Non-repudiation of Forwarding
Traceability of Confidential Data Via Multiple Recipients

Rainer Schick and Christoph Ruland
Chair for Data Communications Systems, University of Siegen, Hoelderlinstr. 3, Siegen, Germany

Keywords: Non-repudiation, Data Leakage Protection, Security Service, Data Tracking, Evidence Generation.

Abstract: Nowadays, it can be assumed that valuable private data can be securely transmitted from one sender to one (or more) recipients. An unsolved problem following the transmission is addressed by this paper. The sender of some confidential information does not know what happens with the data after the transmission. If the message appears in a place it should not, the originator does not know who published it unauthorized. In order to solve this problem, this paper introduces a new non-repudiation service that allows tracking the way of protected data via several recipients.

1 INTRODUCTION

As far as confidential data is concerned, these data can be protected against unauthorized access in different ways. But what happens if allegedly trustworthy receivers misbehave? How to find out who is the data leak? These questions are often neglected in companies and other institutions. For the originator of sensitive private data it would be best if there would be a new security service that provides traceability of confidential information.

The new service deals with the topics of *Endpoint Security* and *Data Leakage Protection* (Scheidemann, 2008). Actually, one of the largest problems of companies is the unauthorized use of private devices by their employees. Large amount of data can be stored on such insecure devices and the damage may be huge if such a device gets lost. The new non-repudiation of forwarding service (NRFS) introduced in this paper collects so-called tracking data from multiple recipients and provides traceability of protected data. The tracking data prove the forwarding of confidential information and are updated for each transmission. If a dispute arises, these data are used to generate evidence. The conflict resolution after the evidence generation phase is out of scope of the NRFS.

After this introduction, related work are figured out in the next chapter. Chapter 3 then describes the basic idea of non-repudiation services and figures out the innovations and advantages of the NRFS. The Data Tracking Protocol (DTP) introduced in chapter 4 is designed to realize the NRFS. The protocol ensures that the tracking data are protected against targeted manipulations using a security module. Finally, in chapter 5 some conclusions are presented and an outlook to future work is given.

2 RELATED WORK

The ISO/IEC 13888 standards describe 8 different non-repudiation services (ISO/IEC 13888-1, 2009; ISO/IEC 13888-2, 2010; ISO/IEC 13888-3, 2009). General information about non-repudiation services are described in ISO 13888-1. Examples for symmetric techniques are given in part 2, asymmetric techniques in part 3. These services provide protection against an individual falsely denying the involvement in a particular action or event. For example, the sender can request a token which proves the receipt by the designated recipient. The recipient in turn requests a token which proves the forwarding to the sender. The goal of the NRFS is to prove the action of **forwarding** by allegedly trusted users.

Non-repudiation services and their underlying protocols usually should be **fair** (Zhou and Gollmann, 1996; Kremer et al., 2002), so that no party gets an advantage over another party. The NRFS does not exchange token between sender and receiver, so the aspect of fairness does not need to be considered.

Regarding the reliability of the NRFS, false positives must be prevented under all circumstances. No manipulation should lead to a user falsely being suspected. Manipulations that prevent the expose of an

Schick R. and Ruland C..
Non-repudiation of Forwarding - Traceability of Confidential Data Via Multiple Recipients.
DOI: 10.5220/0004053303870390
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 387-390
ISBN: 978-989-8565-24-2

attacker should also be prevented, if possible.

There exist other approaches to provide traceability of data. One is digital watermarking (Liu et al., 2005; Wang et al., 2001; Cox et al., 2008). Digital watermarks support copyright holders to track data leaks if an unauthorized copy is found. Watermarks can be embedded visible or invisible and have to cope with different problems: The embedding capacity is limited in relation to the size of its carrier (Barg et al., 2003) and the embedding algorithms depend on the file format. Another approach is Digital Rights Management (DRM). This technique is often used to prevent unauthorized copies of multimedia data. This is done by installing proprietary software and by using online activation mechanisms. DRM is considered controversially, and many experts claim that unauthorized copies cannot be prevented (INDICARE Project, 2006; Schneier, 2001).

3 NON-REPUDIATION OF FORWARDING

3.1 Non-repudiation Services

The goal of non-repudiation services is to protect the parties involved in a transaction against the other party falsely denying the participation in a particular event or action. For example, a sender of a message M can generate evidence for sending it. The recipient in turn generates evidence of the corresponding receipt. These evidences are called non-repudiation token.

(Zhou and Gollmann, 1996) and (ISO/IEC 10181-4, 1997) divide non-repudiation services into four, (Ford, 1994) and (RFC 4949, 2007) into six phases. The following list refers to the compact representation as shown in (ISO/IEC 10181-4, 1997):

1. Evidence generation: The critical action occurs and evidence is generated.
2. This phase includes the transfer, storage and request of the evidence.
3. The evidence is verified by a trusted authority.
4. Dispute resolution: Evidence is retrieved from storage, presented and again verified to resolve the dispute.

If symmetric techniques are used, the token must necessarily be verified by a Trusted Third Party (TTP) in case of a dispute. Using asymmetric techniques, the TTP is not mandatory. Nevertheless, the authenticity of the applied public keys must be guaranteed. Non-repudiation policies may enforce that only TTPs are allowed to generate the token. Usually, a URL to the used policy is part of the generated token. A non-repudiation service must permit a trusted authority to verify if a given signature was applied to given data. This authority checks if the private signature key corresponds to a given valid certificate.

In contrast to existing non-repudiation services, the NRFS collects evidences for multiple transactions. Each sender and recipient adds certain information to the protected data (Schick and Ruland, 2011b; Schick and Ruland, 2011a). Spoken clearly, for each action unique tracking data are added to the confidential message. That is, the NRFS allows incremental updates of the tracking data for each forwarding and thus tracking the whole way of data from the originator to the last recipient.

3.2 Requirements of the NRFS

The main goal of the NRFS is to provide traceability for confidential data over multiple recipients. Additionally, the originator *must* be able to prove to be the source of the information and the protected message *must not* be accessible by the recipient unless his or her unique tracking data are indelible added. Finally, the plaintext data output to the recipient *must* be accompanied by unique tracking data. These tracking data *should* not be erasable. At least any manipulation of these data *must* be recognized reliably.
To achieve these requirements, a security module is needed to realize the DTP. This module is mandatory for different reasons: It provides access control and ensures that the confidential message is output to the user only if the embedded tracking data are authentic. Most importantly, the private and secret keys required by the DTP can be securely stored, without even the owner of the module knowing the keys. Specified Protocol Data Units (PDUs) are transmitted between the security modules of the users.

3.3 Service Description

The NRFS implies a closed group of recipients (e.g. a company network), so that the TTP may be represented by the initial sender O. The TTP should not be involved in each transaction, so that the role of the TTP is *off-line*. Digital signatures and transaction timestamps are used to generate and provide the evidence. Thus, the NRFS is an asymmetric non-repudiation service. Table 1 summarizes the service descriptions and shows that the NRFS consists of two different data processing parts. The security module processes the encrypted data and handles the private and secret keys of its owner, while the digital watermark will be embedded into the plaintext message M.

Table 1: Description of the non-repudiation of forwarding service.

	SECURITY MODULE	WATERMARK
CLASS OF NRS:	Non-Repudiation of Forwarding	Non-Repudiation of Forwarding
ROLE OF TTP:	Off-line	Off-line
TYPE OF EVIDENCE:	Digital Signature, Timestamp	Digital Signature, Timestamp
GOAL OF EVIDENCE:	Proof of forwarding to all sender	Proof of last authorized receipt
USER OF SERVICE:	Data originator, all recipients	Data originator
CONCERNED USER:	All sender	Last authorized recipient

4 DATA TRACKING PROTOCOL

4.1 Goals of the Data Tracking Protocol

The DTP is designed to fulfill the requirements specified in chapter 3.2 und thus to realize the non-repudiation of forwarding service. The basic ideas of the DTP have been described in (Schick and Ruland, 2011b; Schick and Ruland, 2011a). Figure 1 shows the abstraction of the NRFS from the user's point of view. The user does not need to have knowledge about the underlying protocol. Instead, certain data are input as parameters into the service primitives provided by the security module through the service access points (SAP). Finally, certain data are output to the user. The communication between two service users is realized by the DTP.

The use of a Public-Key Infrastructure (PKI) is a basic requirement of the DTP and the existence of an appropriate PKI is assumed for the DTP. This includes the verification of digital certificates, reconciliation with a Certificate Revocation List (CRL) and checking the *nonRepudiation* bit in the *keyUsage* extension of X.509v3 certificates (RFC 5280, 2008).
Different functions (called service primitives) must be provided by the security module. Users must be able to initialize and configure the service, send and receive data and finally generate evidences in case of a dispute. The functionality of the protocol and each function provided by the security module are briefly described in the following.

4.2 Tracking Data

The tracking data are used to track the way of message M if a dispute arises. These data consist of unique identifiers which distinguish the participating users and the protected message M. The size of the

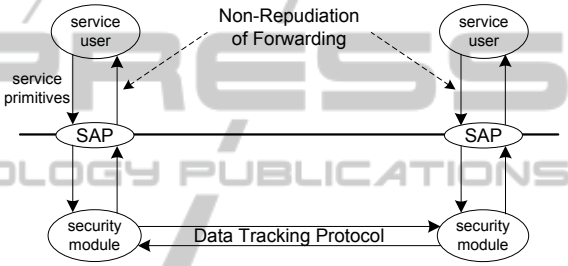

Figure 1: The different layers from the user's point of view.

tracking data should be kept as small as possible because of the security module. On the contrary, these data are used to generate evidence, so they have to be both unique and provable authentic. This is a common problem in information security - security increases overhead and complexity. The tracking data must be protected from several attacks. This includes protection from targeted manipulations, traffic flow analyses and privacy aspects (concerning the user identifers). More detailed descriptions of the protection mechanisms will be part of future work.

4.3 Functions of the Security Module

With the security module, the required private and secret keys must be generated and stored within a secure environment. The owner of the module must not have access to these keys, otherwise he or she would be able to tamper data. Additionally, the confidential message M must not be output to the receiver if any manipulation is detected or if M (or its originator) is not provable authentic. If so, the security module has to stop data processing and signalize an informative error message. Thirdly, the tracking data must be added to M before the receiver gets access to it. The authenticating signatures must also be generated and verified by the security module. Hence, the module

must provide the following functions:

1. **Initialize.** Lets the originator configure the DTP and prepare the data for the protocol. The required keys are also generated by this function.
2. **Send.** If data should be forwarded to the next authorized receiver, this function must be used. It sets up a secure communication channel and sends encrypted data.
3. **Receive.** Processes the received encrypted data. If the data are in good condition, the watermarked plaintext and encrypted storage data are output.
4. **Evidence-TD.** Generates the non-repudiation token based on the tracking data accompanying the protected data containing *M*.
5. **Evidence-WM.** Generates the token based on the digital watermark which has been inserted into the plaintext message.

5 CONCLUSIONS

With the non-repudiation of forwarding service, confidential data can be tracked via multiple recipients. Evidence can be generated to prove the whole way of protected data. The service is split into two parts: The first part relies on a security module and the second part inserts digital watermarks into the plaintext that output to the recipient.

The data processing part provides a high level of security. The user is not able to access the confidential data unless the security module accepts the received data as valid. The security services of peer entity authentication, non-repudiation of origin, data integrity and access control are provided. The user is not in possession of any private or secret key. Instead, these keys are managed by the security module.

In future work, the key management must be described and information about secure key storage and distribution must be given. Moreover, legal aspects of the NRFS should be analyzed. The requirements that are necessary to make the non-repudiation token valid evidences must be pointed out. Due to the required computational power of digital watermarking algorithms, an appropriate security module must be found. Finally, that module should provide the service primitives described in this paper.

ACKNOWLEDGEMENTS

This work is funded by the German Research Foundation (DFG) as part of the research training group GRK 1564 - 'Imaging New Modalities'.

REFERENCES

Barg, E., Blakley, G. R., and Kabatiansky, G. A. (2003). Digital fingerprinting codes: Problem statements, constructions, identification of traitors. In *IEEE Transactions on Information Theory Vol. 49*, pages 852–865.

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., and Kalker, T. (2008). *Digital Watermarking and Steganography*. Elsevier, second edition edition.

Ford, W. (1994). *Computer Communications Security: Principles, Standard Protocols and Techniques*. Prentice Hall, first edition edition.

INDICARE Project (2006). Consumer's guide to digital rights management.

ISO/IEC 10181-4 (1997). *Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework*. International Organization for Standardization.

ISO/IEC 13888-1 (2009). *Information technology - Security techniques - Non-repudiation - Part 1: General*. International Organization for Standardization.

ISO/IEC 13888-2 (2010). *Information technology - Security techniques - Non-repudiation - Part 2: Mechanisms using symmetric techniques*. International Organization for Standardization.

ISO/IEC 13888-3 (2009). *Information technology - Security techniques - Non-repudiation - Part 3: Mechanisms using asymmetric techniques*. International Organization for Standardization.

Kremer, S., Markowitch, O., and Zhou, J. (2002). An intensive survey of fair non-repudiation protocols. In *Computer Communications Vol. 25*, pages 1606–1621.

Liu, R., Trappe, W., Wang, J., Wu, M., and Zhao, H. (2005). *Multimedia Fingerprinting Forensics for Traitor Tracing*. Hindawi Publishing Corporation.

RFC 4949 (2007). *Internet Security Glossary, Version 2*. Network Working Group.

RFC 5280 (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Network Working Group.

Scheidemann, V. (2008). Endpoint security: Data loss prevention.

Schick, R. and Ruland, C. (2011a). Data leakage tracking - non-repudiation of forwarding. In *Communications in Computer and Information Science Vol. 251*, pages 163–173.

Schick, R. and Ruland, C. (2011b). Document tracking - on the way to a new security service. In *IEEE Conference on Network and Information Systems Security*, pages 89–93.

Schneier, B. (2001). The futility of digital copy prevention.

Wang, Y., Doherty, J. F., and van Dyck, R. (2001). A watermarking algorithm for fingerprinting intelligence images. In *John Hopkins University*, pages 21–24.

Zhou, J. and Gollmann, D. (1996). A fair non-repudiation protocol. In *IEEE Symposium on Security and Privacy*, pages 55–61.