An Improved Kerberos Intra-domain Authentication Protocol Based-On Certificateless Public-Key Cryptography

Wang Juan[1], Cao Man-cheng[1], and Fang Yuan-kang[1,2]

[1] Chizhou College, Chizhou, Anhui
[2] Information Science and Technology School Nanjing University of Aeronautics and Astronautics Nanjing China
Fyk80@163.com

Abstract. The paper sums up some improvements in Kerberos intra-domain authentication protocol included in many domestic and foreign literatures. By analyzing the limitations of those improvement schemes, an improvement in Kerberos intra-domain authentication protocol based on certificateless public-key thought is proposed. The analysis shows that the improvement proposal can overcome some defects in the original Kerberos intra-domain authentication protocol, such as the key escrow problem and network intermediaries attack, etc. Moreover, the improvement also meets the demand of security proposed by key agreement protocol, which has a certain security and perspective of application in the process of network identity authentication.

Keywords: Kerberos, Intra-domain Authentication, Security Attributes, Certificateless Public key cryptography.

1 Introduction

Kerberos[1], which has intra-domain and inter-domain authentication modes, is a widely-used identity authentication protocol based on the trusted third party, developed firstly by the Project of Athena in Massachusetts Institute of Technology (MIT). The nucleus of Kerberos is the authentication center – Key Distribution Center (KDC), which consists of authentication server AS and Ticket Granting Server（TGS）. The basic principal is as follows: If a user wants to access some application server, it must get its identity authentication in KDC and obtain the ticket to visit the application server, which provides direct service for the user with the ticket.

The method adopted by traditional Kerberos intra-domain authentication protocol is symmetric data encryption standard DES, in which there exists such limitations as clock synchronization being difficult, password guessing attack, complicated storage and management of keys, not providing digital signature, and undeniable mechanism[2], which lead to poorer internet protocol security.

Due to the limitations of traditional Kerberos intra-domain authentication protocol, many literatures at home and abroad have improved it by adopting asymmetric (public key) encryption system RSA, called for short, Kerberos RSA protocol[3-6], which, to

D. Jin and S. Lin (Eds.): Advances in MSEC Vol. 2, AISC 129, pp. 489–496.
springerlink.com

some extent, overcomes those limitations existing in traditional Kerberos. However, RSA is not so perfect, because it has such weaknesses as slower encryption/decryption speed, and lower execution efficiency[7]. If public key system is adopted to encrypt and decipher in the process of transmitting data, the authentication efficiency must be affected.

In order to make up the defects of poorer security of symmetric key system and lower execution efficiency of public key system, literature [8-9] has improved Kerberos protocol by mixing symmetric data encryption system DES with asymmetric (public key) encryption system RSA, called for short, mixed-system Kerberos intra-domain authentication protocol. The improvement, to some extent, has eased the limitations in traditional Kerberos and Kerberos RSA by combining higher execution efficiency of symmetric encryption system with higher security of public key encryption system. Moreover, in order to prevent the possible internal attack existing in mixed-system Kerberos intra-domain authentication protocol, literature [9] has proposed a safer Diffie-Hellman key exchange protocol – public keys in mixed encryption scheme should adopt Diffie-Hellman key exchange protocol.

But after analyzing the improved Kerberos intra-domain authentication protocol in literature [9], the researcher found there are still drawbacks in it. That's because, after clients (C) and application server (S) passed identity authentication, the two sides' exchanging of parameters used in producing consultation session keys, is still transmitted with Kc.s encryption generated by Kerberos. Thus, Kerbers may still possibly intercept and capture the parameters exchanged by both sides, and then gain session keys by impersonating as C and consulting with S. Therefore, such session keys are not safe.

In sum, on the basis of a certificateless public key Cryptography system[10], the paper has proposed Kerberos intra-domain authentication key agreement scheme, which may solve the above problems efficiently,and can meet the demands of the present known key agreement protocol's security attributes.

2 Related Pre-knowledge

2.1 Key Agreement Protocol's Basic Security Attributes

Literature [11-12] lists several security attributes needed to investigate while making a security analysis of most protocols at present.

a) Key Hidden Authentication（KHA）. Each user of the protocol believes that only the protocol's participants know session keys, which cannot be obtained by attackers. Providing key agreement protocol identified by keys hidden can resist man-in-the-middle attack.

b) Known Session Key Security（KKS）. Even if some previous session key is exposed or obtained initiatively by attackers, the attackers cannot get access to any other session keys.

c) Forward Security（FS）. Long-term private key exposure of a protocol participant cannot affect the security of his previous session keys.

d) Resist Key Compromise Impersonation Attack(KCI). If A's long-term private key is breached, the attacker may disguise as A, but he cannot disguise as any other entity in the name of A.

e) Unknown Key Shared Security (UKS). If the shared session key of both transmitter and receiver is K, the attacker cannot enforce the session key shared by both sides as K′.

f) Keys' Uncontrollability (KU). All participants of the protocol cannot control the output of session keys, which is called session keys' uncontrollability of the protocol.

2.2 Linear Diffie-Hellman Problem

Set G1, G2 respectively for a q order group, q is a large prime number, G1 is an additive group; G2 is a multiplicative group; P is a generator of G1. Discrete logarithm problem in G1 and G2 is an intractable problem. If the map $\hat{e} : G1 \times G2 \rightarrow G2$ satisfies the following properties, this map is called an admissible bilinear map. [13]

1) Bilinearity: Given arbitrary $P,Q \in G1$ and arbitrary $a, b \in Zq^*$, then the equation $\hat{e}(aP, bQ)=\hat{e}(P,Q)ab$ can be established.

2) Non-degeneracy: If $P, Q \in G1$ exists, the inequality $\hat{e}(P,Q) \neq 1$ can be established.

3) Calculability: For any $P, Q \in G1$, there is an effective algorithm to calculate $\hat{e}(P,Q)$.

Difficult problems related to cryptography calculation:

(1) Calculating discrete logarithm problem (DLP): Given P, Q, assume that $Q=n P (n \in Zq^*)$ exists, find n.

(2) Calculating Diffie-Hellman problem (CDH): Given P, aP, bP, among which, a, b $\in Zq^*$, calculate abP.

(3) Calculating Bilinear Diffie-Hellman problem (BDH): Given P, aP, bP, cP, among which, a, b, $c \in Zq^*$, calculate $\hat{e}(P,P)abc$

2.3 Certificateless Public-Key Cryptography Principles and Processes

At the Asian Cryptography Meeting in 2003, some experts like Al-Riyami proposed the thought of certificateless public-key cryptography, which, still on the foundation of linear Diffie-Hellman problem, is a cryptosystem based on public key infrastructure (PKI) and identity characteristics[13-14]. The cryptosystem is equipped with a key generation center (KGC), whose primary role is to create a partial private key for users. Following that, the users can obtain their long-term private keys by combining one of their random secret values with the partial private key produced by KGC; and gain their public keys by combining the secret value with the system public key of KGC. That is to say, in the certificateless public-key system, the user's private keys are produced through his own calculation with the participation of KGC. Thus, the user's private keys are only known by the user himself, which solves the key escrow problem in the public key system. The process of a certificateless Public-key cryptosystem is consisted of the following four steps:

(1) System Initialization: G1, G2 are the two cyclic groups with order for q on an elliptic curve. The map $\hat{e} : G1 \times G2 \rightarrow G2$ is a bilinear map. Choose a one-way cryptographic hash function

H1 : $\{0,1\}^* \rightarrow G1$; H2 : $\{0,1\}n \times G2 \rightarrow Zq^*$ (n stands for plaintext length). A random number $s \in Zq^*$, generated by KGC and saved as a system master key, together

with P∈G1, a generator of G1, can create KGC system public key Ppub=sP. Then the system parameters params={G1,G2,ê,q,P, Ppub,H1 } can be disclosed.

(2) Extract Partial Private Key: The user A provides his identity information IDA to KGC. After KGC verifies A's identity, QA=H1(IDA) and partial private key DA=sQA can be extracted. Then, through a secret security channel, QA, DA can be transmitted to the user A, who may verify the authenticity of DA by means of the equation ê(DA,P)=ê(QA,Ppub).

(3) Choose A Secret Value: The user A chooses randomly a value xA∈G1 as his own secret value.

(4) Generate Private Key and Public Key: At the client side, after the user A inputs the partial private key created by KGC and his own secret value xA, A's long-term private key SA =xADA=xAs QA and public key PA= xAPpub= xAsP can be generated.

3 The Improvment of Kerberos Intra-domain Authentication Protocol Based-On Certificateless Public-Key Cryptography

3.1 Certificateless Intra-domain Authentication Key Agreement Protocol Adopted by This Paper

The protocol includes three consultation entities,A key generation center and both parties of intra-domain communication A and B. A and B must use the shared key obtained through consultation to start a secure session. KGC's public parameters are {G1,G2,ê,q,P,H1 } and each parameter description is the same as above. KGC generates randomly a system master key s∈Zq* and calculating system public key Pkgc=sP.

According to the theory of Certificateless Public-key Cryptography in section 1.3, clients A and B must submit respectively their identity information IDA and IDB to KGC, which will return the results to them after it calculates both parties' partial private keys DA=sQA=sH1(IDA) and DB=sQB=sH1(IDB). Then the combination of the secret value xA,xB∈Zq*, chosen randomly and separately by A and B, with the partial private keys DA and DB, returned by KGC, will generate their own long-term private keys: SA=xADA and SB=xBDB, public keys: PA=xAP and PB=xBP, and temporary session keys:

S'A=DA+xAQA=(s+xA)QA
S'B=DB+xBQB=(s+xB)QB

The processes to obtain the shared session keys through consultation are as follows:

(1) After A and B choose randomly and separately the secret number r1,r2∈Zq*, calculate TA=r1QA and TB=r2QB.

(2) A must transmit <IDA,TA,PA, MACKA(IDA,TA,PA)> to B, and meanwhile B must transmit <IDB,TB,PB, MACKB(IDB,TB,PB)> to A. Moreover, they must verify the integrity of their messages, among which MACkx is the user X's message authentication code used to guarantee the data's integrity.

A→B:IDA, TA, PA, MACKA(IDA, TA, PA)
B→A:IDB, TB, PB, MACKB(IDB, TB, PB)

If:

MACKA(IDA, TA, PA)= MACKB(IDB, TB, PB)

MACKA(IDB, TB, PB)= MACKB(IDB, TB, PB)

The equations illustrate that the message exchange process is not subject to malicious attacks, which may ensure to generate a shared session key through negotiation. If the verification results do not match, key negotiation must be carried on again.

(3) A and B calculate respectively KA and KB :

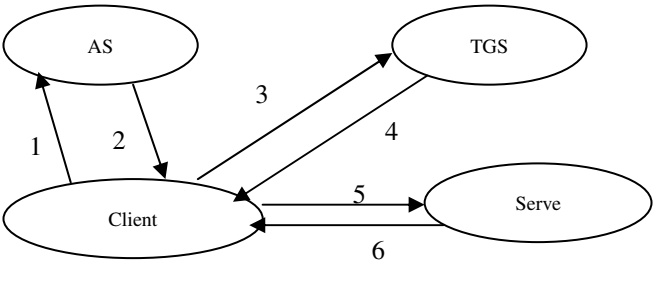
KA=ê(S'A,P)r1· ê(TB, Pkgc+PB) =ê(S'A,P)r1· ê(TB, Pkgc+PB) =ê((s+xA)QA,P)r1· ê(r2QB,(s+xB)P)=ê(QA,P)r1(s+xA) ê(QB,P)r2(s2+xB) ;

KB=ê(S'B,P)r2· ê(TA, Pkgc+PA) =ê(S'B,P)r2· ê(TA, Pkgc+PA) =ê((s+xB)QB,P)r2· ê(r1QA,(s+xA)P)=ê(QB,P)r2(s+xB) ê(QA,P)r1(s+xA)

This time, the equation K= KA= KB may be verified, and so K is the shared session key obtained through negotiation.

3.2 Improved Kerberos Intra-domain Authentication Protocol

In the new improved scheme, the function of KGC (Key Generati on Center) in certificateless public key system is integrated into that of KDC (Key Distribution Center) in Kerberos, where the registered user's public key is stored. Shown as Figure 1, if the registered client visits intra-domain application server, KDC will at first generate the system master key s∈Zq* and the system public key Pkdc=sP. Then the registered client's partial private key DC and the intra-domain application server's partial private key Ds will be generated by KDC, too. After that, C (client) and S (server) choose their own secret values c and s, and generate, through calculation, their respective public key, private key and temporary key PC/RC/ TC and Ps/Rs/Ts. The newly improved Kerberos intra-domain authentication protocol may be described with formula's symbolization as follows: E and D represent Encryption Algorithm and Decryption Algorithm respectively; KPx and KRx indicate X's public key and private key respectively; Authenticatorx,y signifies that x is the authentication ticket to access y; and r stands for a random number extracted to prevent replay attacks.



1 to request ticket license; 2 ticket license; 3 to request service ticket; 4 service ticket; 5 to request service; 6 to offer two-way authentication

Fig. 1. Kerberos Intra-domain Authentication Processes

Step 1: From AS, C obtains the ticket TGT to visit TGS.

1) C->AS: DKRc(IDc) ,IDtgs,R1

Client (C) sends a request message to get access to TGS from AS, and the message includes C's signing messages and a random number R1 used to illustrate that the access request toward AS is new.

2) AS->C: Ptgs, TGT

Once AS verifies C's identity, it will transmit to C TGS' public key and the ticket to access TGS: TGT= EKPtgs(IDc, ADc, Pc,Lifetimes1).

Step 2: From TGS, C obtains the service ticket (ST) to access application server.

3) C->TGS:TGT,Authenticatorc,tgs

Client (C) shows TGT to TGS, and submits the authentication ticket Authenticatorc,tgs = EKPtgs (IDc,IDs,R2) to TGS,

4) TGS->C:EPc(Ps, ADs), ST

TGS transmits to C the generated ticket ST= EKPs(IDc, ADc,IDs,Pc,Lifetimes2,R2) and S' public key and address encrypted with C's public key.

Step 3: C and S accomplish the two-way identity authentication.

5) C->S: ST, Authenticatorc,s

Holding the service ticket (ST) issued by TGS, C submits to S the authentication ticket Authenticatorc,s =EKPs(IDc,IDs,R3), used to get access to the application server.

6) S->C:EPc(R3)

S returns R3 to C.

The above processes mainly accomplish the two-way identity authentication between C and S. According to the certificateless key agreement protocol proposed by this paper, C and S may obtain the shared session key through a key negotiation. The processes are as follows:

7) C->S:EKRc(Tc=r1Qc)

8) S->C:EKRs(Ts=r2Qs)

C calculates the session key Kc=ê(S'c,P)c • ê(Ts, Pkdc+Ps) =ê(S'c,P)c • ê(Ts, Pkdc+Ps) =ê((s+xc)Qc,P)c • ê(sQs,(s+xs)P)=ê(Qc,P)c(s+xc) ê(Qs,P)s(s+xs)) ;

S calculates the session key Ks=ê(S's,P)s • ê(Tc, Pkdc+Pc) =ê(S's,P)s • ê(Tc, Pkdc+Pc) =ê((s+xs)Qs,P)s • ê(cQc,(s+xc)P)=ê(Qs,P)s(s+xs) ê(Qc,P)c(s+xc)

K=Kc=Ks is the final session key obtained through negotiation.

4 Security Analysis

Both literature [9] and Kerberos intra-domain authentication protocol improved on the basis of certificateless public key in this paper introduce the key agreement protocol, in which both parties of communication obtain the session key through consultation in order to avoid the third party's interception that cannot be proved. This paper adopts certificateless public-key encryption technique, thus the user's public key and private key can be generated automatically with the participation of KDC, which solves the key escrow problem in the original protocol. Meanwhile, the complicated verification of the public key system in PKI (Public Key Infrastructure) can also be omitted, which enhances the system's operating efficiency. Moreover, Kerberos' server only needs to save all users' public keys. Therefore, even if the server is breached, attackers can only obtain the users' names and their public keys. Without obtaining the users' private keys, the attackers cannot get the system service.

As for the security of the key agreement protocol, this scheme completely meets the demands proposed in Section 1.1.

a) Key Hidden Authentication (KHA). Supposed an attacker X communicates with S in the name of C, it may choose a random number x and transmit Tx =xQc, Pc to S, and therefore obtains Ts and Ps. However, X cannot gain C's temporary private Tc. Besides, to work out s from Ts = sQs is equal to solving a discrete logarithm problem (DLP). Therefore, the protocol can provide the function of key hidden authentication.

b) Known Session Key Security (KKS). While executing each key agreement protocol, both participants C and S may reselect a random number as the secret value and obtain a new session key through consultation. Therefore, if a session key is let out, it cannot influence the conversations before or after the session key.

c) Forward Security (FS). Presumed an attacker obtains C's long-term private key Sc, he cannot work out Xc through Sc= xcDc due to a discrete logarithm problem (DLP). Thus, he cannot obtain C's short-term key S'c. Moreover, the attacker does not know the temporary secret random number r1 chosen by C, so the session key K cannot be influenced. Therefore, the exposure of C's private key cannot lead to the reveal of its session key. Even if KDC's primary secret key s is exposed, and an attacker can work out their partial private keys, but because KDC does not know both Client and Server's private keys, the attacker cannot obtain Client's long-term and temporary keys. Likewise, he cannot work out the session key. For that reason, the protocol has the attribute of forward security.

d) Resist Key Compromise Impersonation Attack (KCI). Presumed an attacker X knows the application server S' private key Rs =xs·Ds, and if he wants to personate client C to communicate with S, X must accurately figure out K = Kc= Ks. Kc=ê(S'c,P)c·ê(Ts, Pkgc+Ps). Not knowing the secret value c, X cannot exactly calculate Kc. Similarly, not knowing the short-term key Ts and the secret value s, X cannot calculate Ks, either. Hence, the protocol has the ability to resist key compromise impersonation attack.

e) Unknown Key Shared Security (UKS). Supposed attacker A enforces C and S to share the session key K′, but it is impossible for them to share a session key because both C and S' identities are unauthenticated and there is no consultation between them. After the key agreement is reached, C and S need to confirm the message integrity to verify the validity of the session key. Therefore, the agreement has the unknown key shared security.

f) Keys' Uncontrollability (KU). In the agreement, the parameter values required to generate the session key , such as <IDc, Tc, Pc>, <IDs,Ts,Ps> are provided by the parties involved in the agreement. Namely, the session key is generated through C and S' joint consultations, in which one party is not controlled by the other. Furthermore, either party cannot pre-determine the session key value. Therefore, the agreement has keys' uncontrollability.

5 Summary

This paper has improved Kerberos intra-domain authentication protocol on the basis of certificateless public-key cryptography thought. The analysis shows that the improvement proposal can solve more effectively some problems existing in the original Kerberos intra-domain authentication protocol, such as the shared session key escrow problem, the third party's interception of secret message that cannot be proved,

etc. Moreover, the improvement scheme is more practical because it meets the security demand proposed by the key agreement protocol in literature [11-12]. However, the scheme also has its own defect – to increase the amount of calculation of all communication parties. With the deep and further study of the protocol, the corresponding optimization measures will be adopted to satisfy people's higher requirements for security and practicality of the identity authentication technique in the complicated network environment.

Acknowledgment. The authors would like to thank the anonymous referees for the useful suggestions for improving this paper. This project is supported by Anhui Natural Science Foundation of (KJ2011B108) and the National High Tech Research and Development Plan of China under Grant No.2009AA010307.

References

[1] Steiner, J.G., Neuman, B.C., Schiller, J.I.: Kerberos:An Authentication Service for Open Network Systems. In: USENIX Conference Proceedings, pp. 191–202 (February 1988)
[2] Bellovin, S.M., Merritt, M.: Limitations of the Kerberos Protocol. In: Winter 1991, USENIX Conference Proceedings, pp. 253–267. USENIX Association (1991)
[3] Ganesan, R.: Yaksha: augmenting Kerberos with the public key cryptography. In: Proceedings of the Internet Society Symposium on Network and Distributed System Security, pp. 132–143. IEEE Computer Society Press (1995)
[4] Liu, K.-L., Qing, S.-H., Meng, Y.: An Improved Way on Kerberos Protocol Based on Public-Key Algorithms. Journal of Software (6), 872–877 (2001)
[5] Mo, Y., Zhang, Y.-Q., Li, X.: Study of the Attacks on Kerberos Protocol and Countermeasures. Computer Engineering 31(10), 66–69 (2005)
[6] Tian, J.-F., Bi, Z.-M., Zhang, J.: An Improved Way on Kerberos Protocol Based on Public-Key Algorithms. Microelectronics & Computer 25(9), 161–164 (2008)
[7] Zhou, T., Wang, J.-Y., Li, M.-J., Li, Z.-J.: Analysis and Comparison of the Kerberos Protocol's Versions. Computer Science 36(2), 119–128 (2009)
[8] Tang, W.-D., Li, W.-M., Zhou, Y.-Q.: Improving Kerberos protocol with ElGamal algorithm. Computer Engineering and Design 27(11), 2063–2065 (2006)
[9] Hu, Y., Wang, S.-L.: Research on Kerberos identity authentication protocol based on hybrid system. Journal of Computer Applications, 1659–1661 (June 2009)
[10] Al-Riyami, S.S., Paterson, K.: Certificateless Public Key Cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
[11] Blake Wilson, S., Johnson, D., Menezes, A.: Key agreemen tp rotocols and their security analysis. In: Proc. of the 6 th IMA Inter2national Conference on Cryptography and Coding, p. 30245. Springer, Heidelberg (1997)
[12] Liu, W.-H., Xu, C.-X.: Certificateless two-party key agreement scheme without bilinear pairing. Application Research of Computers 27(11), 4287–4292 (2010)
[13] Lippold, G., Boyd, C., Gonzalez Nieto, J.: Strongly Secure Certificateless Key Agreement. In: Shacham, H., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 206–230. Springer, Heidelberg (2009)
[14] Zhang, L., Zhang, F.-T.: A Method to Construct a Class of Certificateless Signature Schemes. Chinese Journal of Computer 32(5), 940–945 (2009)