Proc. 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus '05). LNCS 3592, Springer-Verlag, Heidelberg 2005, 1-9.

Privacy Enhanced Technologies: Methods – Markets – Misuse

Hannes Federrath

University of Regensburg
hannes.federrath@wiwi.uni-regensburg.de

Abstract. Research in Privacy Enhancing Technologies has a tradition of about 25 years. The basic technologies and ideas were found until 1995 while the last decade was dominated by the utilisation of such technologies. The question arises if there is a market for Privacy Enhanced Technology. The answer is yes, however Privacy Enhancing Technology may not have been broadly known yet in order to make it profitable. The governments or non-profit organisations must therefore run such systems or at least promote their further development and deployment. Especially governments have however conflicting interests: While governments of democratic nations are responsible to keep the freedom of citizens (and privacy as a part of it), governments also need instruments to prosecute criminal activities. Subsequently, Privacy Enhancing Technologies have to consider law enforcement functionality in order to balance these different targets.

1 Introduction

Privacy Enhancing Technology (PET) enables the user of communication systems to protect himself or herself from being traced his or her activities and behaviour. PET addresses **confidentiality** aspects:

- Anonymity of a sender or recipient (hiding the identity of a user),
- Unobservability of communication relations (hiding who is communicating with whom) or
- generally the unlinkability of actions (events).

The terminology and attacker models mostly used in PET are described in [1]. John Borking can be considered as the creator of the term "Privacy Enhancing Technology (PET)" when he invented the Identity Protector [2].

Encryption (or cryptography in general and public-key encryption in particular) can be understood as a basic building block for PET systems. Other building blocks are dummy traffic and broadcasting:

- Sending random bits at every time interval hides when a meaningful encrypted message is sent.
- Sending every encrypted message to everybody hides which message a receiver is interested in and who is the intended recipient.

Table 1. Timeline of the development of modern PET

Year	Idea / PET system
1978	Public-key encryption [3]
1981	MIX, Pseudonyms [4]
1983	Blind signature schemes [5]
1985	Credentials [6]
1988	DC network [7]
1990	Privacy preserving value exchange [8]
1991	ISDN-Mixes [9]
1995	Blind message service [10]
1995	Mixmaster [11]
1996	MIXes in mobile communications [12]
1996	Onion Routing [13]
1997	Crowds Anonymizer [14]
1998	Stop-and-Go (SG) Mixes introduced [15]
1999	Zeroknowledge Freedom Anonymizer (service meanwhile closed)
2000	AN.ON/JAP Anonymizer [16]
2004	TOR [17]

The timeline of development of modern PET systems has its beginning in 1981 when Chaum published his paper "Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms" [4]. From this time Chaum published further striking ideas (see Table 1) every two or three years for about a decade. Based on Chaum's new building blocks (MIX, blind signatures, credentials, DC network) the field has become broader and moved towards research in applications of Privacy Enhancing Technologies.

2 Methods

Since 2000 the research community on PET systems has its own Workshop on Privacy Enhancing Technology (PET 20*xx*). Another related conference is the Workshop on Information Hiding (IH). Technical descriptions of new ideas in PET can mostly be found in the PET- and IH-Workshop-Proceedings.

2.1 Building blocks

As usual in the development of security systems a lot in PET systems is about trust. Most privacy enhanced systems should fulfil strong requirements, such as:

- no trust into the network operator, *and*
- no trust into one centralised station.

When reading "new" ideas on PET systems many young researchers in the field firstly think of a trusted third party to protect the privacy (or more general the security) of someone. However, almost everything can be protected by a trustworthy third station. For example, hiding communication relations is easy

if an intermediate station (proxy) is used. However, the communication parties must trust this proxy. The idea of strong PET systems is to avoid this kind of trust: Users should not feel compelled to trust the network operator, nor one single station.

The most important methods and building blocks for PET systems are

- for privacy preserving communication systems (e.g. anonymous communication):
  - Chaumian MIXes [4] and their descendants Mixmaster [11] and SG-Mixes [15],
  - DC networks [7], and
  - Blind-message service [10],
- for privacy preserving transactions (e.g. anonymous payment, identity management):
  - Blind signatures [5], and
  - Credentials [6].

2.2 Example: MIXes

From a practical point of view the MIX concept is the best-known and mostly used. MIXes [4] realise the unlinkability of the sender and recipient of a message. A MIX works as an intermediate station (similar to a proxy). However, by sending a message through more than one MIX the users need not trust one station. It is clear that the attacker is not allowed to control all MIXes of a chain: At least one MIX operator must be trustworthy – *no matter who*.

A MIX collects a number of messages of equal lengths from many distinct senders, discards repeats, changes their encoding, and forwards the messages to a successor-MIX in a different order. The last MIX in the chain sends the message to the recipient. Change of encoding of a message can be implemented using public-key encryption. Since decryption is a deterministic operation, repeats of messages have to be discarded. Otherwise, the change of encoding does not prevent tracing messages by traffic analysis.

For a further description and comparison of MIX-types and their attacker models we suggest reading [18]. A comprehensive bibliography of PET can be found at [19]. The MIX concept is used for example in Mixmaster [11], JAP [20], and TOR [21].

3 Market

Is there a market for such systems? First of all we consider privacy as a natural need of people. Therefore over the last 15 years so-called privacy activists have been running lots of systems free of charge to the users, e.g. anonymous remailer systems (anon.penet.fi, Cypherpunk-Remailers, Mixmaster) and World Wide Web anonymisers (Anonymizer.com, JAP [20], TOR [21]). Some of these

systems are still hard to use: They come just as command line tools, without graphical user interfaces, with very limited availability and reliability.

In order to make privacy tools useable for a broad mass, developers have to concentrate on the improvement of user interfaces. Pretty Good Privacy (PGP) can be seen as a very good example in terms of dramatically increased usability from its first versions until now.

Besides availability and reliability issues, the **usability** of PET systems may decide whether a system is ready for the market and for commercial use. Therefore, the well-known MIX-based anonymiser JAP could be a good basis for market research because JAP has been designed to fulfil both requirements: security *and* usability. See Figure 1 for a screenshot of JAP. [22] gives a short description of the JAP system architecture.

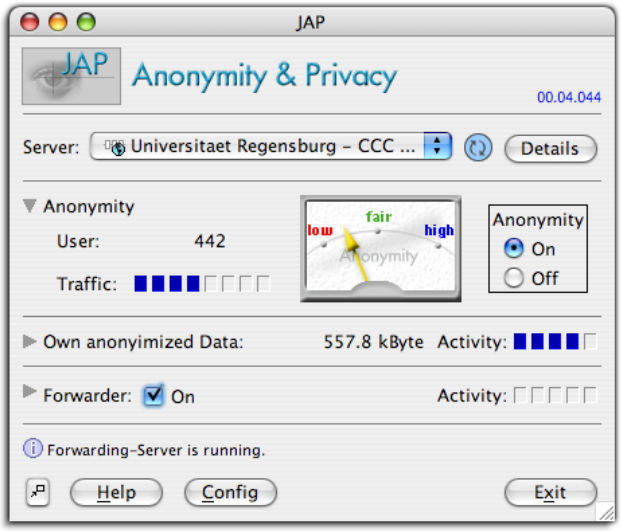

Fig. 1. Screenshot of JAP

3.1 Willingness to pay for anonymity

The following results are based on the JAP anonymity system and its usage. In her survey [23] Spiekermann found out that about 3/4 of the users are power users, and 1/4 are normal or sporadic users (see Table 2): If someone is using an anonymity system he or she will probably use it heavily.
In [24] similar results are shown – differentiated by European and US users. Because these numbers represent the users of a system free of charge, people were asked for their willingness to pay for anonymity services. 60 % of the users are willing to pay, 40 % are not (see Table 3).

Table 2. Heaviness of usage of anonymity systems

	Type of user
73 %	heavy users (use an anonymity system at least daily)
10 %	protect their privacy at least twice a week
17 %	use such systems sporadic (less than twice the week)

An interesting point is that the willingness to pay for anonymity is independent of the heaviness of usage [23].

Table 3. Willingness to pay for anonymity services

	Charge for anonymity service
40 %	not willing to pay
50 %	would pay between 2,50 EUR and 5 EUR monthly
10 %	willing to pay a monthly charge above 5 EUR

3.2 Anonymised content

Another interesting question is which content or requests people want to anonymise. The following analysis has been done with 150 requests randomly picked from URLs anonymised by the JAP system in June 2005.

About 44 % of the anonymised requests can be categorised as entertainment (see Table 4). About 18 % of the JAP users stay anonymously when using Web-based services (search engines, route planners, etc.). E-shops are surprisingly not approached anonymously. Nearly the same applies for health-portals.

Table 4. Requested content via an anonymity service

	Category of content
44 %	Entertainment:
	33 % erotic, pornography
	8 % private homepages, cinema, amusement, ...
	3 % games
18 %	Services: search engines, route planners, stock quotes, ...
8 %	Companies, institutions, universities, ...
8 %	Web-based E-mail services (e.g. Hotmail, GMX, ...)
3 %	News, newspapers, magazines, sports news
1 %	Health information
0 %	Shops, markets, ebay, e-commerce, ...
18 %	Misc: not reachable, not categorisable

3.3 Regions

Although anonymity services hide the connection between clients (users) and servers (e.g. web-sites) such systems do not hide who is using an anonymity service (but of course what the user is looking for). From May–June 2005 the JAP project has classified the incoming IP addresses according to countries and regions in order to find out from where the JAP anonymity system is used. Table 5 shows that JAP is used mainly in Europe and Asia. In America the TOR system [21] as a comparable system funded by the Electronic Frontier Foundation (EFF) will probably attract Americans more than JAP (as a European project). Another problem for American users could be that the main part of the JAP servers (MIXes) is currently installed in Europe. Therefore, the connection to JAP servers might be too slow for Americans.

Table 5. Regions of JAP usage

	Region
60 %	Europe
27 %	Asia
12 %	America
1 %	Rest of the world

Because JAP is a German project it was clear that a significant proportion of the users would come from Germany. We furthermore suspected that the project is sufficiently known in the US to attract users. An analysis of the data brought to light that a remarkable portion of the users came from the Arab part of the world. See for example the day-line of 27 May 2005 (Figure 2): During the night-hours (Central European Time) the largest number of users came from Saudi Arabia.

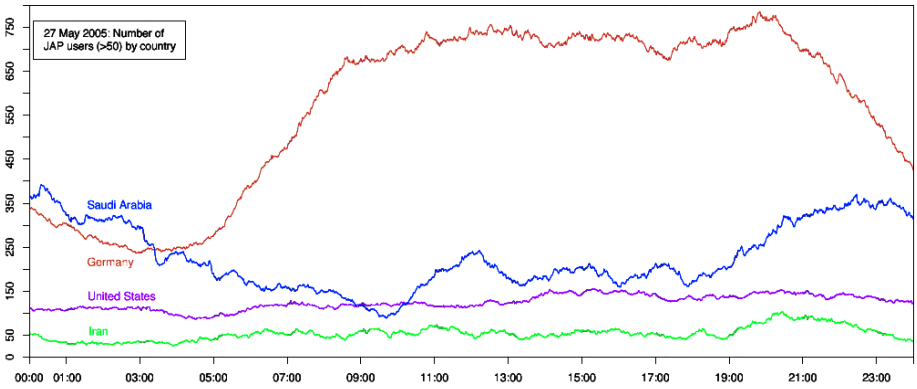

Fig. 2. Usage of JAP (day-line)

4 Misuse

Staying anonymous on the Internet may attract criminals.

The JAP project is currently approached 4-5 times per month on average by law enforcement agencies and private complaints. See Figure 3 for the development of inquiries between July 2001 and December 2004. We are pleased that there is relatively few abuse compared to the 3-4 terabytes of anonymised data every month by the JAP project.

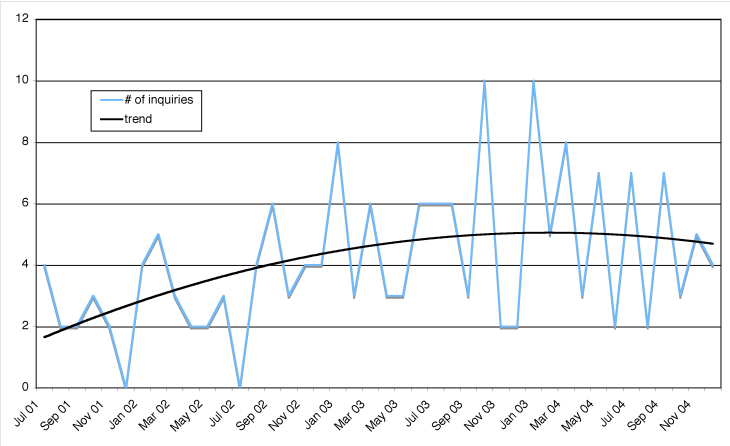

Fig. 3. Number of inquiries by law enforcement agencies and private complaints

A typical inquiry by law enforcement agencies contains the date and time of the incident and the IP address of the anonymity service (usually the IP address of the last MIX), and asks for the IP address assigned to the related user at the entry point (usually the first MIX) of the anonymity service. Because anonymity services should provide unlinkability of incoming and outgoing messages no data exists to answer the inquiry. An observation will only be possible if all MIXes in the chain log connections. MIXes will however usually not log anything since logging is equivalent to "self-mutilation".

Although the number of JAP users grew over the time, the number of inquiries did not. We think that this has the following reasons:

- More and more honest people are using JAP. At the beginning of the service probably criminals were highly attracted. However, the vast majority is using anonymity services for legal purposes.
- Law enforcement agencies are meanwhile used to the fact that anonymity services like JAP do not collect any data. As soon as the police is recognising that JAP has been used, an inquiry would not provide new evidences. The anonymity service therefore won't learn about the real dimension of misuse.

German operators of telecommunication systems are obliged by German law to intercept transmissions if a court is ordering it. This court order can be issued if and only if the crime is listed in a catalogue of very grave crime types. In June 2003 the JAP project received such an order.[1] Since then the open-source software of the JAP-MIX servers contains a function for tracking users. This function has to be activated in all MIXes of a chain if a certain outgoing (anonymised) message has to be linked to its originator, i.e. sender. To make this function useful for criminal investigations all MIXes have to receive such a court order. If the MIXes are spread over the whole world international law is necessary to oblige the MIX operators.

Acknowledgements

I'd like to thank Patrizia Buckel, Stefan Köpsell, Henry Krasemann and Wolfgang Pöppl for their help in providing and analysing the empirical data on JAP usage, Thomas Nowey for critically reading through the paper, and finally Christian Schläger for his patience. Furthermore the JAP project is grateful for funding by the German government.

References

1. Pfitzmann, A., Köhntopp, M.: Anonymity, unobservability, pseudonymity, and identity management – A proposal for terminology (2000-2004) `http://dud.inf.tu-dresden.de/Literatur_V1.shtml`.
2. Hes, R., Borking, J.J., eds.: Privacy Enhancing Technologies: The path to anonymity. revised edition, A&V 10, The Hague (1998)
3. Rivest, R.L., Shamir, A., Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. CACM **21** (1978) 120–126 reprinted: 26/1 (1983) 96-99.
4. Chaum, D.: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. Communications of the ACM **24** (1981) 84–88
5. Chaum, D.: Blind Signatures for Untraceable Payments. In Rivest, R.L., Sherman, A., Chaum, D., eds.: Proc. CRYPTO '82, New York, Plenum Press (1983) 199–203
6. Chaum, D.: Security without Identification: Transaction Systems to Make Big Brother Obsolete. Communications of the ACM **28** (1985)
7. Chaum, D.: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology **1** (1988) 65–75
8. Bürk, H., Pfitzmann, A.: Value exchange systems enabling security and unobservability. Computers & Security **9** (1990) 715–721
9. Pfitzmann, A., Pfitzmann, B., Waidner, M.: ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead. In: Proc. Kommunikation in verteilten Systemen (KiVS). IFB 267, Springer-Verlag, Berlin (1991) 451–463

[1] Details of the so-called "BKA case" (BKA is the German Federal Bureau of Criminal Investigation) are reported at `http://anon.inf.tu-dresden.de/strafverfolgung/index_en.html`.

10. Cooper, D.A., Birman, K.P.: Preserving privacy in a network of mobile computers. In: 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos (1995) 26–38 http://cs-tr.cs.cornell.edu:80/Dienst/UI/1.0/Display/ncstrl.cornell/TR8%5-1490.
11. Cottrell, L.: Mixmaster & Remailer Attacks (1995) http://www.obscura.com/~loki/remailer-essay.html.
12. Federrath, H., Jerichow, A., Pfitzmann, A.: Mixes in Mobile Communication Systems: Location Management with Privacy. In Anderson, R.J., ed.: Proc. 1st Workshop on Information Hiding. Volume 1174 of Lecture Notes in Computer Science., Springer-Verlag, Berlin (1996) 121–135
13. Goldschlag, D.M., Reed, M.G., Syverson, P.F.: Hiding routing information. In Anderson, R.J., ed.: Proc. 1st Workshop on Information Hiding. Volume 1174 of Lecture Notes in Computer Science., Springer-Verlag, Berlin (1996) 137–150
14. Reiter, M.K., Rubin, A.D.: Crowds: Anonymity for Web Transactions. DIMACS Technical Report **97** (1997)
15. Kesdogan, D., Egner, J., Büschkes, R.: Stop-and-Go-MIXes Providing Probabilistic Security in an Open System. In Aucsmith, D., ed.: Proc. 2nd Workshop on Information Hiding. Volume 1525 of Lecture Notes in Computer Science., Springer-Verlag, Berlin (1998) 83–98 http://www.cl.cam.ac.uk/~fapp2/ihw98/ihw98-sgmix.pdf.
16. Berthold, O., Federrath, H., Köhntopp, M.: Project "Anonymity and Unobservability in the Internet". In: Proc. Workshop on Freedom and Privacy by Design / Conference on Freedom and Privacy 2000, Toronto/Canada, April 4–7, 2000, Association for Computing Machinery, ACM, ISBN 1-58113-256-5 (2000) 57–65
17. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. In: Proceedings of the 13th USENIX Security Symposium. (2004)
18. Raymond, J.F.: Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In Federrath, H., ed.: Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability. Volume 2009 of Lecture Notes in Computer Science., Springer-Verlag, Berlin (2001) 10–29
19. The Free Haven Project: Anonymity bibliography (2005) http://www.freehaven.net/anonbib/.
20. JAP: The JAP Anonymity & Privacy Homepage (2000-2005) http://www.anon-online.de.
21. TOR: An anonymous Internet communication system (2004) http://tor.eff.org/.
22. Golembiewski, C., Hansen, M., Steinbrecher, S.: Experiences running a web anonymising service. In: Proc. 14th Intl. Workshop on Database and Expert Systems Applications (DEXA'03), Prague, Czech Republic, IEEE Computer Society (2003) 482–486
23. Spiekermann, S.: Die Konsumenten der Anonymität – Wer nutzt Anonymisierungsdienste? Datenschutz und Datensicherheit DuD **27** (2003) 150–154
24. Spiekermann, S.: The desire for privacy: Insights into the views and nature of the early adopters of privacy services. International Journal of Technology and Human Interaction **1** (2004)