Computer Networks 81 (2015) 245–257

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A delegation based cross trusted domain direct anonymous attestation scheme

Li Yang [a,b,*], Jianfeng Ma [a], Wenjing Lou [c], Qi Jiang [a]

[a] School of Cyber Engineering, Xidian University, Xi'an 710071, China
[b] State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an 710071, China
[c] Department of Computer Science, Virginia Polytechnic Institute and State University, Falls Church, VA 22043, USA

ARTICLE INFO

Article history:
Received 18 June 2014
Received in revised form 29 January 2015
Accepted 23 February 2015
Available online 28 February 2015

Keywords:
Trusted computing
Remote attestation
DAA
Delegation
Cross trusted domain

ABSTRACT

Direct Anonymous Attestation (DAA) is a complex cryptographic protocol for remote attestation and provides both signer authentication and privacy. It was adopted by the Trusted Computing Group (TCG) as a technical standard. However, the DAA scheme in TCG specifications is designed for the single trusted domain attestation, and cannot be deployed in different trusted domain directly. It limits its application range in mobile networks, cloud computing, Internet of Things networks when users and authentication servers belong to different domains. Based on delegation of the trusted relationship, a new cross trusted domain direct anonymous attestation scheme is proposed in this paper. The proxy signature is used for trusted relationship delegation among different domains, and the DAA method is used for the computation platform authentication when a trusted platform accessing different trusted domains. Then the authentication protocol is designed and analyzed under Canetti–Krawczyk (CK) model for the platform remote attestation. The further analysis shows that our proposal can resist platform masquerade attacks and replay attacks, and the authentication protocol is provably secure. The security of the DAA remote attestation system is enhanced by the session key agreement. Finally, a prototype implementation and some experiments are given, the results show that the proposed scheme is effective and suitable for cross domain applications.

1. Introduction

Trusted Computing (TC) technology was developed by the Trusted Computing Group (TCG). Their technical specifications have been both accepted by the academia and industry. The core of TC is embedding a cryptography chip called Trusted Platform Module (TPM) [1] into the platform functions. Nowadays millions of TPMs have been shipped with personal computers. As a relative independent security co-processor, TPM can provide encryption function, protected storage, hardware assistance for security mechanism and function. TPM is also the base for measuring and validating the trusted attribution for the platform. According to TCG specifications, the identity of the TPM should be protected during the Remote Attestation (RA), that is when a TPM proves to a remote verifier, its real identity cannot expose to or be deduced by the verifier.

For the identity privacy protecting in remote attestation, TCG adopts two kinds of method, one is the Privacy-CA based scheme [2], the other is the Direct Anonymous Attestation (DAA) scheme [3]. The Privacy-CA method is defined by TCG in TPM Specification Version 1.1b, as an

[*] Corresponding author at: School of Cyber Engineering, Xidian University, Xi'an 710071, China. Tel.: +86 139 9282 2998.

E-mail addresses: yangli@xidian.edu.cn (L. Yang), jfma@mail.xidian.edu.cn (J. Ma), wjlou@vt.edu (W. Lou), qijiang@mail.xidian.edu.cn (Q. Jiang).

http://dx.doi.org/10.1016/j.comnet.2015.02.023
1389-1286/© 2015 Elsevier B.V. All rights reserved.

authority of the Certificate Authority, the Privacy-CA issues the identity certificate to the TPM. During the period of attestation, while the TPM shows his certificate to a verifier, the verifier will send the certificate back to the Privacy-CA then checks the certificate with the Privacy-CA together. In this case, Privacy-CA becomes the bottleneck of the system because of participation in each attestation round.

To overcome this security shortcoming, TCG adopts the Direct Anonymous Attestation (DAA) scheme in TPM Specification Version 1.2 for protecting the privacy of the platform better. We can call it as a traditional DAA scheme, as shown in Fig. 1. There are three types of participants in the traditional DAA scheme: the trusted platform including a Host and its TPM, the DAA Issuer, and the Verifier. The trusted platform, which owns a TPM, can join the DAA Issuer's group as a member. The DAA Issuer verifies the legitimation of the trusted platform, then issues a DAA certificate to it. The trusted platform can make a DAA signature on messages under the DAA certificate, here, the TPM is the real signer with the help of the Host. The Verifier can verify the membership from the signature which means holding a valid DAA certificate, but he cannot learn the identity of the TPM. Therefore, the trusted platform, the DAA Issuer and the Verifier form a single trusted domain system, which is managed by the DAA Issuer commonly.

In the real condition, different TPM manufactures set their DAA Issuers and form independent trusted domains, while the participants in different trusted domains trust their own domain managers. But under some cases such as mobile wireless networks, Internet of Things networks, cloud computing, the verifier and the platform (Host and TPM) may locate in different trusted domains. For example, users in mobile networks are usually roaming from the home network to a visiting network. Generally, the home network and the visiting network are different trusted domains while the user platform should be authenticated [4]. Therefore, they may trust certain DAA Issuers which are designated by different TPM manufactures.

However, in the traditional DAA scheme as defined in TCG specifications, the DAA certificate issuer and the verifier are in a single trusted domain. The DAA certificate of one certain TPM is trusted only in its own domain, but is not trusted in the other network domains. The verifier in one trusted domain does not trust the certificate belonged to a TPM which is published in other trusted domains. So, the traditional single-domain DAA protocols cannot function normally when the trusted platforms and the verifiers are in different domains. The problem of the TPM authentication in cross trusted domain must be considered.

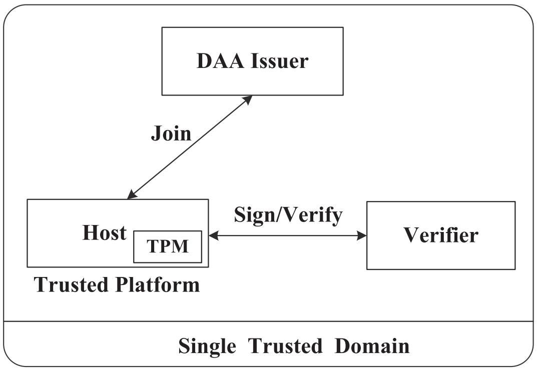

Fig. 1. Single trusted domain DAA.

Based on the delegation of the trusted relationship, we propose a new Cross Trusted Domain Direct Anonymous Attestation (CTD-DAA) scheme in this paper. Our scheme includes two stages, the first is the domain attestation, the second is the platform attestation. We integrate them into one round of remote attestation in consideration of the efficiency. For the domain attestation, we design a trusted relationship delegation model between different trusted domains. By using the proxy signature [5], the domain manager, a trusted domain server, can delegate his domain signature right to the signer, a trusted platform with TPM. Under the delegation model, we design the platform attestation by using a group signature [6] and knowledge proof based DAA method [7], then the platform identity may be verified directly by the verifier when he accesses another trusted domain. In order to ensure the security of the attestation, we design our authentication protocol for the remote attestation according to the proposed CTD-DAA system under a provable secure model-the CK model [8]. As a benefit of it, the security of the authentication protocol is enhanced by a session key agreement between the trusted platform and the verifier. Then we give the proof on the security and anonymity of our protocol under Strong RSA Assumption, decisional Diffie–Hellman assumption and computational Diffie–Hellman assumption. The further analysis shows that our proposal can resist on platform masquerade attacks and replay attacks. Finally, we implement a prototype of the proposed scheme and give some experiments on it. The results show that the proposed scheme is effective and suitable for the cross trusted domain authentication such as mobile networks.

The rest of this paper is organized as follows. We introduce related works in Section 2, and some cryptographic preliminaries in Section 3. We give the model of our cross trusted domain DAA in Section 4, and in Section 5 we describe the detailed processing of our CTD-DAA scheme, in Section 6 we give our CTD-DAA authentication protocol and the security proof and property analysis, security function and efficiency analysis are given in Section 7, and we show the implementation and experiments of CTD-DAA scheme in Section 8, the last section gives the conclusions of our work.

2. Related works

The first DAA scheme was introduced by Brickell et al. [3] in 2004, which is adopted by TCG as its technical specification as we mentioned above, called the BCC-DAA scheme for brevity. But BCC-DAA scheme cannot be used for cross trusted domain authentication directly, because the DAA Issuer, trusted platforms and verifiers are in a single trusted domain, other than the complex interactions and overmuch computation between the TPM and the verifier.