

An Anonymity Revocation Technology for Anonymous Communication

Giannakis Antoniou¹, Lynn Batten² and Udaya Parampalli³

¹ The University of Melbourne, giannos.antoniou@gmail.com

² Deakin University, lmbatten@deakin.edu.au

³ The University of Melbourne, udaya@csse.unimelb.edu.au

Abstract: A number of Privacy Enhancing Technologies (PETs) have been proposed in the last three decades offering unconditional communication anonymity to their users. Unconditional anonymity can, however, be a security threat because it allows users to employ a PET in order to act maliciously while hiding their identity. In the last few years, several technologies which revoke the identity of users who use PETs have been proposed. These are known as anonymity revocation technologies (ARTs). However, the construction of ARTs has been developed in an ad-hoc manner without a theoretical basis outlining the goals and underlying principles. In this paper we present a set of fundamental principles and requirements for construction of an ART, identifying the necessary features. We then propose an abstract scheme for construction of an ART based on these features.

Keywords: Privacy, Communication Anonymity, PET, Accountability

1. Introduction

There are many technologies which offer privacy services, for example anonymity [15], to their users; these are known as Privacy Enhancing Technologies (PETs). PETs may offer anonymity at the communication layer (i.e. the source IP Address) or at the data layer (i.e. the name, and the home/work address of the user). For the purpose of this paper, we refer only to those PETs which offer anonymity to the clients (in a client-server communication) at the communication level. Examples of these are TOR [12], Anonymizer [6] and Crowds [16].

In such a PET scheme a user who wants to act anonymously sends a message to a set of nodes, known as PET entities, which are then responsible for forwarding the message to a destination party such as a server (a responder). PET entities may be located in a country other than that in which the user or destination party reside,

and so different legislation about the privacy rights of citizens may apply to these locations. For instance, as described in [17], new legislation in the EU forces the communication providers to store the data exchanged by their customers for a specific period of time before destroying it. However, this legislation does not apply to communication providers outside of EU.

A PET protects the right of users who wish to act anonymously, while an anonymity revocation technology (ART) reveals the identity of the users who are suspected of violating some rules and are hiding behind a PET. Therefore, full anonymity is a security threat[13] and the necessity to find a balance between privacy and accountability is great [7]. Although there are ARTs which are applied in an environment without a PET, the scope of this paper focuses on the ARTs which revoke the anonymity of the users who hides their identity by using a PET.

Several papers (eg. [7], [11] and [9]) identify the problems associated with technologies offering anonymity and agree that there is a need for a system which offers a controllable level of privacy in order to prevent malicious users from abusing PET services. Differing legislative rights make it difficult to determine the most appropriate underlying principles on which such ‘controllable’ privacy should be based.

Several PETs are currently available over the Internet. Thousand of Internet users around the world can use these technologies for free and in some cases with a very low cost. Examples of available technologies are <http://www.anonymizer.com>, <http://www.idzap.com>, <http://www.torproject.org> and <http://www.anonymprom.com>. Although designing an appropriate ART requires a delicate approach, it is unclear whether any of these PETs have applied an ART in order to discourage users from acting maliciously. Moreover, the necessary theoretical background for ART designers to design such technologies is not available.

In this paper we analyse existing ARTs based on features we identify as being fundamental to all requirements for such a technology, and we propose an abstract scheme which captures these features.

The paper is organised as following. In Section 2 we describe the work and the directions in the field of ART and in Section 3 we propose principles underlying ARTs. In Section 4 we present the conditions required by an ART in order to fulfil the principles introduced in Section 3. In Section 5 we identify a set of parameters which describe an ART and we propose an abstract scheme for an ART based on the identified parameters. In Section 6 we compare existing ARTs with respect to the principles and requirements of a good ART. In Section 7 we discuss the abstract scheme with respect to the principles introduced in Section 3 and we conclude the paper in Section 8.

2. Current Work in the Area of Anonymity Revocation Technologies

In [9] the authors mention the important role of trust for an ART, list six requirements of an ART and propose an ART scheme. However, applying that ART scheme over Crowds [16], violates one of these requirements because it requires not only the initiator (as the requirement states) but all the PET entities to be aware of the ART. An important requirement, which we will also adopt in the next section, is the necessity to retain the accountability of the actions of the third trusted party who is responsible for revoking the anonymity of a user.

In [18] the authors prove that the majority of communication anonymity schemes can enhance techniques to offer selective traceability. However, in this case, more than one PET entity needs to be aware of the ART.

Existing ARTs can be divided into two categories. In the first category are the ARTs which begin to take action based on the characteristics (e.g. the content and the source/destination address) of the sent message of a user. Examples of ARTs from this category can be found in [14], [3], [1] and [8]. However, most ARTs are included in the second category which take action based on external or undefined factors; examples of these can be found in [8], [9] and [11]. In [7] the authors study the balance between privacy and accountability and propose that the goal of such a balance is that we should not reveal the identity of honest users but should reveal the identity of dishonest users.

Existing ARTs have been developed without following a concrete set of principles or requirements, as discussed in Section 6. Our aim in the next section is to fill this gap by proposing a set of general principles which should be expected of a good ART.

3. Principles of an Anonymity Revocation Technology

In this Section we propose three basic principles expected of a good ART. The two goals proposed in [7] (and described in the previous Section) are extended here and chosen as basic principles of a good ART because they both contain clear and reasonable expectations of the participated entities from an ART.

Principle 1)

- 1a. *The identity of a malicious entity must be revealed and*
- 1b. *Enough information/evidence must be provided to prove its involvement.*

Principle 2) *The identity of an innocent user must be protected.*

In addition to the above, we propose the following as a third principle:

Principle 3) *The desired characteristics of a PET must not be violated by the ART.*

The first principle protects the responders (e.g. servers) from users who want to act maliciously. It has two-fold goals. The first goal is to discourage potential malicious users from taking advantage of a PET and acting maliciously against servers. The second goal is to assure servers that those guilty will face the legal consequences. If 1a is not in place, the servers will deny communications coming from PETs; as a result, the communication anonymity of honest users will not be possible. By having in place a PET and an ART which supports the Principles 1a and 1b, the servers will be able to communicate securely with users who use PETs, but will be less inclined to communicate with users who do not use PETs.

The second principle protects an honest user from a rogue ART. Although a PET protects the identity of the user from the corresponding server and from all other entities, it should not protect the identity from the administrator of an ART. An ART which does not respect the second principle is unlikely to be accepted by users [5] (an example is the Clipper chip [10]).

The third principle protects the integrity and the desired [4] characteristics of a PET from an ART. This principle is based on the assumption that a PET cares only about the identity of users who are not malicious. Protecting the identity of users who are malicious lies outside of a PETs' goal. This principle is necessary to ensure that an ART operates as an extension technology of a PET, supporting its goals and not as a contradictory technology. In a client-server communication, both parties should use the system without being discouraged by the system's features.

In the next section we propose six requirements of an ART in order to achieve the three general principles.

4. Requirements of an Anonymity Revocation Technology

In this section we propose six requirements of an ART which guarantee the three major principles. All of these requirements are needed to guarantee all three general principles (as shown in Table 1). Thus, in a formal sense, the requirements are complete. For the purposes of this paper, the administrator of an ART is called investigator. Our requirements of an ART are as follows:

R1) *An investigator is responsible, and thus liable, for the decision to begin the anonymity revocation procedure.*

Although the role of an investigator is played by a trusted third party, the less we need to trust somebody, the better. For this reason the investigator must be responsible and liable for its action or lack of action. In case the investigator is not

liable, then an investigator could deny revealing the identity of a malicious user (therefore, it protects a malicious user and violates the first general principle) or the investigator could reveal the identity of an honest user which means that it violates the second and the third general principles.

An ART which has the investigator liable for its actions does not prevent but at least discourages the investigator from acting dishonestly.

R2) An investigator decides to reveal the identity of a user based on an agreement which a user has agreed to respect.

The investigator should not subjectively decide whether to reveal the identity of the user or not based on the criteria of the investigator. A user is considered malicious only in case he/she violates any of the agreements/ rules/ legislations and the user knew about these rules. The user has the right to know what is acceptable and what is unacceptable. This is especially important for cases where the client, the investigator and the server are located in different countries, which follows different legislation rules. Although an action in the country of the client may be considered legal, the same action in the country of the server may be considered as illegal. What is going to happen if the client and server are located in a country where an action of the client is considered legal but that action is considered illegal in the country of the investigator? In order to avoid such surprising results, the client, the server and the investigator should be aware/acknowledge the same rules (even though the client may not follow them) and the investigator should decide whether the user acted maliciously or not based on these rules. An ART should prevent a user to repudiate that he/she agreed to follow these rules.

R3) An investigator decides to reveal the identity of a user only in case the user violates the agreement.

In case a user does not violate any agreement, the user is not considered as malicious, and therefore, his/her identity should not be revealed. The ART should employ techniques to offer non-repudiation of the actions of the users. Otherwise, a user may repudiate that he acted like this. Also, if there is no technique offering non-repudiation, a malicious user may be masqueraded, act maliciously by violating some rules and blame innocent users. In case the user did not violate any agreement, the investigator should not be able to reveal the identity of the user.

R4) Before an investigator decides that the identity of a user must be revealed, the level of anonymity of that user should not be reduced.

An ART should not need to reveal the identity of the users to multiple entities before determining that these users are honest. This requirement is necessary to prevent an ART violating the functionalities of a PET.

R5) The anonymity revocation of a user should not affect the anonymity of others.
Without this requirement, the third general principle is violated.

For example, an ART which reveals the identity of one or more clients in order to prove that one client acted maliciously is unacceptable to the users and also violates the second and third general principles.

R6) *Only the investigator should be able to detect the identity of the malicious user.* Otherwise, the reliability of the ART as well as the reliability of the PET is in danger.

All of the above requirements are useless if an entity other than the investigator could reveal the identity of a user.

Requirements Principles	R1	R2	R3	R4	R5	R6
Principle 1	√	√	X	X	X	√
Principle 2	√	√	√	X	√	√
Principle 3	√	√	√	√	√	√

Table 1 - The table illustrates which requirements serve specific general principles

From a practical perspective, several factors may prevent an ART from achieving its objective and from being applicable in an environment where the client and the server (in client-server architecture) are located in a different country and the PET entities are distributed globally. One implication of this is that an ART should be PET-independent, which means that the functionalities, the level of anonymity revocation and the operation of an ART should not be affected by the applied PET.

Another implication is that if an anonymity revocation procedure requires the use of exchanged messages of a user, the ART should store only the required limited volume of information (exchanged messages), for a limited duration. For instance, the legislation in the EU in which a communication provider is required to preserve exchanged messages of its clients for 6 months is impossible from a practical perspective.

In this section we identified a basic set of requirements for achieving the general principles proposed in Section 3. In the next section, we will focus on the parameters which characterise any ART and which also affect the fulfilling of some of the identified requirements.

5. Analysis of an Anonymity Revocation Technology

In this section we identify and describe the characteristics based on which we will develop an abstract scheme. Although the characteristics are not exclusive, they give a clear idea about the potentials and weaknesses of an ART. We will not develop a detailed description of the actual ARTs, but rather focus in an abstract

way on their characteristics. Prior to identifying these characteristics, we describe the environment as well as the necessary parameters, which should be involved in an ART.

Alice communicates anonymously with Bob through a *PET*. Only an attestor *A* knows Alice and can link her exchanged messages with Alice. An adversary *X* wants to know the identity of Alice for *Re* reasons, based on information which is held for duration *D* by entity *L*. Investigator *Inv* has a level *LoR* of responsibility to perform an anonymity revocation investigation based on the request of *X*. However, *X* needs to provide proof *Pr* to *Inv* that *X* has the *R* right to know the identity of Alice. Alice and *X* have a level *LoT* of trust in *Inv*. However, *Inv* can create problems *C* for Alice in case *Inv* is compromised. *Inv* uses evidence *Evi* in order to identify Alice. *Inv* can prove that Alice was the entity who was communicating with Bob by providing strength *S* of evidence to *O* entities.

P: Is the *PET* to which an ART can be applied. An ideal ART should be applicable to as many *PETs* as possible. It is important to allow a *PET* to co-exist with an ART.

X: Is the entity which makes the request to begin the anonymity revocation. For example, the entity *X* could be a receiver of the message, such as a server, or an intermediate entity such as a *PET* node. It could also be a government who wants to know with whom a specific client communicated.

Inv: Is the entity who investigates the requests of the *X*. More than one entity could play this role. It is a usual practice by some existing ARTs to distribute the responsibilities to multiple entities.

A: Is any entity that can link an exchanged message with the identity of Alice before the investigation completion.

Re: Is the reason that *X* wants to know the identity of Alice. Alice may have sent malicious messages to *X* or *X* may suspect that Alice has violated some rules.

R: Is the right of *X* to know the identity of Alice. *X* has the right to know the identity of Alice if *X* and Alice had an agreement and Alice violated the agreement or if the legislation allows *X* to identify Alice under some conditions which have been met.

L: Is the entity at which the necessary information for identified Alice is located.

D: Is the maximum duration that the entities need to store information to assist the anonymity revocation. In case the duration is too long and too much data are required to be stored, practical problems are arisen. The smaller the duration is, the more practical the mechanism can be.

LoR: Is the level of responsibility for the investigator to investigate and identify Alice. An investigator with a low level of responsibility may avoid performing the investigation.

LoT: Is the level of trust which Alice and *X* have for the investigator. In case the level of trust is low, Alice or *X* may avoid using the system. The trust allows

Alice and X to believe that the investigator will act honestly based on their agreement.

Pr: Is a proof that Alice’s anonymity must be revealed.

C: Is the consequence of the dishonest act of the investigator against Alice.

Evi: Is the strength of information which the Investigator relies on in order to identify Alice.

S: Is the strength of the evidence that the investigator is using to prove that is Alice who communicated with Bob.

O: Are the entities who can be convinced by the results of the investigator. It is desired that Alice should not be able to deny her actions. A sub-union of *O* has an authority on Alice.

Requirements	R1	R2	R3	R4	R5	R6	Practical
Parameters	<i>Lo</i>	<i>R</i>	<i>Re</i>	<i>LoT</i>	<i>LoT</i>	<i>C</i>	<i>P</i>
	<i>R</i>	<i>S</i>	<i>Pr</i>	<i>Pr</i>		<i>S</i>	<i>L</i>
	<i>Lo</i>		<i>Evi</i>	<i>Evi</i>		<i>O</i>	<i>D</i>
	<i>T</i>		<i>S</i>				
	<i>S</i>						

Table 2 - The table shows which parameters (except the parameters which represent entities) are useful for achieving the requirements

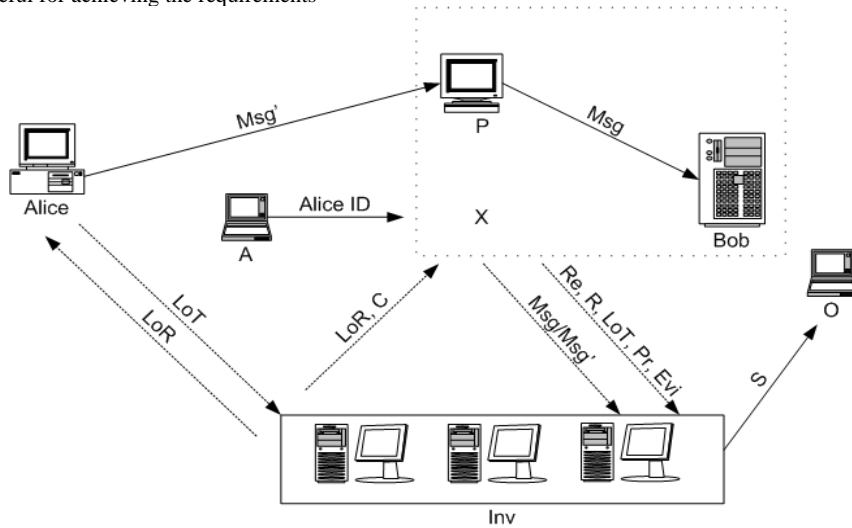


Figure 1 -An abstract scheme based on parameters of an Anonymity Revocation Technology

The values of some of the parameters affect some of the requirements. These are shown in Table 2. We visualise in Figure 1 the interaction of those parameters in an abstract scheme.

6. Analysis of the Existing ARTs Based on the Requirements

In this section we analyse three ARTs based on the six requirements (Table 3) introduced in Section 4. We also describe (Table 4) the principles these ARTs follow in regards to the general principles introduced in Section 3. The three selected papers found in the literature introducing ARTs are those of Antoniou G. et al [3] (AntG), Claessens J. et al [9] (GlaJ) and Kopsell S et al [14] (KopS).

In AntG the investigator follows a set of rules, in order to decide whether the client acted maliciously or not. These rules have been electronically signed by the client, which confirms the client's agreement to respect these rules. Moreover, exchanged client messages are linked with these rules. The client cannot argue that he/she did not know what is legal and what is not. Further, the exchanged client messages are electronically signed, so the client cannot deny sending the messages. However, a malicious co-operation between the investigator and the related server can reveal the identity of a client. Moreover, the investigator cannot prove to anyone that an innocent user acted maliciously. After a request from the server, the investigator has no other choice but to check whether the client violated the rules or not. In case the investigator tries to deny revealing the identity of the client, the server has enough information to accuse the investigator.

In GlaJ it is up to the investigator to begin the revocation procedure. The investigator follows its own subjective rules, which the client may not even know their existence. A dishonest investigator can easily reveal the identity of an innocent user.

In KopS, as with GlaJ, the investigator decides whether a message is suspicious (the paper reveals the identity of the users who are just suspicious, not malicious) or not based on the investigator's subjective rules. Therefore, the investigator can reveal the identity of an innocent user.

All three ARTs partly fulfilled (Table 3) the third requirement (R3) since no ART can fully prevent a malicious investigator revealing the identity of an innocent user. However, in each ART they employ a mechanism to prevent it from happening.

In AntG, the investigator, who has been selected by the client, needs the malicious co-operation of the related server and it is that server who must first contact the investigator since the investigator is not aware of the server. A similar ART with the AntG is RPINA [1] with an enhanced mechanism [2] to hide the identity of the investigator from the server. That mechanism can also be enhanced in AntG.

In GlaJ, a trustee entity participates in the anonymity revocation procedure; therefore, the client relies on the honesty of that entity.

In KopS, there are two entities (part of the investigation team) who evaluate whether the client is a suspect or not (based on their own criteria), in order to

prevent the anonymity revocation of a non-suspect client. However, the client may not trust any of these investigators.

ARTs	AntG	GlaJ	KopS
Requirements			
R1	√	X	X
R2	√	X	X
R3	Partly	Partly	Partly
R4	√	√	√
R5	√	√	√
R6	√	√	√

Table 3 -The table illustrates which requirements are fulfilled for each ART.

ARTs	AntG	GlaJ	KopS
Principles			
Principle 1 a)	√	√	√
b)	√	X	X
Principle 2	Partly	X	X
Principle 3	Partly	X	X

Table 4-The table illustrates which principles are fulfilled for each ART. In AntG partly achieve the principles 2 and 3 because it doesn't completely fulfill the third requirement (R3).

7. Discussion

Anonymity revocation technologies may have difficulty operating in the presence of PETs. The problem is exacerbated when several PET nodes are involved and located in various countries applying differing privacy legislation. For example, PETs such as Crowds and Tor have PET nodes around the world. Therefore, we argue that it is appropriate to apply an ART where the PET nodes are not involved in the anonymity revocation procedure.

It is possible for a user who wants to communicate anonymously to allow intermediate entities to have access to the content of the exchanged message. However, any ART should acknowledge that the messages exchanged between a user and the related responder are confidential and that a PET supports full confidentiality of the forwarded messages.

As previously stated, this work focuses on some key requirements of an ART, and analyses them in a standard setting. Examples of some characteristics which were not taken into consideration are the duration of an investigation, the economical aspect and the cost (in respect to the bandwidth and computation)

which is required for an ART to function. While these factors may be important when designing an ART, they are not significant to the objectives.

8. Conclusion and Future Work

Anonymity revocation technologies which can collaborate with and complement privacy enhancing technologies are increasingly necessary in an online environment used both for business and social activities. The significant contribution of this paper is the establishment of a theoretical basis on which to combine both technologies in an appropriate way. We propose three basic principles expected of an ART and its interaction with a PET. We show that these principles can be achieved by the implementation of ARTs with six requirements (Section 4), thus demonstrating that good ARTs are achievable. In Section 6, we consider and compare three recent ARTs from the point of view of the six requirements which form part of our specification.

Our work can help both ART and PET designers to gain a better understanding of the major issues and conflicts between the parties involved. It can also be used to evaluate existing ARTs and PETs in various environments and based on the needs.

In future work, we will design and build an ART adhering to the abstract scheme presented here, which fulfils the proposed requirements and respects the general principles. We also plan to perform an extended analysis of existing and new ARTs based on the characteristics described in Section 5.

References

1. Antoniou, G., Gritzalis, S.: RPINA- Network Forensics Protocol Embedding Privacy Enhancing Technologies. In: al., A.T.e. (ed.): International Symposium on Communications and Information Technologies. IEEE Press, Bangkok, Thailand (2006)
2. Antoniou, G., Jancic, A., Parampalli, U., Sterling, L.: Applying a cryptographic scheme in the RPINA protocol. Digital Forensics and Incident Analysis, 2007. WDFIA 2007. Second International Workshop on (2007) 65-74
3. Antoniou, G., Sterling, L., Gritzalis, S., Udaya, P.: Privacy and forensics investigation process: The ERPINA protocol. Comput. Stand. Interfaces **30** (2008) 229-236
4. Argyrakis, J., Gritzalis, S., Kioulafas, C.: Privacy Enhancing Technologies: A Review. Electronic Government (2003) 282-287

5. Bellin, D.: Who Holds the Keys? The US Government & Cryptography Policy. *Computer and Society* (1994) 6-7
6. Boyan, J.: The Anonymizer: Protecting User Privacy on the Web. *Computer-Mediated Communication Magazine* **4** (1997)
7. Burmester, M., Desmedt, Y., Wright, R.N., Yasinsac, A.: Accountable Privacy. *LECTURE NOTES IN COMPUTER SCIENCE* **3957** (2006) 83-95
8. Chida, K., Shionoiri, O., Kanai, A.: Secure Anonymous Communications with Practical Anonymity Revocation Scheme. *Advances in Information and Computer Security* (2007) 352-364
9. Claessens, J., Diaz, C., Goemans, C., Preneel, B., Vandewalle, J., Dumortier, J.: Revocable anonymous access to the Internet? *Internet Research: Electronic Networking Applications and Policy* **13** (2003) 242 - 258
10. Denning, D.E., Smid, M.: Key escrowing today. *Communications Magazine, IEEE* **32** (1994) 58-68
11. Diaz, C., Preneel, B.: Accountable Anonymous Communication. *Security, Privacy and Trust in Modern Data Management*. Springer-Verlag (2006) 15
12. Dingledine, R., Mathewson, N., Syverson, P.: Tor: the second-generation onion router. *Proceedings of the 13th conference on USENIX Security Symposium-Volume 13 table of contents* (2004) 21-21
13. Farkas, C., Ziegler, G., Meretei, A., Lörincz, A.: Anonymity and accountability in self-organizing electronic communities. *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society* (2002) 81-90
14. Kopsell, S., Wendolsky, R., Federrath, H.: Revocable Anonymity. *Proc. Emerging Trends in Information and Communication Security: International Conference, ETRICS* (2006) 6-9
15. Pfitzmann, A., Hansen, M.: Anonymity, unlinkability, unobservability, pseudonymity and identity management— a consolidated proposal for terminology: 2008: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf: Last Access - 8th of May 2008
16. Reiter, M.K., Rubin, A.D.: Crowds: anonymity for Web transactions. *ACM Transactions on Information and System Security* **1** (1998) 66-92
17. Ticar, K.: A closer look at data retention. *International Journal of Technology Transfer and Commercialisation* **6** (2007) 87-99
18. von Ahn, L., Bortz, A., Hopper, N.J., O'Neill, K.: Selectively Traceable Anonymity. *Designing Privacy Enhancing Technologies, LNCS (pre-proceedings)* (2006) 199-213