Experiences Running a Web Anonymising Service

Claudia Golembiewski
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein
Holstenstr. 98
D-24103 Kiel, Germany
c.golembiewski@datenschutzzentrum.de

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein
Holstenstr. 98
D-24103 Kiel, Germany
marit.hansen@datenschutzzentrum.de

Sandra Steinbrecher
Freie Universität Berlin
Institut für Informatik
D-14195 Berlin, Germany
steinbrecher@acm.org

Abstract

The research project "AN.ON – Anonymity online" focuses on developing and providing a web anonymising service. This service provides anonymity and unobservability against external observers, the user's ISP and the operators of the service themselves. AN.ON is being promoted by the German Federal Ministry of Economic Affairs for three years (2001-2003). Main criteria for the design of the web anonymising service are security, trustworthiness, performance and usability. Of utmost importance is legal compliance, especially with respect to data protection law. In the submitted paper the project partners, Dresden University of Technology resp. Freie Universität Berlin and Independent Centre for Privacy Protection Schleswig-Holstein, Germany, describe technical background, legal topics, economic issues, socio-political side effects and practical experiences in developing and operating this web anonymising service.

1 Introduction

Since January 2001 Dresden University of Technology resp. Freie Universität Berlin and Independent Centre for Privacy Protection Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein), a German data protection authority, co-operate in the research project "AN.ON – Anonymity online" sponsored by the German Federal Ministry of Economic Affairs and Technology.

AN.ON focuses on the development of a system that enables anonymous web access [1]. This system consists of a client software called JAP and a chain of several intermediate servers called mixes [4]. The JAP software is an Open Source Software which everybody is able to download free of charge from the Internet. It has to be installed on the user's computer. JAP acts as a local proxy between the user's browser and the Internet and provides anonymous communication on the Internet. In contrast to common anonymising proxy servers AN.ON also guarantees its users' anonymity against operators of a mix.

Chapter 2 elaborates the user's motivation for using the AN.ON system. In Chapter 3 a more detailed description of the technical background is given.

The anonymising service developed has to be in compliance with law, especially the data protection law. The Independent Centre for Privacy Protection Schleswig-Holstein elaborates the legal obligations in the project. Chapter 4 presents the legal topics of running such an anonymising service. In Chapter 5 the problem of misuse of the AN.ON system is shown, describing the number and types of misuse cases that became known.

Economic issues, as shown in Chapter 6, play an important role as well when providing a web anonymising service. The results of a survey offered on the AN.ON project website where demographic data of typical AN.ON users and their potential willingness to pay for the service are depicted. Besides, in Chapter 7 socio-political effects, especially the possibility of the AN.ON system to overcome censorship restrictions, are briefly mentioned.

Chapter 8 concludes the text and provides an outlook to possible future legal and technological development.

2 Motivation for anonymous web access

Using Internet services nowadays means leaving digital traces that can easily be stored and aggregated. Many parties, such as advertising companies, employers, insurance companies, secret services or criminals, are interested in interpreting these traces to create individual profiles of Internet users.

A survey about motivation of AN.ON usage was offered on the project website (http://www.anon-online.de) in July 2001. It could be filled in by users of the AN.ON system voluntarily and anonymously. Until April 2002 about 1,800 surveys were filled in. Of course the data collected in the survey cannot be treated as representative because only committed AN.ON users filled in the survey, and users may have filled in the survey more than once.

Apart from these immanent problems of the survey, the evaluation revealed some statistic data about the users' motivation to use the AN.ON system. Most users utilise the web anonymising service for private reasons (more than 80 %). Their main motivation is protection against profile building of their surfing behaviour (approx. 85 %) by Internet service providers, web servers and providers of advertising banners. To prevent the police or secret services from spying on Internet users seems to be only important for approx. 50 %. About 40 % do not only want to browse on the Internet anonymously, but also want to distribute information by sending anonymous e-mail or use web forums anonymously.

The AN.ON system only allows anonymous web surfing, i.e. all services based on HTTP or HTTPS (for real end-to-end encryption where JAP does not act as SSL proxy), including e.g. download of files if realised in this manner. Because we expect a higher risk of misuse in anonymously distributing information than in browsing the web, it does not offer anonymous e-mail accounts or support P2P file exchange. Technically it would be possible to support all programmes based on the socks protocol. However, these additional services were offered, the cases of misuse that might occur (e.g., copyright infringement or defamation) and their handling or prevention would probably exceed the personal resources within the project.

3 Technical background

In the AN.ON project, anonymisation of web requests is reached by sending the requests not directly from the user to the web server but encrypted through a chain of intermediate mix servers. The mix principle was theoretically invented for anonymous e-mail more than 20 years ago [4]. Real-time communication requires an efficient adaption of this idea. AN.ON deploys symmetric channels [8], 1024 Bit plain RSA and AES-128 in OFB mode (using of SSL crypto library). It consists of three components which are illustrated in Fig. 1:

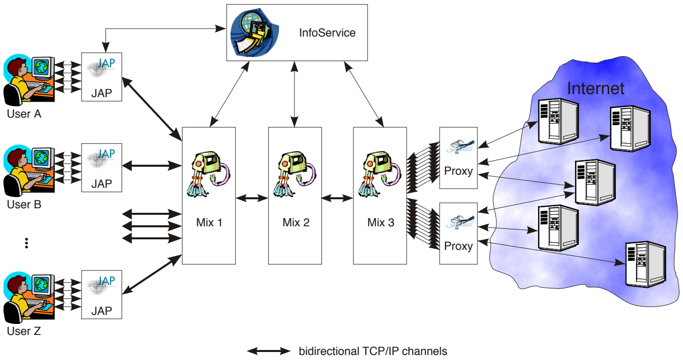


Figure 1. AN.ON Architecture

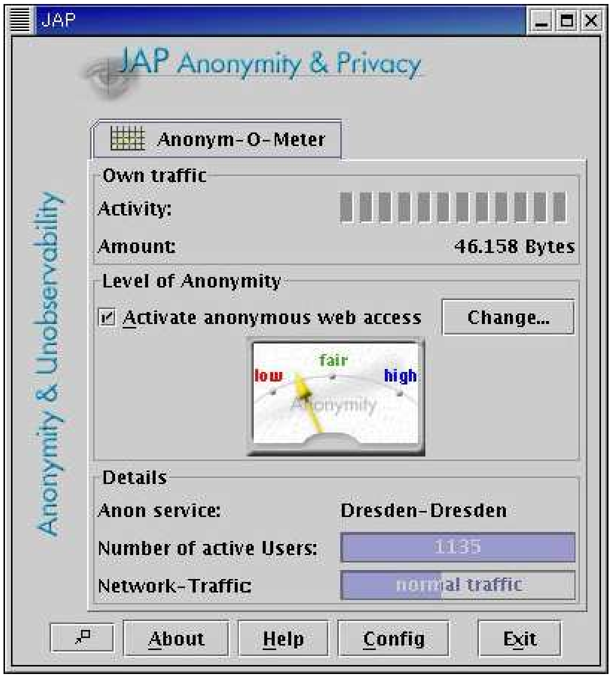
- **Mix Cascades:** In contrast to mix networks (where the sequence of mixes used by a user is freely selectable) the user can only choose between mix cascades, i.e. fixed sequences of mixes. Each single mix in a cascade should be run by an independent institution. The users' web requests are routed in data packets via channels through the chosen mix cascade. Each mix collects the packets sent during a certain time frame by several users, changes their appearance and sequence, and outputs them for the next mix or the web server requested. The packets are multiply encrypted by the client and will be decrypted while travelling through the mix cascade. The output packet of the last mix is the original plain text web request.

- **JAP:** The client software JAP has to be installed on the user's computer. Its main function is to prepare the web requests for a mix cascade by encrypting them multiple times and then send them to the mix cascade chosen by the user depending on his confidence in the institutions running the mixes. Specific port numbers are used; if the client computer is located behind a firewall, JAP may act as SSL proxy using port 443 for the route to the first mix.

- **InfoService:** The InfoService informs the user about the current anonymity level, the mix cascades available and their current workload.

Fig. 2 shows a screenshot of JAP which visualises the current anonymity level, the chosen mix cascade, the number of active users and the network traffic.

Against outsiders a user is anonymous within all users currently using the same mix cascade. Because of the



Activity:

Amount: 46.158 Bytes

☑ Activate anonymous web access

Anon service: Dresden-Dresden

Number of active Users: 1135

Network-Traffic: normal traffic

Figure 2. JAP Screenshot

mixes' decryption their in- and outcoming data packets (which all have the same length) are unlinkable even for an attacker observing all communication channels. The system guarantees unlinkability as long as at least one mix in the cascade works correctly.

AN.ON itself does not keep any profiling statistics about web surfers or the usage of the service. This is guaranteed by two means: Every mix provider has signed a commitment not to store any information about users, and AN.ON is based on Open Source Software. In principle everyone may inspect and make sure that the software provides the expected functionality and does not have trapdoors.

Compared to direct non-anonymous communications the use of the AN.ON system causes a delay and traffic load which is linear in the number of mixes and users. Since all requests (and responses) of all users of a cascade are transferred via several links (mixes), in particular the communication costs are determined by the number of mixes of the cascade. We experienced that the cryptographic operations did not significantly influence the performance of the system whereas the communication bandwidth between two mixes is currently the bottleneck. In practice the delay for users of fast Internet connections (DSL users) is noticeable; for users of low-bandwidth Internet connections there is no difference.

A more detailed description of the AN.ON system and the current strengths and weaknesses can be found on the project website (http://www.anon-online.de).

4 Legal issues

In August 1997 the German Information and Communication Services Act (http://www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf) was introduced. The German legislator regulated among other things the protection of personal data used in teleservices. As part of the Information and Communication Services Act, the Teleservices Data Protection Act was enacted. The law contains many regulations for the processing of personal data by providers. Thus, personal data may be collected, processed and used by providers for performing teleservices only if permitted by the Teleservices Data Protection Act or some other regulation or if the user has explicitly given his consent, cf. paragraph 3 I Teleservices Data Protection Act.

In Germany there is the right to use the Internet in an anonymous way prescribed by law. Paragraph 4 VI of the Teleservices Data Protection Act says: "*The provider shall make it possible for the user to utilise and pay for teleservices anonymously or under a pseudonym if this is technically possible and if this can be accomplished at reasonable effort. The user shall be informed of this possibility.*" Teleservices are bound by law to offer the user anonymous use and payment. In particular, the provider must not store (possibly) personal data such as the IP address; also data retention for unspecific purposes of law enforcement is not allowed. In carrying out this obligation AN.ON's purpose is to enable anonymous use of the Internet according to the specifications of the Teleservices Data Protection Act.

Strong data protection is subject of many discussions. For example [6] criticises almost all privacy-friendly obligations as dangerous. However, [9] points out that users should be empowered to protect themselves in spite of the increasing profiling activities of private organisations.

5 Aspects of misuse

One of the research questions is whether and how AN.ON's anonymising system is misused by criminals. Shortly after starting the anonymising service there were both criminal prosecution agencies like police or public prosecutor's offices and private individuals who complained about misuse of the anonymising service. They asked for data which would identify the Internet user suspected to such misuse. Because AN.ON stores no user-related data, we have to inform the requesting parties that no data about the user's identity exists.

In order to realise the aim of offering anonymous and unobservable web access on a technical level, the allocation of IP addresses to individual users or to other identifying features is avoided. The anonymising server does not save log files with user-related data. So we cannot provide any information about specific users. And anyway in Germany there

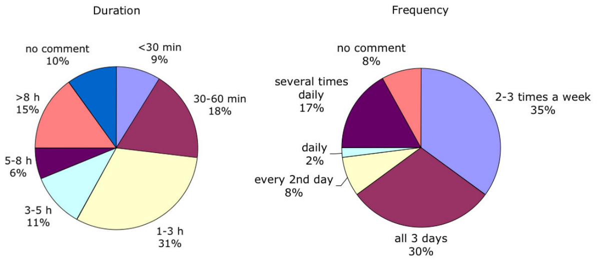


Figure 3. AN.ON Usage

exists no legal obligation to store data about users for purposes of the criminal prosecution agencies. On the contrary it is prohibited by the Teleservices Data Protection Act to create log files with user-related data that are not necessary for providing teleservices or to charge the user for the use of teleservices (cf. paragraphs 5 and 6 of the Teleservices Data Protection Act). As the use of the anonymising service is free of charge, there is no need to store any user-related data for providing the anonymising service. Accordingly the anonymising service is absolutely in line with German data protection and teleservices law [2].

In August 2002 we published statistics about usage and misuse of the system. Within 13 months the software JAP had been downloaded about 100,000 times and 1.2 million sessions had been anonymised. During this time we got 32 complaints regarding possible misuse of the system. In 17 cases criminal prosecution agencies requested a specific AN.ON user's identity. The backgrounds of these requests were attempts of criminal offenses e.g. fraudulent use of credit cards. Furthermore we got 15 requests from private persons or companies. In proportion to the numbers of anonymised sessions the frequency of complaints is very low. In our analysis we conclude that there is little evidence of criminal usage of the AN.ON system, and the system is mostly used to legitimately protect simply the privacy of users [7]. We are aware that this result is just a snap-shot.

Because AN.ON users are even anonymous against the mix operators, it is impossible to determine the absolute number of users. Therefore we speak of 'times' of usages instead of 'users'. The survey among AN.ON users asked for the frequency and duration of AN.ON usage. The respective statistics is shown in Fig. 3. The combination of user answers to the two questions leads to a value of estimated 18 hours usage per week as average usage time of the survey's participants.

The providers of Freedom (http://www.freedom.net), a commercial anonymising service based on mixes which was available until autumn 2001, noticed a higher rate of misuse. Their system provided a pseudonymous communication structure usable by pseudonyms which could be created by users. Their incident statistics is based on these pseudonyms (in contrary, AN.ON users do not have individual pseudonyms and therefore our misuse statistics cannot be pseudonym-based). Freedom's data from May 2000 to February 2001 [3] showed that only 13 % of misuse can be categorised as web surfing ('alleged credit card fraud, site defacements, guestbook abuse, etc.') while 82 % were misuse cases of information distribution by the way of e-mail ('alleged spam, dropboxes, and harassment') or Usenet ('alleged impersonation, inflammatory posts, copyright infringement, etc.'). Their overall ratio of misuse incidents to pseudonyms was below 0.2 %.

6 Economic issues

In Chapter 2 the motivation for anonymous web access had been shown among other things on the basis of the survey offered on the AN.ON project website in 2001. An important question is whether users of the Internet are willing to pay for using the anonymising service. This question was asked to the users of the AN.ON system within the scope of the survey. It is important to note again that this survey is not representative for the German population, but nevertheless it gives important information:

About 60 % of the AN.ON users are not older than 30 years. Additional 23 % are under 40 years old. So it can be pointed out that most of the users are younger people. In the scope of the survey the interviewees were asked if and how much money they are willing to pay for using the anonymising service. The evaluation of the survey identifies three groups of users: About 40 % of the users are not willing to pay anything. Approx. 50 % would pay 2.5 to 5 Euro per month. 10 % of the asked users would pay more than 5 Euro per month. The survey also shows that the willingness to pay is independent from the frequency of the use [10].

Another important question is to know in which way the financing of the anonymising service in the future could be realised. On the one hand there could be a system in which users have to pay for the service, based on the extent of usage (frequency or volume) or within a flat-rate fee. On the other hand it is possible that the state offers the use of the anonymising service by operating mix-servers. So the state could provide its citizens possibilities to protect their right to privacy in an effective way [2]. This may be especially relevant for e-government or e-democracy applications which today are typically based on HTTP or HTTPS, e.g., if the state would like to offer its citizens anonymous e-voting.

7 Socio-political side effects

A number of countries and companies censor the Internet access of their citizens resp. users by filtering their web requests following a set of censorship policies stating which web sites are allowed or prohibited. Zittrain and Edelman made an empirical analysis of Internet filtering in China to determine policies that might be used [11].

In the survey among AN.ON users approx. 12 % stated as a reason for using the AN.ON system the possibility to overcome censorship of their Internet access. Also the support e-mails that reach the technical staff indicate this motivation of users. Because AN.ON hides destination and content of an IP packet by encryption so that only the address of the first mix can be observed, censorship policies based on destination addresses or content keywords cannot work.

This impact of AN.ON, valuable for many users all over the world, was not planned to be addressed within the project. But lately some journalists and members of large companies asked for advice because it was not possible for them any longer to use the anonymous web access through JAP. Some countries and companies already have inhibited the access to the AN.ON system (i.e. added the addresses of the AN.ON mixes to their censorship policies) to trace their citizens resp. users again.

8 Conclusion and outlook

Our experience running a web anonymising service is that there is a desire to remain anonymous while using the Internet. About 40 % of the users of anonymising services do not only consume information on the Internet, but also want to distribute some. Our decision to offer anonymous web surfing only seems to keep the overall misuse rate lower than Freedom's until now. We regard as necessary to work out reasonable checks and balances between interests of protecting users' privacy and of effective criminal prosecution. Our goal is to provide anonymity on the network layer as a basic service for identity management, in particular methods to express needs of authenticity and identification on a higher layer and to implement them [5].

The states should be aware that at least e-government applications or other democratic-related activities such as e-voting require a basic protection of users in the Internet, even against the Internet service providers or anonymity providers. Therefore a high degree of anonymity on the network layer is needed. Based on a democratic principle, the privacy of all users should be protected – the states should not go for a solution where only those users get privacy protection who are willing to pay an extra fee for their anonymity.

Nevertheless, the communication costs and expenses for maintaining such a system may also be carried by the users themselves. Therefore, a billing component is currently integrated into the AN.ON system.

The possible change of the legal situation in terms of data retention will challenge anonymity providers. We hope to give input into the international discussion whether data retention could make sense and how to come to satisfying solutions both for privacy and law enforcement.

References

[1] O. Berthold, H. Federrath, and M. Köhntopp. 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*, pages 57–65. Association for Computing Machinery, ACM, ISBN 1-58113-256-5, 2000.

[2] O. Berthold, C. Golembiewski, and S. Steinbrecher. Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes. In *IT-Sicherheit im verteilten Chaos, Tagungsband 8. Deutscher IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik (BSI)*, pages 203–216. SecuMedia Verlag, Ingelheim, 2003.

[3] B. Bratzer and A. Elkin. Experience with Abuse Management in a Privacy-Enhancing System. In *FIRST Conference on Computer Security Incident Handling & Response*, Toulouse, France, 2001.

[4] D. Chaum. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM*, 24(2):84–88, Feb. 1981.

[5] S. Clauß, A. Pfitzmann, M. Hansen, and E. Van Herreweghen. Privacy-Enhancing Identity Management. The IPTS Report. Special Issue: Identity and Privacy, Sept. 2002. www.jrc.es/pages/iptsreport/vol67/english/IPT2E676.html.

[6] H. Fiedler. Der Staat in Cyberspace. *Informatik-Spektrum*, 24(5):309–314, 2001. (Erwiderung zu diesem Beitrag: [9]).

[7] C. Golembiewski. Das Recht auf Anonymität im Internet – Gesetzliche Grundlagen und praktische Umsetzung. *Datenschutz und Datensicherheit DuD*, 27(3):129–133, 2003.

[8] A. Pfitzmann, B. Pfitzmann, and M. Waidner. ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead. In *Information Security, Proc. IFIP/Sec'91*, pages 245–258, Amsterdam, 1991.

[9] A. Roßnagel. Freiheit im Cyberspace. *Informatik-Spektrum*, 25(1):33–38, 2002.

[10] S. Spiekermann. Die Konsumenten der Anonymität – Wer nutzt Anonymisierungsdienste? *Datenschutz und Datensicherheit DuD*, 27(3):150–154, 2003.

[11] J. Zittrain and B. Edelman. Empirical analysis of internet filtering in china. Berkman Center for Internet & Society, Harvard Law School, Update: 11. Dec. 2002. http://cyber.law.harvard.edu/filtering/china/.