SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks. 2009; **2**:255–258
Published online 2 October 2008 in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.61

An identity-based single-sign-on scheme for computer networks

Jian Ren*,†
Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824-1226, U.S.A.

Summary

Conventionally, no user identification is required for a user to log into a security-protected system. User authentication is based on what the user knows, or what the user has, which can be easily shared among others. Moreover, when multiple systems are involved, the user is then required to authenticate to each system individually and repeatedly. In this paper, we present a scheme to achieve secure user identification and authentication to multiple security-protected systems simultaneously through a single operation. The proposed scheme is based on the well-known RSA cryptosystem, the discrete logarithm problem, and the subset-sum NP-complete problem. Security analysis shows that the proposed scheme is secure to all known security attacks and can be easily implemented in various environments including very resource constrained environment such as Smart Cards. Copyright © 2008 John Wiley & Sons, Ltd.

KEY WORDS: identification; authentication; Smart Card; single-sign-on

1. Introduction

Wireless networks and Internet has seen tremendous growth in electronic commerce in recent years. As we rely more and more on computer networks for data transfer, security has become one of the most important and urgent need for evident reasons. Among different techniques, user authentication has been widely used to provide access control to shared networks, applications, and individual user accounts. Conventionally, access control and user authentication are based on either a login name and password pair, or through a physical card together with a personal identify number (PIN) (e.g., credit card, ATM card, and membership card, etc.), which can be easily shared among others. Moreover, when multiple accounts are involved, the user is then required to authenticate to each account. As a reality, the situation tends to be complex and inconvenient as the number of accounts increases. *In addition to the complexity, these approaches cannot provide an adequate security protection from hostile attacks*. Meanwhile, there is generally no simultaneous built-in user identification.

To address these issues, in this paper, we present a scheme which can achieve secure user identification [1–4] and authentication to multiple accounts simultaneously through a single operation. This scheme can be implemented in various environments,

*Correspondence to: Jian Ren, Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824-1226, U.S.A.
†E-mail: renjian@egr.msu.edu

including Smart Cards, computer networks, wireless communication networks, and distributed computer networks. When applying to an enterprizing environment, this scheme can also be used to provide an easy and strong authentication for *single-sign-on* to multiple security-protected network domains [5], which increases the network security [6] significantly with a highly simplified identity based authentication process.

In the proposed scheme, the user can prove his identity and authenticate to his accounts through the typical identification process. The security of the proposed identification scheme is based on the well-known RSA cryptosystem, the discrete logarithm problem, and the subset-sum NP-complete problem. Security analysis shows that this scheme is secure to all known security attacks.

It is important to point out that Windows 2000 and Windows XP operating systems provide built-in Smart Card [7] interface, which enables the proposed scheme be implemented in Smart Card painlessly at a minimal cost, meanwhile achieving high security for various network access and user identification.

The remaining part of this paper is organized as follows: In Section 2, the proposed scheme is presented. The security verification is presented in Section 3. In Section 4, the security analysis is provided. In Section 4, the scheme is further analyzed from implementation point of view, including complexity and memory requirements. We conclude in Section 5.

2. The Proposed Scheme

Suppose there exists a trusted authority (TA) [2]. The identification number of an individual user is denoted by ID. TA first generates an RSA public and private key pair (e, n) and (d, n) according to Reference [8], where $n = pq$, $\phi(n) = (p-1)(q-1)$, p and q are larger prime numbers. TA then selects $s+1$ integers $a_0, a_1, a_2, \ldots, a_s$ randomly, such that $\gcd(a_0, a_1, \ldots, a_s) = 1$.

Define

$$f(x) = a_0 + a_1 x + \cdots + a_s x^s \bmod \phi(n) \qquad (1)$$

where s should be larger than the number of organizations that the user will register and be a member.

2.1. User's Enrollment in TA

To register in the TA, let $\mathrm{ID} = h(id)$ be user U's personal identification number as described in References [3,4], where id can contain the user's fingerprints, SSN and DNA etc. and h is a hash function. The purpose of the individual ID is to uniquely and unambiguously identify the user from others. The user's ID is then signed by the TA using its RSA private key. That is, $\mathrm{ID}_{\mathrm{Sign}} = \mathrm{ID}^d \pmod n$. The numbers ID, $\mathrm{ID}_{\mathrm{Sign}}$, and $T = (\mathrm{ID}^{a_0}, \mathrm{ID}^{a_1}, \ldots, \mathrm{ID}^{a_s}) \bmod n$ are all sent back to the user, or stored in user U's Smart Card so that only user U can read them.

2.2. Organization's Enrollment in TA

An organization, or a group is a unit where an individual user can register to establish an account or become a member. Since $\gcd(a_0, \ldots, a_s) = 1$, TA can select a C such that

$$\gcd(f(C), \phi(n)) = 1 \qquad (2)$$

According to Euclid's Algorithm [6], a G can be very easily computed such that

$$f(C) \cdot G = 1 \pmod{\phi(n)} \qquad (3)$$

G serves as organization G's public identity and C as the private key. In addition, TA should keep $f(C)$ secret to itself for organization G's identity verification.

2.3. User's Organization Enrollment

The process for a user U to enroll in organization G is described as follows:

1. U: Provides ID and $\mathrm{ID}_{\mathrm{Sign}}$ to group G to confirm the authenticity of U's identity.
2. G: Calculates

$$\prod_{j=0}^{s} (\mathrm{ID}^{a_j})^{C^j} = \mathrm{ID}^{f(C)} \pmod n \qquad (4)$$

   where C is the secret key of organization G.
3. G/U: Stores $\mathrm{ID}^{f(C)}$ in user U's Smart Card as user U's enrollment record in G.

Since $\mathrm{ID}^{f(C)\cdot G} = \mathrm{ID} \pmod n$, Equation (4) can be used to verify this enrollment by both G and U.

DOI: 10.1002/sec

3. Identity Proof

The proof of user's identity and membership of multiple organizations can be performed simultaneously with a single operation. If user U has enrolled t organizations, without loss of generality, we may assume that U has enrolled $G_1, G_2, \ldots, G_t$.

To verify that user U has enrolled any l ($1 \leq l \leq t$) organizations: $G_1, G_2, \ldots, G_l$, U needs to prove to the verifier V for having the secret information $\mathrm{ID}^{f(C_i)}$ ($i = 1, 2, \ldots, l$), which can be verified as follows:

1. U: Select a random number `rand` and let $r =$ `rand` $\|$ `Timestamp` ($0 < r < n$). Computes $x = r^{eG_1G_2\cdots G_l} \pmod n$;
2. U: Sends $r \prod_{i=1}^{l} \mathrm{ID}^{f(C_i)} \pmod n$, x and ID to V;
3. V: Verifies that

$$\left(r \prod_{i=1}^{l} \mathrm{ID}^{f(C_i)}\right)^{eG_1\cdots G_l} \stackrel{?}{=} x\mathrm{ID}^{e(G_2G_3\cdots G_l+\cdots+G_1G_2\cdots G_{l-1})} \bmod n \quad (5)$$

This verification can be repeated multiple times. User U will be considerate as a legitimate user if and only if Equation (5) is true for each verification. The concatenation of `Timestamp` in r with a pre-defined allowable time shift prevents 'play-back' attack.

4. Security Analysis

The user enrollment in TA eliminates the possibility for an illegitimate user to impersonate and/or to steal a valid user's ID. The organizational enrollment assures that each organization is authorized to accept individual user's enrollment. While the user's enrollment in organizations enables a user account or membership be created properly in the organizations.

The security of the proposed scheme is based on the security parameters and the identity proof process. They will be analyzed separately in this section.

4.1. Attack on Security Parameters

The security parameters of the proposed scheme include three types of security parameters:

1. TA's security parameters: $p, q, d, a_0, \ldots, a_s$ and $f(C)$;
2. Organization's security parameters: C;
3. User's security parameters: $T = (\mathrm{ID}^{a_0}, \ldots, \mathrm{ID}^{a_s})$, $\mathrm{ID}^{f(C)}$.

The security parameters p, q, and d are the TA's RSA security parameters. Up to now, as long as p and q are large enough, breaking the system security parameter d is *equivalent* to break the RSA system, which are computationally infeasible [8].

The security parameters $a_0, \ldots, a_s$ only appeared in the exponent in the form of ID^{a_i} with $\mathrm{ID} = h(id)$. The recovery of the a_i's is *equivalent* to break the discrete logarithm problem (DLP). We do not know any polynomial technical that can compute DLP. Without a_i's and C, nobody is able to compute the $f(C)$. In fact, the computation of $f(C)$ from C is essentially a subset-sum NP-complete problem, which is known to be intractable [9]. To compute $f(C)$ from a single G is *equivalent* to break the RSA system since G can be viewed as an RSA public key, and $f(C)$ can be viewed as the corresponding RSA private key. In summary, the TA's security parameters are secure under known security attacks.

We recommended that p and q be integers of 512-bit (or longer). Then the corresponding n would be a 1024-bit integer. To derive a_i from ID^{a_i} requires to calculate the discrete logarithm $\log_{\mathrm{ID}} \mathrm{ID}^{a_i} \pmod n$, which is difficult if a_i is a large number [9–11] and there is no effective method available.

For the security parameter C of account G, there is no tangible way to compute C since even $f(C)$ is unknown. In fact, even if $f(C)$ is known, the recovery of C requires to solve the subset-sum NP-complete problem. Therefore, C is also secure.

We still need to discuss the security of user security parameters. The security of the user secret $T = (\mathrm{ID}^{a_0}, \ldots, \mathrm{ID}^{a_s}) \pmod n$ relies on the fact that $a_0, \ldots, a_s$ are all unknown large integers. Therefore, ID^{a_i} are unknown and secure. For the same reason, $\mathrm{ID}^{f(C)}$ is unknown and secure.

In summary, all the security parameters are secure under known security attacks. Therefore, the scheme is secure.

4.2. Attack on Identity Proof

Now that it is computationally infeasible to recover any of the security parameters, the stealing of other people's ID and security parameters are

DOI: 10.1002/sec

impracticable. Moreover, the random selection of `rand` in concatenation with the `Timestamp` makes reply and forge attacks of identity proof intractable.

5. Implementation

To implement this scheme, each user needs to maintain the following security parameters:

1. TA's information: n, d, and e;
2. User's enrollment record in TA: ID, $\mathrm{ID}_{\mathrm{Sign}}$, and $T = (\mathrm{ID}^{a_0}, \ldots, \mathrm{ID}^{a_s}) \pmod{n}$;
3. User's organizational enrollment record: $\mathrm{ID}^{f(C_i)}$ for each organization G_i $(i = 1, \ldots, t)$.

Suppose p and q are both 512-bit integers, then the (maximal) length of all the above mentioned security parameters is 1024 bits. Therefore, the TA information is equal to 1024×3 bits, the user's enrollment record in TA is $1024 \times (2 + (s + 1)) = 1024 \times (s + 3)$ bits, and the organizational enrollment record is $1024 \times t$ bits.

Let $s = 100$, $t = 100$, and each user enrolls up to 100 organizations, then the total number of bits that needs to be stored in user U's Smart Card is equal to $1024 \times 3 + 1024 \times (s + 3) + 1024 \times t = 1024 \times (s + t + 6) = 1024 \times 206 = 210944$ bits, or 25.75 K bytes. Therefore, a Smart Card with 32 K bytes read-only memory (ROM) is sufficient for this implementation. This type of Smart Cards is widely available commercially [7].

In verification process, the computations required are quite limited since only simple exponential calculations, multiplications, and additions are needed. All these operations can be implemented efficiently in a resource constrained environment such as a Smart Card or a mobile hand-held device. The verification can also be implemented in a dedicated verification device. In either case, it can achieve communication network security, single-sign-on and identification simultaneously through a single operation.

6. Conclusion

To overcome the inefficiency and security weakness of the conventional user identification and authentication schemes, in this paper, we developed a scheme to securely identify and authenticate the user to multiple accounts simultaneously through a single operation. It was shown that the new scheme is secure to all known security attacks. We also demonstrated that this scheme can be easily implemented in various environments, including Smart Cards and wireless communication networks.

Acknowledgements

The author thanks the anonymous reviewers for their valuable comments on an earlier version of this paper.

References

1. Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signatur problems. In *Advances in Cryptology—Crypto'86*, 1986; 186–194.
2. Schnorr CP. Efficient identification and signatures for smart cards. In *Advances in Cryptology—Crypto'89*, 1989; 239–252.
3. Shoup V. On the security of a practical identification scheme. In *Advances in Cryptology—Eurocrypt'96*, 1996; 344–353.
4. Simmons GJ. An impersonation proof identity verification scheme. In *Advances in Cryptology—Crypto'87*, 1987; 211–215.
5. The Open Group. Single sign-on. http://archive.opengroup.org/public/tech/security/sso/
6. Stallings W. *Cryptography and Network Security—Principles and Practices* (3rd edn). Prentice Hall, 2003.
7. U.S. General Services Administration, Smart Card Standards and Interoperability. http://www.smartcard.gov
8. Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the Association for Computing Machinery* 1978; **21**(2): 120–126.
9. Cormen TH, Leiserson CE, Rivest RL, Stein C. *Introduction to Algorithms* (2nd edn). The MIT Press, 2002.
10. Diffle W, Hellman ME. New directions in cryptography. *IEEE Transactions on Information Theory* 1976; **22**: 644–654.
11. ElGamal TA. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* 1985; **31**(4): 469–472.

DOI: 10.1002/sec