SCIS 2003 The 2003 Symposium on
Cryptography and Information Security
Hamamatsu,Japan, Jan.26-29,2003
The Institute of Electronics,
Information and Communication Engineers

An Adaptive Authentication Protocol based on Reputation for Peer-to-Peer System

Hyunrok Lee * tank@icu.ac.kr

Kwangjo Kim * kkj@icu.ac.kr

Abstract— The services on the Internet were previously focused on the server-oriented system, but recently changed into a kind of distributed computing, peer-to-peer (simply P2P) systems which can be applied to instant messaging, collaborate computing, etc. Like a real face-to-face trust relationship, each peer with complicated trust relationship faced complex security problems. Especially, an authentication problem among peers will be an important issue. Although P2P network must not only provide pseudonymity but also satisfy strong authentication in case that a peer does business transaction with another one, most of current P2P services just adopt a weak authentication method using pseudonym and password. In this paper, we propose an Adaptive Authentication Protocol based on Reputation(AAPR) which can satisfy requirements ranging from pseudonymity to strong authentication based on certificate. Also we consider the context–dependent reputation concept and the minimization of certificate issuing cost by using different type of certificate under the concept of zero-dollar cost certificate if required.

Keywords: authentication, reputation system, peer-to-peer

1 Introduction

These days, the Internet exhibits three valuable characteristics. Compared with the environment of the Internet for previous years, it is rapidly growing in terms of the amount of information exchanged, the capacity of bandwidth and the power of computing resource. First of all, massive information is flowing via network. Second, the network bandwidth is increasing. Lastly, the power of computing resources are growing. So the Internet needs a new paradigm, that is different from existing one such as server oriented paradigm, which can handle three characteristics well.

A new peer-to-peer (simply P2P) system has been attracted a focus of public attention. The services on the Internet were previously focused on the server-oriented system, but recently changed into a kind of distributed computing, P2P systems which can be applied to instant messaging, collaborate computing, etc. SETI@home[23] have empowered millions of users to contribute their computing powers to work on a common computational analysis. An instant messaging services have enabled users to communicate and collaborate instantly with their peers on the Internet or the intranet. And a file sharing service embodied by applications like Napster[19], Gnutella[11], etc. has offered a compelling and intuitive way for the Internet users to find and share resources directly with others. A peer can have both client and server processes at the same time. The P2P computing[21] is direct sharing of computing resources and services between peers in arbitrary network. Such a P2P computing can be categorized largely into pure P2P and hybrid P2P[20]. The former is that all peers have the same capability and responsibility to build symmetric communications. The latter is that some servers can facilitate the interaction between the peers even if they perform the interaction directly.

Most of current P2P services have security problems which play an obstacle to practical use. Like a real face-to-face trust relationship, each peer which has a complicated trust relationship is entangled in complex security problems. Especially, an authentication problem among peers will be an important issue. Although P2P network must not only provide pseudonymity but also satisfy with strong authentication in case that a peer does business transaction with another one, most of current P2P services just adopt a weak authentication method using pseudonym and password[19, 15, 14, 18, 1] or does not support any authentication[23, 11, 8, 16]. Furthermore, the Groove Network[12] provides public key based strong authentication mechanism. However, this mechanism both needs a central server that provides directory service for retrieving user's public key every time and does not have a legal force that can control and settle a dispute. Even if Dietrich et al. [9] proposed a strong authentication mechanism and a reputation management for P2P system, they did not cope with server oriented paradigm and also did not support pseudonymity and minimizing the cost of issuing certificate.

Therefore, those are not suitable to serious P2P commercial transaction which can occur in the near future such as exchanging valuable information of knowledge,

* International Research center for Information Security (IRIS), Information and Communications Univ. (ICU), 58-4 Hwaam-dong, Yusong-gu, Daejeon, 305-732, Korea

applying e-commerce, etc. And also those do not satisfy requirements like pseudonymity which are required in trivial services.

In this paper, we propose an adaptive authentication protocol based on reputation(AAPR) which can satisfy requirements ranging from pseudonymity to strong authentication based on certificate without particular server. Also we consider the context–dependent reputation concept and minimizing the cost of issuing certificate due to use different type of certificate used under the concept of zero-dollar cost certificate if required. The zero-dollar cost certificate does not need a price which imposes the cost on issuing certificate by a legal Certificate Authority(CA) except for the cost of processing power which is necessary in the time for generating and signing certificate.

This paper is organized as follows: In Section 2, we briefly introduce the concept of P2P system including trust, a secure multicast technique for requesting information from arbitrary peers and previous works. Section 3 describes the requirements for P2P system authentication and proposed protocol. We compare authentication protocols in Section 4 and finally concluding remarks and future work will be made in Section 5.

2 Preliminaries

2.1 Related Works

2.1.1 P2P system and Trust

A P2P system is different from the traditional client-server model because the peers work as both clients and servers as stated before. While they can request information to other servers, they also simultaneously have performed the operation of servers and responded to requests for information from other clients. The value of network increases gradually as the number of joining peer grows because it not only takes resources and services from a source, but it also has the ability to share that resources and services with other sources. These resources and services include the transaction of payment, the exchange of information, the sharing processing cycles, the sharing files, etc. The P2P computing has an additional feature that is allowing systems to have temporary associations with one another; having groups of things come to join and be active for a while, and then separate.

Such a P2P system can be categorized largely into pure and hybrid P2P system. The pure P2P shares the data and the resource in equal condition without central server. It dynamically discovers other peers on arbitrary network and interacts with each of them for sending and receiving content. Gnutella[11] and Freenet[10] are typical examples. On the other hand, the hybrid P2P has a central server which has a role about controlling and mediating the peers, but the peers communicate directly each other. Napster[19] is a well-known example of hybrid P2P.

In order to protect "the tragedy of the commons"[13] that also can be applied in digital resources, the authors [7] suggested how the accountability can be achieved by utilizing micropayments and reputations in P2P systems. Accountability measures based on micropayments require that each party offer something of value in exchanging information. Such micropayments can be categorized into nonfungible and fungible micropayments. The former does not purchase a real price, however it pays a proof of work(POW), showing that a peer performed some computationally difficult problem; a price via processing in other words. The latter uses commonly a digital cash which can offer a real cash in an exchange. Both of these schemes may be used to protect against resource allocation attacks. For selecting a trustworthy peer, the P2P systems can employ the concept of reputation to ensuring accountability. The advantage of applying the concept of reputation in authentication is to avoid dangerous peer and punish/reward via network. The previous proposal[2]show how reputations and trusts can be adopted in virtual communities which is like P2P communities. Moreover, the JXTA[4] which is to establish such a decentralized trust model and to build a recommendation system from SUN Microsystems and a white paper[17] from OpenPrivacy.org provides a P2P framework for building intercommunicating systems using opinion accumulation based on the concept of reputation. But these works related in reputation concept take an initial step for designing system.

2.1.2 Secure multicasting

Canetti et al.[5] presented solutions to the authentication problem based on Message Authentication Code (MAC) with shared key mechanism which can be regarded as middle–solution between traditional MAC and digital signature. This multicast authentication scheme for a single source can be adopted effectively into transmitting recommendation messages from a peer requester to other peer who has connected in the same community with the set of keys.

2.2 Previous Works

In this subsection, we describe various authentication mechanisms for using P2P system till now. But we ignore some typical P2P services such as [10, 6, 24] in here because those services concentrate on providing anonymous publishing called as censorship–resistant publishing system not authentication mechanism.

There are a number of well-known products available that permit insecure file and resource sharing in P2P. Gnutella[11], which is famous in audio file sharing, identifies a peer with IP address and pseudonym. Kazza[16] and e–Donkey[8] are a software program for sharing any files by identifying each other with their pseudonyms. SETI@Home[23] is typical example of CPU sharing system that also uses pseudonym and IP address for processing the signal.

Napster[19]–like services allow peers to use a central discovery and lookup server to find the location of audio files that can directly be downloaded from other peers. In Napster, weak authentication is supported by user's pseudonym and password. Instant messengers[15, 14, 18, 1],that are widely spread for direct communication on the Internet, also use the password–based authentication.

To provide strong authentication, called challenge–response authentication scheme is utilized into P2P system. The authentication of Groove[12] has two different purposes. One is that their scheme binds users to their electronic identities, and the other is that link actions; such as modification to file, chat message and keystroke to electronic identities. In order to maintain multiple keys, the public/private key pairs are encapsulated in XML tag. The authors of FL02[9] proposed a solution of strong authentication based on reputation management system with PKI. They consider context–dependent feedback gathered in questionnaires.

As mentioned before, current P2P services apply three types for authentication. But all of those authentication mechanisms cannot satisfy various services from file sharing to electronic commerce(EC), also cannot provide the concept of reputation to ensure accountability among peers. Therefore, P2P system needs an adaptive authentication protocol which can accept various services and adopt the concept of reputation.

To the best of our knowledge, there is no relevant authentication mechanism which satisfies considering reputation, providing pseudonymity, guaranteeing strong authentication and minimizing the cost of issuing certificate. So we propose an authentication protocol in the next Section.

3 Proposed Scheme

3.1 Requirements

The requirements of authentication protocol in P2P systems satisfied from pseudonymity to strong authentication to be listed as follows:

R1. *Pseudonymity* : The purpose of most P2P system is that a peer can easily subscribe, leave and access contents. In a trivial information transaction, a peer might want to hide their information with pseudonym. So authentication for P2P must satisfy this requirement.

R2. *Strong authentication*: The authentication between each peer must provide cryptographically strong mechanism to support commercial transaction. It must protect transaction between peers from possible attack, such as man-in-the-middle attack.

R3. *Reputation* : To ensure accountability on P2P network, the concept of reputation must be installed.

R4. *Community authenticity* : Each community member can recognize whether a message was sent by a community member.

R5. *Guarantee* : After executing serious commercial transaction between peers, this transaction can be pending in the court if it was wrong. So the requirement of a legal force that can control and settle a dispute is required. It can be achieved by a formal certificate that is guaranteed by legal CA.

R6. *Flexibility* : It is possible to easily adopt into any P2P systems either pure or hybrid system.

R7. *Cost effectiveness* : The formal certificate issued by CA needs the issuing cost. If a peer is enough to trust like family, we can request only self-signed certificate. This self-signed certificate need not extra cost.

3.2 Our Scheme

The first step of our scheme is to start negotiation to decide selective property such that pseudonymity or strong authentication. For supporting the decision of selective condition, the extra message field is required. This field can contain two types of operation that satisfy conditions. And then it proceeds to the next step of protocol according to the above selective condition. This step consists of two protocols;*Guest* and *Member protocol*. In *Guest protocol*, strong authentication scheme is ignored in order to support pseudonymity that is possible through Gnutella–like authentication using pseudonym. In *Member protocol*, the strong mutual authentication will be executed based on the result of trust value calculation. By using trust value, we can select the relevant certificate. Detailed operation of our scheme will be described in *protocol actions*.

The protocol of the proposed scheme works as follows:

Protocol. ***Adaptive Authentication Protocol based on Reputation*** **(AAPR)**

SUMMARY : A peer α sends a peer β one message that include extra selective field and β responds along the property of the selective field. After β requests recommendation to the remaining peers in the same community, the remaining peers respond recommendation results. Then β calculates the trust value of α from received recommendations. Using variant certificate appropriate for the trust value, authentication and key establishment are performed. After α and β finish the communication, α and β adjust their trust value respectively.

RESULT : (According to user's choice)

1. The pseudonym–based weak authentication between peers.

2. Mutually strong peer authentication and time-variant session key transport with key authentication using different source of certificate based on trustworthy.

Notation.
The notations of our scheme are summarized in Table 1.

System setup.

1. A peer chooses given two operations which is a value of selective fields; sel_G or sel_M.

Table 1: Notations

x	peer(identity) $x \in \{\alpha, \beta, \Gamma\}$, where $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$, $\gamma_i \neq \alpha$ and $\gamma_i \neq \beta$ for $i = 1, 2, \ldots, n$.
$x \rightarrow y$	x sends one message to y or Y.
$P_x(m)$	x's public key encryption to message m.
$S_x(m)$	x's private key signature to message m.
r_x	random numbers of x.
K_x	x's session key.
CK	set of community keys, where $CK = \{CK_1, CK_2, \ldots, CK_l\}$.
CK_x	x's subset of $CK \equiv CK_x \subset CK$.
$MAC(CK, m)$	keyed Message Authentication Code.
$cert_x$	x's certificate.
F_{cert}	formal certificate issued by legal CA.
I_{cert}	informal certificate issued by service provider or super peer node.
S_{cert}	self-signed certificate.
$V_{\{cert_x\}}$	selected x's certificate.
sel_G	selective message for *Guest protocol*.
sel_M	selective message for *Member protocol*.
$permit_x$	allow x to communicate with pseudonym–based authentication.
$refuse$	refuse communication.
$req_{\{m\}}$	request the message m.
C_{BT}	critical business transaction.
R_i	the range of trust, where $R_{min} \leq R_i \leq R_{max}$, for $i = 1, 2, \ldots, n$ $R_{min} = R_1$ =total distrust, $R_{max} = R_n$ =complete trust.
V_i	trust value, where $0 \leq V_i \leq 1$ for $i = 1, 2, \ldots, n$.
W_C	weight factor of category, where $0 \leq W_C \leq 1$.
$\overrightarrow{T_x}$	the vector of trust value of x $(requestor\ ID, category, target\ ID, V_i)$.
$\overrightarrow{T_{x,\gamma_i}}$	$\overrightarrow{T_x}$ from $\gamma_i \in \Gamma$ for $i = 1, 2, \ldots, n$.
$com(x)$	calculated total trust value of x.

2. Each peer has its public/private key pair for encryption and signature.

3. Existing peers on same community share their key previously.

4. Each peer has the trust value of others within specific category(context).

5. Each peer has own initial weight factor of inclination toward optimistic, intermediate or pessimistic. This factor is used for initiating relationship with new peer.

6. Each peer has the table of recommendation for others. It consists of category(context), the weight factor of category(W_C) and recommendation vector as shown in Table 2.

Protocol messages.

- ***Guest protocol:***

$$\alpha \rightarrow \beta : sel_G, \alpha \tag{1}$$

Table 2: Example of recommendation table

Category (Context)	Weight (W_C)	Recommendation vector {(trust value, target ID), ...}
MP3FileRead	1.0	{(0.9, Lee), (1.0, Kim), ...}
MP3FileWrite	0.8	{(0.8, Bob), (0.95, Alice), ...}
...	...	....

$$\beta \rightarrow \alpha : permit_\alpha \tag{2}$$

- ***Member protocol:***

$$\alpha \rightarrow \beta : sel_M, \alpha \tag{3}$$

$$\beta \rightarrow \Gamma : req_{\{\overrightarrow{T_\alpha}\}} | \left[MAC(CK_\beta, req_{\{\overrightarrow{T_\alpha}\}}) \right] \tag{4}$$

$$\Gamma \rightarrow \beta : \quad \overrightarrow{T_{\alpha,\gamma_i}} | \left[MAC(CK_{\gamma_i}, \overrightarrow{T_{\alpha,\gamma_i}}) \right] \tag{5}$$

$$\beta : \quad \textit{Computing trust} \text{ at (13).} \tag{6}$$

$$\begin{array}{rlrl} \beta \rightarrow \alpha : refuse & \text{if} & & com(\alpha) \leq R_1 \quad (7) \\ req_{\{F_{cert}\}} & \text{if} & R_1 < & com(\alpha) \leq R_2 \text{ or } C_{BT} \\ req_{\{I_{cert}\}} & \text{if} & R_2 < & com(\alpha) \leq R_3 \\ req_{\{S_{cert}\}} & \text{if} & R_3 < & com(\alpha) \leq R_4 \end{array}$$

Let $D_\alpha = (r_\alpha, \beta, P_\beta(K_\alpha)), D_\beta = (r_\beta, \alpha, r_\alpha, P_\alpha(K_\beta))$.

$$\alpha \rightarrow \beta : \quad V_{\{cert_\alpha\}}, D_\alpha, S_\alpha(D_\alpha) \tag{8}$$

$$\beta \rightarrow \alpha : \quad V_{\{cert_\beta\}}, D_\beta, S_b(D_\beta) \tag{9}$$

$$\alpha \rightarrow \beta : \quad (r_\beta, \beta), S_\alpha(r_\beta, \beta) \tag{10}$$

$$\alpha, \beta : \quad \textit{Adjusting trust value} \tag{11}$$

Computing trust.
In order to calculate total trust value of a target peer, we have adopted and modified the probabilistic computing method used in [3]. But any computing method can be applied into our scheme to support flexibility. R_{max}, which can be expanded to any range, the maximum trust value means that β trusts α completely. If a peer can define the range, such as selecting from bad, middle and good, then the value of R_{max} is 3.

- Simple model
  Let the recommendation(indirect) trust value is V_1 where $\alpha \Rightarrow \ldots \Rightarrow \gamma_1$ ($\Rightarrow$: indirect trust), and the direct trust value is V_2 where $\gamma_1 \rightarrow \beta$ ($\rightarrow$: direct trust). Then, the trust value of $\alpha \Rightarrow \ldots \Rightarrow \gamma_1 \rightarrow \beta$ with considering the weight factor of category W_c is

  $$com(\alpha) = R_{max} \cdot \left\{ 1 - (1 - W_C \cdot V_2)^{W_C \cdot V_1} \right\} \tag{12}$$

- Generalized model
  When a peer requests recommendation to others, multiple recommendation for single target peer can be arrived. All direct and indirect recommendations in same category have to combine in one value. If for each $1 \leq i \leq m$, there are n_i distinct paths from α to β with edge $\gamma_i \rightarrow \beta$, with

direct trust values $V_{i,1}, \ldots, V_{i,n_i}$, then combined total trust value with W_C is

$$com(\alpha) = R_{max} \cdot \left\{ (1 - \prod_{i=1}^{m} \sqrt[n_i]{\prod_{j=1}^{n_i} (1 - W_C \cdot V_{i,j})} \right\} \tag{13}$$

Protocol actions.
A peer who wants to connect with other peer select initial field from given two operation sel_G and sel_M for negotiate to decide *Guest* or *Member protocol* such that satisfies the following conditions: "strong authentication is not required or required". If an initiator peer α chooses sel_G and sends identifier α in step (1), then β sends $permit_\alpha$ in step (2). And then α and β can communicate with each other. However, it does not influence their reputations.

If an initiator peer α chooses sel_M and sends identifier in step (3), then β requests context–dependent trust vector of α to Γ in same community on step (4). After β receives the trust vector from Γ at step (5), β performs the calculation of trust value in step (6). β determines which certificate is required. And it can request appropriate certificate or refuse all communication in step (7). If $com(\alpha) \leq R_1$ which means total trust value of α less than the degree of total distrust, then β refuses all communication. If $R_1 < com(\alpha) \leq R_2$ or C_{BT} message enabled by β, β cannot trust α and so requests a formal certificate issued by legal CA. $R_2 < com(\alpha) \leq R_3$ means that β has a middle trustworthy to α. β requests informal certificate which is issued from super peer node or control server. The super peer means the leader peer of the community, and the control server represents a kind of server which is managed by a specific P2P service provider. When the trust value meets a condition like $R_3 < com(\alpha) \leq R_4$, β trusts sufficiently α like trust relationship between family. So β requests self-signed certificate to α. Of course, the range of trust value from R_1 to R_4 can be decided by β.

Before step (8), the peer α generates random number r_α and obtains a session key K_α, and then sends $V_{\{cert_\alpha\}}$,D_α and $S_\alpha(D_\alpha)$ to β. The peer β verifies the authenticity of $V_{\{cert_\alpha\}}$, extracts α's signature public key, and verifies α's signature on the data D_α. β then checks the identifier and r_α in message of step (8). Then β also generates r_β and sends message of step (9) to α. The peer α carries out actions analogous to those carried out by β. If all checks succeed, α declares the authentication of β successful, sends message of step (10) for verification, and saves key K_β. After receiving the message, β verifies it. If all checks are passed, β declares the authentication of α to be successful, decrypts K_α using its private key, and saves this shared key. Now α and β communicate with each other using session–key.

After completing all communication between α and β, they adjust their trust value respectively. Finally, they insert the trust value of other party into their recommendation table.

4 Comparison

In this Section, we compare AAPR with others. The comparison is performed whether satisfy the requirements from *R1* to *R7* for P2P authentication or not.

A challenge–response strong authentication based on certificate, which is self–signed or trusted introducer–signed who has no legal force, is provided by using directly PGP[25] in P2P authentication. And it can be easily adopted in any P2P system because of its flexible trust model called "web of trust". So, this scheme supports *R2*, *R6* and *R7*, but does not support *R4* and *R5*. And it partially support *R1* and *R3* because of following two reasons. First, if peer can register different e–mail address, then he can manipulate the key pairs that is generated from an identifier(like pseudonym) and e-mail address of peer. Second, to build a key–ring for trust, the trusted PGP users introduce others but it provides only restrict reputation mechanism.

We can apply directly into existing P2P system that the authentication can utilize PKI[22] which the certificate is issued by a legal trustworthy CA. This scheme satisfies *R2* and *R5*. However, the restrict properties like satisfying legal force, existing TTP(Trusted Third Party), paying cost for issuing formal certificate, etc. is the reason that PKI cannot support *R1*, *R3*, *R4*, *R6* and *R7*.

Four requirements(*R2*, *R4*, *R6*, *R7*) are provided with the attributes of Groove network. Because this system support rigorous authentication in specific network for the environment of collaborating work, it does not achieve *R1*. Also this system neither has legal force nor the concept of reputation. So, two requirements(*R3*, *R5*) is not accomplished.

Although the FL02 is designed originally for P2P system with the concept of reputation, it just satisfy two requirements(*R2*, *R3*).

Our proposed scheme supports all requirements: *R1* is achieved by using selective field which can permit restrict power in *Guest protocol*. If a critical business occurs or not enough to trust a peer, we request formal certificate to the peer(*R5*). Our scheme provides certificate–based strong authentication(*R2*), so we meet security from possible attacks like replay, man–in–the middle attack, etc. *R4* is accomplished by using secure multicasting mechanism. Nevertheless our scheme does not need particular server, it can perform well with any server. Because a hybrid P2P is subset of a pure P2P(*R6*). We adopt the concept of reputation to choose safe peer(*R3*) and use variant certificate to minimize the cost of certificate(*R7*). The result of comparison is summarized in Table 3. In this table, symbols : ◯, △ and × that means the degree of supporting the component of requirements by each corresponding scheme : support, partially support and no support, respectively.

5 Concluding Remarks and Future Work

The P2P computing can be applied to large scale network for sharing information and resource over a network, which has never seen before. Although this

Table 3: The comparison of authentication for P2P

	PGP	PKI	Groove[12]	FL02[9]	AAPR
R1	△	×	×	×	○
R2	○	○	○	○	○
R3	△	×	×	○	○
R4	×	×	○	×	○
R5	×	○	×	×	○
R6	○	×	○	×	○
R7	○	×	○	×	○

enables rapid progress because of its pseudonymity, the lack of security of P2P system makes them less attractive. As well there is no mutual authentication protocol considering pseudonymity, the concept of reputation and the effectiveness of certificate issuing cost. Hence, we proposed an adaptive authentication protocol based on reputation for P2P system that satisfies the requirements. Moreover, we also consider the context–dependent reputation concept for ensuring accountability and propose briefly the method of computing trust among peers that present the way to select variant certificate from a standard certificate issued by legal CA to a flexible self-signed certificate issued by peer itself. We can conclude that our scheme may solve most of the authentication problems in any type of P2P systems which can be either pure or hybrid one.

In order to enhance our scheme, the part of trust measurement and calculation must be extended to be more formalized and defined. And also bootstrapping which called as the first initial step of trust relationship is one of open problems.

References

[1] American Online Instant Messenger Homepage, *http://www.aim.com/.*

[2] A.Abdul–Rahman and S.Hailes, "Supporting Trust in Virtual Communities", *Proc. of IEEE the Hawaii International Conference on System Sciences*, January, 2000.

[3] T.Beth, M.Borcherding and B.Klein, "Valuation of Trust in Open Networks", *Proc. of ESORICS '94*, LNCS 875, pp.3–18, Springer–Verlag, 1994.

[4] R.Chen and W.Yeager, "Poblano: A Distributed Trust Model for Peer-to-Peer Networks", *http://www.jxta.org/project/www/docs/trust.pdf*, Sun Microsystems, 2002.

[5] R.Canetti, J.Garay, G.Itkis, D.Micciancio, M.Naor and B.Pinkas, "Multicast Security: A Taxonomy and Some Efficient Constructions", *Proc. of IEEE INFOCOM'99*, vol. 2, pp. 708–716, New York, NY, March 1999.

[6] R.Dingledine, M.J.Freedman and D.Molnar, "The Free Haven Project: Distributed Anonymous Storage Service", *Proc. of the Workshop on Design Issues in Anonymity and Unobservability*, LNCS 2009, July 2000.

[7] R.Dingledine, M.Freedman and D.Molnar, "Accountability", *Peer-to-Peer: Harnessing the Power of Distruptive Technologies*, Chap.16, pp.271–340, O'REILLY Press, 2001.

[8] e-Donkey Homepage, *http://www.edonkey2000.com*

[9] D. Fahrenholtz and W. Lamersdorf, "Transactional Security for a Distributed Reputation Management System", *EC-Web '02*, LNCS 2455, pp.214–223, Springer-Verlag, 2002.

[10] Free Network Project Homepage, *http://freenet.sourceforge.net/*

[11] Gnutella Homepage, *http://gnutella.wego.com/.*

[12] Groove Networks, "A White paper: Groove Security Architecture", October 2002, *http://www.groove.net/products/workspace/security.html.*

[13] Garrett Hardin, "The Tragedy of the Commons", *Science* 162, pp.1243–1248, 1968.

[14] ICQ.Com Homepage, *http://web.icq.com/.*

[15] Jabber Software Foundation Homepage, *http://www.jabber.org/.*

[16] KaZaA Homepage, *http://www.kazaa.com/*

[17] F.Labalme and K.Burton, "Enhancing the Internet with Reputations : OpenPrivacy white paper", 2002, *http://www.openprivacy.org/papers/200103-white.html.*

[18] Microsoft Network Messenger Homepage, *http://messenger.msn.com/.*

[19] Napster Homepage, *http://www.napster.com.*

[20] L. Olson, ".NET P2P:Writing Peer-to-Peer Networked Apps with the Microsoft .NET Framework", *MSDN Magazine*, Feb, 2001.

[21] Peer-to-peer working group, "What is peer-to-peer?", *http://www.p2pwg.org/whatis/index.html.*

[22] R.Perlman, "An Overview of PKI Trust Models", *IEEE Network Magazine*, pp.38–43, Nov/Dec, 1999.

[23] SETI@Home:The Search for Extraterrestrial Intelligence at Home, *http://setiathome.berkeley.edu/.*

[24] M.Waldman, A.D.Rubin and L.F.Cranor, "Publius: A robust, tamper-evident, censorship-resistant, web publishing system", *Proc. of 9th USENIX Security Symposium*, pp.59–72, august, 2000.

[25] P.Zimmermann, "PGP 7.0 User's Guide", *http://www.pgpi.org/doc/guide/7.0/.*