Transaction Repudiation and Nonrepudiation Defence Techniques

Commented [KP1]: Overall: I enjoyed reading the draft, focused and well researched, See comments and suggestions about improvement below

Commented [MCL2R1]:

Commented [MCL3R1]:

Prepared for:	Krassie Petrova
Prepared by:	Mao Chuan Li
Student ID:	14854389
Submit Date:	2015/05/01
Paper Name:	Information Security
Paper Number:	408217

Executive Summary

The research report topic is defined as *Transaction Repudiation and Nonrepudiation Defence Techniques* with the help and approval of senior lecturer Krassie Petrova, which is to extend the concept of information security service “Nonrepudiation” mentioned in the chapter 3 *Cryptography* in the textbook *Corporate Computer Security*.

International Organization for Standardization defined 5 main categories of security services: confidentiality, integrity, authentication, access control and non-repudiation in 1989 in ISO 7498-2. All the former 4 services have been fully covered in the textbook. Nevertheless, only the nonrepudiation service was given a few words when comparing the HMAC and Digital Signature.

With the rapid development of e-commerce, e-payment, people are more likely to make purchases and do businesses on the internet instead of traditional transactions with physical contacts to take advantage of the low cost and efficiency of internet. While we benefit so much from the new transaction model, a series of security challenges have come to surface. Different from the traditional transactions, we normally do not know the other end of business partners, who could come from anywhere in the world. We may never see them in person even we know his name or his facial pictures for a long time.

An implied distrust between each party becomes a norm, and solving such an issue is the key for a success of any transactions. Among all the security services, the nonrepudiation security service is the one to help set up trust between the transacting parties and help resolve any disputes when there is a breach of the contracts.

A strong and reliable nonrepudiation service gives the distrusting parties a guarantee that the transactions are protected for either the service provider or consumer, and enables the e-commerce, even e-government systems to develop dramatically and improve our daily lives.

So here comes the report to investigate the non-repudiation services in temporal transacting systems in depth.

Contents

1 Introduction

Repudiation is not another new term introduced in computer sciences; on the contrary, it has been an issue in human society since we started businesses thousands years ago, and is often seen in legal settings where one party of a contract refuses to complete the contract or repudiate a signature on a document. With the advent of computer network, and the stimulus of Internet prosperity, people are more likely to do businesses online, while we take advantages of it, the traditional repudiation issue did not fly away, and in contrast, it has become more complex than ever.

The report is not going to discuss any aspect of repudiation in the laws, but will only focus on the threats of repudiation in computer sciences, and all kinds of techniques which can tackle the problem and provide strong and effective evidences for the transacting parties to present to any arbitrator or judge in real life world.

Commented [KP4]: Repudiation or non-repudiation

The report is organized 4 sections:

1. Non-repudiation Services
2. The Evidence of Non-repudiation Services
3. The Requirements of Non-repudiation Services
4. Non-repudiation Protocols
5. Applications of Non-repudiation Services

2 Research Process and Scope

The research was started with a search for “repudiation” in google, from where I yielded a lot of general introduction of concept of repudiation, both for law and computer security. To study further and quickly get a big picture of the concept, I searched for a bunch of power point files.

Commented [KP5]: Why? What bunch is this one?

And bteter use academic language in the report ☺

After going through the PPT files, I decided to find a book specifically for nonrepudiation security service and did a thorough browsing in AUT online library. Luckily I found a book called *Secure Multi-Party Non-Repudiation Protocols and Applications*, which is the only book available in the AUT library written solely for introducing the non-repudiation service. By reading through the chapter 2 of the

Commented [KP6]: Give credit to the author!

book, I grasped a basic idea about what Non-repudiation service is, what elements it contains, what requirements it needs, and what protocols are available, etc.

With the basic concepts in mind, I went back to AUT library to make a purposeful search specifically for non-repudiation evidences, protocols, and applications. In total I hunted down 35 articles related to non-repudiation service as listed in the following table. Due to the time limitation requirement of the report, finally I selected 13 of them as my main study objects apart from the book.

No.	Year	Title	Chosen
1	1996	A fair non-repudiation protocol	Y
2	1997	An efficient non-repudiation protocol	Y
3	1997	Evidence and non-repudiation	
4	1999	Authentication protocols with nonrepudiation services in personal communication systems	
5	1999	Improving fairness and privacy of Zhou-Gollmann's fair non-repudiation protocol	Y
6	1999	Securing digital signatures for non-repudiation	
7	2002	An intensive survey of fair non-repudiation protocols	Y
8	2002	Efficient non-repudiation multicast source authentication schemes	
9	2003	Analysing the security of a non-repudiation communication protocol with mandatory proof of receipt	
10	2004	Non-repudiation protocols for multiple entities	
11	2004	On timeliness of a fair non-repudiation protocol	Y
12	2005	On the security of fair non-repudiation protocols	Y
13	2005	Signcryption with Non-interactive Non-repudiation	
14	2006	A new fair non-repudiation protocol for secure negotiation and contract signing	
15	2007	Automated Design of Non-Repudiation Security Protocols	
16	2007	An email system with non-repudiation service	Y
17	2009	Survey on Nonrepudiation: Digital Signature Versus Biometrics	Y
18	2009	Establishing and preventing a new replay attack on a non-repudiation protocol	Y
19	2009	A fair non-repudiation security protocol with off-line TTP	
20	2010	A remote interactive non-repudiation multimedia-based m-learning system	Y
21	2010	An Efficient Multi Recipient Signcryption Scheme Offering Non Repudiation	
22	2010	The ForwardDiffsig scheme for multicast authentication	
23	2010	Fair non-repudiation for web services transactions	Y
24	2010	Formal Analysis Of Multi-party Non-repudiation Protocols Without TTP	
25	2011	Choosing a Biometric for Nonrepudiation	
26	2012	Non-Repudiation By The Use of Biometrics—Risk Analysis	
27	2012	Group signatures for secure and privacy preserving vehicular ad hoc networks	
28	2012	A shared-secret free security infrastructure for wireless networks	
29	2013	Strong non-repudiation based on certificateless short signatures	
30	2013	Measuring the forensic-ability of audit logs for nonrepudiation	Y
31	2013	Bringing VoIP Signatures to Mobile Devices	Y
32	2013	Non Repudiation for Internet Access by Using Browser Based User Authentication Mechanism	
33	2013	An asymmetric fingerprinting code for collusion-resistant buyer-seller watermarking	
34	2013	An Optimistic Non-repudiation Protocol Focused on Transparent Trusted Third Party	
35	2014	An alternative version of HTTPS to provide non-repudiation security property	

3 Discussion

3.1 Non-repudiation Services

Repudiation is an act to deny the existence of a contract and/or refuse to complete the transaction as agreed upon by two or more parties beforehand. Any party could lead a repudiation, the non-repudiation services are just coming into play to prevent it from happening and facilitate resolving the disputes when it really happens.

In computer network communication systems, repudiation is embodied by the refusal of a message has been sent and delivered by a party, or received by another party. In the context of Non-repudiation services, the following 3 roles of the messaging parties are defined:

1. Originator - who creates the message and originates the transmission to other parties
2. Recipient – who actually received the message from an originator or delivery agent
3. Delivery agent – who stands between the Originator and Recipient to help relay the messages.

With the 3 roles defined, we can draw a message transmission model as Figure 1:

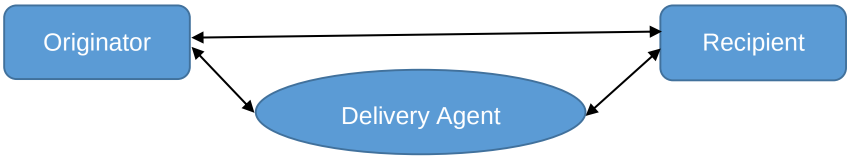

Figure 1 Message Transmission Model

To counter the repudiation threats in the communication against any party in the model, ISO/IEC 13888-1 standard defines 8 sub services:

- non-repudiation of origin – which is to protect Recipient against the Originator who created and sent the message;
- non-repudiation of delivery – which is to protect Originator against the Recipient who received the message and recognized it;
- non-repudiation of submission – which is to protect Originator against the Delivery Agent who received the message transmission request from Originator;

- non-repudiation of transport – which is to protect the Delivery Agent that it has delivered the message out to Recipient;
- non-repudiation of creation – which is to create evidence to prove that the message is created by the Originator;
- non-repudiation of receipt – which is to create evidence to prove that the Recipient has received the message;
- non-repudiation of knowledge – which is to create evidence that the Recipient read the message and recognized the content;
- non-repudiation of sending – which is to prove that the Originator has sent the message out.

3.2 The Evidence of Non-repudiation Services

All of the above 8 services are to provide the transacting parties a proof that could be used to prove that something took place, and used in arbitration, like in a court be presented as evidence for the events or transactions to help resolve the disputes. Any party in the message transmission model could generate evidence or request the other parties to create evidence for him. In any of the non-repudiation service, there are a few phases for evidence generation:

- Non-repudiation request – which is often implicit, and agreed by each party of any transaction before they start business
- Evidence generation – which is generated by either a trust third party or by the potential repudiator autonomously.
- Evidence distribution – which is to distribute the evidence to a trusted third party or the party requested the evidence.
- Evidence verification and retention – the party received the evidence from the potential repudiator need verify the validity of the evidence, after that he needs to safely store the evidence in case there is any repudiation in future needs to be resolve.

In the ISO/IEC 13888-1 standard, there are 2 main types of evidence defined:

- Secure Envelope – which is created and retained by a trusted third party who owns the secret key of a symmetric cryptographic algorithm. This type of evidence has an advantage of computation efficiency because of the usage of symmetric cryptography. Nevertheless, it has a few disadvantages, such as requirement of a third party, unconditional trust on the third party, and the online availability of the third party. All of these have prevented this type of evidence from being widely used and accepted.

- Digital Signature – which could be created by any party in transactions who owns the private keys of an asymmetric cryptographic algorithm. This type of evidence is the most widely accepted and used in modern online transactions and most importantly the laws in most countries have recognized Digital Signature as the equivalent evidence as their handwritten signatures. However, no technique is perfect, the "unauthorized use of the private key", "• Inadequate identification of the private key owner" and "False registration" (Lagou & Chondrokoukis, 2009) are 3 main vulnerabilities of digital signature evidences.

To achieve the same goal to authenticate a user and save the relevant evidence, and address the weakness of Digital Signature, researchers and scientists found a new approach without the help of cryptography, but the nature of human biological data like fingerprint, iris of eyes, facial characters, etc. Because of the individual differences and uniqueness of these characters, these biometric characteristics could be utilized to authenticate and act as evidence in the non-repudiation services. Although this approach seems more reliable than Digital Signature, but in reality, it is used far less than Digital Signature because of the high cost of the devices to read these biometric data.

King (2013) proposed to define a minimum set of attributes of system logs to record necessary user activities when they using the software systems to provide forensic evidences. The idea behind that is the collection of data in computer systems might amount to a degree that is "admissible as evidence in a court of law". His research has not finished yet, hopefully his further study could provide us another approach of generating evidence for user non-repudiation.

3.3 The Requirements of Non-repudiation

For all the non-repudiation services to work well for all transactions, a well-designed protocol has to be put into effect. Before investigating the protocols available, a few significant properties each protocol has to respect need be examined:

- Non-repudiation – undoubtedly all protocols should first meet this requirement;

- Fairness – By nature, all transaction messages are sent either from originator to recipient, or vice versa, at any time one party might have an advantage of obtaining more information than the others and may lead an unfair result. So all the non-repudiation services protocols must all put this in mind to guarantee that either both parties receive the evidence of origination or receipt, or none of them get any valuable information.
- Timeliness/Efficiency – Under the condition of keeping fairness, all protocols should always complete in a finite amount of time, without causing any party to wait a long time for response from the other parties, efficiently.
- Confidentiality – Due to the nature of non-repudiation services to generate and collect evidences, there are more rounds of message flows than normal communications. With the introduction of third parties, there are more chances to expose the confidential messages to either third party or the other end of transaction before completing the transaction. So keeping secret of messages in transactions becomes another important factor need be taken into account of protocol designs.

3.4 The Protocols

In all protocols for non-repudiation services, Jianying and Gollman (1996) proposed a fair non-repudiation protocol, which was so called as “ZG Protocol” in all non-repudiation related literatures. This protocol founded the basis of all later non-repudiation protocols, which all directly or indirectly refer to or improve upon it. Let us first take a brief look at how it works.

Commented [KP7]: Do you know why it is called ZG

Commented [KP8]: Use litearature , in single, always – not literatures

Commented [KP9]:

In all non-repudiation protocols, a notation system is defined to denote the entities and evidences in the protocol runs, the following are the notations for the ZG Protocol:

Commented [KP10]: What is missing is an explanation why it works!

- A – Alice, who creates the transaction message and communicate with other parties, in this case: Trusted Third Party (TTP) and Bob.
- B – Bob, who receives the transaction message and communicate with other parties, in this case: TTP and Alice.
- M – The transaction message to be transferred in plaintext.
- C – Commitment of the message, encrypted with a symmetric algorithm and a temporary Key created randomly by Alice

Commented [KP11]: Not very clear

- K – The Key created by Alice
- L – A unique label chosen by Alice, which can link all related messages together for a transaction.
- F – A flag to mark the intention of the message.
- EOO = sSa (F (EOO), B, L, C) – The evidence of origin of a commitment created by Alice, sent to Bob
- EOR = sSb (F(EOR, A, L, C) – The evidence of receipt of a commitment created by Bob, sent to Alice.
- Sub_K = sSa (F(sub), B, L, K) - The evidence of submission of Key generated by Alice, sent to TTP
- Con_K =sSttp (F (con),A, B, L, K) - The evidence of Confirmation Key created by TTP, available for download for both Alice and Bob.

Commented [KP12]: May need to be explained , and also the meaning of commitment in this context

The communication model is illustrated by the following Figure 2:

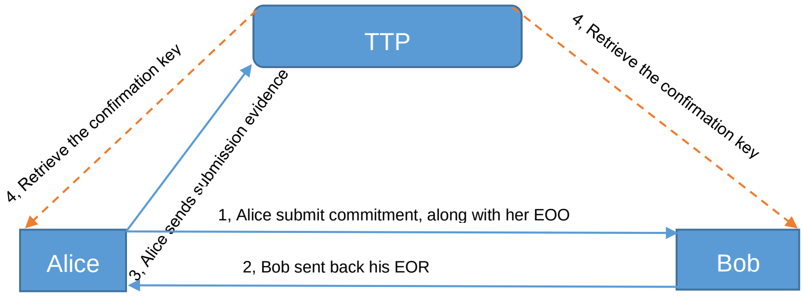
TTP
4, Retrieve the confirmation key
4, Retrieve the confirmation key
3, Alice sends submission evidence
1, Alice submit commitment, along with her EOO
2, Bob sent back his EOR
Alice
Bob

Figure 2: ZG Protocol

3.4.1 Later Protocols Based on ZG's

- A year later, Jianying and Gollmann (1997) extended their previous idea and reduced involvement of TTP to make the protocol more efficient.
- Two years later, Kwangjo, Sangjoon, and Joonsang (1999) examined the ZG's protocol and found 2 problems about fairness and confidentiality, and proposed an improved version of that to fix the problems by setting up a time limit on the NRR evidence and the introduction of Diffie-Hellman key exchange scheme.
- Two more years later, (Botao & Junzhou, 2004) further improved the ZG's protocol based on Kwangjo, Sangjoon and Joonsang's work by introducing a new efficient synchronization scheme to eliminate the need of clock synchronization and timestamp services.

Commented [KP13]: Suggest to remove the bullet points and use just a narrative

- Another year later, Gürgens, Rudolph, and Vogt (2005) analysed the ZG's protocol and successfully compromised it, based on that, they proposed a new protocol.
- Muntean, Dojen, and Coffey (2009) gave the ZG's protocol another attack and breached the security with a replay attack. Fortunately they gave another protocol to solve the issue.

Commented [KP14]: These were food to see but mor needed on how they were improved, different etc

3.4.2 Categories of Protocols

Kremer, Markowitch, and Zhou (2002) reviewed and surveyed most of the protocols for non-repudiation services available in literature, in which they categories all the protocols into 5 groups:

- Without assistant of TTP, such as Markowitch's protocol
- Inline TTP, such as Coffey and Saidha's protocol
- Online TTP, such as Zhou and Gollmann's protocol as depicted in Figure 2
- Offline TTP, such as Zhou and Kremer's protocol
- Transparent TTP, such as Markowitch and Kremer's

Commented [KP15]: It would be good to have all protocols mentioned above categorised, and also to make sure that all protocols mentioned her are also mentioned above (I did not not check, may be they are☺

3.5 The Applications

Commented [KP16]:

Commented [KP17R16]: How is this section different form the previous one, to me it reads like continuing on the able?

The non-repudiation services could and should be applied to any transaction or event needing preserving an evidence for resolving possible disputes. With all the available protocols in market and the evidence related techniques, selecting a best fit protocol and evidence technique for a specific application varies much depending on the context of the application. Here are a few applications and the usages of the techniques:

- Wen, Tong, and Xia (2007) developed a new protocol based on the NRPUM protocol and applied the new protocol to the current SMTP and POP3 email systems to achieve non-repudiation. All email User Agents and Mail Transfer Agents are involved to generate and store a chained evidence of origination, delivery, submission and receipt.
- Adibi (2010) proposed a new e-learning system in the mobile communication environment with the assistance of biometric technologies like iris, voice, face recognition for achieving authentication for the e-learning system and non-repudiation of the users.

Commented [KP18]: Needs to be explained

- Su, Fu, and Zhou (2010) proposed a new protocol based on traditional Web Services transaction model with the help of a new designed online TTP to embed the protocol information in a single Web Services call.
- Marx, Kuntze, and Lauer (2013) developed a new application on Android smartphone based on the proven concept VoIP Signatures to help identify the 2 ends of a LTE based void call and record the non-repudiation evidences to enable a business transaction on smart phone.

Commented [KP19]: These applications need to be explained ?

I stopped reading here

4 Conclusion

In this report, we have presented the basic concepts of non-repudiation services, which include 8 sub services providing different evidences for varying purposes. Then we examined the evidence types that could be generated, stored and presented an adjudicator to for resolving a potential dispute by their irrefutable natures. After that we thoroughly reviewed the most classic fairness non-repudiation protocol and his successors. At last we reviewed a few applications of non-repudiation services in real word businesses.

Due to the limited resources in hand and time for creating the report, the multi-party non-repudiation protocols were ignored in this report intentionally, but only a subset of two-party protocols were examined, and only the main stream protocol proposed by Zhou and Gollman were intensively studied without comparisons with the other protocols in the same period like the one proposed by Coffey and Saidha in 1999.

In future works, besides fixing the above mentioned problems, a thorough survey of the state of the art of non-repudiation service protocols is worthy to create, because the last survey was created by Zhou in 2002, which is way outdated to reveal the latest development status of the services.

5 References

Adibi, S. (2010). A remote interactive non-repudiation multimedia-based m-learning system. *Telematics and Informatics, 27*(4), 377-393. doi: http://dx.doi.org/10.1016/j.tele.2010.01.001

Botao, L., & Junzhou, L. (2004). *On timeliness of a fair non-repudiation protocol*. Paper presented at the Proceedings of the 3rd international conference on Information security, Shanghai, China.

Gürgens, S., Rudolph, C., & Vogt, H. (2005). On the security of fair non-repudiation protocols. *International Journal of Information Security, 4*(4), 253-262. doi: 10.1007/s10207-004-0063-7

Jianying, Z., & Gollman, D. (1996, 6-8 May 1996). *A fair non-repudiation protocol.* Paper presented at the Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on.

Jianying, Z., & Gollmann, D. (1997, 10-12 Jun 1997). *An efficient non-repudiation protocol.* Paper presented at the Computer Security Foundations Workshop, 1997. Proceedings., 10th.

King, J. (2013). *Measuring the forensic-ability of audit logs for nonrepudiation*. Paper presented at the Proceedings of the 2013 International Conference on Software Engineering, San Francisco, CA, USA.

Kremer, S., Markowitch, O., & Zhou, J. (2002). An intensive survey of fair non-repudiation protocols. *Computer Communications, 25*(17), 1606-1621. doi: http://dx.doi.org/10.1016/S0140-3664(02)00049-X

Kwangjo, K., Sangjoon, P., & Joonsang, B. (1999, 1999). *Improving fairness and privacy of Zhou-Gollmann's fair non-repudiation protocol.* Paper presented at the Parallel Processing, 1999. Proceedings. 1999 International Workshops on.

Lagou, P., & Chondrokoukis, G. (2009). Survey on Nonrepudiation: Digital Signature Versus Biometrics. *Information Security Journal: A Global Perspective, 18*(5), 257-266. doi: 10.1080/19393550903300464

Marx, R., Kuntze, N., & Lauer, H. (2013). *Bringing VoIP Signatures to Mobile Devices*. Paper presented at the Proceedings of Principles, Systems and Applications on IP Telecommunications, Chicago, IL, USA.

Muntean, C., Dojen, R., & Coffey, T. (2009, 27-29 Aug. 2009). *Establishing and preventing a new replay attack on a non-repudiation protocol.* Paper presented at the Intelligent Computer Communication and Processing, 2009. ICCP 2009. IEEE 5th International Conference on.

Onieva, J., Lopez, J., & Zhou, J. (2009). Fundamentals of Non-repudiation *Secure Multi-Party Non-Repudiation Protocols and Applications* (Vol. 43, pp. 1-15): Springer US.

Su, R., Fu, S., & Zhou, L. (2010). Fair non-repudiation for web services transactions. *Wuhan University Journal of Natural Sciences, 15*(5), 385-392. doi: 10.1007/s11859-010-0671-1

Wen, D.-y., Tong, C.-g., & Xia, G.-p. (2007). An email system with non-repudiation service. *The Journal of China Universities of Posts and Telecommunications, 14, Supplement 1*(0), 124-130. doi: http://dx.doi.org/10.1016/S1005-8885(08)60026-6

Zhou, J., & Gollmann, D. (1997). Evidence and non-repudiation. *Journal of Network and Computer Applications, 20*(3), 267-281. doi: http://dx.doi.org/10.1006/jnca.1997.0056