www.ijiarec.com

ISSN:2348-2079

Volume-7 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

Secure mobile payment transaction scheme using optimistic fair exchange (OFE) protocols with TPA model

Mr.A.Gokul,[1] Ms. N.Zahira Jahan M.C.A., M.Phil.,[2]

[1]Final M.C.A, Department of MCA, Nandha Engineering College (Autonomous), Erode52.

[2]Associate Professor, Department of MCA, Nandha Engineering College (Autonomous), Erode52.

ABSTRACT

This paper proposes a novel attack detection mechanism, using the trajectory of Arbitrator for identification while still preserving their location privacy communication. A location-hidden authorized message generation scheme is designed for two objectives: first, signaler signatures on messages are signer ambiguous so that the signaler location information is concealed from the resulted authorized message; second, two authorized messages signed by the same signaler within the same given period of time (temporarily linkable) are recognizable so that they can be used for identification. Optimistic fair exchange (OFE) protocols are useful tools for two participants to fairly exchange items with the aid of a third party who is only involved if needed. A widely accepted requirement is that the third party's involvement in the exchange must be transparent message, to protect privacy and avoid bad publicity. At the same time, a dishonest third party would compromise the fairness of the exchange and the third party thus must be responsible for its behaviors. This is achieved in OFE protocols with another property called accountability. It is unfortunate that the accountability has never been formally studied in OFE since its introduction ten years ago. In this paper, these gaps are filled by giving the first complete definition of accountability in OFE where one of the exchanged items is a digital signature and a generic (also the first) design of OFE where transparency and accountability coexist

Keywords: OFE Protocol, Mobile Payment Transaction, Partial Signature, Full Signature, TPA Authentication

INTRODUCTION

OFE is proposed, using the trajectories of Arbitrator s for identification while still preserving the anonymity and location privacy of Arbitrator's. specifically, in OFE protocol, when a Arbitrator encounters an Signaler, upon request, the Signaler issues an authorized message for this Arbitrator as the proof of its presence at this Signaler and time. Intuitively, authorized messages can be utilized to identify Arbitrator s since Arbitrators located at different areas can get different authorized messages.

However, directly using authorized messages will leak location privacy of Arbitrators because knowing an authorized message of a Arbitrator signed by a particular RSU is equivalent to knowing the fact that the Arbitrator has showed up near that RSU at that time. In OFE, a location-hidden authorized message generation scheme is proposed. It serves two purposes. First, Signaler signatures on messages are signer-ambiguous which means a Signaler is anonymous when signing a message.

In this way, the Signaler location information is concealed from the final authorized message. Second, authorized messages are temporarily linkable which means two authorized messages issued from the same Signaler are recognizable if and only if they are issued within the same period of time.

Thus, authorized messages can be used for identification of Arbitrators even without knowing

Author for correspondence:
Department of MCA, Nandha Engineering College (Autonomous), Erode52

the specific Signalers who signed these messages. With the temporal limitation on the likability of two authorized messages, authorized messages used for long-term identification are prohibited. Therefore, using authorized messages for identification of Arbitrators will not harm anonymity of Arbitrators.

OFE is proposed, using the trajectories of Arbitrator s for identification while still preserving the anonymity and location privacy of Arbitrator's. specifically, in OFE protocol, when a Arbitrator encounters an Signaler, upon request, the Signaler issues an authorized message for this Arbitrator as the proof of its presence at this Signaler and time. Intuitively, authorized messages can be utilized to identify Arbitrator s since Arbitrators located at different areas can get different authorized messages.

However, directly using authorized messages will leak location privacy of Arbitrators because knowing an authorized message of a Arbitrator signed by a particular RSU is equivalent to knowing the fact that the Arbitrator has showed up near that RSU at that time. In OFE, a location-hidden authorized message generation scheme is proposed. It serves two purposes. First, Signaler signatures on messages are signer-ambiguous which means a Signaler is anonymous when signing a message.

In this way, the Signaler location information is concealed from the final authorized message. Second, authorized messages are temporarily linkable which means two authorized messages issued from the same Signaler are recognizable if and only if they are issued within the same period of time. Thus, authorized messages can be used for identification of Arbitrators even without knowing the specific Signalers who signed these messages. With the temporal limitation on the likability of two authorized messages, authorized messages used for long-term identification are prohibited. Therefore, using authorized messages for identification of Arbitrators will not harm anonymity of Arbitrators. Detecting attacks (Sybil) in urban wireless networks, however, is very challenging. First, wireless is anonymous. There are no chains of trust linking claimed identities to real arbitrator. Second, location privacy of arbitrator is of great concern. Location information of arbitrator can be very confidential.

It is inhibitive to enforce a one-to-one correspondence between claimed identities to real arbitrator by verifying the physical presence of a vehicle at a particular place and time. Third, conversations between arbitrators are very short. Due to high mobility of Arbitrator, a moving vehicle can have only several seconds to communicate with another occasionally encountered arbitrator. It is difficult to establish certain trustworthiness among communicating Arbitrator in such a short time. This makes it easy for a malicious arbitrator to generate a hostile identity but very hard for others to validate. Furthermore, short conversations among Arbitrator call for online Sybil attack detection. The detection scheme fails if a Sybil attack is detected after the attack has terminated [5-10].

Using group signatures can provide anonymity of Arbitrator and suppress Sybil attacks by restraining duplicated signatures signed by the same Arbitrator. One practical issue of these schemes is that different messages with similar semantics may be ignored from making the decision, which leads to a biased or no final decision. As a result, there is no existing successful solution, to the best of our knowledge, to tackling the online Sybil attack detection problem in urban wireless networks.

- To improve Third party arbitrator need to be online always.
- To arbitrator could be dishonest
- One of the biggest threats to OFE is the arbitrator–verifier collusion: the arbitrator converts a partial signature to a full one without performing any check.
- If the third party is the misbehaving party then, a fully transparent third party is certainly not desirable.

RELATED WORKS

As commonly known, OFE can be constructed from verifiably encrypted signature or sequential two-party multisignature. Several OFE security properties are considered to be important, including (but not limited to): abuse-free accountability (previously called as the variability of the third party in multiuser security security in

chosen-key model no repudiation setup-free and standalone signer ambiguity stateless-recipient impact of system failures on the fairness timely termination and transparent third party (also known as resolution ambiguity). In the following, it only reviews the notion of accountability, which is the focus of this paper.

Accountability

In general, accountability requires that if a desired goal of the protocol is not met then some misbehaving parties should be (rightly) blamed. The introduction of accountability in OFE (and equivalently, accountable OFE) was first given in.

The purpose of accountable OFE is to identify the party who is responsible for the full signature, and thus force the arbitrator and the signer to behave honestly when generating full signatures. This requires that actual signatures (generated by the signer) be distinguishable from resolved signatures (generated by the arbitrator).

In the paper "Optimistic Protocols for Fair Exchange" the authors N. Asokan, Matthias Schunter and Michael Waidner described a generic protocol for fair exchange of electronic goods with non-repudiation. Goods can be signatures (i.e., non-repudiation tokens of public data), confidential data, or payments. The protocol does not involve a third party in the exchange in the fault-less case but only for recovery.

Many commercial transactions can be modelled as a sequence of exchanges of electronic goods involving two or more parties. An exchange among several parties begins with an understanding about what item each party will contribute to the exchange and what it expects to receive at the end of it. A desirable requirement for exchange is fairness. A fair exchange should guarantee that at the end of the exchange, either each party has received what it expects to receive or no party has received anything.

One example for fair exchange is non-repudiation of message transmission which is, in essence, a fair exchange of the message and a non-repudiation of receipt token for the message. In several draft documents, ISO [ISO1, ISO2, ISO3] defines non-repudiation services for transmission of messages and describes protocols that provide them. In particular they define:

- non-repudiation of origin which guarantees that the originator of a message cannot later falsely repudiate having originated that message, and
- non-repudiation of receipt which guarantees that the recipient of a message cannot falsely repudiate having received that message (the ISO draft documents use the term "non-repudiation of delivery").

A straightforward solution for the fair exchange problem, used in these ISO proposals, is to use a third party to ensure fairness by, for example, receiving the items to be exchanged and the expectations of the participants in a first step and forwarding them in the next.

A drawback of this approach is that the third party is always involved in the exchange even if both parties are honest and no fault occurred. Sending messages via a third party can in practice lead to performance problems as it becomes a bottleneck.

In the paper , they described generic protocols for fair exchange which do not involve a third party in the exception-less case: the third party is only involved in the presence of faults or in the case of dishonest participants who do not follow the protocol. The generic fair exchange protocol is "generic" because different types of items, such as data, signatures, or value (in the rest of this document, we use the more common term "payment," which really means a transfer of value) can be exchanged.

In the paper "Efficient Optimistic Fair Exchange Secure in the Multi-user Setting and Chosen-key Model without Random Oracles" the authors Qiong Huang, Guomin Yang, Duncan S. Wong and Willy Susilo stated that Optimistic fair exchange is a kind of protocols to solve the problem of fair exchange between two parties. Almost all the previous work on this topic is provably secure only in the random oracle model. In PKC 2007, Dodis et al. considered optimistic fair exchange in a multi-user setting, and showed that the security of an optimistic fair exchange in a single-user setting may no longer be secure in a

multi-user setting. Besides, they also proposed one and reviewed several previous construction paradigms and showed that they are secure in the multi-user setting.

However, their proofs are either in the random oracle model, or involving a complex and very inefficient NP-reduction. Furthermore, they only considered schemes in the certified-key model in which each user has to show his knowledge of the private key corresponding to his public key.

They considered a relaxed model called chosen-key model in the context of optimistic fair exchange, in which the adversary can arbitrarily choose public keys without showing the knowledge of the private keys. They separated the security of optimistic fair exchange in the chosen-key model from the certified-key model by giving a concrete counterexample.

In the paper "Multi-party Stand-alone and Setup-free Verifiably Committed Signatures" the authors Huafei Zhu, Willy Susilo and Yi Mu demonstrated a gap between the security of verifiably committed signatures in the two-party setting and the security of verifiably committed signatures in the multi-party setting.

They extended the state-of-the-art security model of verifiably committed signatures in the two-party setting to that of multi-party setting. Since there exists trivial setup-driven solutions to multi-party verifiably committed signatures (e.g., two-signature based solutions, they propose solutions to the multi-party stand-alone verifiably committed signatures in the setup-free model. They showed that their implementation is provably secure under the joint assumption that the underlying Zhu's signature scheme is secure against adaptive chosen-message attack, Fujisaki-Okamoto's commitment scheme is statistically hiding and computationally binding and Paillier's encryption is semantically secure and one-way as well as the existence of collision-free one-way hash functions [1-5].

Optimistic fair-exchange protocols was first introduced by Asokan et al, in and formally studied in and in the context of verifiably encrypted signatures. Very recently, Dodis and Reyzin have formalized a unified model for fair-exchange protocols as a new cryptographic primitive called verifiably committed signatures in the two-party setting.

Zhu and Bao have shown that the existence of verifiably encrypted signatures implies the existence of the verifiably committed signatures while the existence of verifiably committed signatures does not imply the existence of verifiably encrypted signatures. As a result, the notion of verifiably committed signatures is a general extension of the notion of verifiably encrypted signatures.

A verifiably committed signature can be setup-driven or setup-free. A verifiably committed signature is called setup-driven if an initial key setup protocol between a primary signer and its trusted third party (TTP) must be involved such that at the end of the key setup protocol, the primary signer and its TTP share a prior auxiliary string.

This shared auxiliary information enables TTP to convert any valid partial signature into the corresponding full signature if a conflict occurs between the primary signer and its verifier. A verifiably committed signature is called setup-free if an individual participant needs not to contact his/her arbitrator(s) even for the registration purpose. Namely, no initial key setup procedure between a primary signer and his/her TTP is involved except for one requirement that the primary signer can obtain and verify TTP's certificate and vice versa.

A verifiably committed signature can be stand-alone or not. A verifiably committed signature is called stand-alone if on input a valid partial signature scheme, the distribution of outputs of a resolution algorithm is identical with the distribution of signatures generated by a full signing algorithm. A verifiably committed signature is called non-stand-alone if it is not stand-alone.

The state-of-the-art verifiably committed signatures are only considered in the two-party setting (a primary signer and a verifier, together with an off-line arbitrator). They are interested in studying stand-alone and setup-free verifiably committed signatures in the multi-party setting throughout the paper by demonstrating that the security of two-party setup-free verifiably committed signatures does not guarantee the

security of multi-party setup-free verifiably committed signatures.

METHODOLOGY

The proposed system covers the notion of optimistic fair exchange (hereinafter referred to as "OFE"). OFE also makes use of a third party (called the arbitrator), but it does not need to be always online; instead, the arbitrator only gets involved if something goes wrong (e.g., one party attempts to cheat or other faults occur).

Suppose A's item is a valid *full signature* (e.g., the signature on a credit card purchase) and B's item is denoted by $Item_B$ (e.g., a book). At the end of the exchange, A should have $Item_B$ and B should have the *full signature*.

- A starts the exchange by generating and sending it to B.
- B verifies the *partial signature* and sends $Item_B$ to An if the *partial signature* is valid.
- Upon receiving $Item_B$, A generates a *full signature* and sends it to B.
- If B does not receive the *full signature*, he can obtain it from the arbitrator who is able to convert the *partial signature* to the *full signature*. This property guarantees that B will obtain the *full signature* if A refuses to send it after Step 2.
- In the above scenario, A is usually called the "signer" and B is called the "verifier." The exchange between the signer and the verifier has attracted much attention from researchers on OFE, and it is also the case which OFE refers to in the remainder of this paper.

For the generic design of OFE with a transparent third party, the proposed system will include some cryptographic primitives which will be used in the implementation of Fair OFE.

- The new system formalizes the notion of accountable OFE, where both the signer and the third party are responsible for their behaviors.
- It also provides a feasible approach for the design of accountable OFE with other properties.
- The proposed system includes a generic (and also the first) design of OFE where the third party is transparent and accountable.
- The design is based on several well-studied cryptographic primitives and satisfied all security requirements.
- The new system makes the first step towards the formalization of accountable OFE with a transparent third party, and there are some issues that need further investigation.

The following modules are present in the paper.

Show network

In this module, a Typical Network (with Signaler Installed) is shown graphically. The panel control is used to draw the node details.

Tpa key creation

In this module, public key and private is generated .The key generated for security purpose is performed using RSA algorithm.

Add signaler

In this module, Road Side unit details such as signaler id, public key, private key, trusted authority id are added and saved to 'Signaler' table. The Signaler will create and pass messages to arbitrator. It will detect attack using the proposed approach.

Update road signaler failure

In this module, failure occurred in Road Side unit details are updated and saved to 'Signaler' table. The Signaler's Active status will be set to 0. The status will be announced to all other Signaler s by the Trusted Agent.

Add neighbour signaler

In this module, neighbour signaler details such as signaler id, neighbour signaler id, distance are added and saved to 'NeighborSignaler s' table. This distance information will assist the sybil attack detection.

View signaler

In this module, Signaler details are fetched from 'Signaler' table. The records are displayed using data grid view control. In this additional, Signaler and its Neighbor Signaler details are fetched from 'NeighborSignaler s' table. The records are displayed using data grid view control.

Add arbitrator

In this module, arbitrator details such as arbitrator id, public key, and private key are added and saved to 'Arbitrator' table.

Show trajectory information

In this module, trajectory path information for each arbitrator is verified. These details help to identify the path traveled by the arbitrator.

Message

The message module is used to update the message between Signalers to arbitrator. The another process is used to know the trajectory of the desired arbitrator, the details contains such as issued arbitrator identity number, received arbitrator unit, trajectory id, Signalers number and entry time of the arbitrator.

Finding suspected attack

This module is used to detect the unauthorized Arbitrator in the network. Here the attack details is executed depend upon the Arbitrator id. The details contain such as traverse path of identity number, road side unit details, entry time of the Arbitrator at all transmission.

Signature verification

In the partial signature creation, the input provided as two pair namely private key of the road side unit and public key of the Arbitrator, the message should be provided then the message should be encrypted and partial signature value executed in the application. The partial signature verification is verified depend upon the selection of road side unit and Arbitrator identity number.

The full signature creation is done by as two pair namely private key of the road side unit and public key of the Arbitrator and data traversed to road side unit to on board unit for further reference then the output are partial signature value and encrypted message. The encryption and decryption process is carried out using Triple DES algorithm.

CONCLUSION

In this paper formalized the notion of accountable OFE, where both the signer and the third party are responsible for their behaviors. This not only is the first complete definition since its seminal introduction a decade ago but also provides a feasible approach for the design of accountable OFE with other properties. As an example, we proposed a generic (and also the first) design of OFE where the third party is transparent and accountable. The design is based on several well-studied cryptographic primitives and satisfies all security requirements defined in this paper.

A concrete instance was also provided to demonstrate that the generic construction is very efficient to instantiate. In this paper only makes the first step towards the formalization of accountable OFE with a transparent third party, and there are some issues that need further investigation. The three kinds of accountability defined in this paper only capture the basic requirements of accountable OFE, in the sense that each accountable OFE protocol must have those properties.

There would be other specific requirements of accountability within concrete scenarios, and identifying those requirements is one of the future work directions. On the other hand, our protocol is only proved secure under the random oracle assumption. While random oracles have been widely used in security proofs, a provably secure protocol without random oracles is certainly more desirable. In the future, we will study how to utilize the inferred information and extend the framework for efficient and effective network monitoring and application design.

The new system become useful if the below enhancements are made in future.

- The application can be web service oriented so that it can be further developed in any platform.
- The application if developed as web site can be used from anywhere.
- The algorithm can be further improved so that intermediate virtual node creation is eliminated.
- The new system is designed such that those enhancements can be integrated with current modules easily with less integration work.

REFERENCES

[1] N. Asokan, M. Schunter, and M. Waidner, "Optimistic protocols for fair exchange," in Proc. CCS'97, 1997, 7–17, ACM.

[2] Y. Dodis, P. J. Lee, and D. H. Yum, "Optimistic fair exchange in a multi-user setting," in Proc. PKC'07, 2007, 4450, 118–133, LNCS, Springer.

[3] Y. Dodis and L. Reyzin, "Breaking and repairing optimistic fair exchange from PODC 2003," in Proc. 2003 ACM Workshop on Digital Rights Management, 2003, 47–54, ACM.

[4] Q. Huang, G. Yang, D. S. Wong, and W. Susilo, "Efficient optimistic fair exchange secure in the multi-user setting and chosen-key model withoutrandomoracles,"in Proc. CT-RSA'08, 2008, 4964, 106–120, LNCS, Springer.

[5] O. Markowitch and S. Kremer, "An optimistic non-repudiation protocol with transparent trusted third party," in Proc. ISC'01, 2001, 2200, 363–378, LNCS, Springer.

[6] H. Zhu,W. Susilo, and Y.Mu, "Multi-party stand-alone and setup-free verifiably committed signatures," in Proc. PKC'07, 2007, 4450, 134–149, LNCS, Springer.

[7] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures (extended abstract)," in Proc. Eurocrypt'98, 1998, 1403,. 591–606, LNCS, Springer.

[8] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," IEEE J. Sel. Areas Commun., 184, 593–610, 2000.

[9] J. Camenisch and I. Damgård, "Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes," in Proc. Asiacrypt'00, 2000, 1976, 331–345, LNCS, Springer.

[10] J. M. Park, E. K. P. Chong, and H. J. Siegel, "Constructing fair-exchange protocols for e-commerce via distributed computation of RSA signatures," in Proc. PODC'03, 2003, 172–181, ACM.