An Anonymous Authenticated Protocol Based on Zero Knowledge Proof

Chao JING [1]

[1] Department of Network, School of Electronics and Computer Science and Technology, North University of China, Taiyuan 030051, Shanxi, China.

Abstract

With the rapid development of the Internet, anonymity and privacy protection in many applications of the scene is critical. The anonymous authentication means that the server can't know the user's identity when they are communicating with each other. In this paper, based on the Wang's zero knowledge proof scheme of possessing a digital signature, we propose a new anonymous authentication scheme. Compared with the Cui-Cao's anonymous authentication protocol based on the ring signature, our scheme has two advantages. First, we don't need to know all users' public keys. And then our scheme reduces the communication traffic largely. We also discuss the security attributes of our new scheme which are authentication, anonymity and unlinkablity. And then we introduce a concrete application of our scheme. Finally, we make a conclusion of this paper.

Keywords: *anonymous authentication; DSA digital signature; Zero-Knowledge proof*

1. Introduction

Network security has become the focus of concern with the development of the Internet applications, the vulnerabilities of network security mechanism have gradually emerged. Related security technology, security agreement was continuously put forward. But these security technology and protocols were mostly for communication of content. While anonymous problem is considering that the sender and the receiver is also occasions of confidential information. An anonymous system attacker wants to get who is who in communication with and even to control or destroy the communication process.

A. Anonymity in Authentication Scheme

Anonymity and privacy protection in many applications of the scene is critical. In the cash shopping or participating in the secret ballot election, People always want to hide their true identity to other participants or these may be eavesdropper. In some of the other scenes, People hope to stop the other unauthorized people from finding their identity through the flow analysis when they display their identity to others, such as the witness reporting the criminal.

As far as user privacy and anonymity is concerned, research on this topic usually focuses on two issues: anonymous communication and user anonymity [1]. Anonymous communication [2] usually provides a communication channel to resist traffic analysis, so that the communicating parties can be anonymous against the eavesdroppers.

A more complicated and seemingly paradoxical issue is user anonymity, which aims at providing users anonymity when they are using the network by letting them hide their identity from the communicating peers. User anonymity existing in an anonymous authentication scheme [3] is a protocol that allows a member called a prover of a group to convince a verifier that he is a real member of the group without revealing any information about his identity. An immediate way to achieve user anonymity is to assign an alias name to each user, and every user will use his alias name to login to perform key exchange with the server, instead of using his real identity. However, such idea does not work since the server could always match user's alias name with his real identity. So the server can know the user's identity. Maybe the attacker can achieve the user's identity from the server. Therefore the server doesn't know the user's identity which is maybe the safest. Recently, there have been some protocols presented to realize safer idea. In this paper, we proposed an anonymous authentication scheme based on the zero knowledge proof which achieves that the server doesn't know the user's identity.

B. Related works

In 2000, Lee and Chang [4] proposed a user identification scheme with key distribution maintaining user anonymity for distributed computer networks. Wu and Hsu, however, showed that the Lee-Chang scheme is insecure against impersonation and identity disclosure attacks [5]. An adversary can plot an impersonation attack to masquerade as a service provider in order to exchange a session key

with a user without being detected in the authentication protocol. In addition, an adversary can plot the disclosure attack to identify a user who requests services with a released session key. Wu and Hsu further proposed an improved scheme to withstand these two attacks, preserving the same security requirements as those of the Lee-Chang scheme. Recently, Yang et al. demonstrated a compromising attack whereby it is possible for an adversary to derive the private keys of users who request services [6].

Following on, it is to deal with anonymous issuer Chien, H. Y., Chen. C. H. [7], Viet. D. Q., Yamamura. A. and Tanaka. H [8] respectively proposed the authentication schemes. However, the former indeed deals with anonymous communication not user anonymity, and the latter uses password tables at the server side and needs a lot of exponential operations. Jing Yang et al. [9] firstly point out the vulnerabilities of both Viet et al.'s and Shin et al.'s anonymous password-based authenticated key exchange protocols, and then propose a new anonymous password-based authenticated key exchange (JZH) protocol. Zhenchuan Chai et al. [10] also propose an efficient password-based authentication and key exchange (CHCL) scheme to preserve user privacy, and they analyze the security requirements of their new scheme. Both of them try to achieve user anonymity without using group or ring signature schemes.

Recently, Cui-Cao [11] find that their user anonymity both exist some security defect. If the connection between the user and the server has been established, and the server wants to guess the user's identity, the probability is 100%, in other words, the server can obviously guess the user's identity. Then Cui-Cao proposed a new anonymous authentication and key exchange protocol. However, their scheme is not realistic to know all user's public key .Therefore their scheme has a large communication traffic which is difficult to put into use .On the same time, we proposed an anonymous identification scheme based on the zero-knowledge proof scheme of possessing a DSA digital signature [12] which eliminated the security vulnerability well and owned sensational properties. It has the superior properties of authentication, anonymity and unlinkablity.

C. Our Contributions

Our contributions in this paper could be summarized as two critical points.

Firstly, based on the Wang's zero knowledge proof scheme of possessing a digital signature, we propose a new anonymous authentication scheme. Compared with the Cui-Cao' anonymous authentication protocol based on the ring signature, our scheme has two advantages. First, we don't need to know all users' public keys. And then our scheme reduces the communication traffic largely.
Secondly, we analyze the security attributes of our new scheme which are authentication, anonymity and unlinkablity. And then we make an introduction of this new scheme's application.

a) organization

The rest of this paper is organized as follows: in section II we briefly introduce the zero knowledge proof. And the later is the description of our proposed suggestion for the designing of anonymous authentication scheme in section III; we also analyze the security properties of our scheme and make an introduction of its application briefly in section IV. The section V concludes this paper.

2. Zero Knowledge Proof

Based on the ideas of undeniable digital signature and confirmer digital signature, a new zero-knowledge proof scheme of possessing a DSA digital signature is proposed which can be used to prevent the arbitrary distribution of digital signature. In this section we briefly review the zero-knowledge proof of possessing a digital signature.

In the following proof ,the system parameters of DSA[13] is assumed to be *p, q, g* (*p* and *q* are respectively 1024 and 160 bits of big prime; $q|p\text{-}1$; $g \in z_p$, the order is *q*; generally $g = h^{(p-1)/q} \bmod p$,$1<h<p\text{-}1$ and $h \in z$). We also assume that P's (the signer's) public key is $y = g^x \bmod p$. The public key can be gained from X.509 or other public key certificate. $x \in R, Z_p$, it's P's private key which represents the singer status information. From the DSA we can know the singer P signed (*r, s*) for the message M.

$$\begin{cases} r=(g^k \bmod p) \bmod q; k \in RZ_q \\ s=[k^{-1}(H(M)+xr)] \bmod q \end{cases} \quad (1)$$

H (.) is the safety hash function. DSA verification is to determine whether the following equation is established.

$$\left\{[g^{(H(M)_s^{-1} \bmod q)} y^{(rs^{-1} \bmod q)}] \bmod p\right\} \bmod q = r \quad (2)$$

If (2) is established, the signature is right. Inversely, it's wrong. To be convenient, we can use the following equation to stand of (2) for short.

$$Z_p g^{(H(M)_s^{-1})} y^{rs^{-1}} = r$$

The signer P wants the verifier V to sure it has the digital signature (*r, s*) for the message M, but which can't let any information about *r* and *s* out. P and V must observe the following zero knowledge proof.

$$ZPK\left\{\alpha,\beta\,|\left[(g^{(H(M)\beta^{-1})\bmod q}y^{(\alpha\beta^{-1})\bmod q})\bmod p\right]\bmod q=\alpha\right\} \quad (3)$$

The α and β stand for P's private information; *r* and *s* are M's digital signature that owned by P; *p, q, g, y* are the shared information between P and V.

In order to simplify (3), we use another type to continue the zero knowledge proof.

Firstly, P computes the commitment value of the r.

$$Z := (y^r \bmod p)\bmod q \quad (4)$$

Then P discloses the commitment value and sends it to V. Next we can simplify (3) in the following zero knowledge proof.

$$ZPK\left\{\alpha,\beta|z\left[\left(y^{\alpha}\right)\bmod p\right]\bmod q\wedge\left[\left(g^{H(M)\beta^{-1}\bmod q}y^{\alpha\beta^{-1}\bmod q}\right)\bmod p\right]\bmod q=\alpha\right\} \quad (5)$$

Also we should notice the following equation.

$$z=y^{\alpha}$$

$$\left[\left(g^{H(M)\beta^{-1}}y^{\alpha\beta^{-1}}\right)\bmod p\right]\bmod q$$

$$=\alpha\Leftrightarrow\left[\left(y^{\left[\left(g^{H(M)}z\right)^{\beta^{-1}}\bmod p\right]\bmod q}\right)\bmod p\right]\bmod q=z \quad (6)$$

The above equation (6) is established apparently. So (5) is equivalent to the following equation.

$$ZPK\left\{\alpha,\beta\mid z=\left[\left(y^{\alpha}\right)\bmod p\right]\bmod q\wedge z\right\}$$

$$=\left[\left(y^{\left[\left(g^{H(M)}z\right)^{\beta^{-1}}\bmod p\right]\bmod q}\right)\bmod p\right]\bmod q \quad (7)$$

$$b := g^{H(M)}z \bmod p \quad (8)$$

The （7）can use the following equation for instead.

$$ZPK\left\{\alpha,\beta\mid z=y^{\alpha}\wedge z=y^{b^{\beta^{-1}}}\right\} \quad (9)$$

The specific meaning that the (9) stands the zero knowledge proof for the following equation.

$$ZPK\left\{\alpha,\beta\mid z=y^{\alpha}\wedge z=y^{b^{\beta^{-1}}}\right\}=\{c,d,s_1,...,s_l\}\in\{0,1\}\times z_q^{l+1} \quad (10)$$

(The α and β are respectively representing the digital signature *r* and *s*.)

3. The Proposed Scheme

Based on the zero-knowledge proof scheme of possessing a DSA digital signature, we proposed our scheme. Our scheme has two creative ideas which make our scheme safer. We start by presenting our scheme in detail, and then discuss the security of the concrete scheme.

(1) The traditional anonymous authentication scheme is most for the two objects：the user and the sever. However, it will become easier for the sever to know the user's identity. The first creative idea of our scheme is that we introduce an intermediate agent (another service producer P_j) to complete the communication between user U_i and service provider P_i. When the user U_i wants to access the service provider P_i, U_i send the message M to P_j. Then P_j verifies the user and uses its private key to give it a digital signature *r* and *s*. As the U_i receives the digital signature, it begins to access the P_i. P_i validates the digital signature to determine whether to allow to access.

(2) If the user sends the digital signature *r* and *s* to sever directly, the sever maybe can compute the user's identity. The second creative idea of our scheme is that we use the above zero knowledge proof to achieve the safe communication between U_i and P_i. After U_i receives the digital signature from P_j, our scheme can be realized on the following style.

1. Firstly, the user U_i chooses a series of random figures like $r_0, r_1, \ldots, r_l \in R, Z_q$

Then U_i begins to compute:

$$c := H(g\,|\,p\,|\,q\,|\,z\,|\,y^{r_0}\,|\ldots|\,y^{\theta_l})$$

$$(c=c[l].....c[1]\in\{0,1\}^l;$$

$$[(y^{\theta_l\bmod q})\bmod p]\bmod q, i=1,...,l;\theta=b^{r_i})$$

2. Secondly, after getting the result, the user U_i uses its secret values which are the digital signature *r* and *s* in fact and in confidence computes:

$$d = r_0\cdot cr \bmod q$$

$$S_i=\begin{cases}r_i;c[i]=0\\ r_i-s^{-1},c[i]=1\end{cases}\quad(i=1, 2\ldots., l)$$

Then we achieve the *c, d* and *s* which constitute the zero knowledge proof.

3. Thirdly, the user U_i sends the zero knowledge proof {*c, d*, s_1, st} to the service provider P_i through the safe channel between them.

4. After the service provider P receives the zero knowledge proof, it uses the shared information *p, q, g, y, M, z, b* to verify the following formula whether to be established.

$$c\overset{?}{=}H(g\,|\,p\,|\,q\,|\,y\,|\,z\,|\,z^c y^d\,|\,t_1\,|\ldots|\,t_l \quad (11)$$

$$t_i=\begin{cases}[(y^{bS_i\bmod q})\bmod p]\bmod q.c[i]=0\\ [(z^{bS_i\bmod q})\bmod p]\bmod q.c[i]=1\end{cases}\quad(i=1,\ldots., l)$$

If (11) is established, the service provider P_i is convinced that the user U_i is a legitimate user. While it's not

established, the user and the service provider can't set up a connect to communicate.

(See Fig.1 the user authentication phase, which is the detailed and visual progress.)

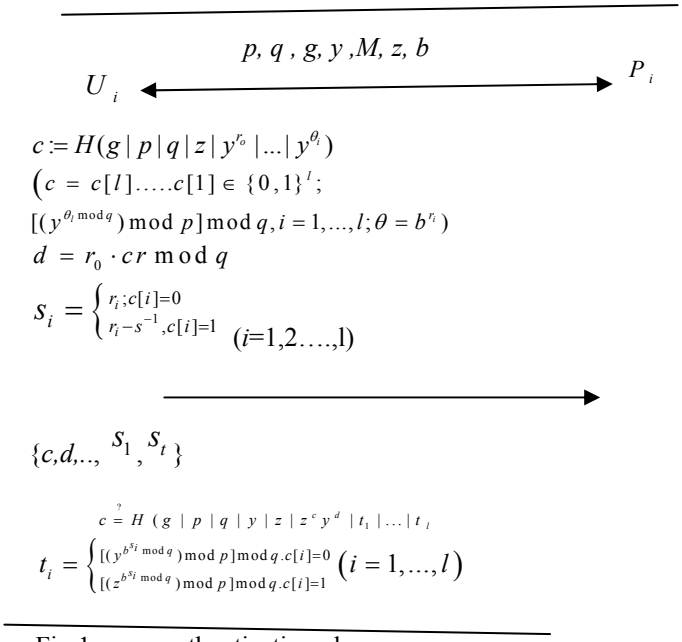

Fig.1 user authentication phase

4. Security Analysis

Here we will discuss the security properties of our proposed scheme, so as to show our scheme meets the following properties. Then we will introduce its application briefly.

A. Security Discussion

Authentication: No one can impersonate a legal user to request the service from the service provider P_i in our new scheme. Because only the legal user can get the digital signature *r* and *s* from the registration center (another service provider).If a user U_i wants to be a legal one, he must registrate in the registration center P_j. So the intermediate agent P_j can identify which user is legal and then give the digital signature to it. If the user U_i is not legal, it can't get *r* and *s*. Namely, it can't communicate with the service provider. What's more, the service provider P_i has no contact with the registration center P_j (another service provider.) So the service provider P_i can't get any information about the user's identity from the registration center P_j. Therefore we can say the user U_i can't be impersonated. Namely, our scheme realizes the authentication.

Anonymity: In our scheme if the actual user does not reveal the digital signature, then any verifier cannot determine who the actual user is. The user U_i chooses a series of random figures $r_0, r_1, \ldots, r_l \in R, Z_q$ to compute and sends the zero knowledge proof $\{c,d,.., s_1,s_t\}$ to the service provider P_i. While the service provider P_i doesn't know how to compute the $\{c, d, s_1, s_t\}$, which is computed in confidence by the user U_i using the digital signature *r* and *s*. What's more, the user U_i owns the digital signature *r* and *s* from the registration center P_j. The service provider P_i and the registration center P_j is unconnected. So the service provider P_i cannot know which user access to it. Namely, it satisfies the anonymity.

Unlinkablitity: If an attacker impersonate the service provider to get the user's identity, in our scheme it is may be impossible. As the user U_i and the service provider P_i use the zero knowledge proof, the service provider P_i can convince the user U_i is legal but cannot know the accurate digital signature *r* and *s* .Every time the service provider P_i received the zero knowledge proof, it starts to verify using the shared information *p, q, g, y, M, z, b* which don't have the privacy information. So the service provider P_i can't achieve any information about the user's identity. The limited anonymity is uncomputational for the service provider P_i. When the user accesses to the service provider two times continuously, the service provider can't compute the identity of the user U_i. The user U_i and the service provider P_i is unlinkablitity.

B. Application

As far as user privacy and anonymity is concerned, research on this topic usually focuses on two issues: anonymous communication and user anonymity. Anonymous communication usually provides a communication channel that resists traffic analysis, so that the communicating parties can be anonymous against the eavesdroppers. A more complicated and seemingly paradoxical issue is user anonymity, which let the users hide their identities from the communicating peers. Here we use a concrete application of our scheme to discuss user anonymity in the environment of distributed networks authentication.

A user Jane wants to download some files from a website Bob; however, he doesn't want to disclose his identity. We assume that Peter is a trusted third party which we regard as the registration center. The process can be described as follows.

(1) Jane wants to access Bob with the message M, firstly Peter uses his private key to generate the digital signature *r* and *s* for M from Jane.

(2) After Jane receives the digital signature *r* and *s*, he begins to choose a series of random figures like $r_0, r_1, \ldots, r_l \in R, Z_q$ and compute with its values in secret, and then get the zero knowledge proof $\{c,d,.., s_1,s_t\}$.

(3) Jane sends the zero knowledge proof {*c, d*, .., s1, s_t} to Bob through the safe channel.

(4) After Bob receives the zero knowledge proof, he uses the shared information *p, q, g, y, M, z, b* to verify if the user is legal. If Bob is legal, Peter will establish the connection with Bob.

4. Conclusions

In recent years, anonymous authentication is attached great importance to preserve user privacy in wired or wireless network environments. In this paper, based on the Wang's zero knowledge proof scheme of possessing a digital signature, we propose a new anonymous authentication scheme. Compared with the Cui-Cao' anonymous authentication protocol based on the ring signature, our scheme has two advantages. First, we don't need to know all users' public keys. And then our scheme reduces the communication traffic largely.

Furthermore, we analyze the security of our new scheme which has the properties of authentication, anonymity and unlinkablity. And then we introduce a concrete application of our scheme.

References

[1] Bo.Z., Wan.Z.G., Kankanhalli.M.S., Feng.B., Deng.R.H.: Anonymous secure routing in mobile ad-hoc networks, Local Computer Networks, 2004. 29th Annual IEEE International Conference on 16-18 Nov. (2004) 102- 108

[2] Arjan Durresi. Anonymous communications in the Internet. Cluster Comput (2007) 10: 57–66, DOI 10.1007/s 10586-007-0006-y

[3] Viet.D.Q., Yamamura.A., Hidema.T.: Anonymous Password-Based Authenticated Key Exchange. In: Maitra, S., Veni Madhavan, C.E., Venkatesan, R.(eds.) INDOCRYPT 2005. LNCS, vol. 3797, pp. 244-257. Springer, Heidelberg (2005)

[4] W.B. Lee, C.C. Chang. User identification and key distribution maintaining anonymity for distributed computer network. Computer Systems Science and Engineering 15(4) (1999) 113-116

[5] T.S. Wu, C.L. Hsu. Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks. Computers and Security 23 (2) (2004) 120-125.

[6] Y. Yang, S.Wang, F. Bao, J.Wang, R.H. Deng. New efficient user identification and key distribution scheme providing enhanced security. Computers and Security 23 (8) (2004) 697-704.

[7] Chien.H.Y., Chen.C.H.: A remote authentication scheme preserving user anonymity, In: Proceedings of the 19th International Conference on Advanced Information Networking and Applications-AINA 2005, 245-248

[8] Viet.D.Q., Yamamura.A., Tanaka.H.: Anonymous password-based authenticated key exchange, Advances in Cryptology INDOCRYPT 2005, LNCS, Vol. 3797, Berlin: Spring-Verlag, (2005) 244-257

[9] Jing Yang, Zhenfeng Zhang. A new anonymous password-based authenticated key exchange protocol. D.R.Chowdhury, V.Rijmen, and A.Das (Eds.): INDOCRYPT 2008, LNCS 5365, pp.200-212, 2008. Springer-Verlag Berlin Heidelberg 2008

[10] Zhenchuan Chai, Zhenfu Cao, and Rongxing Lu. Efficient password-based authentication and key exchange scheme preserving user privacy. X.Cheng, W.Li, and T.Znati (Eds.): WASA 2006, LNCS 4138, pp.467-477, 2006. Springer-Verlag Berlin Heidelberg 2006

[11] Cui hui,Cao tianjie .A Novel Anonymous Authentication and Key Exchange Protocol. Journal of Networks, VOL. 4, NO. 10, 985-992, DECEMBER 2009,EI

[12] Wang shang-ping,Wang yu-min,Wang xiao-feng,Zhang ya-ling,Qin bo.A Zero-Knowledge Proof Scheme of Possessing a DSA Digital Signature [J].ACTA ELECTRONICA SINICA 2004, 32（5）: 878-880.

[13] National Institute Standards and Technology. NIST FLPS PUB 186,

Digital Signature Standard [S] .U.S. Department of Commerce,May 1994

First Author: Chao JING, born in Jan. 1980. Male. He received the master's degree in computer science at July 2006. Currently, he is a lecturer at department of network, school of electronics and computer science and technology, North University of China, Taiyuan, Shanxi, China. His interests are in the network security and automatic control. This paper is supported by Natural Science Funds of Shanxi Province (No. 2010021016-3). E-mail: jingchao@nuc.edu.cn, 172646928@qq.com