ANONYMITY AND ACCOUNTABILITY IN WEB BASED TRANSACTIONS

H.Jayasree[1] Dr. A.Damodaram[2]

[1]Assoc. Prof, Dept. of IT,ATRI,Hyderabad.
jayahsree@yahoo.com
[2]Director - SCDE & Prof. of CSE Dept,JNTUH,Hyderabad.
damodaramaa@jntu.ac.in

ABSTRACT

Decreased privacy is an unavoidable consequence in the drive to make the world a more secure, safer place, according to some analysts. In the on-line world, the conflict between privacy and security manifests itself in a debate between anonymity and accountability. Balance between Anonymity and Accountability is a major concern in web based transactions. The protection of users' privacy when performing web-based transactions is an important factor in the acceptance and use of Internet and web services. There is a tremendous improvement in the automation of the way we pay for goods and services by the variety and growth of electronic banking services available to the consumers. Hence there is a need for the ultimate structure of the new electronic transaction system that has a substantial impact on the personal privacy as well as on the nature and extent of criminal use of E- transactions. This paper presents an approach for such structure.

KEYWORDS

anonymity, accountability, credential system, privacy, security, pseudonyms

1 INTRODUCTION

Anonymity and accountability are supposedly opposing factions in a zero-sum game between privacy and security. Conventional wisdom holds that decreasing anonymity (less privacy) is proportional to increasing accountability (more security). However, as Bruce Schneier, states,
"If you set up the false dichotomy, of course people will choose security over privacy -- especially if you scare them first. But it's still a false dichotomy. There is no security without privacy."
In a similar vein, this document looks at the anonymity "versus" accountability and asserts that both characteristics can and must exist side-by-side in the on-line environment. Neither is enough on its own; and no person or organization should have to make a choice to use only one or the other.

Rapid development of Internet technologies increases the use of this unique medium for collaboration. Efforts to provide interoperability focus mainly on enabling collaboration and privacy protection. Nevertheless, reputation management and accountability are also in demand. Recently, several works have emerged that address these latter problems (see [41, 39, 42, 32, 36, 43,44] for representative examples). In this paper we focus on issues related to anonymity. We argue that total anonymity and unlinkability may lead to increased misuse by anonymous users. Furthermore, profit or reward driven applications cannot be maintained without the users being responsible for their actions. Accountable anonymity, ensuring that a virtual user's real identity cannot be disclosed unnecessarily, is in need.

DOI : 10.5121/acij.2012.3217

Current technologies that provide full anonymity lack accountability, thus the possibility of misuse and the lack of controllability exist. Clearly, there is a trade-off between anonymity and controllability; however, there is a set of applications, where these contradictory concepts are both needed. One example is the co-operation between clinical practitioners, who would need to share *some* of their patients' data. These data accesses may be governed by particular requirements, like *(i)* Personal data of the patient can not be disclosed and *(ii)* personal data of the person who has access to the personal data of a patient can not be disclosed. Works presented by [44, 45, 22, 19] are the closest to ours in that they address the problem of accountable anonymity. However, their solutions are based on fully trusted mediators (e.g., certificate authority, customer care agency, etc.), thus increasing the possibility of abuse if this mediator is compromised. Furthermore, they only provide one layer of anonymity in which the need to validate

whether two virtual entities belong to the same real user (i.e., they are linked) requires the disclosure of the real user's identity. Finally, they do not allow users to monitor their personal data or terminate their personal records if they do not want to participate in a given community any longer. We believe that providing these features would increase the confidence in the privacy protection provided by a system. In our example provided above, protection of the patient is targeted.

Anonymous communication systems have been studied extensively since David Chaum introduced the mix in 1981 [6]. Their principal aim is to hide the fact that Alice is communicating with Bob from network adversaries or corrupt nodes in the anonymity-providing system. Practical anonymous communication systems have been proposed for email [9, 8] and web-browsing [5, 15]. They are based on intermediate nodes relaying the communication and hiding the correspondences between their inputs and outputs to obscure who is talking with whom. An extensive survey of anonymous communication channels and their properties is provided in [7].

2 BACKGROUND

2.1. Anonymity

Anonymity refers to the absence of identifying information associated with an interaction. On-line interactions can facilitate both more and less anonymity than those carried out in the physical world. Interpersonal transactions across the Internet allow greater anonymity at one level, but there is often an identifying data trail left by the Internet user. Such data can include names, date-of-birth, credit card numbers, mailing addresses and buying patterns.

2.2. Accountability

An action is accountable if it can be attributed to someone (or something – such as a service provider – in this context). Accountability on the Internet is made possible by technical attributability. For example, associating a name/identifier to an IP address means that anyone sending malicious content from that location can be traced to that address. This is useful, since a lack of accountability generally means a lack of incentive against bad behavior.

2.3 Motivation for Communication Anonymity

Anonymity is defined by Pitzmann and Hansen in [23] as the" state of being not identifiable within a set of subjects, the anonymity set". This definition implies that, in order to achieve anonymity, we need a large population of users (anonymity set) performing actions in such a way that it is not possible to know which action was performed by which user. Users are more anonymous as the anonymity set and the indistinguishability increase (see [12, 26] for practical anonymity metrics). According to Moore's Law, computer processing power doubles every 18months. Storage capacity grows even faster, doubling every 13 months, according to Kryder's Law. If no anonymity infrastructure is put in place, all communication can (or will soon) be traced, registered, stored, mined, analyzed and aggregated.

Individuals lose control over their personal data, which implies that they become vulnerable to all kinds of commercial and political manipulation. It is also clear that the large amounts of information available on individuals could be exploited for criminal purposes such as identity theft or targeted crime (e.g., it would be useful for burglars to know who are the wealthiest home-owners in a given area and when they are going on holiday). Privacy should therefore not be considered as contradictory with security: the lack of privacy protection may lead to serious security problems. Moreover, privacy protection is only possible using secure systems. In order to avoid these privacy violations, we need to hide the communication patterns of Internet users towards untrusted recipients (e.g., web sites) and external observers (e.g., local eavesdroppers). An anonymous communication infrastructure should therefore be in place in order to protect users' privacy.

2.4 Motivation for Accountability

If a system is deployed for massive use, abuse is unavoidable; moreover, the sense of impunity generated by the impossibility of holding people accountable could further encourage abuse. Without *accountability* mechanisms in place, it is unlikely that an unaccountable system could gather support from public powers and even from many citizens, as security has to be traded with privacy (or, at least, that is a common perception).

Nevertheless, there are strong arguments against trading anonymity with accountability [1]. As we can derive from the definition of anonymity, there is a fundamental difference in the nature of confidentiality and anonymity in communication networks. Confidentiality of the content can be achieved by the communicating partners on their own: when establishing a shared secret, no third entity needs to participate. Even more, one could create a key for encrypting one's own data, without needing external entities. Anonymity is more complex. People act anonymously when their actions cannot be linked to their identities, or more precisely, when there is a set of subjects that could potentially be linked to the action, but there is not enough information to tell which of the subjects relates to the action. While confidentiality can be achieved by those who seek it alone, anonymity needs the cooperation of a group of people, the larger the better. Anonymity is therefore social (as it needs society to work together in order to be achieved), while confidentiality makes sense at the individual level. While criminals would be able to bridge the key escrow systems using their own keys, they are not able to obtain anonymity on their own. If accountability mechanisms are built in the system, then the potential for abuse sharply decreases. Criminals may then choose not to use the system (exposing themselves to leave traces), or choose an unconditionally anonymous network. If this is the case, the people operating the network may find themselves in trouble, depending on the seriousness of the crime and on the legal framework in which they are operating..

2.5 Related Work on Anonymous Communication

Some of the earliest real-time *anonymous communication* systems were based on trusted or semi-trusted relays (e.g., Anonymizer [2] and SafeWeb). In centralized trust systems, the anonymity depends critically both on the security level and on the integrity of the service provider and its staff. Pitzmann et al. proposed in 1991 ISDN Mixes [24], a system to anonymize ISDN telephone conversations. Their design, based on a cascade of relays (mixes), was later adapted for anonymous web browsing and called Web Mixes [3]. A shortcoming of cascade topologies is that they require less effort for attacker to monitor the entry and exit point of the anonymity system. Part of the design has been implemented as a web anonymizing proxy, JAP. The use of multiple intermediate relays between the two ends of the communication improves the trust distribution over the use of a single relay, provided that if some of the relays are honest, the anonymity of the user remains protected. On the other hand, the cascade topology does not have good scalability and availability properties. The JAP design did not consider mechanisms for anonymity revocation; however, upon a law enforcement request for identification of a particular user, an exception had to be made in order to comply with the request.

Onion Routing [16, 17, 25, 27] is a free route mix network topology for unconditionally anonymous communication. Free route mix networks are vulnerable to intersection attacks [4]. The users establish circuits through a number of onion routers of their choice, and distribute symmetric keys to those routers. Data traveling in an established circuit is encrypted in layers, using the symmetric keys distributed to the routers. Tor (*The Onion Router*) [14], an improved second generation of Onion Routing, was proposed and implemented in 2004 (available at http://tor.eff.org/). Two years after deployment, it counts hundreds of volunteer nodes and hundreds of thousands of users, making it a very successful anonymous communication network. Claessens et al. propose in [10] a system for revocable anonymous communication based on blind signatures. They introduce the legal requirements relevant for (revocable) anonymous communication and present a proof-of-concept architecture. Von Ahn et al. [29] propose transformations to add selective traceability to anonymous systems based on threshold cryptography and group signatures. Kopsell et al. [21] proposed a revocable anonymity system based on threshold group signatures and threshold atomic proxy reencryption. All practical low latency anonymous communication systems are vulnerable to adversaries capable of monitoring the entry and exit points: high speed and high volume traffic patterns are too distinct in each connection, making it difficult to hide the correlation of the traffic going in and out [18]. End-to-end full padding solves this problem, but its deployment is very expensive. Whether intermediate solutions, using some cover traffic, can effectively hide the communication patterns, remains an open problem. Also, if all nodes in the anonymous communication path are corrupted by the adversary, then the communication is traceable.

3 REQUIREMENTS

The system should comply with a basic set of requirements (see [13] for more details) which include:

- Application-independence: it should provide a general purpose low-latency bidirectional communication layer.
- Secure anonymity: untraceability of communication (i.e., the path connecting the communication parties is hard to discover), unlinkability of sessions (i.e., from an adversary's point of view, it is hard to link two sessions as related to the same user), load balancing mechanism’s; secure implementation, usability and robustness against attacks.
- Availability: resistance against denial of service attacks and a sufficient number of entry and exit points.
- Scalability: the system must be able to provide service to large numbers of users.

The second set of requirements are an attempt to balance the fundamental right to privacy and the accountability mechanisms needed to make the system acceptable for the public at large and usable at a large scale. Claessens et al. define a complementary set of requirements in [10], where the legal point of view on anonymity and accountability for communication networks is presented.

- *Default privacy protection.* The system must be designed to protect by default the privacy of the users by anonymizing the communication layer. A user remains anonymous unless a judge issues a warrant that demands his identification.

- *Accountability.* The communication system must implement mechanisms that allow for law enforcement, called *identification* and *investigation*. Two types of actions may be considered. First, mechanisms should exist to identify subjects involved in criminal activities acting through the anonymous system (*post factum*). Second, law enforcement agents should be able to conduct investigations of criminal networks (e.g., money laundering), that is, tracing of the communication of a user under criminal investigation.
- *Transparency.* Clear and public policies and contracts that define rights, obligations and liabilities of all parties, as well as the activities that may lead to identification, discourage abuse in the first place.
- *Trust Distribution* is one of the key aspects of the design of the system. In order to be accepted by all entities, the system must be trusted to provide anonymity for honest users, as well as transparent accountability mechanisms for those who abuse the system for criminal purposes. Trust should be distributed, in order to minimize the possibility of a collusion of entities illegally tracing or identifying a user.
- *Identity management at the user's side.* In order to empower the user in the management of his own identities, all the identity and profile information should be kept under the user's control. Users who wish to obtain personalized services may provide the preferences to their service provider without disclosing their identity (e.g., [11, 20]). Service providers may collect the anonymized data generated by the users' transactions, but they will not be able to link the behavioral data to an identifiable individual, neither to link the user's local pseudonym to other organizations' databases.

4 ANONYMOUS COMMUNICATION INFRASTRUCTURE

In order to deploy secure anonymous applications (such as e-voting, anonymous help lines or censorship-free access to information) and privacy enhanced context for user activities in the Internet, an anonymous communication infrastructure is required. If anonymous or privacy-enhanced applications are implemented on top of a non-anonymous communication layer, then most (if not all) efforts at the application layer aimed at protecting the privacy of individuals are useless, as the weaker link for the attacks on privacy and anonymity will be the communication infrastructure. The impact of this weakness may not be underestimated, as fundamental rights (such as freedom of speech or free access to information) are at stake for millions of people living under repressive regimes. By means of anonymous infrastructures and applications, the Internet may become a space of freedom for people whose rights are not respected. Granting access to information resources to developing countries may also enhance mutual understanding between different cultures. It is also worth noting that, in order to prevent segregation of (and possibly reprisals on) a small group of people who make use of anonymous services (the usual suspects), and in order to support the wide deployment of privacy enhanced applications, the critical mass of people using this infrastructure should be the largest possible (ideally, anonymity should be the default for the Internet communication layer). Authenticated, pseudonymous and/or conditional anonymous services can be implemented on top of an anonymous infrastructure, as higher layer authentication protocols may establish the identity of the users (e.g., by means of credentials). Some applications, namely those involving commercial transactions, have a stronger potential of misuse. For these cases, it is necessary to implement controls on the anonymity (within the e-commerce application) in order to prevent fraud.

4.1 Model

In the model, we consider an anonymous communication infrastructure that may be composed of a set of mix servers or may be a peer-to-peer network. Applications would tunnel their communication through this anonymous communication infrastructure. The entry and exit points of this network may be normal nodes or specific nodes. We consider two types of control blocks at two different levels. The first 35 level is the entity level. Mixes or peers can implement control blocks. The second level considers the infrastructure as a whole. The control blocks are in this case placed at the entry and/or exit points of the anonymous network. The two types of controls are access control blocks and exit policy blocks. Access control blocks are placed at the entry of the system. If the access control block is implemented by all entities of the network, then every node of the system will check before accepting a connection. If the access control is done only at the entry of the anonymous network, then only the first node in the network (the access point) will have to check access rights. Note that these access control blocks may be heterogeneous in the network. It may be required that they comply with the legal framework of the country in which the nodes that implement them operate. A similar reasoning applies to exit policies. Exit policies can be implemented either only by the nodes that are exit points of the network (e.g., black lists of web sites) or at every node, even those who act as intermediate hops (e.g., if the topology is that of a restricted route network, the exit policies would determine to which other nodes it connects). Exit policies may also comply with the local legal requirements.

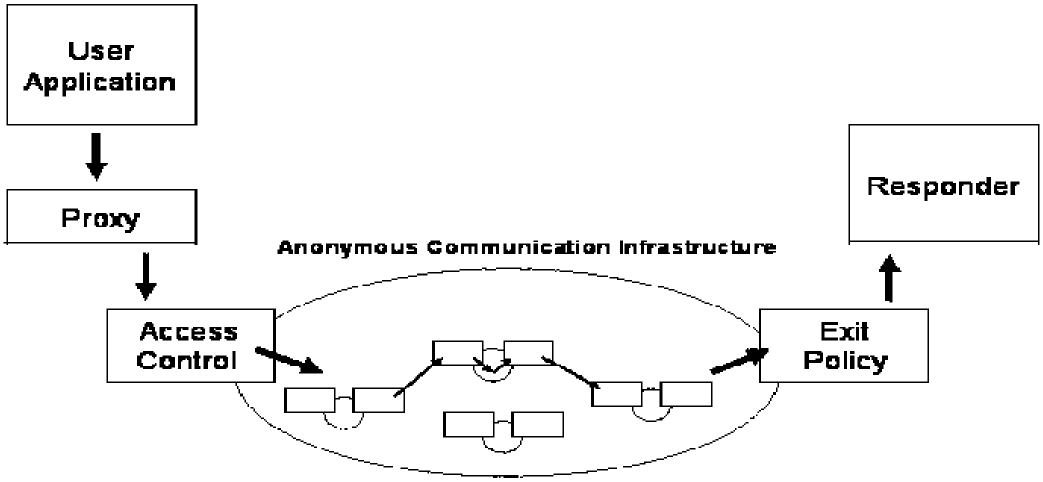

Figure: model

The anonymous communication infrastructure is composed by a network of mix servers or peers. Each of these entities may or may not implement control blocks. On a higher level of abstraction, the anonymous communication network may implement control blocks in its entry and exit points. The user's applications may connect to this anonymous infrastructure through a proxy.

4.2 Control blocks

The two control blocks that are considered in the model are access control and exit policies. These control blocks should not impose a significant overhead for the users. Here we detail some examples of access control and exit policy mechanisms. More research is needed in order to determine the most appropriate controls for such an infrastructure. This choice is also conditioned by the sort of anonymous network that is to be designed and its goals. One possibility would be that mixes offer a paid service. Users could pay for a connection with e-cash micropayments. This technique has the advantage of double spending detection, a mechanism that reveals the identity of a user when he spends twice an electronic coin (user-controlled conditional anonymity). Another possibility would be that users can subscribe to the service. It could be the case that low quality connections (in terms of performance, anonymity, number bandwidth, etc.) are offered for free or at a low price, and high quality of service connections are more expensive. In this case, users would own credentials that would prove them subscribed to a particular service. The access control blocks of the system would check the use rights of the user when establishing a connection.

Different mixes can have different access control policies. For example, it could be the case of a network formed by heterogeneous nodes, some of them offering free service and some paid service. Other scenarios than the ones proposed here could be possible. For example, certain nodes may require that the user has a credential from a trustee that can deanonymize him under certain circumstances. Nodes should not be required to log any information, as this would put a heavy burden on them, discouraging participation, as well as present a hard to control surface of attack.

4.2.1 Exit policies

Exit policies may help node operators modulate their risks and increase user participation in the system. Node operators may provide access to a list of responders (white list). They may as well provide access to all resources expect for a few ones (black lists). Exit policies help prevent abuse of the system in the form of access to illegal content (e.g. child pornography). Nodes should publicly advertise their exit policy; so that users can take choose the most appropriate path of nodes to get to a certain resource.

4.2.2 Other controls

Other control mechanisms that access control blocks and exit policies may be implemented. For example, some systems may periodically run control protocols, in order to detect the nodes which are not complying with the protocols and exclude them from the system. Another form of control is the use of reputation systems. Compliance with the protocols and quality of service of every node may be assessed by the users. Reputation systems may help excluding from the system misbehaving or faulty nodes.

4.3 Building Blocks

An anonymous credential system, allows anonymous yet authenticated and accountable transactions between users and service providers.
A Mix uses(ZK-zero knowledge proofs for):

- registering a pseudonym (called a nym) with an organisation
- getting/issuing a credential for a nym
- showing/verifying a credential

4.3.1 Registering a Nym

A Nym is the pseudonym under which the user wants to be known by an organization.
A mix has two kinds of nyms: ordinary nyms and rootnyms. The user establishes a nym, based on his master secret and a randomly chosen secret.During the registration, the user proves that the nym has been correctly formed. A rootnym is a special nym, based on the user's master secret only. It is hidden in every other nym of that user. Rootnyms are established with a special credential issuing organization, the Root Pseudonym Authority.
There are three basic primitives for registering a nym:

- RegNym, for registering ordinary nyms: RegNym(NymUR)
- RegSignedNym, for registering ordinary nyms RegSignedNym(SigUR,CertUC,NymUR)
- RegRootNym, for registering rootnyms RegRootNym(SigUR,CertUC,RootNymUR)

In both, RegSignedNym and RegRootNym, the user signs the established nym with his signature key, which is certified through an external certificate (which links the user's public key with his identity). Hence, the organization holds a provable link between the (root)nym and the identity certified by the certificate. The signature can be extended to include both, the nym and a message (e.g., the message could contain a description of the user's liability towards the usage of this nym).

4.3.2 Getting/Issuing a credential

IssueCred(NymUI ,CredUI ,CredOptUI ,CredAttrUI) A User, known by an organization by a nym, may request a credential for that nym.
Credentials can have attributes (e.g., age, citizenship, expiration date, . . .),
and options (e.g., one/limited/multi-show).

4.3.3 Showing/Verifying a credential

CredShow(NymUV ,CredUI ,CredShowFeaturesUV , CredShowAttrUV , TranscriptUV ,MsgUV)
The user proves to the verifying organization OV that he owns a credential issued by organization OI . The proof convinces OV that the user knows the user's master secret that is linked to the credential; in addition, the user may choose to reveal (and prove) any attribute, or a property of these attributes (e.g., citizenship is not Indian, age is > 18, . . .). Showing a credential results in a transcript (for OV) which can be used later in double spending and deanonymization protocols. The following anonymity properties are valid:

- Two or more credential shows of the same credential cannot be linked together1 (unless the credential is a one-show credential);
- A credential show does not reveal the pseudonym for which it was issued;
- A credential show cannot be traced to the issuing of the credential.

During a credential show, a message can be signed, which provably links the message to the transcript of the credential show.
A credential show can have three extra features:

- the credential is shown relative to another nym;
- local deanonymization is allowed;
- global deanonymization is allowed.

Credential Show Relative to Another Nym ---The user may show a credential relative to another nym. Here, the user proves to the verifier OV that the nym (NI) on which the credential was issued and the nym (NV) under which the user is known by OV , both belong to the same user. This feature also allows a user to prove that he owns several credentials, and prevents that users collude in presenting credentials. Local and Global Deanonymization Transcripts of anonymous credential shows can be de-anonymized by including a verifiable encryption of the user's identity:

- the nym for which the credential was issued (in case of local deanonymization)DoLocalDeanon(TranscriptUV ,NymUI ,DeAnonTranscriptDUV).
- the user's rootnym2(global deanonymization) DoGlobalDeanon (TranscriptUV , RootNymUR,DeAnonTranscriptDUV).

The user may restrict de-anonymization by including a deanonymization condition, which must be fulfilled before the deanonymizing organization may de-anonymize the transcript of a credential show.

Assumptions

1We assume that no subset of the revealed attributes uniquely identifies the user.
2The rootnym is a special nym. It is hidden in every other nym of the user. The user
can prove that the encrypted rootnym is indeed hidden in the nym for which the credential was issued. The deanonymizing organization can construct a verifiable proof of the deanonymization.
Note: since rootnyms are always provably linked to an external identity, global deanonymization reveals that identity.

4.3.4 Accountability

In order to make a user accountable for a transaction, verifiable proofs are a prerequisite.

- The RootNym and SignedNym primitives establish a verifiable link between a (root)nym (and possibly a message) and an external identity.
- During a credential show, the user can sign a message, which makes the (possibly anonymous) user accountable for that message.

If the credential show was relative to a nym, at least a pseudonym of the user is provably revealed.

If local anonymization is available, the nym for which the credential was issued can be provably retrieved.

If global anonymization is available, the rootnym (and hence the external identity) can be provably recovered.

- Showing more than once a one-show credential, allows the issuing organization to provably recover the nym on which the credential was issued. The structure can fulfill all the anonymity requirements.

5 RELATED WORKS

The increased use of electronic media in everyday life generates new concern regarding users' privacy. Anonymity providing technology has emerged to provide enhanced confidentiality of our private data. Martin [32] gives an overview of the anonym-zing techniques for the Internet. In general, these technologies may provide data or communications anonymity, and may provide personalization. For example, Onion Routing [36], Crowds [34], and Hordes [35] provides connection anonymity. Systems GNUnet [37], Freenet [39], and Napster [33] facilities file-sharing services while guarantees different levels of anonymity. In addition, several models have been developed to support specific applications, such as anonymous e-mail [6, 40] or electronic commerce [39, 31, 30]. In general, current technology to provide anonymity or pseudonymity are either fully anonymous, thus lack accountability, or—if accountability is addressed — fully dependent on a trusted mediator (certificate authority, customer care agency, etc.). Furthermore, they do not provide access to the users to observe their personal data or terminate their data if they do not want to participate in a given community any longer. Finally, they only provide one layer of anonymity, where the need to validate whether two virtual entity belongs to the same real user, requires the disclosure of the real entity's identity. In this paper we provide solutions to address the above shortcomings of these models in a common framework.

6. CONCLUSIONS

Anonymity is expensive to realize if the underlying network/transport layer does not have anonymity built in. Conversely, accountability is relatively easy and inexpensive to achieve if the underlying layer does not support anonymity. Thus, it may not be advisable to primarily focus on achieving accountability and then proceed to level everything down to achieve anonymity/ unobservability; the other way round may prove to be more fruitful. It should be remembered too that just because accountability at the transport layer means that anonymity is nigh on impossible at the application layer today does not mean that this will be the case in the future. What also needs consideration is the concept of non-binary anonymity; which is likely to be more prevalent in the future Information Society. Localised transparency/accountability (i.e. in a specific context) can lead to "graded" anonymity; thereby, increasing privacy outside of the local/specific environment. Finally, it is worth recalling that the promises and guarantees given by service providers with regard to the confidentiality of users' data are only as worthwhile as the governing authorities allow. If a future administration hinders such privacy, then today's industry may well require systems for untraceable communications. This does not mean that everybody should be allowed to carry out transactions anonymously, but it does support the point for essentially anonymous communication infrastructures, on which one can build traceability.

We claim that anonymity often allows people to act without consideration, rudely and can result in serious risks to security. *Accountability* is required to make entities within the system responsible for their acts. The main focus of our research was to provide accountable anonymity. We have discussed the requirements, building blocks to provide anonymous communication. The infrastructure allows realization of untraceable payment systems which offer improved audit –ability, accountability and control compared to current systems, while at the same time offering increased personal anonymity and privacy.

REFERENCES

[1] Abelson H, Anderson R, Bellovin S, Benaloh J, Blaze M, Diffie W, Gilmore J, Neumann P, Rivest R, Schiller J, Schneier B (1997) The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption. World Wide Web Journal 2(3):241-257.

[2] Anonymizer, http://www.anonymizer.com/

[3] Berthold O, Federrath H, Kopsell S (2000) Web MIXes: A system for anonymous and unobservable Internet access. In: Federrath H (ed.) Designing Privacy Enhancing Technologies, LNCS 2009, pp. 115-129. Springer-Verlag.

[4] Berthold O, Pitzmann A, Standtke R (2000) The disadvantages of free MIX routes and how to overcome them. In: Federrath H (ed.) Designing Privacy Enhancing Technologies, LNCS 2009, pp. 30-45. Springer-Verlag.

[5] Oliver Berthold, Hannes Federrath, and Stefan Kopsell. Web MIXes: A system for anonymous and unobservable Internet access. In H. Federrath, editor, Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, pages 115{129. Springer-Verlag, LNCS 2009, July 2000.

[6] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84{88, 1981.

[7] George Danezis and Claudia Diaz. A survey of anonymous communication channels. Technical Report MSR-TR-2008-35, Microsoft Research, January 2008.

[8] George Danezis, Roger Dingledine, and Nick Mathewson. Mixminion: Design of a Type III anonymous remailer protocol. In IEEE Symposium on Security and Privacy, pages 2{15. IEEE Computer Society, 2003.

[9] Ulf Moller, Lance Cottrell, Peter Palfrader, and Len Sassaman. Mixmaster Protocol Version 2. IETF Internet Draft, July 2003.

[10] Claessens J, Diaz C, Goemans C, Preneel B, Vandewalle J, Dumortier J (2003) Revocable anonymous access to the Internet. Journal of Internet Research 13(4):242-258.

[11] Claessens J, Diaz C, Preneel B, Vandewalle J (2002) A Privacy-Preserving Web Banner System for Targeted Advertising. Technical Report 9 p. Katholieke Universiteit Leuven.

[12] Diaz C, Seys S, Claessens J, Preneel B (2002) Towards Measuring Anonymity. In: Dingledine R, Syverson P (eds) Designing Privacy Enhancing Technologies, LNCS 2482, pp. 54-68. Springer-Verlag.

[13] Diaz C, Naessens V, Nikova S, De Decker B, Preneel B (2004) Tools for Technologies and Applications of Controlled Anonymity. Technical Report, 211 p. Project IWT STWW Anonymity and Privacy in Electronic Services.

[14] Dingledine R, Mathewson N, Syverson P (2004) Tor: The Second-Generation Onion Router. In 13th USENIX Security Symposium, pp. 303-320. USENIX.

[15] Paul Syverson, Gene Tsudik, Michael Reed, and Carl Landwehr. Towards an Analysis of Onion Routing Security. In H. Federrath, editor, Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, pages 96{114. Springer-Verlag, LNCS 2009, July 2000.

[16] Goldschlag D, Reed M, Syverson P (1996) Hiding Routing Information. In: Anderson R (ed.) Information Hiding, LNCS 1174, pp. 137-150. Springer-Verlag.

[17] Goldschlag D, Reed M, Syverson P (1999) Onion Routing. In: Communications of the ACM 42(2):39-41.

[18] Hintz A (2002) Fingerprinting Websites Using Traffic Analysis. In: Dingledine R, Syverson P (eds) Designing Privacy Enhancing Technologies, LNCS 2482,pp. 171-178. Springer-Verlag.

[19] M. Waldman, A. D. Rubin, and L. F. Cranor. Publius: A robust, tamper-evident, censorship-resistant, web publishing system. In *Proc. 9th USENIX Security Symposium*, 2000.

[20] Juels A (2001) Targeted Advertising... and Privacy Too. In: Naccache D (ed.) Topics in Cryptology - Proceedings of the Cryptographers' Track at RSA'2001, LNCS 2020, pp. 408-424. Springer-Verlag.

[21] Kopsell S, Wendolsky R, Federrath H (2006) Revocable Anonymity. In: Muller G (ed.): Emerging Trends in Information and Communication Security - ETRICS, LNCS 3995, pp. 206-220. Springer-Verlag.

[22] S. G. Stubblebine and P. F. Syverson. Authentic attributes with fine-grained anonymity protection. In *Lecture Notes in Computer Science*, volume 1962, 2001.

[23] Pitzmann A, HansenM(2000) Anonymity, Unobservability and Pseudonymity: A Proposal for Terminology. In: Federrath H (ed.) Designing Privacy Enhancing Technologies, LNCS 2009, pp. 1-9. Springer-Verlag.

[24] Pitzmann A, Pitzmann B, Waidner M (1991) ISDN-mixes: Untraceable communication with very small bandwidth overhead. In: Effelsberg W, Meuer H,Muller G (eds) GI/ITG Conference on Communication in Distributed Systems, Informatik-Fachberichte 267, pp. 451-463. Springer-Verlag.

[25] Reed M, Syverson P, Goldschlag D (1998) Anonymous Connections and Onion Routing. In: IEEE Journal on Selected Areas in Communications 16(4):482-494.

[26] Serjantov A, Danezis G (2002) Towards an Information Theoretic Metric for Anonymity. In: Dingledine R, Syverson P (eds) Designing Privacy Enhancing Technologies, LNCS 2482, pp. 41-53. Springer-Verlag.

[27] Syverson P, Tsudik G, Reed M, Landwehr C (2000) Towards an Analysis of Onion Routing Security. In: Federrath H (ed.) Designing Privacy Enhancing Technologies, LNCS 2009, pp. 96-114. Springer-Verlag.

[28] The Clipper Chip, http://www.epic.org/crypto/clipper/

[29] Von Ahn L, Bortz A, Hopper N, O'Neill K (2006) Selectively Traceable Anonymity. In: Danezis G, Golle P (eds) Designing Privacy Enhancing Technologies, LNCS (pre-proceedings), pp. 199-213. Springer-Verlag.

[30] D. Kugler and H. Vogt. Off-line payments with auditable tracing. In *Financial Cryptography*, Lecture Notes in Computer Science. Springer-Verlag, 2002.

[31] P. MacKenzie and J. Sorensen. Anonymous investing: Hiding the identities of stockholders. In *Lecture Notes in Computer Science*, volume 1648, 1999.

[32] D. Martin and A. Schulman. Deanonymizing users of the safeweb anonymizing service, Nov. 2002. http://citeseer.nj.nec.com/martin02deanonymizing.html.

[33] Napster. http://www.napster.com/about us.html, 2002.

[34] M. K. Reiter and A. D. Rubin. Crowds: anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[35] C. Shields and B. N. Levine. A protocol for anonymous communication over the internet. In *Proc. of ACM Conference on Computer and Communications Security*,2000.

[36] P. F. S. amd D. M. Goldschlag and M. G. Reed. Anonymous connections and onion routing. In *Proc. IEEE Symposium on Security and Privacy, Oakland, California*, 1997.

[37] K. Bennett, C.Grothoff, T. Horozov, I. Patrascu, and T. Stef. Gnunet —a truly anonymous networking infrastructure. http://citeseer.nj.nec.com/502472.html.

[38] J. Claessens, B. Preneel, and J. Vandewalle. Anonymity controlled electronic payment systems. In *Proc. 20th Symp. on Information Theory in the Benelux*, 1999.

[39] I. Clarke, O. Sandberg, B.Wiley, and T. W. Hong. Freenet: A distributed anonymous information storage and retrieval system. In *Lecture Notes in Computer Science*, volume 2009,2001.

[40] I. Goldberg, D. Wagner, and E. Brewer. Privacy-enhancing technologies for the internet. In *Proc. of 42nd IEEE Spring COMPCON*, 1997.

[41] A. Abdul-Rahman and S. Hailes. Relying on trust to find reliable information. http://citeseer.nj.nec.com/348491.html,2002.

[42] R. Khare and A. Rifkin. Weaving a web of trust. *World Wide Web Journal*, 2(3):77–112, 1997.

[43]G. Zacharia, A. Moukas, and P. Maes. Collaborative reputation mechanism in electronic marketplaces. In *Proc. Of the 32nd Hawai International Conference in System Sciences*, 1999.

[44] M. Venkatraman, B. Yu, and M. P. Singh. Trust and reputation management in a small-world network. http://citeseer.nj.nec.com/296051.html, 2002.

[45] L. Buttyan and J.Hubaux. Accountable anonymous access to services in mobile communication systems. In *Symposium on Reliable Distributed Systems*, 1999.

Authors

H.Jayasree obtained her B.E. in CSE from Bangalore University and M.Tech. in CSE from JNTUH, Hyderabad in 2001 and 2006 respectively. She is currently a Research Scholar of CSE JNTUH, Hyderabad. She is working as Associate Professor, for Aurora's Technological and Research Institute and has 10yrs of teaching experience in various colleges of Hyderabad and Bangalore. Areas of research interest include Computer Networks and Network Security.

Dr Avula Damodaram obtained his B.Tech. Degree in CSE in 1989, M.Tech. in CSE in 1995 and Ph.D in Computer Science in 2000 all from JNTUH, Hyderabad. His areas of interest are Computer Networks, Software Engineering, Data Mining and Image Processing. He has successfully guided 6 Ph.D. and 2 MS Scholars apart from myriad M.Tech projects. He is currently guiding 9 scholars for Ph.D and 1 scholar for MS. He is on the editorial board of 2 International Journals and a number of Course materials. He has organized as many as 30 Workshops, Short Term Courses and other Refresher and Orientation programmes. He has published 35 well researched papers in national and International journals. He has also presented 45 papers at different National and International conferences. On the basis of his scholarly achievements and other multifarious services, He was honored with the award of DISTINGUISHED ACADAMICIAN by Pentagram Research Centre, India, in January 2010.