2014

ISSN : 0974 - 7435 Volume 10 Issue 23

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(23), 2014 [14347-14353]

Vehicle network application node security authentication based on trusted computing and direct anonymous attestation

Ren Shuai[1], Zhao Xiangmo[1], Zhang Tao[2,*], Lou Zongzong[1]
[1]School of Information Engineering, Chang'an University, Xi'an, (CHINA)
[2]School of Electronic Control Engineering, Chang'an University, Xi'an, (CHINA)
E-mail: zt904@foxmail.com

ABSTRACT

Security is a basic requirement for vehicle network or other networks. But there is little security strategy special for vehicle network. The existing network security strategy, which applies to fixed network very well, cannot satisfy the requirement of vehicle network. In this paper, trusted computing and direct anonymous attestation theories are adopted to establish protocol system of trusted vehicle information authentication, thus the security of authentication process for nodes in vehicle network can be improved. It is illustrated that the efficiency of verification can be increased and the possibility of being attacked can be decreased.

KEYWORDS

Traffic information security; Vehicle networks; Trusted computing; Direct anonymous attestation; Zero-knowledge proof.

INTRODUCTION

Vehicle networks (VN, for short) become more and more important in most of the vehicle electronic systems. It can not only solve the problems of circuit complexity and wiring harness increasing, but also provide the technical basis for the application of novel electronic and computer technologies in communication and resource sharing. As a result, vehicle network can be the support for vehicle-mounted information and control system [1].

Different from traditional communication network, there are not any fixed infrastructures in vehicle network. Vehicle network can still provide the solution for wireless communication network: communication within specific vehicles (or some mobile nodes) can be achieved by wireless connections, and communication within vehicles (or some mobile nodes) far apart from each other can be realized by information routing of the vehicle in the middle of the interval [2]. Ever-changing topological structure of the network is resulted by the keep moving nodes in vehicle network, so the security authentication can’t be guaranteed. And it is very easy to be invaded by illegal nodes, which will destroy some applications in specific region of vehicle network [3,4]. At the same time, the requirements of transmission rate and quality of communication and bandwidth increase with the development of more new and complex applications in the vehicle, for example, enhanced safety and entertainment solutions. The terminal users expect the same level of entertainment functions and data in the vehicle as know from home. Existing vehicle control networks, based on the LIN (the Local Interconnect), CAN (the Controller Area Network), and FlexRay standards, are not designed to cover these increasing demands in terms of bandwidth and scalability that we see with various kinds of ADAS (the Advanced Driver Assistant Systems) [5]. Worse yet, these existing schemes or standards can’t satisfy an ever-growing demand for security.

In this paper, trusted computing [6] will be applied in order to identify the nodes in vehicle network. At the same time, DDA (Direct Anonymous Attestation) [7,8] will be used to set up a node security authentication part, in order to improve the security of the whole vehicle network.

This paper is structured as follows: The first section will introduce the background of topics, research significance. The second section will introduce the related research ideas and methods of vehicle networks, and it will also present the existing security problems of vehicle networks. The third section will illustrate the details proposed by this paper for vehicle networks nodes security by trusted computing and direct anonymous attestation. The fourth section will give the results of security analysis and conclusions of verification procedure. The fifth section is the research conclusions for this article. And the last section will represent the acknowledgments.

VEHICLE NETWORK AND SECURITY PROBLEMS

The emergence and development of vehicle network bring us not only obvious security vulnerabilities, but also the flexibility increase of wireless access. So some inherent characteristics of vehicle network are actually the potential vulnerabilities, which are shown in the table (1).

As a self-organized network without centrality, cooperation between nodes is necessary for finding and maintaining routing of vehicle network. Limited resource and ability and insufficient effective physical protection of vehicle network are all resulted by the mobility of nodes. The main categories of threaten to routing security are shown in table (2).

Table 1. Security problems of vehicle network

Problems	Description
Vulnerability of node	With limited processing and computing ability, it is impossible or difficult for mobile nodes to operate the complicated public key encryption operations. The attackers can force the nodes to reconstruct or consume the power maliciously and even push DSA (denial of service attack).
Insufficiency of infrastructure	Without unified certification authority to infrastructure, traditional e-commerce security scheme is no longer suitable for mobile vehicle network [9].
Threaten of routing mechanism	Routing mechanism design of vehicle network is used to protect accessible routing information, integrity of routing information and reliability of information routing [10].

Considering the vulnerability and insecurity, it is necessary to solve the problem of wireless node authentication. This paper will introduce trusted computing theory. It is the important characteristic of trusted computing to achieve high security level authentication of vehicle network at a lower cost, which will be mainly used in this paper.

Table 2. Routing security threaten to VN

Routing security threaten	Description
Tampering	Routing information is tampered with by the attackers, and false routing information will be made using forged identity nodes.
Hiding	Hidden in reliable routing nodes by some special methods, the attackers can control routing protocol and launch an attack, and control network communication flow.

TRUSTED SOLUTIONS FOR VN NODES

Trusted computing is actually a hardware Trusted Platform Module, TPM for short. TPM can provide hardware basis for the connection from network nodes to trusted environment by physics. TPM security chip is the trusted root to avoid being tampered. The function of trusted root based on TPM is to achieve security authentication when accessing the network by direct anonymous attestation (DAA for short). DAA is a strategy to provide security assurance for authentication, it can also achieve remote authentication and authorized authentication without revealing its identify. The principle of DAA is shown in Figure 1.

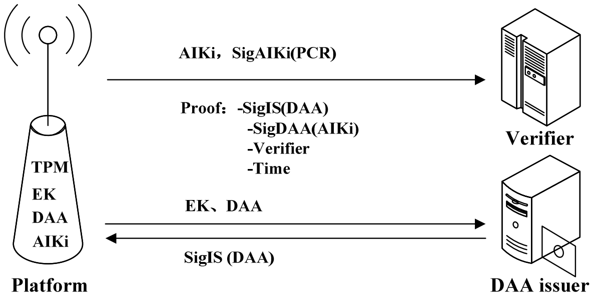


Figure 1 : Direct Anonymous Attestation Strategy

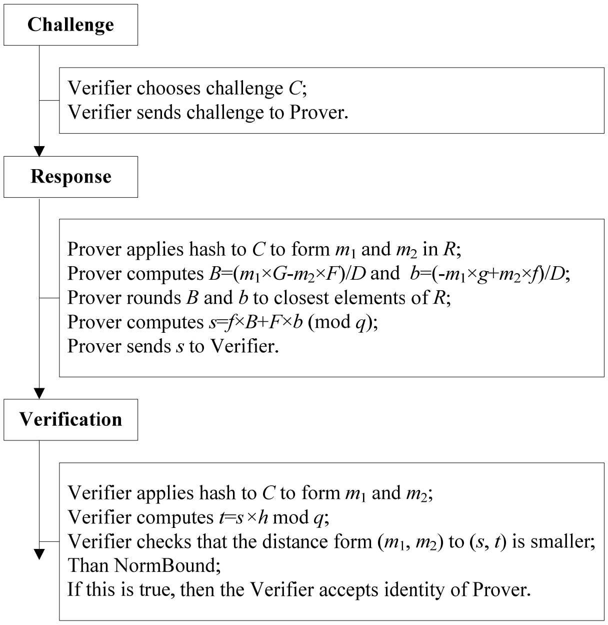
Camenisch-Lysyanskaya digital signature mechanism is adopted by DAA [11] to issue certificates for TPM member public keys. This mechanism can be divided into four steps:

(1) Issue four public keys *n*, *a*, *b* and d by DAA publisher, where n is the modulus of RSA algorithm. The signature on the information can be represented by *x*, which can meet the requirements of the following formula: $c^e = a^x b^s d \bmod n$;

(2) The public key signed by TPM is $DAA = a^x \bmod n$, where x is the secret key of TPM;

(3) s' is picked as a random number to compute $c' = cb^{s'} \bmod n$, and c' is sent to the verifier;

(4) The verifier should operate the following formula $s + es' = s''$, and $d \equiv c'^e a^{-x} b^{-s''} \bmod n$ is put in this formula. If the equation is true, it means that TPM really knows c, e, s'' .



Verifier chooses challenge *C*;
Verifier sends challenge to Prover.

Prover applies hash to *C* to form m_1 and m_2 in *R*;
Prover computes $B=(m_1\times G-m_2\times F)/D$ and $b=(-m_1\times g+m_2\times f)/D$;
Prover rounds *B* and *b* to closest elements of *R*;
Prover computes $s=f\times B+F\times b$ (mod *q*);
Prover sends *s* to Verifier.

Verifier applies hash to *C* to form m_1 and m_2;
Verifier computes $t=s\times h$ mod *q*;
Verifier checks that the distance form (m_1, m_2) to (*s*, *t*) is smaller;
Than NormBound;
If this is true, then the Verifier accepts identity of Prover.

Figure 2 : The verification of zero-knowledge proof

Zero-knowledge proof [12], which is the basis of DAA, can prove its identification without disclosure of protected information. A zero-knowledge proof system of knowledge is actually a protocol between two parties called the prover and the verifier. The prover has some information that she wants to prove to Victor, but she doesn't want to tell the secret itself to Victor [13]. The verifier asks the prover a series of questions, trying to find out if the prover really knows the secret or not. The verifier does not learn anything of the secret itself, even if he would cheat or not adhere to the protocol [14].

The mathematical basis of zero-knowledge proof is the difficulty and congruence class problem based on discrete logarithm. Two main kinds of typical methods to achieve zero-knowledge proof are Schnorr authentication scheme and Fiat-Shamir protocol, which are based on difficulty problem of discrete logarithm. These authentication schemes are all based on the traditional zero-knowledge proof schemes, which are as Fiugre 2 and Figure 3 [15]:

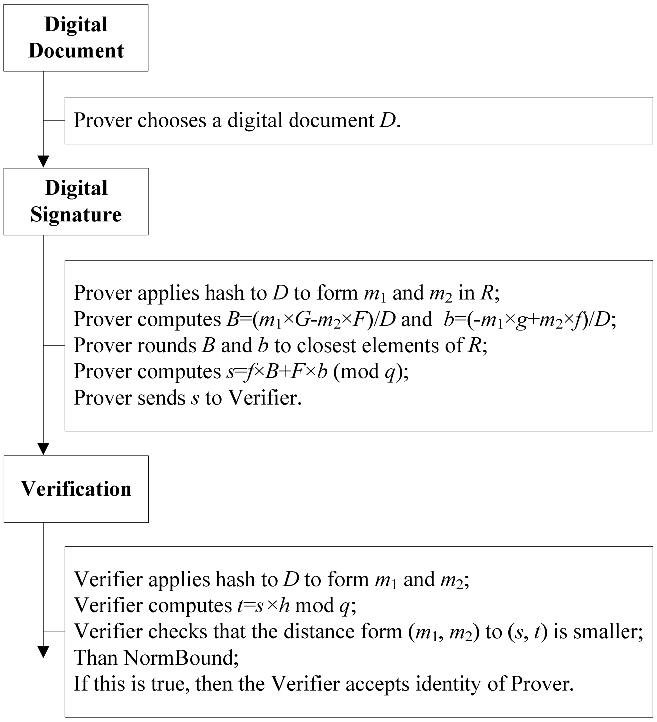

Digital Document
Prover chooses a digital document D.
Digital Signature
Prover applies hash to D to form m_1 and m_2 in R;
Prover computes B=(m_1×G-m_2×F)/D and b=(-m_1×g+m_2×f)/D;
Prover rounds B and b to closest elements of R;
Prover computes s=f×B+F×b (mod q);
Prover sends s to Verifier.
Verification
Verifier applies hash to D to form m_1 and m_2;
Verifier computes t=s×h mod q;
Verifier checks that the distance form (m_1, m_2) to (s, t) is smaller;
Than NormBound;
If this is true, then the Verifier accepts identity of Prover.

Figure 3. Digital signature of zero-knowledge proof

Zero-knowledge proof system has two parameters p and q, which are two prime numbers. And q is the prime factor of p-1, $g \neq 1$, and $g^p \equiv 1 \bmod q$. The certifier takes x_p to operate $y_p \equiv g^{x_p} \bmod p$. Certifier P has known x_p, y_p, p, q, g, and verifier *V* has known p, q, g. Then Schnorr authentication can be divided into four steps:

(1) *P* generates a random number $r_1 \in GF(p)$, where $r_1 \neq 0$ and $S \equiv g^{r_1} \bmod p$ is operated. And *P* sends (y_p, S) to *V*;

(2) *V* generates a random number r_2, and r_2 is sent to *P*;

(3)*P* operates $v = r_1 + r_2 x_p \bmod p$ and sends v to *V*;

(4) *V* verifies whether g^v is equal to $S(y_p)^{r_2}$ .If g^v is equal to $S(y_p)^{r_2}$, should accept *P*, otherwise refuse.

This protocol was proposed by Fiat and Shamir as an identification scheme which is based on the difficulty of extracting square roots mod n when the factors of n are unknown. There is, however, a trade-off between the transmitted information size and memory size. The traditional Fiat-Shamir protocol may lead to a higher probability of forgery [16]. K.Ohta and T.Okamoto extended the original Fiat-Shamir scheme to overcome the above mentioned problem. And in this paper, this improved Fiat-Shamir scheme will be used to achieve the zero-knowledge proof process.

It is supposed that there are *k* numbers about the identification of *P*, and the *k* numbers are $x_{p1}, x_{p2}, \cdots x_{pk}$. It is set that $n = pq$, and then it is necessary to operate $y_{pi} \equiv x_{pi}^2 \bmod n$. In the public document, the identity recorders of *P* can be represented by ID. And ID is a sequence such as $y_{p1}, y_{p2}, \cdots, y_{pk}$. The implementation steps are the following:

(1) A random number represented as r will be chosen by *P*, and $r \in Z_n$. After that, it is necessary to compute $r^2 \bmod n$. And (P, r^2) will be assigned to *V* as an array by *P*;

(2) $b=(b_1,b_2,\cdots b_k)$ will be assigned to *V* as a sequence by *P*, and the value of b_i can be zero or one, which is obtained randomly. So it is easily to extract that $b_i \in \{0,1\}$, $i=1,2,\cdots,k$;

(3) It will be reasonable for *P* to operate $y=rc_1c_2\cdots c_k$. And the result value of y will be sent to *V*, where $c_i=\begin{cases}1, & b_i=0\\ 0, & b_i=1\end{cases}$;

(4) Verification will be carried out by *V*. And if $y^2=r^2\prod_{i=1}^{k} y_{pi}^{bi} \bmod m$, the result will be accepted, otherwise it will be rejected by *V*.

In the existing vehicle networks, potential security risks are resulted by lack of trusted authentication interlink age. Trusted computing can provide a high level trusted proxy mechanism for mobile agents. By trusted computing, a trust management for mobile agent running environment can be given. The core component of trust management is the keys generation which is based on the low level TPM [17]. Based on trusted computing, the original authentication and network trusted verification system should be improved firstly, thus the nodes trust problem of vehicle network can be solved.

The first improvement is to connect nodes of network users to TPM, which is the basis for achieving trusted installation. Terminal of TPM, one single security module and its endorsement key (EK for short) are used to generate the only DAA EK of independent group. This is the first step for issuing trusted certification based on trusted computing in vehicle network.

The second improvement is to add DAA issuing mechanism of third-party. Network nodes (TPM) of the third-party publisher are responsible for the verification efficiency and the transmitting of DAA secret key signature to network nodes.

The last transformation is to adopt new and special authentication servers. Because DAA private key *x* may be obtained from TPM, the authentication servers are used to monitor and detect fake TPM effectively.

The process of this mechanism can be divided into the following three steps:

(1) The authenticated party is asked to operate $NV=\zeta^x \bmod \Gamma$, where *P* is a fake name.

(2) If the extracted data x is issued, the verifier will use this useless data to compute the above formula and compare with the NV from the authenticated party. If these two values are the same, the TPM is a fake one.

(3) If many same NV authentication requests are received at the same time or continuously, it should be determined whether or not the negative authentication will be given by specific applications and risk management strategy in order to satisfy some special situation such as the extracted data x has not been discovered.

In the above mechanism, the verifier is allowed to detect the fake TPM. And when using the different value changed in a certain frequency for every authenticated party, the verifiers can get some chance based on NV. Thus, the permission server should be divided into two parts, and one of them is used to authorize checking and accessing verification. According to the changes in three aspects, structure of vehicle network based on trusted computing is shown in Figure 4.

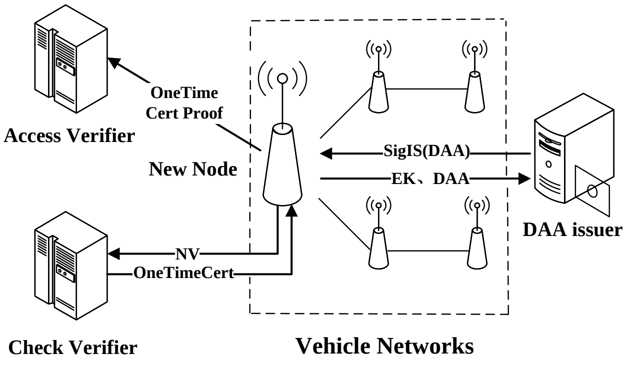


Figure 4 : Structure of VN based on trusted computing

There are three parts of this certification system. First, the user should generate a pair of DAA EKs and apply to the issuer for DAA public key certification before the application to license server. Second, DAA issuer will send the secret signature to the user after the verification. Last, the user apply to the license server again to produce a signature related to AIKi, verifier and time and to certify the possessing a signature related to DAA secret key from DAA issuer.

SECURITY ANALYSIS AND VERIFICATION CONCLUSIONS

The most fundamental function of vehicle network based on trusted computing is to protect the reverse of equipment secret key. In the above simulation environment, zero-knowledge proof of TPM can solve secret key reverse and ensure the security of system because it is based on discrete logarithm difficulty. It is illustrated that the user has used EK public key only once when applying for DAA public verification to the issuer. At the same time, the user uses the group signature to ensure the users in the same DRMA group use the same DAA public key. DAA issuer can only identify the trusted legal users and make sure they have a pair of legal DAA secret key by EK public key and zero-knowledge proof. But both the issuer and verifier can't determine the accurate identify information of users by DAA public key, hence the anonymous attestation is achieved. The procedure of Figure 4 can be extracted and the steps of it are shown as Figure 5. At last, the security steps based on authorization check and verification of accessing nodes attestation server are in the following:

(1) Interacting with TPM, Check-verifier can do frequency analysis and blacklist detection for it. Check-verifier can also sign and issue the one-time certificate and frequency certificate by binding DAA to TPM.

(2) Interacting with TPM, Access-verifier can determine whether the TPM accessing is permitted according to frequency certificate by using random numberζ.

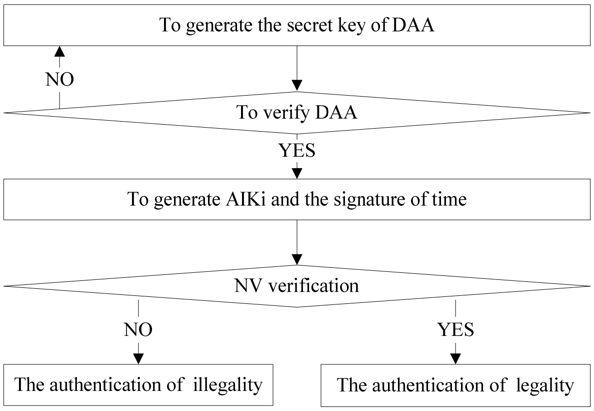

To generate the secret key of DAA
NO
To verify DAA
YES
To generate AIKi and the signature of time
NV verification
NO
YES
The authentication of illegality
The authentication of legality

Figure 5. Standard steps of simulation platform in Figure 4

According to the above analysis, trusted computing is an effective mechanism for vehicle network in order to satisfy the dependence on network nodes. The advantages of this mechanism can be concluded as follows:

(1) It is impossible to identify a node by DAA public key, which can be used to ensure the reliability of this node, so the privacy of the node and the security of the accessing can be assured.

(2) Simulation experiment has verified DRMS of trusted computing. And there is no bottleneck problem in system because DAA certificate will be issued only for once.

(3) DAA certificate can be issued to manufacture and purchased platform. This characteristic is helpful to improve the security of vehicle network based on trusted computing.

CONCLUSIONS

Vehicle network security is a new research filed with weakness, such as existent malicious nodes, which will result bigger hidden troubles on transportation based on vehicle network. And the offenders will not be investigated and held accountable most of the time. In this scheme, trusted computing theory is used to verify and monitor the network before the accessing of nodes to network. This theory can make sure the reliability of network nodes and the security of vehicle network. The future research will focus on authentication and assessment of vehicle network, TPM and other similar platforms.

ACKNOWLEDGMENTS

Our research was funded by several Projects, and the names and numbers of these Projects are as follows: 1. The National Natural Science Foundation of China (Grant No. 61402052). 2. Basic Research Project of Shaanxi Province Natural Science Foundation (Grant No. 2013JM8018). 3. The Special Fund for Basic Scientific Research of Central Colleges of Chang'an University (Grant No. 2013G1241118 and 2013G2241020).

REFERENCES

[1] Wanke Cao, Tianxia Zhang, Yongquan Jia. Integrated Technology of Vehicle Network Based on CAN. The Sixth World Congress on Intelligent Control and Automation, **2:** 8301-8305 **(2006)**.

[2] T. Ernst. The information technology era of the vehicular industry, ACM SIGCOMM Computer Communication Review, **36(2)**: 49-52 **(2006)**.

[3] Manabu Tsukada, Jose Santa, Olivier Mehani, Yacine Hhaled, and Thierry Ernst. Design and Experimental Evaluation of a Vehicular Network Based on NEMO and MANET. EURASIP Journal on Advances in Signal Processing, **2010**: 1-18 **(2010)**.

[4] Kyusuk Han, Swapna Divya Potluri, and Kang G. Shin. On Authentication in a Connected Vehicle: Secure Integration of Mobile Devices with Vehicular Networks. Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, 160-169 **(2013)**.

[5] Peter Hank, Steffen Muller, Ovidiu Vermesan, Jeroen Van den Keybus. Automotive Ethernet: In-vehicle networking and smart mobility. Design, Automation & Test in Europe Conference & Exhibition (DATE), **2013:** 1735-1739 **(2013)**.

[6] Wu Hao, Wu Guoqing. On the Concept of Trusted Computing and Software Watermarking: A Computational Complexity Treatise. Physics Procedia, **25:** 465-474 **(2012)**.

[7] Brickell, E.; Li, Jiangtao. Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities. IEEE Transactions on Dependable and Secure Computing, **9(3)**: 345-360 **(2012)**.

[8] Xi Li, Feng Dengguo, Qin Yu, Wei Feng, Shao Jianxiong, Yang Bo. Direct Anonymous Attestation in practice: Implementation and efficient revocation. Privacy, Twelfth Annual International Conference on Security and Trust (PST), 67-74 **(2014)**.

[9] Kyusuk Han, Divya Potluri S., Shin K.G. On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks. ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 160-169 **(2013)**.

[10] Xia Yamei, Cheng Bo. A Vehicle Routing Problem based on intelligent batteries transfer management for the EV network. China Communications. **11(5)**: 160-170 **(2014)**.

[11] Geric S., Vidacic T. XML digital signature and its role in information system security, Proceedings of the 35th International Convention, 1520-1525 **(2012)**.

[12] Kaaniche N., El Moustaine E., Laurent, M. A Novel Zero-Knowledge Scheme for Proof of Data Possession in Cloud Storage Applications. 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 522-531 **(2014)**.

[13] Alfredo De Santis, Giuseppe Persiano. Zero-knowledge proofs of knowledge without interaction. Proceedings of 33rd Annual Symposium on Foundations of Computer Science, **1992:** 427-436 **(1992)**.

[14] Chengming Qi. A Zero-Knowledge Proof of Digital Signature Scheme Based on the Elliptic Curve Cryptosystem. Third International Symposium on Intelligent Information Technology Application., **3**: 612-615 **(2009)**.

A. Klimm, S. Vogel, J. Becker. Hyperelliptic Curve Cryptoarchitecture for Fast Execution of Schnorr and Okamoto Authentication Protocols. IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), **2011:** 196-203 **(2011)**.

[15] K.Ohta, T.Okamoto. Practical extension of Fiat-Shamir scheme. Electronics Letters.**24(15)**: 955-956 **(1988)**.

[16] Zhidong Shen; Xiaoping Wu; Jing Zhan. Trust management for mobile agent system based on trusted computing platforms. Wireless Communications, Networking and Information Security (WCNIS), **(2010)**.