International Journal of Computer Applications Technology and Research
Volume 2– Issue 4, 396 - 399, 2013, ISSN: 2319–8656

Secure Communication Using Generalized Digital Certificate

Bismin V Sherif
Viswajyothi College of Engineering and Technology, Kerala, India

Andrews Jose
Viswajyothi College of Engineering and Technology, Kerala, India

Abstract:- A digital certificate is the combination of a statement and a signature of the statement, signed by a trusted certification authority. This work proposes using generalized digital certificate (GDC), for user authentication and key agreement for efficient secure communication. A GDC contains user's public information, such as the information of user's digital driver's license, digital birth certificate, etc., and a digital signature of public information signed by a trusted certificate authority(CA). In GDC, user does not have any public and private key pairs, therefore key management in using GDC is much simpler than public key digital certificate. The digital signature component of GDC is used as the secret token of each user that will never be exposed to any verifier. Instead, the owner proves to the verifier that he has the knowledge of the signature by correctly responding to the verifier's challenge. The session key established using proposed approach can be used for secure communication between the entities.

Keywords: Generalized Digital Certificate; User Authentication; Key Establishment; Certification Authority; Secure Communication

1. INTRODUCTION

Digital certificate is a form of an electronic credential for the Internet. Similar to driver's license, employee ID card etc, a digital certificate is issued by a trusted third party to establish the identity of the certificate holder. The trusted third party who issues the Digital Certificate is called as the Certification Authority (CA). Digital certificate is actually the combination of a statement and a digital signature of the statement. X.509 public-key digital certificate has been widely used to provide authentication on the user's public key contained in the certificate. In X.509 public key digital certificate, the statement normally contains the public key along with some general information's , which is signed by trusted certification authority. The user is authenticated if he is able to prove that he has the knowledge of the private key corresponding to the public key contained in the X.509 public-key digital certificate. However, the public key digital certificate itself cannot be used to authenticate a user since a public-key digital certificate contains only public information and can be easily recorded and played back once it has been revealed to verifier. A new form of digital certificate is introduced in the paper[1]. The approach mentioned in the above paper enables a user to be authenticated and a shared secret session key to be established with his communication partner using any general form of digital certificates. This general form of digital certificates can be anything like a digital driver's license, a digital birth certificate or a digital ID, etc, which can be called as *generalized digital certificate (GDC).* A GDC contains user's public information and a digital signature of this public information signed by a trusted Certification Authority. This digital signature will never be revealed to the verifier directly. Therefore, the digital signature of a GDC becomes a security factor which can be used for user authentication.

In GDC, the public information does not contain any user's public key. Since user does not have any private and public key pair, this type of digital certificate is easier to manage than the X.509 public-key digital certificates. The digital signature of the GDC is used as the secret token of each user. The owner of this kind of digital certificate never reveals signature of GDC to a verifier in plaintext. Instead, the owner computes a response to the verifier's challenge to prove that he has the knowledge of the digital signature of GDC. Thus, owning a GDC can provide user authentication in a digital world.

In addition, a secret session key can be established between the verifier and the certificate owner during this interaction. And the two parties can be further communicate by encrypting the messages using this secret session key. But the same key is used between the participants for encrypting the whole messages in that session. From this it is clear that a hacker who continuously monitor their communication can easily decrypt the messages, which compromises the secrecy of the information. This approach also has the disadvantage, what symmetric key encryption concepts undergoes. So an innovative approach which can overcome the above mentioned problem is presented in this paper. And with the proposed method digital certificate can be efficiently generated and the participants can be securely communicated.

2. RELATED WORKS

The two fundamental services in secure communication are user authentication and key establishment. Wide researches have been conducted on both of these areas. But most of the works have been carried on public key digital certificate. A number of signature schemes for generating signatures have also been developed over years.

The most widely using digital certificate is X509 public key digital certificate[2]. In cryptography, a public key digital or identity certificate is an electronic document that uses a digital signature to bind a public key with an identity information such as the name of a person or organization, their address, etc. This certificate can be used to verify that a public key

belongs to an individual. The problem with public key digital certificate approach is it can be easily recorded and played back once it has been completely revealed to the verifier. Since it deals with public and private key pairs, key management with public key digital certificate is difficult.

This proposed scheme is related to the Identity based cryptography[3]. In ID based system, each user must register at a private key generator(PKG). If the user is accepted, PKG will generate a private key for the user. The identity like name or email ID can be consider as user's public key. In ID-based system, it is assumed that each user already knows the identity of his communication partner. Based on this assumption, there is no need, to authenticate the identity, which can be consider as the its main advantage. Due to this assumption, ID-based cryptography is only limited to applications that communication parties know each other prior to communication. But in the GDC concept, the user does not need to know any information of his communication partner. The public information of a GDC, such as user's identity, can be transmitted through the network and verified by each communication entity. That is GDC schemes support general PKI applications, such as Internet e-commence, that communication entities do not need to know each other prior to the communication.

3. PROPOSED APPROACH

The entities involved in the digital certificate application are:

a) Certificate Authority (CA): CA is the person or organization that digitally signs a statement. The X.509 public-key digital certificate contains a statement, including the user's public key, and a digital signature of the statement. The difference between the GDC and the existing public-key digital certificate is that in a GDC, the public information does not contain any user's public key, which helps the easier management of the certificate.

b) Owner of a GDC: The owner of the GDC is the person who receives the certificate from a trusted CA over a secure channel. The owner needs to compute a valid response to the verifier's challenge in order to be authenticated and establish a secret session key.

c) Verifier: The verifier is the person who challenges the owner of a GDC and validates the answer using the owner's public information.

With this scheme, the owner of a GDC never needs to reveal the digital signature of the GDC in plaintext to the verifier under any circumstances. Instead, the owner proves that he has knowledge of the digital signature by generating the correct response to the verifier's challenge.

The proposed protocol should satisfy the following security requirements.

1) **Unforgeability**: A valid response can only be generated by the certificate owner who knows the digital signature of the Gneralized Digital Certificate.

2) **One-wayness**: No other person can derive the digital signature of the certificate based on any interaction.

3) **Nontransferrability**: A response to a verifier's challenge cannot be transferred into a response to another verifier's challenge, which would otherwise create impersonation of the user.

This work specifies the method for using this concept in discrete logarithm based protocol, with mechanism for efficient secure communication. This is built on the combination of traditional DL-based protocol and Diffie – Hellman Assumption. The proposed approach has mainly three phases :Registration phase, User Authentication phase and Key Establishment Phase.

3.1 Registration phase

Let A be the certificate owner and B be the verifier. To obtain a GDC, A needs to register at a CA. The CA uses the ElGamal Signature[4] concept to generate the signature for user A's message. The ElGamal signature scheme is a digital signature scheme which is based on the difficulty of computing discrete logarithms. . It helps the verifier to confirm the authenticity of a message m sent by the signer to him over an insecure channel.

The user sends the information from any one of digital certificates like birth certificate, digital Identity cards etc to the CA and CA generates the digital certificate using ElGamal Signature scheme. In ElGamal scheme, a large prime p and a generator g in the order of $p-1$ are supposed to be shared by all the users. The signer selects a random private key $x \in [1, p-2]$ and computes the corresponding public key

$$y = g^x \bmod p$$

The signer randomly selects a secret parameter $k \in [1, p-1]$ with $\gcd(k, p-1) = 1$ and computes

$$r = g^k \bmod p$$

Then, s is solved by knowing the signer's secrets, x and k, as

$$m = ks + rx \bmod p - 1$$

where m represents the message digest of the message m'. (r, s) is defined as the digital signature of the message m'. The signature component s is a function of the statement. Each owner needs to keep it secret from the verifier in the authentication process. The signature (r, s) can be verified by checking whether the equation

$$g^m = y^r r^s \bmod p$$

holds true.

3.2 User authentication phase

If user wants to obtain service from any service provider, provider must ensure that the user is the right one. For this, in user authentication phase the following operations are performed.

Step 1: User will not directly reveal the signature component s to the verifier.

The user A passes his user information m'_A and parameters (r, S) to the verifier B, where

$$S = r^s \bmod p$$

Step 2: After receiving m'_A and (r, S), the verifier checks whether

$$g^{mA} = y^r S \bmod p$$

where y is the public key of the CA. If this equality holds true, the verifier B randomly selects an integer $vB \in [1, p-2]$ and computes a challenge

$$c_B = r^{vB} \mod p$$

and send c_B to the user A. Otherwise, the user authentication fails and the protocol is stopped.

Step 3: The user A first uses his secret s to compute the Diffie-Hellman secret key

$$K_{A,B} = C_B{}^{s} \mod p$$
$$K'_{A,B} = D(K_{A,B})$$

where $D(K_{A,B})$ represents a key derivation procedure with $K_{A,B}$ as an input. This key derivation procedure also enforce security to the authentication process. Then user A randomly selects an integer $v_A \in [1, p-2]$ and computes

$$C_A = r^{vA} \mod p.$$

After that the response is calculated as

$$Ack = h(K'_{A,B}\ C_B \| C_A),$$

where $h(K'_{A,B}\ C_B \| C_A)$ represents a one-way hash function using the key $K'_{A,B}$. The user A sends Ack and C_A back to B and waits for the response from verifier.

Step 4: After receiving the Ack and C_A from the user A, the verifier B uses his secret v_B to compute the secret key using the Diffie-Hellman concept.

$$K_{B,A} = S^{VB} \mod p$$

And this key is given as input to the key derivation procedure and computes $K'_{B,A}$ as

$$K'_{B,A} = D(K_{B,A})$$

then computes

$$h(K'_{B,A}\ C_B \| C_A)$$

and checks whether $h(K'_{B,A}\ C_B \| C_A)$= Ack is true. If this condition holds, verifier confirms that user is authenticated. Then user and verifier enters into the key establishment phase.

3.3 Key establishment phase

In this phase, user and verifier establishes symmetric secret key for securing further communication. On the user side, the key established is:

$$K_1 = C_B{}^{vA} \mod p$$

where vA is the secret of user A and C_B is the challenge from verifier B. On the verifier side, the key established is:

$$K_2 = C_A{}^{vB} \mod p$$

where vB is the secret of Verifier B and C_A is the challenge from User A. The established secret key on both side are symmetric:

$$K_1 = C_B{}^{vA} \mod p = r_A{}^{vAvB} \mod p$$
$$K_2 = C_A{}^{vB} \mod p = r_A{}^{vBvA} \mod p = K_1$$

For the further communication between the parties this established secret key is used for encryption and decryption of the message. But if same key is used for encrypting the whole messages in the session, attacker who continuously monitor the system may got an idea about the secret key established between the partners. So for communicating the highly confidential messages, the key can be changed for each messages as follows.

For encrypting the first message, the established key itself is used. For the second message, the key is generated by XORing the first required bits of previous message with first same number of bits of the previous key. Similarly keys for all further communication can be generated.

$$K1 = r_A{}^{vAvB} \mod p$$
$$K2 = K1 \text{ XOR } m1$$
$$K3 = K2 \text{ XOR } m2$$

where k1,k2etc represents first 16 bits of corresponding key and m1,m2 represents first 16 bitsof message.This concepts guarantees high security to the communication between the partners.

3.4 Security analysis and discussions

In this section, the unforgeability, one-wayness and nontransferability of the proposed user authentication and key establishment protocol is analysed. To perform a forgery attack, the attacker needs to send a valid pair (r, S) in step 1) and the corresponding Ack in step 3) in order to impersonate the certificate owner effectively. A valid pair (r, S) alone in step 1) cannot be used to authenticate the certificate owner since this pair of parameters can be easily solved by the attacker from the following equation

$$g^{mA} = y^r S \mod p$$

But, it is computationally infeasible for the attacker to find the discrete logarithm of because of the security of ElGamal signature scheme. Therefore, it is computationally infeasible for the attacker to get a pair (r, s) to satisfy

$$g^{mA} = y^r r_A \mod p$$

Due to the Diffie-Helman Assumption, without knowing the secret exponent of S, it would be infeasible for the attacker to compute the key K_A, and forge a valid response Ack in step 3.But, the certificate owner obtains the secret exponent of S from CA during the registration phase and the certificate owner can be authenticated successfully in step 3). In summary, the security of the unforgeability of the proposed protocol is provided through the security of ElGamal signature scheme and the DHA. So, the proposed protocol is secure against forgery attacks. The computation of s from S is infeasible since it is a discrete logarithm problem.In step 3, the user uses the secret to compute the Diffie-Hellman key $K_{A,B}$. Although the verifier knows the Diffie-Hellman key K_A; but due to the DHA, the verifier will never obtain the secret s. Therefore, the proposed protocol satisfies the one-wayness property. A valid response Ack can only be generated by the certificate owner, who knows the secret signature component s.But the digital signature of GDC is never passed to the

verifier, the verifier cannot pass the complete GDC to any third party, whether which is possible with X509 public key digital certificate. So, a valid response *Ack* cannot be transferred into a response of another verifier's challenge. Therefore, the proposed protocol ensures non-transferability. Since the secret key established between the communication parties can be changed for each message, using the proposed method confidential messages can be securely communicated through the network.

4. CONCLUSION

The concept of GDC that can be used to provide user authentication and key agreement is proposed. A GDC contains user's public information, such as the information from user's digital driver's license, passport, digital birth certificate, etc., and a digital signature of the public information signed by a trusted certificate authority(CA). Since GDC does not contain any user's public key, it is easier to manage than X509 public key digital certificate. The digital signature of the GDC is used as secret token of each user that will never revealed to any verifier in any context. Instead, the owner proves to the verifier that he has the knowledge of the signature by responding with valid acknowledgement to the verifier's challenge. The secret key established during these communication can be used for securely transmitting the further messages.

5. REFERENCES

[1] L. Harn and J. Ren, "Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications", IEEE trans. on Wireless Communications, vol.10, pp. 2372-2379, 2011.

[2] Network Working Group, "Internet X.509 public key infrastructure certificate and crl profile, RFC: 2459," Jan. 1999.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology: Proc. Crypto'84, Lecture Notes in Computer Science vol. 196, (Berlin), pp. 47- 53, Springer-Verlag, 1985.

[4] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete loarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469-472, 1985.

[5] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature schemes based on discret logarithm," Electron. Lett., vol. 30, no. 24, pp. 2025-2026, 1994.

[6] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. Assoc. Comp. March., vol. 21, no. 2, pp. 120-126, 1978.