Token Based Contract Signing Protocol using OTPK

Bhagyashree Bodkhe[1,] Ms. Pallavi Jain[2,]

[1]Department of Computer Science and Engineering, Shri Vaishnav Institute of Technology and Science, Indore (M.P.), India

ABSTRACT:

In the Information Security field there are many of the techniques that make the application secure by exchanging data between two parties. A fair exchange is required for increasing the chances of attack. Hence a new contract signing protocol is proposed based on the OTPK (one time private key) scheme. This protocol will allow two parties to exchange their digital signature between them by signing contract. The proposed protocol ensures fairness such that either both parties receive each other's signatures or neither of them. The proposed protocol uses offline Trusted Third Party (TTP) that will be brought into play only if one party is cheating in other case, the TTP remains inactive. The idea is to use a better authentication between two parties in which a token is send to the TTP in response to that one private key is generated that is used for the authentication between two parties and after a certain amount of time that key has be destroyed. Thus with OTPK scheme the key is not stored at any place so the storage cost will be reduced.

Keywords: *asymmetric, digital signature, fairness, OTPK, private key, TTP, security.*

I. INTRODUCTION

In electronic transactions the involved parties do not trust each other; hence a contract signing is needed in this situation. The contract signing is simple in the paper based scenario due to the existence of simultaneity. Two hard copies of the same contract are signed by both people at the same place and at the same time. After that, each one keeps one copy as a legal document that shows both of them have committed to have the contract. Therefore the other party must provide the signed contract to a judge in court if one party does not abide. Forging a signature is a difficult matter for a false person would need to be present physically to produce it. Instead simultaneity is achieved through the notion of fairness. Contracts play an important role in many business transactions. Traditionally, paper-based contracts it is necessary that the contract is signed by both the parties at same time and at the same venue. Both the parties sign a copy of the contract for every contracting party so that every party has a copy of the signed contract. If the parties, however, are not able to meet to sign the paper-based contract, then signing an electronic contract is an alternative. The problem with signing electronic contracts, however, is exchanging the signatures of the parties, especially where there is a lack of trust between parties. One party may send the other party their signature on the contract but may not receive the signature of the other party in return. To solve the problems of exchanging digital signatures, contract signing protocols are used. Contract Signing Protocols ensure that either contracting parties receive signature or neither of them. Thus a new, efficient contract signing protocol is proposed. The proposed protocol is based on offline trusted third party (TTP) that brought into play only if one party fails to send their signature on the contract. In the normal execution of the protocol, the transaction parties will exchange their signatures directly.

1.1 One Time Private Key

In daily life there are various electronic transactions possible for the quick transfer of information from one party to other. During the exchange of information between two parties fairness between the parties is important otherwise it will give rise to various types of attacks [9]. Thus to overcome such limitation a secure technique for strong authentication is One time private key in which sender and receiver uses his/her own key for the authentication and when the encryption and decryption is performed at both the end by sender and receiver then the key will be destroyed.

Salient features of OTPK

- OTPK is only for One-time use. The certificate is short-lived.
- Each time a signature is needed; the key is generated, certified, used to sign the transaction, and then deleted.
- Key always remains in client possession throughout the short lifetime, and never stored on a permanent basis.
- Main security lies in the online certification process where the user would use strong (2-factor) authentication to the CA.

II. BACKGROUND

A Contract Signing protocol is a new way of securing the exchange of data information over the internet, since the chance of cheating over the network has been increased, hence the solution is implement a new and efficient protocols for the prevention from various attacks in the network as well as different online applications such as E-commerce can be done securely. Also during the exchange of information between two parties fairness is maintained and no party can cheat the other in an optimistic manner.

III. RELATED WORK

The contract signing protocol will allow two parties to sign the same contract and then exchange the digital signature between them. The proposed protocol ensures fairness in such a way that it offers parties greater security: either both parties receive each other’s signatures or neither of them. But the fair exchange always needs a trusted third party.

In 2011 Alfin Abraham[1] has proposed a Abuse-Free Optimistic Contract Signing Protocol which allow the two parties to sign the contract using digital signature. This protocol is based on RSA technique. In this protocol the contract is signed using multiple TTP’s thus there is no single point of failure will cause and with multiple TTP’s the chances of attack will be less.

In 2011 Alfin Abraham, Vinodh Ewards, Harlay Maria Mathew [2] has implemented optimistic fair digital exchange protocol. Here in this paper he made a survey of optimistic and fair exchange protocol. Optimistic, means the third trusted party (TTP) is involved only in the situations where one party is cheating or the communication channel is interrupted.

In Park et al.’s RSA-Based Multisignature Protocol [5] Here in this protocol he use RSA signature and multisignature model for an efficient fair exchange protocol and for zero knowledge proof.

In Verifiable Escrows Based Protocol [2] that allows two parties to exchange digital signatures so that either each party gets the other’s signature, or neither party does. Here the trusted third party is used as an “escrow service”. The basic idea is that Alice, the initiator, encrypts her signature under the public key of the trusted third party. So Bob, the responder, can have it decrypted by the trusted third party. Together with this escrow scheme a standard “cut-and-choose” interactive proof is used which make it verifiable. In the sense that the player who receives this escrow can verify that it is indeed the escrow of a signature of the desired form with a correct condition attached. This protocol makes use of three sub-protocols: an abort protocol for the initiator, a resolve protocol for the receiver, and a resolve protocol for the initiator. The protocol can also be used to encrypt data for maintaining data integrity while it is exchanged through the internet.

In 2004 F. Bao, G. Wang, J. Zhou, and H. Zhu proposed Fair Contract Signing Protocol [6]. In thisprotocol, two mutually distrusted parties exchange their commitments to a contract in such that either each of them can obtain the other’s commitment, or neither of them does. A efficient approach for fair contract signing is using an invisible trusted third party. TTP comes into play when one party is cheating. The protocol is a generic scheme since any secure digital signature scheme and most of secure encryption algorithms can be used to implement it.In 2006 Generic Fair Non-Repudiation Protocols with Transparent Off-Line TTP [8] was proposed.In this non-repudiation service irrefutable evidences need to be generated, exchanged, and validated via computer networks. After the completion of such a transaction, each involved party should obtain the expected items. If any dishonest party denies his/her participation in a specific transaction, others can refute such a claim by providing electronic evidences to a judge. This non-repudiation protocol [8] is a generic fair protocol with transparent off-line TTP. This protocol is exchanges a digital message and an irrefutable receipt between two mistrusting parties over the Internet. At the end of this protocol execution, either both parties obtain their expected items or neither party does.

IV. PROBLEM SPECIFICATION

Although there are many authentication techniques implemented for the contract signing between two clients but here the digital signature is based on RSA digital signature scheme and the trust in a single TTP is divided into multiple TTP. Thus this proposed protocol avoids single point of failure but doesn't provide an authentication between two parties and where the chances of cheating are more. The trapdoor commitment scheme explained in makes this protocol an abuse free one where the abuse freeness is a necessary property in contract signing but is not very efficient as per the authentication is concerned.

4.1 Objectives

- To determine mutual authentication between sender and the receiver.
- To determine simulation of data transmission between sender and receiver and multiple TTP's.
- To determine separate generation of one time private key.
- To determine simulation of contract signing.

V. PROPOSED SCHEME

As shown in the figure 1 is the architecture proposed for the contract signing protocol using OTPK, here in this technique the authentication or the digital signatures generated is one time and as soon as the transmission is successful the key is destroyed.

1. First of all one party needs to register on the TTP and make request for signing to TTP .Both the parties are issued an OTP token that can be sending over a secure channel.
2. The OTP token will be used for the authentication between two parties.
3. During the generation of digital signatures an OTPK module is used which consists of:

- First of all generating public-private key pair for authentication of user.
- Each user need to provide the OTP token to the CA.
- So that the CA will verifies the authentication of user if the authentication get succeed the key pair will destroyed.

4. Thus the contract is signed between two parties in a secure way using TTP.
5. When the communication is over between parties then TTP destroys the secret key generated.

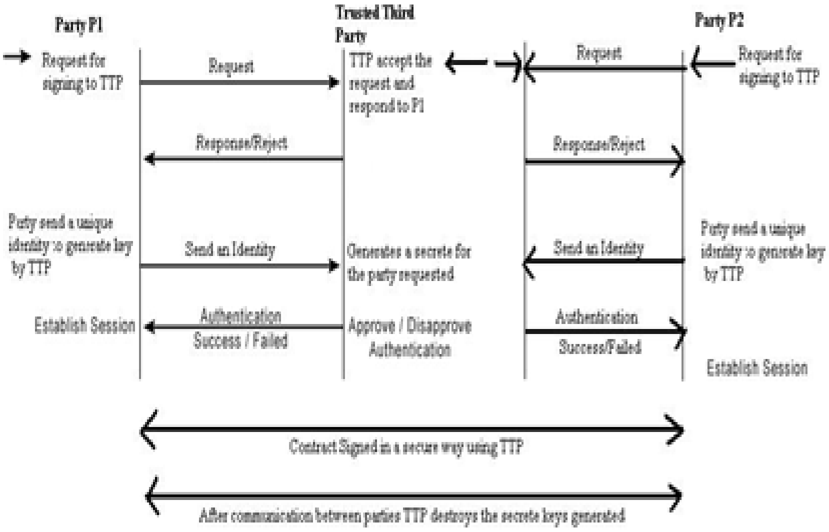
Party P1
Trusted Third Party
Party P2
Request for signing to TTP
Request
TTP accept the request and respond to P1
Request
Request for signing to TTP
Response/Reject
Response/Reject
Party send a unique identity to generate key by TTP
Send an Identity
Generates a secrete for the party requested
Send an Identity
Party send a unique identity to generate key by TTP
Establish Session
Authentication Success / Failed
Approve / Disapprove Authentication
Authentication Success/Failed
Establish Session
Contract Signed in a secure way using TTP
After communication between parties TTP destroys the secrete keys generated

Figure 1. Architecture of OTPK scheme

VI. CONCLUSION

The aim of this paper is construct a new and efficient token based contract signing protocol with Multiple TTP's using One time private key (OTPK).Thus this protocol not only solve the problem of single point of failure by using multiple TTP's but allow the Key to always remains in client possession throughout the short lifetime, and never stored on a permanent basis so help in reducing the storage cost and thus providing security against various attacks.

REFERENCES

[1] Alfin Abraham, “An Abuse-Free Optimistic Contract Signing Protocol with Multiple TTPs”, IJCA Special Issue on “Computational Science – New Dimensions & Perspectives” NCCSE, 2011.

[2] Alfin Abraham, Vinodh Ewards, Harlay Maria Mathew”, A Survey on Optimistic Fair Digital Signature Exchange Protocols”, Alfin Abraham et al. / International Journal on Computer Science and Engineering (IJCSE).

[3] N. Asokan, V. Shoup, and M. Waidner, “Optimistic fair exchange of digital signatures,” IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp.591–606, Apr.2000.

[4] Giuseppe Ateniese, “ Effcient Verifiable Encryption (and Fair Exchange) of Digital Signatures”, ACM 1999.

[5] Jung Min Park, Edwin K.P. Chong, Howard Jay Siegel,” Constructing Fair-Exchange Protocols for E-commerce Via Distributed Computation of RSA Signatures”, ACM 2003.

[6] F. Bao, G. Wang, J. Zhou, and H. Zhu, “Analysis and improvement of Micali’s fair contract signing protocol,” in Proc. ACISP’04, 2004, vol. 3108, LNCS, pp. 176–187, Springer-Verlag.

[7] S. Micali, “Simple and fast optimistic protocols for fair electronic exchange,” in Proc. PODC’03, 2003, pp. 12–19, ACMPress.

[8] G. Wang, “Generic non-repudiation protocols supporting transparent off-line TTP,” J. Comput. Security, vol. 14, no. 5, pp.441–467,Nov.2006.

[9] Vinod Moreshwar Vaze,” Digital Signature on-line, One Time Private Key [OTPK]”, International Journal of Scientific& Engineering Research Volume 3, Issue 3, March -2012 1 ISSN22295518”.

[10] O. Markowitch and S. Kremer. An optimistic non-repudiation protocol with transparent trusted third party. In: Information Security Conference (ISC’01), LNCS 2200, pp. 363-378. Springer-Verlag, 2001.

[11] Y. Dodis and L. Reyzin, “Breaking and repairing optimistic fair exchange from PODC 2003,” in Proc. ACM Workshop on DigitalRights Management (DRM’03), 2003, pp. 47–54, ACM Press.