IADIS International Journal on Computer Science and Information Systems
Vol. 4, No. 2, pp. 59-72
ISSN: 1646-3692

SECURITY MECHANISMS OF A LEGAL PEER-TO-PEER FILE SHARING SYSTEM

Sebastian Schinzel. *Darmstadt University of Applied Sciences. Haardtring 100, 64295 Darmstadt, Germany*

schinzel@colonwq.org

Martin Schmucker. *Security Technology Department, Fraunhofer Institute for Computer Graphics Research IGD. Fraunhoferstraße 5, 64283 Darmstadt, Germany*

m.schmucker@gmx.de

Peter Ebinger. *Security Technology Department, Fraunhofer Institute for Computer Graphics Research IGD. Fraunhoferstraße 5, 64283 Darmstadt, German*

peter.ebinger@igd.fraunhofer.de

ABSTRACT

Contrary to Digital Rights Management systems (DRMS), CONFUO©O [Schmucker, M. and Ebinger, P., 2005] is a legal peer-to-peer file sharing application that controls content distribution as opposed to content usage. A central entity called Trusted Third Party (TTP) validates whether users are allowed to legally distribute a particular content and users within the CONFUO©O system enable peer monitoring to identify irregularities.

Several of the core features (such as inter-user observation) have not yet been tested or approved for use on the Internet. This article demonstrates the iterative improvement of CONFUO©O's security over conventional DRM systems. A summary of the extensive security analysis performed to identify threats and potential vulnerabilities resulting from the abuse of this new protocol is presented and led to the discovery of a possible Denial-of-Service (DoS) threat. In this installment, several advances for CONFUO©O's architecture involving the introduction of public-key technology and user-based accountability are presented, which significantly increase the overall security of the system.

KEYWORDS

Content Distribution, Content Monitoring, Fingerprinting, P2P, Perceptual Hashing, Secure Distribution

1. INTRODUCTION

The primary advantage of well-designed peer-to-peer (P2P) networks is their ability to scale. The available bandwidth per peer theoretically stays constant independently of the number of peers on the network. Similarly participating peers share storage capacity and thus P2P networks are ideally suited for the distribution of media content. On the downside, peer-to-peer networks tend to be more complex. Services that can be implemented with ease on highly centralized networks are rather difficult to deploy on pure peer-to-peer networks. The difficulty for copyright owners to control distribution of their content is another drawback of peer-to-peer networks and this irreversible distribution of copyrighted multimedia content leads to numerous cases of intellectual property infringement.

The music industry reacted to rampant infringement on intellectual property rights by introducing Digital Rights Management (DRM) systems. DRM systems strongly interfere with accustomed consumer content usage patterns. The imposed restrictions are increasingly unacceptable by today's media savvy consumers: they have already experienced the benefits of unprotected content distributed through P2P networks. The primary purpose of existing DRM systems is to control content usage. DRM protected content distributed via P2P networks or other uncontrolled channel remains protected[1]. These DRM systems however are under full control of their owners, which imposes severe security risks (cf. [Arnold, M. et. al, 2003]) and possibly omnipresent leaks such as the 'analog hole'. In addition to leaks (which allow the creation of an unprotected version of previously protected DRM content) there are also distribution channels that cannot be controlled (e.g. the so-called DarkNets [Biddle et. al, 2002]).

In contrast to traditional DRM systems the primary aim for the development of the CONFUO©O architecture was to support new and niche artists by enabling the distribution of free and promotional content. The network is therefore legal (operationally). Section 2 discusses the relation of this article with the state of the art. Security of content distribution is discussed in section 3 which flows into section 4 and outlines the initial system design and related analysis. Section 5 identifies potential problems and attacks while sections 6 and 7 address these issues with modeled solutions. Section 8 describes how the improved protocol copes with lost or compromised user accounts. The conclusion and outlook for the future are finalized in section 9.

2. RELATED WORK

[Kim, J. et. al, 2005] discusses general threats to P2P systems with respect to interoperability, autonomy, availability, integrity, vulnerability and confidentiality and the authors discuss different security methods. There are, however, additional problems that threaten users and service providers, namely the illegal exchange of copyrighted data and related consequences such as the loss of user privacy.

For any P2P system designed for content sharing, different categories of security issues can be identified. For example, [Sung , J. et. al, 2006] and [Steinebach, M. and Hassler, Ch.

[1] DRM systems are not restricted to content protection as they can also represent the creation of new business models based on content usage.

2006] address the restriction of illegal distribution of copyright protected content. In contrast to CONFUO©O, add-ons to existing P2P networks are investigated. Add-ons are not considered in CONFUO©O. On the one hand, these add-ons cannot really increase the security of a patchy basis. On the other hand, the add-on DRM is opposed to users' P2P experience. Further authors such as [Chothia T. and Chatzikokolakis, K., 2005] and [Good, N. and Krekelberg, A., 2003] investigate user related issues, i.e. anonymity and privacy protection. This is already considered in the CONFUO©O architecture by the use of pseudonyms that are managed by a TTP. Further categories of security include the availability of the service and the trust to the P2P system and its users. For example, [Aberer, K. et. al, 2005] and [Naoumov N. and Ross, K. 2006] investigate load balancing and denial-of-service attacks. And trust related issues, system integrity and inter-user trust are discussed, e.g. by [Datta, A. et. al, 2003] and [Liebau, N. et. al, 2006].

This article addresses availability of service and trust to the CONFUO©O system, especially accountability and non-repudiation. It summarizes an analysis of the CONFUO©O system and the identified weaknesses. The analysis investigates the potential abuse of the original implementation and a weakness in the original protocol is identified that allows a denial of service (DoS) attack against the CONFUO©O system. A solution to this problem is presented that prevents this DoS attack and coevally strengthens accountability and non-repudiation by using a (flat) public-key infrastructure.

3. CONFUO©O

The goal of CONFUO©O [Schmucker, M. and Ebinger, P., 2005] [Schmucker, M. et. al, 2005] was to build a distribution framework for the legal and secure distribution of content that takes into consideration both content owners' interests as well as consumers' needs. By definition, secure and legal distribution requires that the distribution channel is 'content aware' and sanctions legal content use while preventing unapproved content use or exchange. Each content piece distributed on the network is assigned to an owner who defines permissions for its exchange[2]. Unknown/unidentified content is blocked from being distributed on this network unless it is registered with distribution permission and assigned to a specific content owner. CONFUO©O assures that consumers exclusively acquire content legally and creates user awareness of, and user responsibility for, their actions within the system.

3.1 Content Identification

The core of CONFUO©O is the reliable identification of content performed with perceptual hashing technology. Perceptual hashing ensures the digital fingerprint is always similar for the same content independently of its format or its encoding. As the fingerprint consists of local descriptors even content segments can be identified [Cano, P.et. al, 2003] [Haitsma, J. and Kalker, T., 2003] [Bardeli, R. and Kurth, F., 2004]. The fingerprint is part of each content item's unique identifier (ContentID) used on the network.

[2] A content owner can also prohibit content exchange.

3.2 Mutual Observation

The problem with existing content sharing networks is that the control instance that ensures legal exchange is put on top of the existing P2P network architecture. The proposed CONFUO©O platform requires users to observe each other while sharing content, whereby each peer becomes a control instance. Content receiving peers calculate the fingerprint of received content and compare it to the fingerprint of the content it requested. Both fingerprints must be equal, otherwise a fraud attempt is identified and the mismatch is reported to a Trusted Third Party (TTP), which validates the exchanged content. The TTP is therefore essential for legal content exchange and, by design, its failure must not allow illegal exchange[3].

4. EXCHANGE PROTOCOL

Security analysis tests performed on the original CONFUO©O system as presented in [Schmucker, M. and Ebinger, P., 2005] are shown here. For clarity we start with the description of the CONFUO©O exchange protocol, necessary to understand the security analysis which follows in section 5.

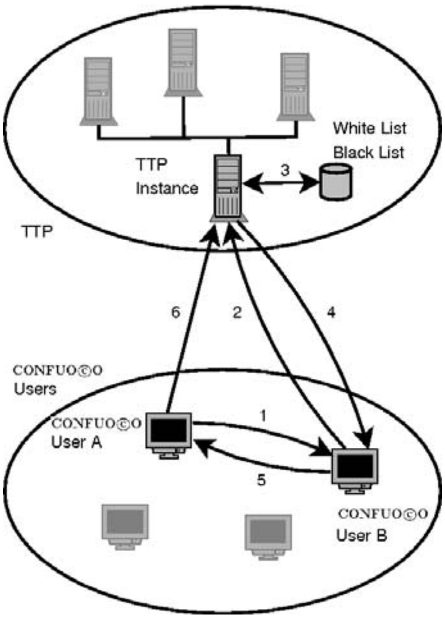

Figure 1. Overview of the protocol used to validate content exchanges at a TTP

As shown in *figure 1*, the analyzed transaction protocol consists of the following steps:

[3] Replication of a TTP and DoS style attacks are potential weakness of any network system, CONFUO©O aims to eliminate any additional security leaks.

1. CONFUO©O user A sends a message to CONFUO©O user B stating that she wants to perform a transaction, thus requesting the download of content.
2. The CONFUO©O user application of user B sends a request for the validation of a transaction to a TTP. This request includes the ContentID (fingerprint) of the content.
3. The TTP checks the validity of the content against a white and black list of known content.
4. The TTP sends to user B a positive message (thus validating the request), a message that the transaction is invalid (and why), or a message stating that the content is at present unknown to the CONFUO©O system (not listed on either white or black lists).
5. User B sends the requested content or related error message to user A.
6. CONFUO©O user A calculates the fingerprint of the received content and compares it to the fingerprint included in the ContentID of the requested content, the result is sent to the TTP.

5. SECURITY RISKS

From an attacker's point of view, the CONFUO©O system consists primarily of a client-server architecture network that connects the CONFUO©O user application with a TTP. User applications communicate among each other within a peer-to-peer network and both networks are required for each transaction between two CONFUO©O users. Extensive security analysis on CONFUO©O performed in [Schinzel, S., 2005] clearly showed that the TTP is the most vulnerable process for attack as the TTP controls authentication of content distributed on the network. The TTP is a central instance which cannot be implemented as a peer-to-peer network and therefore maintains a single point of failure for the system. The following two sections describe both security related vulnerabilities discovered in the CONFUO©O protocol as a result of thorough security analysis.

5.1 Distributed Denial of Service

User A could start many transactions/TTP requests in parallel with various users[4] with little effort (compared to the overall overhead of the resulting transactions). This scenario involves a mass of users trying to receive transaction validation from the TTP simultaneously. As a consequence the TTP is flooded with validation requests according to action 2 (as outlined in section 4) causing increased network traffic, more Input/Output actions (I/O lookups to the white list and black list), and increased computing resources to manage simultaneous connections. This is a serious threat to the CONFUO©O system as each request originates from a different source, making it difficult for the TTP to distinguish between a legitimate user request or those that are part of the attack. Countermeasures are therefore difficult to develop and the attack is likely to succeed unless methods (such as those proposed in section 6.1) are used.

[4] It is assumed that user A already knows which users have the specific content.

5.2 User Accountability in the Exchange Protocols

The purpose of the CONFUO©O system is to provide a content-sharing system that guarantees to users that content in the CONFUO©O system can be shared legally, that the content does not infringe upon Intellectual Property Rights of artists. This legality is not fully attained with solely technological means, but with the combination with user accountability. If both participants of a transaction attempt to distribute unauthorized content, it would most likely be undetected by the CONFUO©O system as neither client would report the fraudulent fingerprint to a TTP. This is an identified weakness to the security of the CONFUO©O system. However, in practice this situation would be difficult as it requires both fraudulent users to know that the other is also fraudulent. Furthermore, both users must avoid suspicious behavior when in contact with legitimate users.

6. IMPROVED EXCHANGE PROTOCOL

The following sections describe the improvements of the CONFUO©O protocol to solve risks described in section 5.

6.1 Shifting the Effort to the Requester

The weakness of the original protocol (as described in section 4) relating to DoS attacks originates from a design that places most of the load in a transaction on the TTP and the users that offer content. In the original protocol, the requesting user has very little effort. The improved protocol moves the validation process to the requesting user A and the TTP. The initiating CONFUO©O user A conducts the exchange validation process at the TTP before the user contacts user B. The new protocol and a comparison to the original protocol version are shown in figure 2 on the next page.[5]

6.2 Accountability

All users are accountable for their actions performed within the CONFUO©O system. This is not achieved by logging each action of every user, but by detecting patterns of misbehavior. Other users who communicate with the suspected user detect these patterns. Detected anomalies are automatically forwarded to the TTP, which then initiates an investigation of the suspect.

[5] There are many services on the Internet that provide centralized client-server services well protected from DoS style attacks (Google search engine and Akamai hosting service for example), an approach that the CONFUO©O system can exploit to defeat DDoS attacks aimed at the TTP directly.

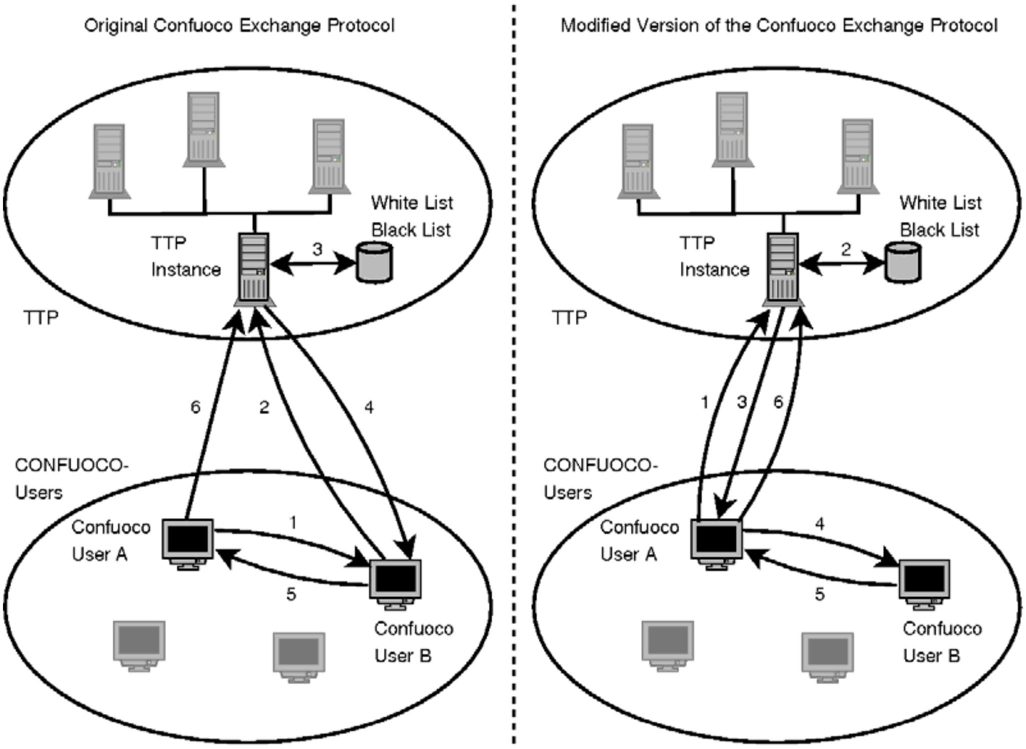

Figure 2. Overview of the modified protocol with comparison to the original

The original CONFUO©O exchange protocol had only limited user accountability capabilities. The mismatch of provided and received fingerprints6 was one pattern that can be detected by the system (cf. step 6, section 4). Under the old CONFUO©O protocol, fraudulent reports of mismatching fingerprints were impossible to identify as user applications communicate directly. The advanced protocol (as outlined in section 6.1) eliminates the threat of false-positives (whether initiated intentionally or not).

6.3 Introduced Problem with Modifications

The modified protocol shown in figure 2 addresses the possible Distributed Denial of Service (DDoS) attack (section 5.1) but opens the door to another security risk: The requesting user A could just pretend to validate a transaction at the TTP. User B so far has no means to reliably check whether the TTP agreed with the transaction or not. This security breach is possible because users cannot individually verify validation; they must trust a statement of user A without additional proof. This system, based on only one trust relationship between CONFUO©O users and the TTP is unacceptable and must become transitive in order to close the opportunity for exploitation. Specifically, a CONFUO©O user must be able to trust a

[6] Indicating that the user has changed her CONFUO©O software.

statement made by the TTP that was delivered through another user. It is crucial to eliminate all possibilities that the delivering user modified the content of the message.

6.4 Integrity Protection of TTP Permission Messages

In order to guarantee the authenticity and integrity of exchanged validation messages created by the TTP, we attached a digital signature based on public-key cryptography to the message. We call the message-signature-tuple a “ticket”. The ticket contains the ContentID ID, the time t_{start} from when it is valid and the time t_{expire} when it expires. This data is signed using the signature function S and the private key of the TTP K_{TTP} . The signature s is therefore generated[7] as:

$$s = S((ID + t_{start} + t_{expire}),K_{TTP})$$

This signature is also included in the ticket and is forwarded from the requesting CONFUO©O user to the user hosting the requested content. With these additions, a CONFUO©O user is able to verify that the TTP created the message and that the message’s integrity is kept.

7. IMPROVED PROTOCOL WITH USER-SPECIFIC KEY PAIRS

The improved exchange protocol offers transaction-based accountability by identifying cases in which one CONFUO©O user cheats and by reporting the cases to the TTP. Nevertheless, the TTP is not able to determine which participant was the offending user. An illegal transaction between two fraudulent users will not be detected as neither user would report the incident (as discussed in section 5.2).

In order to add user-based accountability to the system, the TTP must investigate communication between users that participate in a transaction. Recording communication between two users is of use only if authenticity and integrity of the recorded messages can be guaranteed, no matter by whom the traffic recording was delivered. Digital signatures are used again to solve this problem. The improved protocol described in this paper requires each user to have their own key-pair to add non-repudiation to messages. These key-pairs are tied to the pseudonym of a user.

An infrastructure is needed to manage keys appropriately including the creation, certification and revocation of keys and certificates respectively. A detailed proposal of such an infrastructure that deals with the detection of compromised keys, the distribution of revocation information, and the handling of invalid signatures is given in [Schinzel, S., 2005]. The following outlines the various steps of content querying and exchange, and analyzes them with respect to the requirements for authenticity, integrity protection and the resulting need for message signing (cf. figure 3).

[7] The + symbol denotes a concatenation of two strings.

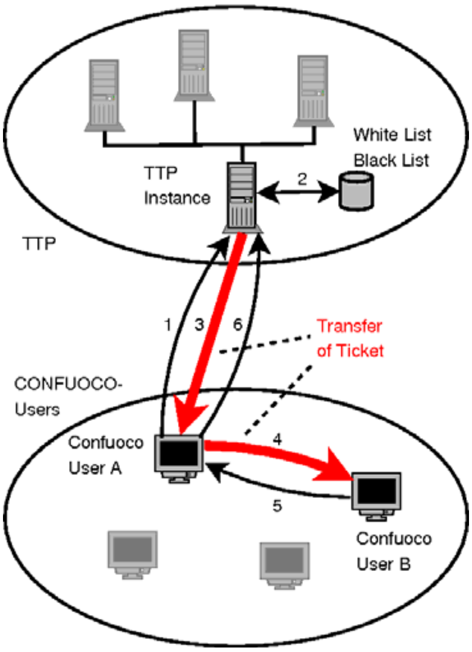

Figure 3. Overview of the improved exchange protocol with tickets

Search content: Attaching a signature to query and search results is not necessary as the legality of content in the CONFUO©O system does not rely on content name rather the content itself (using perceptual hashing).

Select content: This request asks for the fingerprint (ContentID) of the selected content. The ContentID is important for the accountability of the system, because in this step, a user finally decides to download identified content. It must therefore be signed so that the non-repudiation of the ContentID is guaranteed.

Validate content (action 1, 2 and 3): The TTP is directly involved in this communication. Signing of the messages is not required.

Transfer content (action 4 and 5): The sender of the content must not be able to repudiate that the content was sent. Therefore the transfer of the content has to be signed by the sender.

Validate transaction (action 6): The user directly communicates with the TTP. Therefore there is no need to digitally sign this component.

This method ensures protocol messages for content selection and content transfer are signed adding non-repudiation capabilities to the exchange protocol, and allowing the TTP to unambiguously identify cheaters in the CONFUO©O system.

8. REVOCATION OF USER-SPECIFIC KEY PAIRS

As the approach of user-specific key pairs requires the management of a large amount of certificates, efficient mechanisms for certificate revocation are required. Key compromise must be reliably detected and the revocation information has to be distributed to the CONFUO©O user application as quickly as possible.

8.1 Detection of Key Compromises in the CONFUO©O System

There are several reasons for revoking a certificate. For example, the need to block a fraudulent CONFUO©O user account or a key compromise may cause the revocation of a certificate. This section identifies ways to detect a key compromise in the CONFUO©O system.

The detection of a key compromise is not an easy task in the CONFUO©O system as most users are not aware that they work with sensible cryptographic information while using the CONFUO©O user application. Creating user awareness for cryptographic techniques and their applications is not feasible within the CONFUO©O system. If a user’s laptop gets stolen, her home PC gets hacked or the hard drive fails and is thrown in the garbage even though it still contains valuable data, the user should revoke her own CONFUO©O keys. The probability that this happens is however expected to be low. Therefore, the CONFUO©O system needs a way to find out about compromised key by itself.

Cryptographic systems are usually not able to detect key compromise automatically and the detection is usually a process outside the systems that uses the key. Often the belonging person has to decide when the key was compromised. The system should guide the users in the CONFUO©O system to find out, whether a key was compromised, or not. This is done by letting the CONFUO©O user answer well chosen questions in order to decide if a key was compromised. The user is queried every time a CONFUO©O user application is newly installed. The default action is that all former CONFUO©O keys and certificates of the user installing the application are revoked. The disadvantage of this is that a CONFUO©O user can only install the CONFUO©O user application on a single computer because certificates of other applications are revoked when the application is installed on another computer. As a CONFUO©O user should be able to run the CONFUO©O user application on several computers, this is an unacceptable restriction.

A possible solution is to ask the user if this is currently the only instance of the CONFUO©O user application she uses. Only if the user states that this is the only installation of the CONFUO©O user application, the certificate is revoked.

This leads to another problem, because keys of inactive users are only revoked when the key expires, even when the key has been compromised a long time before. An inactive CONFUO©O user is someone, who does not use the CONFUO©O user application anymore, or is a user, who has registered within the CONFUO©O system and lost her password. In the latter case a user may just create a new account, leaving the former user account and the keys inactive. This can be solved by automatically revoking keys of a user if she has not used the system for a certain time. If the user logs in again, a new key pair is created automatically by the CONFUO©O user application. Another possibility is to choose the expiration time of the used keys rather short, between one hour and several days, in order to limit the potential damage, which can be caused through a compromised key.

8.2 Distribution of Revocation Information

The information about revoked certificates is stored in a central database, which is located inside the TTP. This information is also used by the CONFUO©O user application and has to be distributed in the CONFUO©O system. In [Schinzel, S., 2005] several methods of distributing certificate revocation information to users have been introduced. Here, the different methods from the CONFUO©O point of view are analyzed. A decision table is created to find the best revocation method of CONFUO©O user certificates (see table 4.1).

There are several criteria to decide, which revocation method is best for the CONFUO©O system. Each of the criteria is weighted with a number between 0 and 4, where 0 means that the criterion does not matter at all, and 4 states that the criterion is crucial for the CONFUO©O system.

The revocation methods themselves are also weighted in the range of 0 to 4 according to the criteria. 0 means that the revocation method does not fit the particular criterion at all, 4 means that the revocation method fits the criterion perfectly. The following describes the attributes of the decision table in detail.

- **Time Delay** The maximal time (worst case) it takes for a CONFUO©O user application to recognize the revocation of a certificate. It is assumed that the CONFUO©O user application is permanently connected to the Internet. The CONFUO©O system is a legal file-sharing system and guaranties that only legal transactions take place and therefore certificate revocation of malicious users should be performed as soon as possible. However, it is not crucial for the system if one or two illegal transactions may be executed before a user is completed excluded from the system. Therefore the weight of this criterion is 2.
- **Service Dependency** There are revocation methods that depend on the availability of an additional service. This attribute shows the supplementary complexity introduced to the CONFUO©O system by using the revocation method. The weight for this criterion is 2.
- **Costs for TTP** This measure determines the costs that arise for the TTP for the given revocation method. The cost for the TTP is a very important criterion because the TTP is a crucial bottleneck for the CONFUO©O system and must be scalable. It is important not to burden the TTP with too much workload. Therefore the weight of this criterion is 4.
- **Costs for User** The additional costs a user has to tolerate if the CONFUO©O system is equipped with the method of revocation. The ease of use for the CONFUO©O user application also depends on the costs a user has to pay to use the system. These costs include necessary network bandwidth, amount of traffic per time, hard disk space, which is taken by the CONFUO©O user application, and CPU time that the application needs. The weight for this criterion is 1.
- **Development Costs** Finally, it is important to know how expensive the development of a revocation method is. This measure is also directly proportional to the additional complexity for the CONFUO©O system. The more complex an application is the more expensive it is to be developed and maintained. Complex applications also tend to be more error prone. Therefore the weight for this criterion is 3.

Now that the attributes of the decision table are fixed, values are assigned to the attributes of each revocation method in order to fill the decision table. The following text describes the evaluation process. The assigned values are shown in table 8.1.

Table 1. Decision table of possible revocation methods

	Weight	**Copy of CRL**	∑	**OCSP**	∑	**Short Lifetime**	∑
Time Delay	2	1	2	4	8	2	4
Service Dependency	2	3	6	0	0	4	8
Costs for TTP	4	0	0	1	4	3	12
Costs for User	1	2	2	1	1	3	3
Development Costs	3	2	6	0	0	4	12
∑			**16**		**13**		**39**

Peers hold local copy of CRL This certificate revocation method regularly issues CRLs and offers them to clients. The clients download the CRL and check whether incoming certificates are listed in the stored CRL or not. The CRL expires after a while and clients have to download a new copy of the CRL. As CRLs are downloaded just before the expiration time of the previous CRL, the maximum time it takes for revocation information to reach the CONFUO©O user application is the lifetime of CRLs. CRL files can be hosted using a common HTTP or FTP servers, which are both widely used and well understood protocols. A special service is not required. Because of the peak load, caused by the CONFUO©O user community that downloads the newly issued CRL when the former CRL expires, the costs for the TTP are high. The user of the CONFUO©O user application has to download the CRL frequently and has to save it to disk. Both network traffic and required hard disk memory space are low compared to today’s network bandwidth and hard disk space of end user computers. Even if additional functionality is needed in order to offer this revocation method, the necessary effort is expected to be relatively low, as parts of the service can be achieved using existing standard software, e.g. HTTP servers.

Online Certificate Status Protocol OCSP is a query service that enables users to query a server to check the revocation status of certificates. As the user just asks for the status of a single or a set of certificates, the transferred amount of traffic is low and the responses of OCSP are always up to date. OCSP is the most up to date and accurate certificate revocation distribution method in this analysis. However, OCSP highly depends on the availability of the OCSP responder service. The OCSP responder introduces another single point of failure in the CONFUO©O system. Even if the costs for the TTP are not as high as for the revocation method *Copy of CRL*, the TTP is expected to handle a lot of traffic that is caused through the OCSP responder. The additional costs for the CONFUO©O user are the increased latency of the OCSP request. Costs of development are expected to be high as OCSP is a relatively complex protocol.

Short Key Lifetime Short expiration times of keys allow to not use any revocation mechanism at all. If a key was compromised, it could only be abused for a very limited time. The expiration time of the keys can be chosen short enough to deal with inactive CONFUO©O user accounts. This is another convenient side effect of a short lifetime of cryptographic keys. The time delay from the revocation of a certificate to the time the information about the revocation reaches the CONFUO©O user applications depends on the lifetime of the certificate. It is comparable to time delay in *Copy of CRL* because both depend on an expiration time.

The certification service has to be included in the TTP software, so there is no additional dependency for the service. This is because the CONFUO©O system already depends on the certification service. The costs for the TTP are comparably low, only the certification service has to be more powerful than before. The costs for the CONFUO©O users are also low because only the public key has to be sent to the TTP in order to get certified. The development costs of this service are therefore expected to be low.

The decision table (see table 8.1) clearly shows that a short lifetime of CONFUO©O user certificates is the revocation method that fits best to the specific requirements of the CONFUO©O P2P system.

9. CONCLUSION AND OUTLOOK

Extensive security analysis of the CONFUO©O system resulted in the identification of two potential security vulnerabilities. An adversary could trigger a Distributed-Denial-of-Service attack against the system based on the regular usage of the content exchange protocol or could compromise security by masking content validity. We introduced digitally signed validation tokens called “tickets” (using public-key technology and digital signatures to ensure security) in order to ensure the authenticity and integrity of messages. In the former version of the protocol, unauthorized transactions could not be associated with a particular user. The new protocol requires peers to sign certain messages, which adds non-repudiation to the protocol. This structure allows the TTP to analyze sent messages during a transaction, thus identifying fraudulent transactions. We chose a short lifetime of certificates to cope with lost or compromised certificates.

The proposed CONFUO©O system opens new possibilities for the fair exchange of legal media content controlled by content producers without the need to implement intrusive DRM. We hope this protocol is another step towards fair usage of multimedia content and the popularization of DRM free media.

ACKNOWLEDGEMENT

The work described in this paper was partially funded by the European Commission as part of ECRYPT - European Network of Excellence in Cryptology through the IST programme under contract IST-2002-507932.

REFERENCES

Aberer, K. et. al, 2005. Multifaceted Simultaneous Load Balancing in DHT-based P2P systems: A new game with old balls and bins, *Self-star Properties in Complex Information Systems*. Springer.

Arnold, M. et. al, 2003. *Techniques and Applications of Digital Watermarking and Content Protection*. The Artech House Computer Security Series. Artech House, Norwood, MA, USA.

Bardeli, R. and Kurth, F., 2004. Robust identification of time-scaled audio. *Proceedings of the AES 25th International Conference on Metadata for Audio*. London, UK, 2004.

Biddle et. al, 2002. The darknet and the future of content protection. *In ACM CCS Workshop on Security and Privacy in Digital Rights Management*, LNCS.

Cano, P.et. al, 2003. A review of algorithms for audio fingerprinting. *In International Workshop on Multimedia Signal Processing.* US Virgin Islands.

Chothia T. and Chatzikokolakis, K., 2005. A Survey of Anonymous Peer-to-Peer File-Sharing , *IFIP International Symposium on Network-Centric Ubiquitous Systems (NCUS 2005)*. Nagasaki, Japan.

Datta, A. et. al, 2003. Beyond "web of trust": Enabling P2P E-commerce, *IEEE International Conference on E-Commerce Technology*. Newport Beach, California, USA.

Good, N. and Krekelberg, A., 2003. Usability and privacy: a study of Kazaa P2P file-sharing, *Proceedings of the conference on Human factors in computing systems (CHI).* Fort Lauderdale, Florida, USA.

Haitsma, J. and Kalker, T., 2003. Speed-change resistant audio fingerprinting using auto-correlation. *Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processin. (ICASSP)*. volume 4, pages 728–731.

Kim, J. et. al, 2005. Security issues in peer-to-peer systems. The 7th International Conference on Advanced Communication Technology (ICACT 2005). Korea.

Liebau, N. et. al, 2006. Charging in Peer-to-Peer Systems based on a Token Accounting System. In: Proceedings of 5th International Workshop on Advanced Internet Charging and QoS Technologies (ICQT'06), June 2006.

Naoumov N. and Ross, K. 2006. Exploiting P2P systems for DDoS attacks, *InfoScale '06: Proceedings of the 1st international conference on Scalable information systems.* New York, NY, USA.

Schinzel, S., 2005. *Security mechanisms of a legal peer-to-peer system*. Bachelor thesis, University of Applied Sciences in Darmstadt, http://www.colonwq.org/ download/thesis05.pdf.

Schmucker, M. et. al, 2005. Alternative Distribution Models based on P2P. *In Proceedings of 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution (AXMEDIS 2005): Virtual-Goods-Workshop*. Florence, Italy, December 2005. IEEE Press.

Schmucker, M. and Ebinger, P., 2005. Promotional and Commercial Content Distribution based on a Legal and Trusted P2P Framework. *In 7th International IEEE Conference on E-Commerce Technology*. München, Germany.

Steinebach, M. and Hassler, Ch. 2006. Discouraging File Sharing Piracy by Search Response, *4th International Workshop for Technical, Economic and Legal Aspects of Business Models for Virtual Goods*. Leeds, UK.

Sung , J. et. al, 2006. DRM Enabled P2P Architecture. *The 8th International Conference on Advanced Communication Technology (ICACT).* Korea.