AN.ON — Privacy Protection on the Internet[*]

by Hannes Federrath

AN.ON "Anonymity online" is a joint project (2001-2003) from Dresden University of Technology and the Privacy Commissioner of Schleswig-Holstein/Germany. Its aim is to enable every user to protect his privacy on the internet.

Using Internet services nowadays means leaving digital traces. More and more companies try to use these traces to create individual profiles of Internet users. Moreover especially people searching for help or advice in the Internet do not want others to get knowledge of their problems or diseases. Just imagine drug-related advisory services or medical information services. Even in the field of E-Commerce anonymity plays a big role because no one is happy receiving spam email as a result of his Internet activities.

The AN.ON project wants to help everyone to protect his E-Privacy. The open-source software developed within the project tries to reach this goal. The client software JAP provides anonymous and unobservable communication in the Internet. Upon this basis any privacy related Internet service could be built. JAP runs on the JAVA platform and is easy to install and use to enable greenhorns among the intenet user to protect their privacy. Two scenarios using JAP are thinkable:

- JAP helps to protect the personal privacy of a single user. JAP can be installed on the user's computer to protect his Internet actvities.

- JAP helps to protect the privacy of an organization. JAP can also be installed on a dedicated machine, for example on a proxy or firewall. There JAP serves as a privacy gateway for the entire company, and there is no need to install software on the users workstation. This might be very useful for companies in order to hide their transactions and/or research activities on the Internet against observation by competitors or against other spying activities. (Note that a single user within the organization is traceable by the organization.)

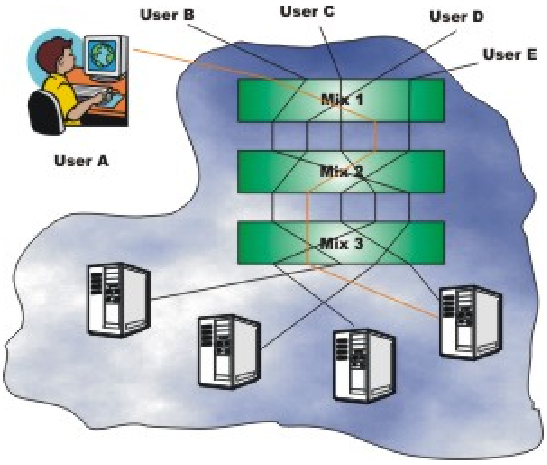
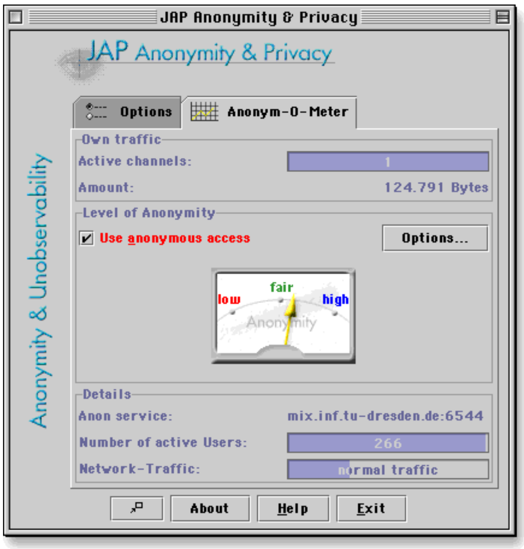


Figure 1: Architecture of the system

JAP acts as a local proxy between the browser and the insecure Internet. All requests for web pages go directly to JAP, and are multiply encrypted there. Instead of directly fetching the requested pages, the request is forwarded through a chain of multiple intermediate servers (named Mixes by the inventor of the theoretical background, David Chaum) offered or initiated by the AN.ON project. The encrypted requests travel through these chain of Mixes to the final destination on the Internet. The web server's responses are returned along the same route. Figure 1 illustrates the architecture of the system.

The multiple layers of encryption protect all messages. A Mix samples messages in a batch, changes their coding (removes one layer of encryption) and forwards them all at the same time,

[*] A sightly modified version has been published in: ERCIM News No. 49, April 2002, 11.



Own traffic
Active channels: 1
Amount: 124.791 Bytes

Level of Anonymity
☑ Use anonymous access

Details
Anon service: mix.inf.tu-dresden.de:6544
Number of active Users: 266
Network-Traffic: normal traffic

Figure 2: JAP user interface

but in a different order. All messages have the same length. The final system developed within An.ON will withstand so-called traffic analysis: Even an adversary observing all communication links cannot decide which incoming and outgoing packet belongs to each other. A surfer remains anonymous within the group of all users of the service.

The system protects a user's Internet behaviour against tracing as long as at least one Mix in the chain works correctly. The Mixes are run by different organizations who were willing to participate in the AN.ON project. The chaining also prevents these Mixes from observing. Thus the system provides anonymity even against the anonymity service itself.

The client program (JAP) is running on the Java platform. JAP works on all major platforms, for instance Windows, Macintosh, Linux, Solaris etc. The Mix-servers are written in C++ and work on many different platforms including Windows NT, Linux, Solaris, Irix and other Unix-like operating systems. JAP and Mixes are Open-Source software. Everybody may inspect it and convince himself, that the software provides the expected functionality and contains no hidden trapdoors. Figure 2 shows the user interface.

Future research in the AN.ON project concentrates on integrating a payment function in JAP and research on services (e.g. pseudonymous email) that might be built upon the infrastructure AN.ON already provides. We are always looking for partners - ISPs, IT security companies, networking companies, privacy commissioners - who are willing to operate a Mix and would like to support the idea of providing a world wide anonymity service. We are open to partners who want to discuss commercialization of our service.

AN.ON is a joint project from Dresden University of Technology and the Privacy Commissioner of Schleswig-Holstein/Germany. From 2001 to 2003 the project is sponsored by the German Federal Ministry of Economics and Technology.

Link:
http://www.anon-online.org/

Please contact:
Hannes Federrath
Dresden University of Technology, Germany
Tel: +49 351 463 38247
E-Mail: jap@inf.tu-dresden.de