Int. J. Communications, Network and System Sciences, **2011, 4, 622-625**
doi:10.4236/ijcns.2011.410075 Published Online October 2011 (http://www.SciRP.org/journal/ijcns)

A Threshold Signature Scheme Based on TPM*

Zhi-Hua Zhang[1], Si-Rong Zhang[1], Wen-Jin Yu[1], Jian-Jun Li[1], Bei Gong[2], Wei Jiang[2,3,4]
[1]*China Tobacco Zhejiang Industrial Co. Ltd, Hangzhou, China*
[2]*College of Computer Science, Beijing University of Technology, Beijing, China*
[3]*State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China*
[4]*Key Laboratory of Information and Network Security, 3rd Research Institute, Ministry of Public Security, Shanghai, China*
E-mail: *tekkman_blade*@126.*com*
Received August 12, 2011; *revised August* 27, 2011; *accepted September* 29, 2011

Abstract

For the traditional threshold signature mechanism does not considers whether the nodes which generate part signature are trusted and the traditional signature strategy doesn't do well in resisting internal attacks and external attacks and collusion attacks, so this paper presents a new threshold signature based on Trusted Platform Module (TPM), based on TPM the signature node first should finish the trust proof between it an other members who take part in the signature. Using a no-trusted center and the threshold of the signature policy, this strategy can track active attacks of the key management center and can prevent framing the key management center, this strategy takes into account the limited computing power TPM and has parameters of simple, beneficial full using of the limited computing power TPM.

Keywords: TPM, Threshold, No Trusted Center, Bilinear Map

1. Introduction

Rapid development of the computer and network technology has made human society into the information age. The rapid popularization of the Internet and the rapid progress of internet technology have greatly promoted the development of the productive forces. Now the electronic commerce, the electronic government affairs and other services are widely used, the problem of information security has become more and more prominent, the information disclosure, the network crime and system invaded events are increasing day by day. Therefore, how to block network security hole, eliminate security concerns and protect the important or sensitive information has been paid highly attention by academics and even the whole society. For the Internet is distributed environment, it is easy to appear a phenomenon that a single node is malicious attacked, and a network node is attacked , it may cause the security of the whole network system security is destroyed. So, if the important information or important operation is stored or finished by a single node, it will increase security risk. In network environment, people may suspect that a given network server is secure and reliable, but it can still be reasonable to think that most servers are normal. Therefore, based on the assumption, trust entities can be structured, that most the network nodes of a group are secure and reliable. The important information storage or the execution of an important operation can be completed through cooperation of the members of the group.

Threshold solution provides a good solution for the above problems. The threshold cryptosystem is a relatively new research field, it main concerns that a cryptography operation once finished by one entity is scattered to a group consisted of many entities to complete, threshold signature is an important part of the study of threshold cryptography, in 1991 threshold signature is presented by Desmedt and Frankel presented [1], since then many kinds of threshold signatures have come into true [2-4]. In the threshold signature scheme, a private key is shared by n users in the group, and not as the normal signature that the private key is only held by a single user. So when it needs to sign a given message, each user needs to produce part signature, then the part signatures are combined to generate a whole signature. In 1994 the Ham puts forward two threshold group signature based on discrete logarithm scheme [5,6], one scheme has a trusted center the other has no trusted center, but the traditional threshold signature mechanism does not considers whether the nodes which generate part signature are trusted, so this paper presents a new

*Correspondence Authors: Bei Gong and Wei Jiang.

threshold signature based on Trusted Platform Module (TPM), the signature node first prove itself is trusted, and then it can generate signature, the scheme presented in this paper don't need trusted center, and according to TPM limited ability, the scheme is based on the identity of the TPM, the scheme is based on discrete logarithm and also don't need Trusted center, comparing with traditional threshold signature this scheme has a higher efficiency.

2. Preliminaries

2.1. Computational Diffie-Hellman Problem

Given group $G=<g>$ and g is the generator of $G=<g>$, g^a, g^b, $a,b\in Z_p$, if a,b is not public, g^{ab} is difficult to compute.

2.2. Bilinear Groups

Group $G_2=<g_1>$ and group $G_2=<g_2>$ is two p additive groups, p is a large prime number. The discrete logarithm in group G_2 and G_1 is difficult to solve. ϕ is computable reconstruction from G_2 to G_1. Group G_1, G_2 is a pair of bilinear group if and only if satisfying the following properties:

1) Computable bilinear: For any $\eta\in G_1$, $\gamma\in G_2$, there exists computable mapping: There exists computable mapping $\mathrm{e}: G_1\times G_2\to G_3$ (G_3 is a cyclic group whose order is q) satisfying $\mathrm{e}\left(\eta^a,\gamma^b\right)=\mathrm{e}\left(\eta,\gamma\right)^{ab}$.

2) Non-degenerative: For the generators on the group g_1, g_2, $\mathrm{e}\left(g_1,g_2\right)\neq 1$.

2.3. Shamir Threshold Scheme

Given secret s, it is divided to n parts, each part is a subkey. Each part of the information is called a subkey or is the shadow, which is owned by a sharing member. If there are k or more than k members, s can be reconstructed, less than k member, s can not be reconstructed. This scheme is (k,n) secret segmentation threshold scheme, k is the threshold value.

Given a limited domain $GF(q)$, q is a large primer, and $q\geq n+1$, s is a random number in $GF(q)/\{0\}$, and $k-1$ coefficients $a_0, a_{1,L}\cdots, a_{k-1}$ are also in ${}_RGF(q)/\{0\}$, $(i=1,2,\cdots,n)$. So a $k-1$ polynomial can be constructed in $GF(q)/\{0\}$, we can construct the polynomial, the polynomial is $f(x)=a_0+a_1x\cdots+a_{k-1}x^{k-1}$ the subkey of n members $p_{i1}, p_{i2},\cdots, p_{ik}$ is $f(i)$,every k members $p_{i1}, p_{i2},\cdots, p_{ik}$ can construct s by using the following equations:

$$\begin{cases} a_0+a_1\left(i_1\right)+\cdots+a_{k-1}\left(a_1^{k-1}\right)=f\left(i_1\right) \\ a_0+a_1\left(i_2\right)+\cdots+a_{k-1}\left(i_2^{k-1}\right)=f\left(i_2\right) \\ \cdots\cdots\cdots\cdots \\ a_0+a_1\left(i_k\right)+\cdots+a_{k-1}\left(i_k^{k-1}\right)=f\left(i_k\right) \end{cases}$$

$i_l\ (1\leq l\leq k)$ is different each other, so by using

$$f(x)=\sum_{j=1}^{k} f\left(i_j\right)\prod_{\substack{l=1\\ l\neq j}}^{k}\frac{\left(x-i_l\right)}{\left(i_j-i_l\right)}(\mathrm{mod}\, q),$$

$s=f(0)$ can be constructed.

3. Signature Scheme

3.1. Set up

Given $(G_a,+),(G_b,\cdot)$ is p order addition group and multiplication group, g^a is the generator of, $\mathrm{e}: G_a\times G_a\to G_b$ is bilinear map, $H_1:\{0,1\}^*\to G_a$, $H_1:\{0,1\}^*\times G_2\to Z_p^*$ are no collision hash function.

3.2. Units

Signature node will send own node state information and configuration information of platform to other node to prove whether it is can be trusted, if it is trusted, the signature process can be continued, if it is not trusted, the signature process will be terminated, at the same time signature node request other nodes to send their configuration information and state of their platforms, signature node needs to judge whether other nodes' configuration state information meet its own security strategy, this trust proving process is a two-way process, signature nodes need to evaluate the credibility of the other nodes, while the other nodes need to evaluate the credibility of the signature, after completing two-way evaluation the signature node can continue the signature operation, trust proving process is shown as the following (**Figure 1**).

3.3. Equations

1) For U_i in the signature node subset $U=\{U_1,U_2,\cdots,U_n\}$, first U_i selects a random number N_i, then U_i sends $m_1=\left(N_i, PCR_{needj}, SML_j\right)$ to $U_j, i\neq j$, PCR_{needj}, SML_j, SML_{needj} is the configuration value and measurement value of $U_j, i\neq j$ that U_i asks $U_j, i\neq j$ to send to U_i.

2) When $U_j, i\neq j$ receives $m_1=\left(N_i, PCR_{needi}, SML_j\right)$, it distills PCR_{needj}, SML_j and judges whether PCR_{needj}, SML_j meets the security stagy of $U_j, i\neq j$, if PCR_{needj}, SML_j does not meet the security stagy of $U_j, i\neq j$, the signature process will be terminated, else

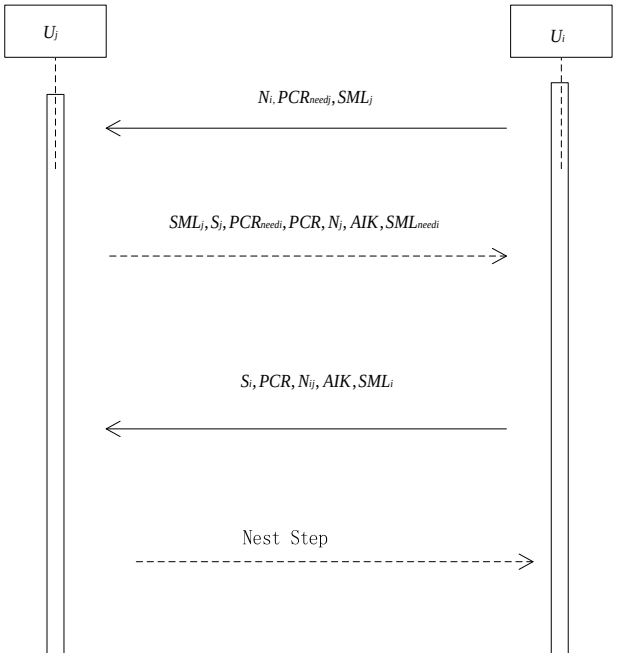

Figure 1. Two-way trust evaluation.

$U_j, i \neq j$ selects a random number N_j and reads PCR from the local TPM, then $U_j, i \neq j$ uses AIK to generate the signature $S_c = Signm_1\left(PCR, N_j\right)_{AIK}$ and reads the measurement log SML_j, at last $U_j, i \neq j$ will send $m_2 = \left(SML_j, S_j, PCR_{needi}, PCR, N_j, AIK, SML_{needi}\right)$ encrypted by conversation key K to U_i, PCR_{needi}, SML_i are the configuration information and measurement log of the platform which $U_j, i \neq j$ ask U_i to provide.

3) When U_i receives $m_2 = \left(SML_j, S_j, PCR_{needi}, PCR, N_j, AIK, SML_{needi}\right)$, it judges whether PCR_{needi}, SML_j meets the security stagy of U_i, if PCR_{needi}, SML_j does not meet the security stagy of U_i, the signature process will be terminated, else U_i selects a random number N_{ij} and reads PCR from the local TPM, then U_i uses AIK to generate the signature $S_s = Signm_1\left(PCR, N_{ij}\right)_{AIK} \lim_{x\to\infty}$ and reads the measurement log SML_i, at last U_i will send $m_3 = \left(S_i, PCR, N_{ij}, AIK, SML_i\right)$ encrypted by conversation key K to $U_j, i \neq j$.

4)When $U_j, i \neq j$ receives $m_3 = \left(S_i, PCR, N_{ij}, AIK, SML_i\right)$, it distills PCR, SML_i to judges whether PCR, SML_i meets the security stagy of $U_j, i \neq j$, if PCR, SML_i meets the security stagy of $U_j, i \neq j$, the double-way trust proof between U_i and $U_j, i \neq j$ is completed.

3.4. The Generation of Signature Key

1) U_i in $U = \left\{U_1, U_2, \cdots, U_n\right\}$ random selects $S \in Z_p^*$, it computes $PK = Sg_a$ and publish $PK = Sg_a$, U_i selects $d_1 \in Z_p^*$ and computes $PK_1 = d_1 g_a$.

2) For every $U_j, i \neq j$ in $U = \left\{U_1, U_2, \cdots, U_n\right\}$, according to threshold values t, a $t-1$ polynomial $f_{U_i}(x) = a_{Ui0} + a_{Ui1}x \cdots + a_{Ui2}x^{t-1} \bmod q$ ($a_{Uit} \neq 0$) is constructed, for each signer $U_j, i \neq j$, it computes $\delta_{i,j} = f_{U_i}\left(ID_j\right)$ and sends $\delta_{i,j}$ to other users, each $U_j, i \neq j$ in $U = \left\{U_1, U_2, \cdots, U_n\right\}$ will computes $\delta_i = \sum_{j=1}^{n} \delta_{i,j}$, then according the identity of TPM and threshold values the private key of U_i can be computed, first

$$k = \left(\sum_{i=1}^{t} \delta_i \cdot \prod_{j=1, j\neq i}^{t} \frac{-ID_j}{ID_i - ID_j} \right) \bmod p,$$

$n = k + c$, $c \in Z_p^*$ is computed, U_i takes g_a^n as its part public key PK_2, the U_i will compute $d_2 = Sg_a^n \bmod p$, at last the public key of U_i is $\left(PK_1, PK_2\right)$ and the private key of U_i is $\left(d_1, d_2\right)$.

3.5. Some Common Mistakes

When U_i needs to sign the message m, U_i first selects $r \in Z_p^*$ and computes $l = \mathrm{e}\left(PK_2, PK\right)^r$, $h = H\left(m, r\right)$, $\sigma = \left(r - h\right), d_2 - hd_1 PK_2$, $\left(h, \sigma\right)$ is the signature of m.

3.6. The Verification of Signature

When the verifier receives $\left(h, \sigma\right)$, the verifier computes whether $h = H\left(m, r\right)$ and

$$l = \mathrm{e}\left(\sigma, g_a\right)\left[\mathrm{e}\left(PK_1, PK_2\right)\mathrm{e}\left(PK_1, PK_2\right)\right]^h$$

are true, if they are true, the verifier will accepts the signature.

4. Security Analysis

4.1. Validity of the Scheme

We first prove the validity of our scheme, according to the bilinear map, the following

$$\begin{aligned}
&\mathrm{e}\left(\sigma, g_a\right)\left[\mathrm{e}\left(PK_2, PK_1\right)\mathrm{e}\left(PK_2, PK\right)\right]^h \\
&= \mathrm{e}\left(\left(r-h\right)d_2 - hd_1 PK_2, g_a\right) \cdot \\
&\mathrm{e}\left(hd_1 PK_2, g_a\right)\mathrm{e}\left(hSPK_2, g_a\right) \\
&= \mathrm{e}\left(\left(r-h\right)d_2, g_a\right)\mathrm{e}\left(hSPK_2, g_a\right) \\
&= \mathrm{e}\left(rsPK_2, g_a\right) = \mathrm{e}\left(PK_2, PK\right)^r = l
\end{aligned}$$

is true, so our scheme is right.

4.2. The Security of Private Key

The private key of our scheme has two parts d_1, d_2, d_1 is generated by U_i, for

$$k = \left(\sum_{i=1}^{t} \delta_i \cdot \prod_{j=1, j \neq i}^{t} \frac{-ID_j}{ID_i - ID_j} \right) \bmod p$$

$n = k + c$, $c \in Z_p^*$, $d_2 = Sg_a^n \bmod p$, and d_2 needs at least t members to, n, k are the secret parameters, so if a adversary know (d_1, d_2), it means the adversary has resolve the discrete logarithm problem.

Any t members can not know the private key, according to the $t-1$ polynomial, t members can know the constant item of any member, but c is a secret value, so even if t members can not know the private key, so the private key of U_i is secure.

4.3. No Forgery of Signature

Only t members can generate a signature and only U_i know member $n = k + c$, after the computing $d_2 = Sg_a^n \bmod p$ receiving v', it can generate the private key (d_1, d_2), the attestation scheme described in this paper is based on CDCH assume, and in probability polynomial time anyone can't get any information about the private key of U_i, so forging a signature of U_i is not feasible.

For the Private key $S \in Z_p^*$, $S \in Z_p^*$ is independent in the signature process , there is no product on $S \in Z_p^*$, so the scheme can resist the replacing the public key attack in literature [7,8].

5. Conclusions

In this paper a new threshold signature based on Trusted Platform Module (TPM) is presented, based on TPM the signature node first should finish the trust proof between it an other members who take part in the signature, then the signer can generate signature. The scheme is based on discrete logarithm and also don't need trusted center, comparing with traditional threshold signature this scheme has a higher efficiency.

6. Acknowledgements

Part of this paper's work is supported by Ph.D. Start-up Fund of Beijing University of Technology (No. 007000 54R1763). Part of this paper's work is supported by Opening Project of Key Lab of Information Network Security, Ministry of Public Security (No. C11610). Part of this paper's work is supported by Opening Project of State Key Laboratory of Information Security (Institute of Software, Chinese Academy of Sciences) (No. 04-04-1). Part of this paper's work is supported by National Soft Science Research Program (No. 2010GXQ 5D317).

7. References

[1] Y. Desmedt and Y. Frankel, "Shared Generation of Authenticators and Signatures," *Proceedings of Cryptology-CRYPTO*'91, Springer-Verlag, Berlin, 1991, pp. 457-469.

[2] C. M. Li, T. Hwang and N. Y. Lee, "Remark on the Threshold RSA Signature Scheme," *Stinosn D. LNCS* 773: *Advances in Cryptology-CRYPTO*'91, Springer-Verlag, Berlin, 1994, pp. 413-420.

[3] R. Gennaro, S. Jareeki, H. Krawczyk, *et al*., "Robust Threshold DSS," *BMaurer U. LNCS* 1109: *Advances in Cryptology-EUROCRYPT*'96, Springer, Berlin, 1996, pp. 157-172.

[4] C. T. Wang and C. H. Lin, "Threshold Signature Schemes with Trace Able Signers in Group Communications," *Computer Communications*, Vol. 21, No. 8, 1998, pp. 771-776. doi:10.1016/S0140-3664(98)00142-X

[5] L. Ham, "Group-Oriented (t, n) Threshold Digital Signature Scheme and Digital Multi-Signature," *IEEE Proceedings of Computers and Digital and Technique*, Vol. 141, No. 5, 1994, pp. 307-313. doi:10.1049/ip-cdt:19941293

[6] F. Hess, "Efficient Identity Based Signature Schemes Based on Parings," *Proceedings of Selected Areas in Cryptography*. *SAC*'02, Springer, Berlin, 2003, pp. 310-324.

[7] X. Chen, F. Zhang and K. Kim, "A New ID Based Group Signature Scheme from Bilinear Pairings [EB/OL]," 2003. http://eprint. Iacr.org/2003/1 16.pdf.

[8] M. C. Gorantla and A. Saxena, "An Efficient Certificate-Less Signature Scheme," *Proceedings of Computational Intelligence and Security*, Springer, Berlin, 2006, pp. 110-116.

