Asian Journal of Information Technology 7 (8): 370-373, 2008
ISSN: 1682-3915

Application of Trusted Computing to the Adhoc Networks Security

Ren Shuai, Zhang Tao, Mu Dejun and Zhang Degang
College of Automation, Northwestern Polytechnical University,
Xi, an Shaanxi 710072, Pepole Republic, China

Abstract: As Adhoc networks own characteristics, the existing fixed network security strategy can not be effectively implemented. Trusted Computing theory will be imported into Adhoc networks based on researching the Adhoc network. To optimize authentication link of the Adhoc networks, we make use of trusted computing platform module in hardware level and Direct Anonymous Attestation theory. The application effectively solves the Adhoc nodes security issues thus, raising the Adhoc network against attacks.

Key words: Network security, Adhoc network, trusted computing, zero-knowledge proof

INTRODUCTION

Adhoc Network provide mobile devices with a wireless communications network. In Adhoc network, there is no fixed infrastructure such as base stations and mobile switching center. The mobile node, which within the scope of communication can direct communicate with each other through a wireless connection, for those who are far from the nodes will rely on the other nodes for routing message.

Mobile nodes in Adhoc network certainly lead to the Network topology constantly changing. The node security can not be certified. It easily makes the Adhoc network invaded and attacked by illegal nodes. Therefore, this study will introduce trusted computing theory to the Adhoc network, play the advantages of trusted computing on node authentication, use of Direct Anonymous Attestation theory to increase the links of node security authentication and improve Adhoc network security.

Adhoc network and security analysis: Mobile Adhoc network brought us the ability of wireless access flexibility, while many of its inherent characteristics are also potential vulnerability (Ping *et al*., 2005), specific performance.

Node vulnerability: As network nodes are usually formed by many portable mobile devices, which lack the necessary physical protection, it can easily be lost, capture thus, falling into the attacker's control. At the same time, as the handling capacity and computing power of mobile nodes are limited, making a number of mobile nodes can not or difficult to make complex public-key cryptography computing. In addition, some attackers can force node reorganization or making complex operation to consume power, which launched a special type of denial of service attack.

Lack infrastructure: The lack of infrastructure makes the centralized authentication institutions and e-traditional security solutions no longer applicable to the mobile Adhoc network.

Threat of Adhoc routing mechanism: Adhoc network routing security designed to protect the accessibility of routing information, routing information's integrity and reliable routing for the message. As a non-central and self-organizing network, finding routing and maintain of Adhoc network need to mutual cooperation between the nodes. On the other hand, node mobility let its own resources and capacity limited and lack effective network physical protection. All these have made Adhoc network routing mechanism face a variety of security threats (Tingyao *et al*., 2005). It can generally be divided into the following categories:

Routing forging: Routing forged is that attacker tamper, forging routing information and faking a number of identity nodes to make false routing information.

Routing hiding: Routing hiding is that an attacker hide reliable routing by special way (only formed by internal legitimate routing nodes). It makes the routing protocol can be only controlled by the routing attacker, so that communication network flow to the attacker control.

Corresponding Author: Ren Shuai, College of Automation, Northwestern Polytechnical University, Xi, an Shaanxi 710072, Pepole Republic, China

From the above discussion, it indicates that making mobile Adhoc Network so vulnerable and insecure is the wireless node authentication issue, which was not fundamental resolved. It will introduce the trusted computing theory in the following study. The application of trusted computing is to achieve the purpose of high-security authentication under the low transmission costs in mobile Adhoc network.

BASED ON THE TRUSTED COMPUTING OF ADHOC NODES CREDIBLE SECURITY SOLUTIONS

Overview of trusted computing

The concept of trusted computing: In 2003, the Trusted Computing Group (TCG) was officially established and developed a hardware-level Trusted Platform Module (TPM). To connect up network nodes and TPM by physical means to provide hardware basis to the construction of trusted environment. TPM tamper-proofing secure chip provide terminal trust roots function. At present, TCG has offered two versions of the TPM solution. One is the Privacy CA in the TPM 1.1 version (TCG, 2001) and the other is Direct Anonymous Attestation (DAA) in the TPM 1.2 version (Zhidong *et al*., 2006; Liming *et al*., 2007).

Based on the feature of TPM trust roots, the use of Direct Anonymous Attestation in TPM 1.2 achieve accessing network security authentication and enables network node security and trustworthy in the Adhoc network environment.

Direct anonymous attestation: Direct anonymous attestation is a strategy (Brickell *et al*., 2004) that can be achieved authorizing identity authentication in the remote authentication, when not to expose their identity. The principle is the certified (TPM) generate the DAA group signature key and get signature (certificate) on DAA key from DAA issuer. That was later, the certified generated signature by DAA key on AKIi, Verifier and Time and show the DAA PKI to the DAA verifier. The step of TPM v1.2 is shown in Fig. 1.

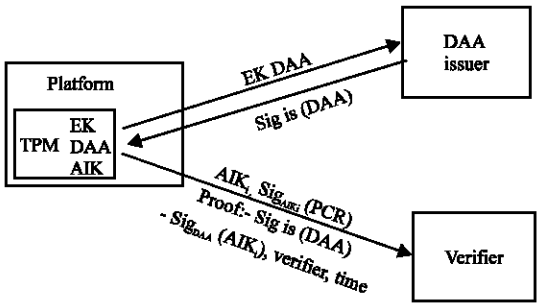

Fig. 1: The step of TPM v1.2

DAA use Camenisch and Lysyanskaya (2003) signature scheme on the TPM to generate public key of the certification. Following is Camenisch-Lysyanskaya signature scheme of 4 steps:

S_1: Public key of DAA issuer released the public key: (n, a, b, d), where n is an RSA modulus, signature on message x is triple (c, e and s), such that $c^e = a^x b^s d \bmod n$.

S_2: TPM sign the public key of TPM $DAA = a^x \bmod n$, when x is the key of TPM.

S_3: Get random number s', calculate the $c' = cb^{s'} \bmod n$ and send c' to the verifier.

S_4: Verifier calculates $s + e\,s' = s''$, bring it into $d = c'^e a^{-x} b^{-s''} \bmod n$. If the Eq. was establish, it can prove that TPM master the c, e, s''.

The basis of DAA is the zero-knowledge proof, which is developed by the Bell Labs and the University of Cambridge in the early 1990s. In zero-knowledge proof, a person (or devices) do not have to expose secrets and can also prove that they really know the secret. The mathematical basis of zero-knowledge proof is the discrete logarithm's difficulties and congruence class problem. There are several specific ways to achieve DAA such as, Schnorr and Fiat-Shamir.

This study will introduce two programmes of zero-knowledge proof.

Schnorr authentication: It is based on the difficulty of discrete logarithm. System parameters are p and q, which are 2 prime numbers, q is p-1's the prime factor, $g \neq 1$ and $g^p \equiv 1 \bmod q$. Prover chooses x_p and calculates $y_p \equiv g^x \bmod p$.

Prover learns x_p, y_p, p, q, g and verifier learns p, q, g. Following is Schnorr authentication of 4 steps:

S_1: Prover get random number $r_1 \in GF(p)$, $r_1 \neq 0$ calculate $S \equiv g^{r_1}$ and send (y_p, S) to verifier.

S_2: Verifier gets random number r_2 and send it to Prover.

S_3: Prover calculate $v = r_1 + r_2 x_p \bmod p$ and send v to verifier.

S_4: Verifier checks $g^v = S(y_p)^{r_2}$?. If Eq. is equal, Verifier accept the Prover, or reject.

$$g^v \equiv g^{(r_1 + r_2 x_p)} \bmod p \equiv g^{r_1}.(g^{x_p})^{r_2} \bmod p$$
$$\equiv g^{r_1}.(y_p)^{r_2} \bmod p \equiv S(y_p)^{r_2}$$

Fiat-shamir: In Fiat-Shamir, Prover's identity has k secret numbers, $x_{p1}, x_{p2}, \ldots x_{pk}$. Order n = pq and calculate $y_{pi} \equiv x^2_{pi} \bmod n$, public document's ID: $y_{p1}, y_{p2}, \ldots, y_{pk}$, concrete steps are as follows:

S_1: Prover gets random select number of calculations, Prover sent to Verifier.

S_2: Verifier sent $b = (b_1, b_2, \ldots b_k)$ to P, b_i is randomly number $b_i \in \{0,1\}$, i = 1, 2, ..., k.

S_3: Prover calculate $y = rc_1, c_2 \ldots, c_k$ and gave y to Verifier, which $c_i = \begin{cases} 1, & b_i = 0 \\ 0, & b_i = 1 \end{cases}$.

S_4: Verifier Check y and then if $y^2 = r^2 \prod_{i=1}^{k} y_{pi}^{bi} \bmod m$, accepted, if not is rejected.

Security solutions of Adhoc nodes based on the trusted computing: Since, there is lack of trusted authentication links in the original Adhoc network, making Adhoc network security presence hidden dangers. Based on the Trusted Computing theory, transform the original certification system in the aspect of network trusted authentication, so as to solve Adhoc network nodes trusted problem.

Alteration of Adhoc network based on the trusted computing: According to trusted computing theory, the study transforms the original the Adhoc network in 3 areas:

Connecting TPM with Internet user's nodes: Introducing TPM into user nodes will be the basis of achieving trusted Adhoc. With the TPM terminals, using a single security module and its own signature key (EK) can generate the only independent group DAA signature key. It is the trusted certification's starting point based on the whole trusted computing in Adhoc network.

Adding DAA third-party publishers in Adhoc: DAA third-party publishers are responsible for verifying the efficiency of network nodes (TPM) and sent DAA key signatures to the network nodes.

Adding authentication server in Adhoc: As there is a possibility, of the DAA private key x may have be taken from the TPM, so in order to effectively monitor and detect counterfeit TPM, the node authentication server should be included in Adhoc network.

Authentication mechanisms of the Adhoc network based on trusted computing are as follows:

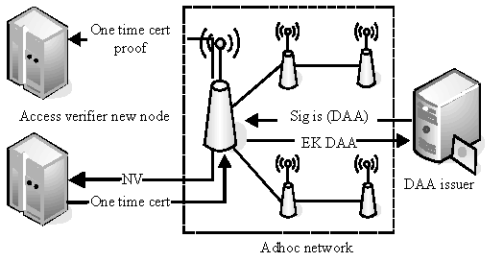

Fig. 2: The structure of Adhoc network based on the trusted computing

S_1: Request the certified to calculate $NV = \zeta^x \bmod \Gamma$, which P is called the pseudonym (have the same $NV = \zeta^x \bmod \Gamma$, certified can be distinguished between different P).

S_2: If x had been published, the verifier calculates NV with invalid x and compares the NV, which calculated by the certified. If the same, which is the counterfeit TPM.

S_3: At the same time or continuously received a lot of the same certification request of NV, determining whether the certification results are negative in accordance with specific applications and risk management strategies. To handle the x that has not yet been found.

Each the certified use certain frequency to change the different, also give the verifier opportunities of analysing based on NV (Nützel and Beyer, 2006). So, the permits server should be separated into tow servers, 1 is authorized check verifier and other is access verifier.

According to the above 3 transformations, the structure of Adhoc network based on the Trusted Computing is shown in Fig. 2.

The Adhoc network certification system based on trusted computing:

S_1: When, TPM access in the Adhoc, the node with the only TPM signature key EK produce a DAA group signature key and apply for public key.

S_2: Second, DAA issuer sent key to the node of Adhoc after the public key been verified by DAA publisher.

S_3: Finally, node apply to the adjacent nodes to proved its own generate the AIKi, verify and signature by time; to proved its own have key signature on DAA issuer.

CONCLUSION

Network nodes use DAA public key EK (identifier) to apply certification only ones.

The entire system uses a group signature, making a number of the same group user (TPM) have the same DAA public key. Thus, DAA publisher can only determine whether the applicant be a trusted nodes and a legitimate DAA key through EK public key and direct anonymous proof.

The most fundamental of Adhoc is protection key reversal of equipment. In DAA-Adhoc network, the difficulty of discrete logarithm is the basis of zero-knowledge proof. The mathematical resolve the issue of key reversal and prove the Adhoc nodes' security.

The security steps based on the authorized check verifier and access verifier in node authentication server are as follows:

S_1: Firstly, TPM interacts with the Check-verifier. Check-verifier make frequency analysis and detection blacklist, issued the one-time certificate and frequency certificate with DAA.

S_2: Second, TPM interacts with Access-verifier. Access-verifier use random to decide whether to allow TPM access services based on frequency certification.

According to above analysis, Adhoc network based on the Trusted Computing can be an effective mechanism to meet the network nodes trusted. The advantage lies:

- No 1 could use the DAA public key to determine, which the specific node is thus, guaranteeing the Adhoc nodes trusted.
- In the whole network of Adhoc, DAA certificate issued only once, so there is no bottleneck. This quality is very suitable for the characteristics Adhoc networks.
- DAA certificate can be issued to manufacturers, can also be issued to the purchase of the platform. It is easily to promote the Adhoc network security based on Trusted Computing.
- The separation of Check-verifier and Access-verifier eliminate the appearance of a fake TPM and greatly enhanced the security system.

If Adhoc technology abuse, will lead to a lot of Internet crime, which can not be held responsible to theoffenders, so this study raise Adhoc network based on trusted computing. Use theory of trusted computing to certificate and monitor the network nodes before accessing network and to ensure the trusted of network node, making Adhoc network more comprehensive and security. Future research will focus on the comprehensive assessment of Adhoc network and certification between TPM and other platforms. As the trusted computing development, the Adhoc will achieve a new level.

REFERENCES

Brickell, E., J. Camenisch and L. Chen, 2004. Direct anonymous attestation. Proc. 11th ACM Conf. Compu. Commun. Security, pp: 132-145.

Camenisch, J. and A. Lysyanskaya, 2003. A Signature Scheme with Efficient Protocols. Security in Communication Networks: Third International Conference, SCN 2002, pp: 268-270.

Liming, H., X. Sun, Y. Shutang and L. Songnian, 2007. A Method to Implement Full Anonymous Attestation for Trusted Computing Platform. Wuhan Uni. J. Nat. Sci., pp: 101-104.

Nützel, J. and A. Beyer, 2006. How to Increase the Security of Digital Rights Management Systems without Affecting Consumer's Security. Emerging Trends in Info. Commun. Security, pp: 368-380.

Ping, Y., J. Yichuan, Z. Shiyong and Z. Yiping, 2005. A Survey of Security for Mobile Adhoc Networks. Acta Electronica Sinica, pp: 893-899.

Tingyao, J., Y. Jinghua and L. Qinghua, 2005. Survey on the Security for Mobile Adhoc Networks. Appl. Res. Com., pp: 1-4.

Trusted Computing Group (TCG), 2001. Main Specification version1.1a [EB/OL]. http://www. Trustedcomputinggroup.org,/down-l0ads/Icg_ spec_1_1b.Zip.

Zhidong, S., Z. Huanguo, Z. Miao, Y. Fei and Z. Liqiang, 2006. The Mechanism about Key and Credential on Trusted Computing Platform and the Application Study. Wuhan Uni. J. Nat. Sci., pp: 1641-1644.