Certificateless Key Generation and Agreement Protocol for Virtual Private Networks

Harish Patil, Gowthami Yadav
(Department of Computer networks, Vishweshwaraya Technological University)

Abstract **- Virtual Private Network is a network that provides inter-connectivity to exchange information between the nodes that belongs to the network. A Virtual private network possesses all the features of the private network and is built on existing network, but they suffer severe security problems, particularly authentication problem. This paper introduces a authenticated key agreement protocol based on certificateless cryptography to authenticate users to establish a secure session between them. The proposed protocol attempts to mitigate the man-in-middle and key compromise impersonation attacks. It is found to be more efficient protocol.**

Keywords - ***Virtual private network, Authenticated key agreement, key generation, certificateless public key cryptography, identity based public key cryptography.***

1.INTRODUCTION

A virtual private network have been efficient tools that provide inter-connectivity to exchange information between different (remote) parties that belong to a specific network .The VPN possesses all the features of the private networks which provide closed community of legitimate users that use resources and services .In a VPN,the traffic is within the network without being affected by the traffic from outside the network and vice versa. The term virtual means it is build upon existing network (eg. Internet).The vpn is based on tunneling, which is the process of using internetwork infrastructure to transfer data to a network over another network [1].before tunneling the users need to authenticate before transfer of data.

VPN uses passwords in order to authenticate them but this method is vulnerable to different types of attacks[2].vpn enhances this by two factor authentication that prove the identity of the users by what user knows and something in their possession ie,token. Recently vpn's make use of X.509 digital certificates to authenticate users generally suffers two major problems managing certificates and scalability of the infrastructure.

The alternative is to use authenticated key agreement protocol is used to allow two or more parties to establish a secure session key over open networks each party can encrypt any message such that only the parties sharing secret key can decrypt the message. Authenticated key agreement should not only be secure against passive adversaries but also active adversaries who impersonate one party to communicate with another party.

The idea of key agreement protocols has been realized in public key infrastructure[3].identity based public key cryptography[4],certificate based public key cryptography[5] and certificateless public key cryptography[6].PKI protocols experience a heavy certificate management load while ID-PKC requires all the participants to trust an authority (key escrow).A malicious KGC can compute the session keys of the participating entities, thus fully trusting an authority a very strong assumption especially over open networks. Hence ID-PKC seems more suited for smaller networks or closed groups.CL-PKC combines the advantages of the ID-PKC and the traditional PKI.In CL-PKC[15], first an identity dependent partial private key is received from KGC.The entity compute its private key using partial private key and a secret known only to the entity. The entity generates a public key which matches their private keys too. As a result the trust is reduced on KGC.The PKC is more suitable for open networks.

2.BACKGROUND

A. SSL VPN

The SSL VPN is a transport layer protocol, it provides confidentiality, integrity, and digital signature [7].The SSL VPN consist of one or more devices by which the user can connect to from his/her web browser and the traffic between vpn device and the web browser is encrypted using the SSL[8].To prepare using vpn based on the PPTP,L2TP,IPSEC ,it is required to install client software which of high cost.Therefore,the using of SSL is more convenient because it does not require the installation of any software[9].

B.EXISTING SYSTEM

Authentication in VPN: Virtual private Networks use different techniques for authentication. Those techniques developed gradually from using user names and passwords to using digital certificates. In the following, we give some details about these techniques.

a. Single Factor Authentication:

The most popular authentication method is the username and password[10]. The advantage of this method is easiness to implement and its cheap cost. The disadvantage is that the user may forget the password which results in many calls to helpdesk. Consequently, a user tends to select an easy password that he/she can remember and also it will be easy to guess by an attacker. From the previous discussion the risks in using the password authentication method led to the appearance of the two factors method.

b. Two Factor Authentication:

The solution of the authentication problem in the VPNs is enhanced by using the two factors authentication method, where the identity of a user is proved by something that the user knows (password) and something that belongs to him/her (one time PIN/token)[11]. This approach is facing problems such as difficulty of managing the token, the costs of issuing token for a client and revocation of the token for some client.

c. Digital Certificate:

A more advanced authentication method that is used with the VPNs is the digital certificates. A digital certificate can be issued for a user or a client (PC) and is stored in a smart card. The digital certificate authentication is considered the most secure authentication technology for VPNs. It does not need knowledge (as password) but on possession. A smart card that contains a digital certificate needs to be protected by some additional code like PIN or fingerprint. This adds additional overhead because the user needs reader to use smart card also to replace the smart card by token it has the previous problems of the second method. Moreover, the use of digital certificate has problems of certificate management in addition to the complexity of infrastructure of PKI.

C. Brief history on key agreement protocols based on certificateless cryptography: The certificateless public key cryptography (CL-PKC) was first proposed by Al-Riyami and Paterson in 2003 [15]. The CL-PKC is an intermediate between Public Key Infrastructure (PKI) and Identity based Encryption (IBE). The CL-PKC was proposed to solve the problem of managing certificates in PKI and the key escrow problem in the identity based encryption by generate part of the private key in the key generating Center (KGC) and the rest is generated at the clients side, there is no need for using certificate.

Autenticated key agreement protocols with pairing
Al-Riyami and Paterson but it different in the calculation of the private key. In 2008 Swanson[16] made analysis of existing certificateless key agreement protocol and prove the failure of these protocols to satisfy key compromise impersonation attacks and known temporary session specific information security. In 2009 Lippold et al[17] proposed formal model for certificateless KAP based on Swanson their security model is stronger than Swanson because it assumes the party uses the replaced public key in his computation rather than the original public key as in Swanson. The Lippold et al protocol is unacceptable because it uses 10 pairing to calculate the session key. In 2010 Zhang[18] et al proposed efficient AKA protocol that requires one pairing operation. In 2011, Mokhtarnameh et al proposed new scheme for AKA and claim that the protocol is secure but Yang et al prove the protocol is vulnerable to man in the middle attack.

Authenticated Key agreement protocols without pairing:

Because the relative computation cost of a pairing is approximately twenty times higher than that of a scalar multiplication over elliptic curve group different protocols were proposed without pairing. In 2011 He et al[19] proposed key agreement protocol. In 2011 Xing et al[20] proposed a new pairing free certificate less key agreement protocol. In 2011 He and chen[21] propose a new protocol. He,Padhye and chen [22] proposed a new key agreement protocol. In 2012 Mohammed et al[23] proposed a new key agreement protocol. They carried out a modification in the binding technique of Al-Riyami and Paterson and proved the security of their scheme in the standard security model.

Two or more parties agree on a shared key,Both parties contribute with input,Diffie-Hellman model used today.Authenticated Key Agreement ensures that only the intended parties can compute the session key.Bilinear pairings of elliptic curve groups used extensively today (provides shorter keys) .

3.PRELIMINARIES

3.1 Assumptions

A. Bilinear Groups

Let $G1$ be a cyclic additive group of prime order q and $G2$ be a cyclic multiplicative group of prime order q, P is a generator of $G1$; assume that the Discrete Logarithm Problem (DLP) is hard in both $G1$ and $G2$. DLP is explained in the following subsection. An admissible pairing e is a bilinear map $e: G1 \times G1G2$, which satisfies the following three properties:

1)Bilinear: for P, Q $G1$ and, a, b , we have $e(aP,bQ) = e(P,Q)ab$;

2)Non-degenerate: $e(P, P)$ 1;

3)Computable: The map e is efficiently computable. The Weil [12] and modified Tate [13] pairings on elliptic curves can be used to construct such bilinear maps.

B.The security of the proposed protocol relies on the standard Computational Diffie-Hellman (CDH) and Bilinear Diffie- Hellman (BDH) problem assumptions

which are understood to be computed with minor probability.

1)Discrete Logarithm Problem (DLP): Given *P*, *Q* *G1*, find *n*such that *P* = *nQ* whenever such *n* exists.

2)Computational Diffie–Hellman Problem (CDHP): Given a tuple (*P*, *aP*, *bP*) *G1* for a, *b* , find the element *abP*.

3)Bilinear Diffie–Hellman Problem (BDHP): Given (*P, xP, yP, zP*) *G1* for some *x, y, z* chosen at random from , compute*e(P, P)xyz G2*.

4 PROPOSED PROTOCOL

The target is to achieve higher degree of security by creating one public key for a corresponding private key using the features of ID-PKC[14] . The relevant proposed algorithms are presented in this section.

KGC executes Setup algorithm to generate master-key and system parameters. Then, it runs Partial-Private-Key-Extract algorithm to extract the partial private key for each entity. Every entity chooses a secret value and computes its public and private key. Subsequently, two entities run key agreement algorithm online in order to share a session key.

Setup and Partial-Private-Key-Extract .

1) KGC performs the following steps during the Setup process:

a)Select a cyclic additive group *G1* of prime order *q,* a cyclic multiplicative group *G2* of the same order, a generator *P* of *G1*, and a bilinear map *e: G1* × *G1* ->*G2*.

b)Choose a random master-key, *s* ∈ Zq* and set *P0* = *sP*.

c)Choose cryptographic hash functions, *H1*: {0, 1}* ->*G1*,*H2*: *G2*-> {0, 1}*n*.

2)Entity *A* sends its identity *IDA* to KGC.

3)KGC generates the partial private key for entity *A* using the following steps:

a)Compute *QA* = *H1* (*IDA*).

b)Generate the partial private key *DA* = *sQA*.

4)The system parameters (*G1, G2, e, P, P0, H1, H2, n*) are published while the master-key *s* ∈ Zq* is kept in KGC.

5)Entity *A* executes:

a)Set-Secret-Value: choose a random value, *xA*∈ Zq* as the entity's secret value.

b)Set-Private-Key: generate the private key, *SA* = *xADA*.

c)Set-Public-Key: compute the public key, *PA* = *xAQA*.

Key-Agreement

Assume that an entity *A* with identity *IDA* has a longterm private key *SA* = *xADA* and public key *PA* = *xAQA*, and an entity*B* with identity *IDB* has private key *SB* = *xBDB* and public key *PB* = *xBQB*. *A* and *B* participate in the key agreement protocol as follows:

1)*A* chooses a short-term private key, *a* ∈ Zq* randomly and computes *TA* = *aP*. *B* chooses a short-term private key, *b*∈ Zq* randomly and computes *TB* = *bP* .

2)*A* sends (*PA*, *TA*) to *B*. *B* sends (*PB*, *TB*) to *A*.

3)*A* computes *h* = *aTB* and *KAB* = *e* (*TA* + *PA*, *bP0* + *SB*). *B*c omputes *h* = *bTA*, and *KBA* = *e* (*aP0* +*SA*, *T*B + *PB*).

4)*A* and *B* have the same shared secret *KAB* = *KBA* =e(P,P)abs e(P,QB)asxB e(QA,P)bsxA e(QA,QB)sxAxB, The session key is *K* = *H2* (*QA,QB, h, KAB*).

5. SECURITY ATTRIBUTES

1) Known-key secrecy: A and *B* choose random *a and b* respectively in each protocol run; they will have distinct session key in each run. Thus, compromising the secret keys will not affect the next session key to be generated.

2) Forward secrecy: Even if the adversary knows the long-term private keys of *A* and *B*, the adversary still needs to compute *h* from *TA* and *TB* which is a CDH problem.

Therefore, compromising the long-term private keys of all entities will not reveal previously established session keys. As a result, the proposed protocol achieves perfect forward secrecy.

3)KGC forward secrecy: CL-PKC based schemes do not have key escrow problem. If an adversary has the KGC's master private key, *s*, the previously established session keys will not be exposed. Although the adversary may generate the partial private key, both the short-term and long-term private keys of an entity are needed in order to compute the session key.

4)Key-compromise impersonation:

Assume that an adversary knows the private key of *A*, *SA*, and impersonates *B* to share the session key with *A*. The adversary will have the knowledge on *SA*, *aP*, and *b*, however, he would not be able to compute e(P.QB)asxB as *SB* is unknown. Another option is to compute *asxBP* which is a CDH problem.

5)Unknown key-share resilience: As *QA* and *QB* are used for computing the session key, each entity knows who he shares the key with.

6)No key control: Minimum two entities collaborate together to generate a session key using their random short-termprivate keys. However, key control can be imperfect when *A* sends its (*PA*, *TA*) to *B*, but *B* does not send its (*PB*, *TB*) to *A*. This particular security attribute can be supported externally using special error checking or troubleshooting methods in the protocols.

7) Known session-specific temporary information security: Even the adversary compromises the short-term private keys of a session; he will not be able to compute the session key as the long-term private keys are unknown to him.

8)Passive attack: Assume that the adversary observes the messages (*PA*, *TA*, *TB*, *PB*) transferred between the entities and he knows the master key of KGC, *s*. The adversary will not be able to compute the session key as he needs to calculate *abP*from *aP* and *bP*. This is a CDH problem.

CONCLUSION:

In this paper, secure and efficient certificateless authenticated key generation and agreement protocol are presented which produces distinct public key for a corresponding private key. In the original scheme, a dishonest KGC could restore an entity's public key by one for which it knows the secret value without fear of being recognized. However, in our proposed scheme, the existence of two public key for an identity can only result from the existence of two partial private keys binding that entity to two different public keys; only KGC could have created these two partial private keys. Thus, the new binding technique makes the KGC's substitute of a public key noticeable. The security analysis shows that the key agreement protocol achieves almost all of the known desirable security attributes such as known-key secrecy, key-compromise impersonation, unknown key-share, known session-specific temporary information security, forward secrecy and no key control. Furthermore, it conveys better efficiency in contrast to the existing protocols. In addition, the key generation and agreement protocols reduce the amount of trust on KGC. Currently, among the future work that we plan to pursue includes investigating the efficiency of the proposed protocol in distributed environments, e.g. peer-to-peer and grid computing platforms.

REFERENCES

1. P. Arora, P.Vemuganti, P. Allani,2001. Comparison of VPN Protocols IPSec, PPTP, and L2TP, George Mason University.
2. R. Oppliger, Internet and Intranet Security, 2nd Edition, 2002.
3. R. Younglove, "Public key infrastructure. how it works," *Computing & Control Engineering Journal*, vol. 12, pp. 99–102, 2001.
4. A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO 84 on Advances in cryptology*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, p. 47–53.
5. C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Proc. EUROCRYPT'03*. Berlin, Heidelberg: Springer- Verlag, 2003, p. 272–293.
6. S. S. Al-riyami, K. G. Paterson, and R. Holloway, "Certificateless public key cryptography," in *Proc. Asiacrypt'03*. Springer-Verlag,2003, p. 452–473.
7. The Government of the Hong Kong Special Administrative Region, VPN security,2008
8. S. Hua, The advantages and the implementation of SSL VPN, Heng Shui University, 2011.
9. Y. Kuihe, C. Xin, Implementation of Improved VPN Based on SSL, The Eighth International Conference on Electronic Measurement and Instruments, 2007
10. Remote Access VPN, A cryptovision whitepaper
11. Strong Authentication for Secure VPN Access, Arcot Systems,2011 Available: http://www.ca.com/~/media/Files/whitepapers/strong-authentication-for-secure-vpn-access-wp.pdf
12. A. Menezes, S. Vanstone, and T. Okamoto, "Reducing elliptic curve logarithms to logarithms in a finite field," in *Proc. STOC'91(Symposium on Theory of Computing),* New York, NY, USA: ACM, 1991, p. 80–89.
13. G. Frey, M. Muller, and H.-G. Ruck, "The tate pairing and the discrete logarithm applied to elliptic curve cryptosystems," *IEEE Transactions on Information Theory*, vol. 45, no. 5, pp. 1717 – 1719, July 1999.
14. Q. Yuan and S. Li, "A new efficient id-based authenticated key agreement protocol," Cryptology ePrint Archive: Report2005/309, 2005.
15. S. Al-Riyami ,K. Paterson, Certificateless Public Key Cryptography, 2003
16. C. Swanson, Security in key agreement: Two-party certificateless schemes, master Thesis, University of Waterloo,2008
17. G. Lippold, C. Boyd, and J. M. G. Nieto, Strongly secure certificateless key agreement, in Pairing, ser. Lecture Notes in Computer Science, vol. 5671. Springer-Verlag, 2009, pp. 206--230.
18. L. Zhang, F. Zhang, Q. Wu, and J. Domingo-Ferrer, Simulatable certificateless two-party authenticated key agreement protocol, Inf. Sci., Vol. 180, pp. 1020--1030, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.ins.2009.11.036 (Accessed 15/02/2012).
19. D. He, J. Chen, and J. Hu, A pairing-free certificateless authenticated key agreement protocol, International Journal of Communication Systems, 2011, (In press) DOI: 10.1002/dac.1265
20. H. Xiong, Q. Wu, and Z. Chen, Toward pairing-free certificateless authenticated key exchanges, in Information Security, 14th International Conference, ISC 2011, Xian, China, October 26-29, 2011. Proceedings, ser. Lecture Notes in Computer Science, X. Lai, J. Zhou, and H. Li, Eds., vol. 7001. Springer, 2011, pp. 7994.
21. D.He, Y.Chen, An efficient certificateless authenticated key agreement protocol without bilinear pairings
22. D.He, S.Padhye, J.Chen, An efficient certificateless two-party authenticated key agreement protocol
23. N. Mohamed, M.Hashim, E.Bashier and M. Hassouna, Fully-secure and efficient pairing-free certificateless authenticated key agreement protocol, 2012.