parameters and then distributing them. Servers respond to user's request and verify its validity distributedly. At meanwhile, every server involved in authentication phase should authenticate itself to the user too. Each server has a name in format of {*department name* || *ID*}, where "||" means concatenation. The registered user can accomplish mutual authentication with department's servers in authentication phase. Note that s is the one and only one enterprise-wide secret. On the contrary, there should be several different r s, each for one particular department. We will demonstrate later that s is used in authenticating servers while r is used in authenticating users.

2.1 Detailed Scheme

2.1.1 Setup Phase

In setup phase, the enterprise's dealer E is in charge of initializing enterprise-wide parameters and generating the secrets stored in every server.

Step 1: E randomly chooses a number $s \in \mathbb{Z}_q^*$ and computes $P_{pub} = sP$. The system parameters are $\{G_1, G_2, q, P, P_{pub}, \hat{e}, H_1, H_2, H_3\}$, which should be distributed safely to all of this enterprise's servers and clients. s is kept secretly in E.

Step 2: Suppose department D with name N_D is organized by E. D has a set of servers, denoted by $S_i \in A, i = 1,...,n$. For each server $S_i \in A$, E assigns an arbitrary unique string ID_i to it and computes $Pk_i = H_1(N_D \| ID_i)$, $Sk_i = sPk_i$ then sends ID_i and Sk_i to S_i secretly. Now, every server $S_i \in A$ has a unique ID_i and a private/public key pair (Sk_i, Pk_i), in which Sk_i should be kept secretly, while Pk can be easily rebuilt with the knowledge of N_D and ID_i.

Step 3: After generating private and public key pair for ever server, E can now initialize secrets for user registration and authentication. E randomly chooses a number $r \in \mathbb{Z}_q^*$ and $a_1, a_2, ..., a_{t-1} \in \mathbb{Z}_q$, then it constructs a polynomial of degree of $t-1$: $f(x) = (r + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}) \bmod q$. After that E computes the secret share $r_i = f(i) \bmod q$ for each $S_i \in A, i = 1,...,n$ and distributes them safely to each server. The secret r is held by E while secret share r_i is kept secretly by

$S_i \in A, i = 1,...,n$. If there is another department, E repeat the process in step 2 and step 3 to initialize secrets for its servers.

2.1.2 Registration Phase

In order to get registration to department D, user U first chooses a password P_U, which is easy to memorize, and then sends it with his or her username N_U secretly to E. E computes user U 's mater key $K_U = rH_1(N_U \| P_U)$ and his or her shared

secrets $K_i = H_2(ID_i, K_U)$ with every $S_i \in A, i = 1,...,n$, where ID_i is the arbitrary unique string assigned to S_i in the setup phase. Then the couple $\{N_U, K_i\}$ is sent to S_i secretly. After that, E can erase any information about P_U, K_U and K_i, and then the registration phase is done. K_i is obviously a strong secret and should be kept secretly in S_i. We can see later that after the authentication phase, it can be used to derive a secure session key between U and S_i.

2.1.3 Authentication Phase

We assume the network between client terminal C and servers of D is insecure. The user U roams up to C and wants to get mutual authentication with D. The method U used to accomplish such an authentication is to provide three pieces of memorable information: the department's name N_D, his or her username N_U and his or her password P_U. The dealer E can be offline in this phase.

Step 1: After user U inputs N_D, N_U and P_U to the client C, C first chooses t out of n servers in department D. We denote the selected servers as $S_i \in B$ where B is a subset of A. We also denote the index of these t servers by set $I = \{i_1, \ldots, i_t\}$ where I is a subset of $\{1, \ldots, n\}$. Then, C selects a random element $x \in \mathbb{Z}_q^*$ and computes $R = xH_1(N_U \| P_U)$. After that, C chooses a *nonce* to indicate this authentication process with $S_i \in B$, and sends $\{\text{Requese}, nonce, N_U, R\}$ to them.

Step 2: On receiving C's request, the server S_i first retrieves the corresponding $\{N_U, K_i\}$ indicated by N_U from its local storage, and then computes $R_i = r_i R$. After that, S_i randomly picks a number $y_i \in \mathbb{Z}_q^*$ and computes $Y_i = y_i P$, $h_i = H_3(nonce, R_i, Y_i)$ and $Z_i = y_i P_{pub} + h_i Sk_i$, where Sk_i is S_i's private key generated in the setup phase. Finally, $\{\text{Reply}, nonce, ID_i, R_i, Y_i, Z_i\}$ is send to C as a reply, in which ID_i is the arbitrary unique string assigned to S_i in the setup phase.

Step 3: On receiving replies with the proper *nonce* from these t servers, C first rebuilds the public key Pk_i for each $S_i \in B, i \in I$ by computing $Pk_i = H_1(N_D \| ID_i)$, where N_D is inputted to C by user U in step 1, and then verifies these servers one by one. To accomplish this, C computes $h_i = H_3(nonce, R_i, Y_i)$, $V_i = Y_i + h_i Pk_i$ for every S_i's reply, and checks that $\hat{e}(P, Z_i) = \hat{e}(P_{pub}, V_i)$. If it does not hold, C can send a complaint to S_i, or send a request to another server. This step is over when all verifications are passed.

Step 4: We assume that all the servers $S_i \in B$ sent the correct reply. After confirming these replies, the client C computes $K_U = \sum_{i \in I} \lambda_i x^{-1} R_i$ for the user U, where $\lambda_i = \prod_{j \in I, j \neq i} \frac{-j}{i-j} \bmod q$ is the coefficient of Lagrange interpolation formula. After that, C can compute $K_i = H_2(ID_i, K_U)$ to obtain the shared strong secret with every S_i. At this point, the roaming user U can safely log into $S_i \in B, i \in I$ from C with the help of K_i. One feasible, but not only method is using this shared long secret to protect a Diffie-Hellman key exchange between C and S_i, to derive a secure session key for further communication.

3. CONCLUSIONS

Due to the space limitation, the formal analysis of our scheme's correctness, security and performance is given in the full version of this paper [7]. To the best of our knowledge, we are the first to introduce identity-based cryptography techniques into distributed password-based authentication protocols to achieve efficient and explicit mutual authentication in enterprise information systems. The characteristics of our scheme are summarized as follows: 1) legal roaming users can log in networks safely with their hands empty; 2) the scheme can achieve mutual authentication between user and distributed servers; 3) user's password cannot be revealed by the administrator of the server; 4) the system secret won't leak out even if some of the servers are compromised; 5) the system is still available even if some of the servers are unavailable; 6) the scheme reaches high efficiency in network communication; and 7) the scheme resists replay attack, password guessing attack, stolen-verifier attack and insider attack. Benefit from these characteristics, our mutual authentication scheme can be deployed for enterprise information security frameworks, and at meanwhile provide roaming users with ideal mobility and convenience.

REFERENCES

1. S. Bellovin and M. Merritt, Encrypted key exchange: Password-based Protocols Secure Against Dictionary Attacks, in *Proc. of IEEE Symposium on Research in Security and Privacy 1992* (Oakland, CA, USA, 1992), pp.72-84.
2. W. Fork and B. Kaliski, Server-assisted generation of a strong secret from a password, in *Proc. of 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises 2000* (Gaithersburg, MD, USA, 2000), pp.176-180.
3. D. Jablon, Password authentication using multiple servers, in *Topics in Cryptology,* CT-RSA April 8-12, 2001, LNCS, Volume 2020, (Springer-Verlag: Heidelberg, 2001), pp.344-360.

4. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, in *Proc. Of Advances in cryptology 2001*, *LNCS, Volume 2139* (Springer-Verlag: Heidelberg, 2001), pp.213-229.
5. A. Shamir, How to share a secret, *Communications of the ACM.* Volume 22, Number 11, pp.612-613, (1979).
6. X. Cheng, J. Liu and X. Wang, An Identity-based Signature and Its Threshold Version, in *Proc. of 19th International Conference on Advanced Information Networking and Applications AINA 2005*(28-30 March 2005), pp.973-977.
7. L. Yang, X, Ruan, J. Xu, and G. Wu, *A Mutual Authentication Scheme for Roaming Users Using Memorable Information*, Unpublished work, available by email request (cameling_yang@yahoo.com.cn).