

Usability Inspection of Anonymity Networks

Dhiah el Diehn I. Abou-Tair, Lexi Pimenidis, Jens Schomburg
Chair for IT Security
University of Siegen
Hölderlinstraße 3
57076 Siegen, Germany
{aboutair, pimenidis, schomburg}@fb5.uni-siegen.de

Benedikt Westermann
Centre for Quantifiable Quality of Service in
Communication Systems
Norwegian University of Science and Technology
7491 Trondheim, Norway
westermann@q2s.ntnu.no

Abstract—Today, to be monitored while surfing the web seems to be a natural act and thus tools and applications to achieve online anonymity are more important than ever. The usability of such a tool plays not only a prominent role for each single user; in the area of anonymization networks it usually holds that the protection for every single user is higher, the more users participate. Hence, usability is of great importance, since bad usability decreases the number of potential users.

In this paper we examine the usability of four software implementations for anonymous communication techniques especially with regards to the installation procedure. The usability is evaluated with the help of cognitive walk-throughs. We also inspect the quality of service of these implementations by means of a performance test.

Keywords-HCI; Tor; AN.ON; JAP; JondoNym; JonDo; Anonymity; Usability

I. INTRODUCTION

An increasing number of academic publications are dealing with anonymous communication and its implementation. Most of them deal with technical issues associated with the anonymization process and attacks on the routing mechanisms. They are a crucial basis for good anonymity systems. Beside this, also a huge user basis is seen as an important factor to provide good anonymity [1]. Therefore, it is in most cases¹ essential to acquire as many users as possible. The developers, the providers and some of the users are aware of this need. Hence, they try to advertise new users for their network.

Unfortunately, a huge amount of users neither have expert knowledge nor have good computer skills. Therefore, it is vitally that anonymization networks are easy to use. Thus, usability is an essential matter which can not be compensated by the knowledge of a few experts [4].

Usability with respect to different Tor configurations has been discussed in [5]. However, the work presented in [5] ignored the examination of other anonymity network implementations. The authors of [5] defined certain guidelines in order to examine usability and deployability. In this paper we adapt their principles to maintain compatibility.

¹In Crowds an increasing number of users actually decrease the degree of anonymity [2], [3].

Actually, there are various software implementations of anonymous communication techniques. Due to space and time limitations it is not feasible to observe all of them in this work. We focus on four different systems which are likely to be those with the highest number of participating users. We chose and examined with respect to this demand: Mixmaster (Email Messaging and Usenet) and three low latency networks (Tor [6], I2P, AN.ON/Jap [7]). Regrettably, it was unfeasible to install and configure a pure Mixmaster implementation. Therefore, we chose an alternative Mixmaster client (Quicksilver). The reasons for this are discussed in more detail in section IV-D.

The paper focuses on usability aspects of anonymous web browsing and e-mailing. Especially, it targets at the *installation* process. The installation of software is a unconditional prerequisite for new users to use and participate in an anonymization network. This stresses the importance of its usability.

Once a new user was able to correctly install and configure her system, the *performance* is crucial to convince the user to use the system on a regular basis [8]. Hence, we also conducted a small performance test for some preliminary results to build a more holistic picture of the current situation.

The tests have been conducted using *Windows Vista Home Premium (SP1, 32-Bit)* as this is the most recent operating system of the Windows series. Further, a small-sized performance test was run using the *Ubuntu (8.04)* operating system.

This paper is structured as follows: in section II we discuss how the paper relates to existing works. Section IV presents the evaluation methodology. Our main contribution is a cognitive walk-through which is presented in section IV. We also did a small performance test which is shown in section V. Section VI concludes the paper.

II. RELATED WORK

Comparisons of the most important anonymity network implementations with regard to usability by installation, configuration and their usage are to the extend of our knowledge missing in the academic literature. Existing surveys, e.g. [9] of George Danezis and Claudia Diaz compare

technical characteristics like degree of anonymity [10] or performance. Unfortunately, such a comparison with regard to usability is only found in [5] which focuses on usability and deployability by means of different configurations of Tor.

Remotely related is a work of Rolf Wendolsky, Dominik Herrmann and Hannes Federrath [11]. They did a performance comparison of low latency anonymisation services namely Tor and AN.ON. They showed that users are only willing to use the system as long as it provides a reasonable performance [8]. Thus, performance is important with respect to the user basis. Only with a good performance it is on long-term possible to enlarge the user basis.

III. EVALUATION METHODOLOGY

The evaluation methodology used in this paper in order to evaluate the usability of different anonymization services is the same evaluation methodology as the one presented in [5]. The evaluation methodology is built on a cognitive walk-through method, which identifies four core tasks:

- **CT-1** Successfully install the anonymization software and the components.
- **CT-2** Successfully configure the browser (email client in Mixmaster/Quicksilver case) to work with the anonymization software.
- **CT-3** Confirm that the web-traffic/email is anonymized.
- **CT-4** Successfully disable the anonymization software and return to a direct connection.

Usability itself is measured by the following eight guidelines as presented in [5] :

- **G1** Users should be aware of the steps they have to perform to complete a core task.
- **G2** Users should be able to determine how to perform the steps.
- **G3** Users should know when they have successfully completed a core task.
- **G4** Users should be able to recognize, diagnose, and recover from non-critical errors.
- **G5** Users should not make risky errors from which they cannot recover.
- **G6** Users should be comfortable with the terminology used in any interface dialogues or documentation.
- **G7** Users should be sufficiently comfortable with the interface to continue using it.
- **G8** Users should be aware of the status of the application at all times.

In the next four sections we will discuss our findings based on the above guidelines.

IV. EVALUATION OF THE SYSTEMS

In our tests we make the assumption that an interested individual has come across the name and the website of one of the four anonymization services we analyse here. She

decided to download, install and use each of them. Hence, our evaluation starts with the respective project's website and continues to the usage of a service. In addition, we also check how easy it is for an end user to temporarily deactivate the anonymization service after usage.

A. Tor

1) *Download and Installation of Tor*: Tor's project website² presents a good starting point to achieve anonymity in the Internet, i.e. to accomplish the tasks CT-1 to CT-3. A user can choose on the website between many languages. The website itself has a clear layout. Additionally, the operators of the site use a simple and natural language (conforms with G6). A general explanation on how Tor works is given directly on the first page. Furthermore, a user can find some helpful examples of typical Tor users as well as some links to more detailed information.

The start-page of Tor contains three statements under the title "three pieces of fine print". They clearly state that anonymity in the Internet via Tor may only be achieved if and only if Tor is used correctly. A link to a list of some warnings is given with the aim to prevent the user from fatal errors (conforms with G5).

The statements declare that despite a correct use of Tor, there are still possible attacks that compromise user's protection (conforms with G5). Further, the statements make it clear that no anonymity system is perfect and thus users with a demand for strong anonymity³ should not rely on Tor. Both last declarations provide clarities. However, some users might become scared. This is a dilemma which is not easy to solve. We believe that a good explanation of the circumstances like the Tor site provides, is the best way to deal with the dilemma.

The "Summary" navigation on the right side of the first page contains a button labeled "Download Tor". A click on the button leads to a download page (conforms with G1, G2). Next, users have the opportunity to choose between two Windows installation bundles and one for OS X. An inconsistent point to G1 and G2 is reflected in the absence of a hint to an installation manual. However, if the user clicks on "See advanced choices" she gets to another side which contains links to a step-by-step installation manual as well as more download choices.

As filename for the download "Vidalia-bundle" is suggested. The same name is also used during the installation process as name for the Tor package (see Figure 1). The name is not announced and therefore a novice user might be scared away due to a missing explanation on the link between the terms of "Vidalia" and "Tor" (violates G2).

In the first dialog of the installation the user can choose between nine different languages. Unfortunately, not every

²<http://www.torproject.org/> (25.02.2009)

³However, the term "strong anonymity" is neither defined nor explained.

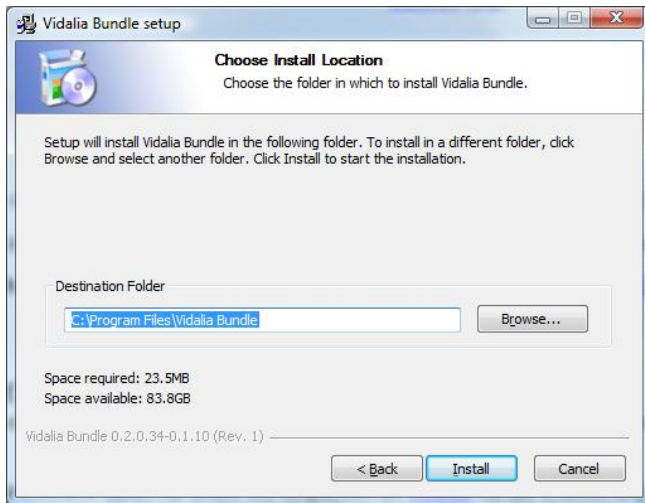


Figure 1. Tor installation wizard

dialog of the following dialogs is fully translated. For instance, the second dialog of Tor’s installer in the German version is not translated at all. Moreover, not every dialog provides the same level of detail, e.g. the Italian version does not provide detailed information on the purpose of the different components on the second dialog. However, even the possibility to choose between different languages greatly contributes to the usability (conforms G2, G6).

The installation process asks the user to install Vidalia (a GUI for Tor, <http://www.vidalia-project.net/>), Privoxy (an application layer filtering web proxy) and Tor button (a Firefox extension). The purpose of the components is several times briefly explained during the installation process. In addition, the installation manual on the project’s website also contains a brief description. The rest of the installation is straight forward. All this supports the user ideally to achieve CT-1 (conforms with G1, G2).

G8 is given through the realization of an installation progress bar which shows the progress of unpacking the program packages. Once the progress bar reaches 100%, the Firefox standard dialogue for installing extensions pops up and provides a recommendation to install Add-Ons only from trusted sources. With the conformation to install the extension, the installation of the Vidalia Bundle is completed. This will be illustrated in an extra dialogue together with the standard check box “Run installed components now” and a link to <https://www.torproject.org/docs/tor-doc-windows>. At this point the confirmation screen signals the user that CT-1 is completed (conforms with G3).

2) *Configuration of Tor:* When the Tor program is started by the user, the Vidalia control panel (see Figure 2) opens and connects to the Tor network. The duration of establishment of such a connection is about two minutes. However, the user is not aware of the application status (violates G8). In addition, there are two new icons in the task-bar installed:

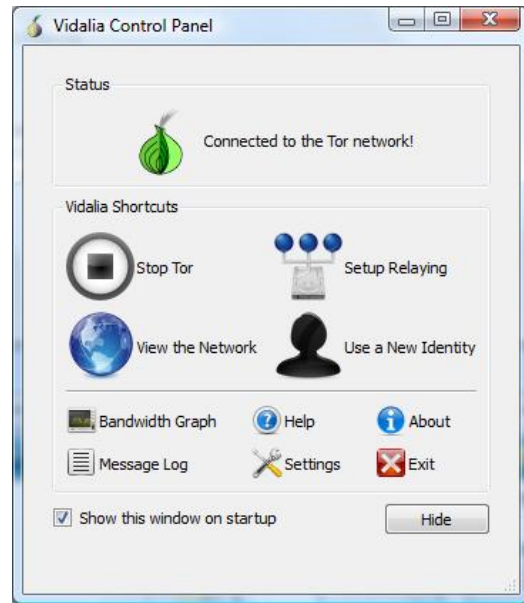


Figure 2. Vidalia console

- a green onion (alternative-text⁴: “connection to the Tor network established”) and
- an animated blue circle with a white “P” (Privoxy).

In Firefox the newly installed plugin adds a cue to the status bar indicating “Tor deactivated”. Once a user clicks on the cue the message changes and following message is displayed if the current Firefox (version 3) is used:

Warning! Torbutton on Firefox 3 is known to leak your timezone and livemark feeds during Tor usage.

In addition, it has not been as extensively tested for Tor security and usability as Firefox 2.

Do you wish to continue anyway?

Due to the warning a user might not know how to proceed (violates G2, G6). Through clicking on the OK button the cue switches to “Tor activated”. Now the user knows that her traffic is anonymized (conforms with G8). With the standard settings Tor works immediately. No further configuration is necessary and thus CT-2 is completed.

3) *Check and Deactivation:* Up to now, the user receives feedback by the “green onion” that Tor is working properly. Unfortunately, the user cannot easily check if her traffic is actually relayed through the Tor network (CT-3). Tor does not provide an easy to find reference like a button or bookmark to such a service, e.g. a website which checks whether the traffic is anonymized or not. Although a server of the Tor project hosts a webservice⁵ which checks, if traffic was relayed through the Tor network.

⁴The text shown by positioning the mouse over a symbol or button.

⁵[http://check.torproject.org/\(27.02.2009\)](http://check.torproject.org/(27.02.2009))

CT-4 can also be easily performed by clicking the cue in Firefox. After the click the traffic will no longer be relayed through the Tor network. The fact that the user has to click on the cue again can be considered as G2 compatible.

B. I2P

1) *Download and Installation of I2P:* The Website⁶ of the I2P project is available in English and German. Their page is clearly arranged and welcomes the visitor with an introduction on I2P. The introduction presents some of the supported applications, gives a brief statement about anonymity and mentions the fact that I2P is evolving over time and should only be used for testing and development purposes.

In their introduction are several notable aspects. Firstly, it is strange that their list of possible applications does not contain web browsing even though it is supported and one of the most important applications in the Internet. The language is technical and maybe too technical for a novice user (violates G6). The picture which explains the function of I2P is also not easy to understand (violates G1, G2). Secondly, the statement that the current software should only be used for testing and development purposes can be seen as a problematic aspect. Without an explanation of the background the statement can distract users.

In order to complete CT-1 a user needs to find the link "Download". We assume that a novice user can achieve this due to the common layout of I2P's website. After a user opened the download site, she is confronted with three different downloadable versions: graphical installer, headless install and source install. The descriptions given for each version might direct novice users to download the graphical version (conforms with G2). Nevertheless, G2 and G6 are violated since the statement regarding the precondition for the installation of I2P (Sun Java 1.5 or higher, or equivalent JRE) does not refer to any manual or explanation. It is uncertain if a novice user knows Java and even knows how to install it without any help. If Java is missing, the execution of the downloaded file will show "Cannot find Java 1.5.0". When the user confirms the error the installer terminates and opens the website of Sun, where the user can download Java (conforms with G1). At the same time it disregards G6, due to the too brief error description.

In case Java is installed correctly, the installer shows in its first dialogue a small welcome message. The following procedure is similar to typical installation processes. The installation progress is, as well as in the case of Tor, displayed by a progress bar. Afterwards the user needs to decide if she wants that the setup routine creates shortcuts on the user's desktop. In the last dialog I2P signals the user that the installation process is finished. This installation

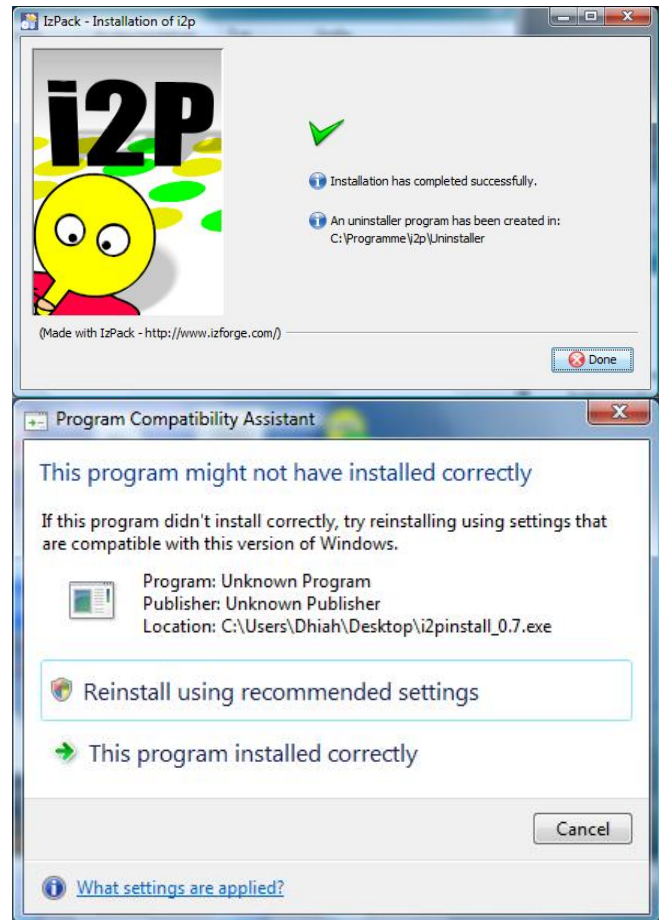


Figure 3. Warning after a successful installation of I2P

procedure is straight forward and complies with G1, G2, G3 and G6; CT-1 is reached.

After the user closes the installer Windows displays a dialogue. It informs the user that the program she wanted to install has maybe not been correctly installed. In addition the dialogue offers the user two different options (see Figure 3). This incident clearly violates several guidelines such as G1, G2 and G8.

If a user selects the default options of the I2P installer, three icons are created on the user's desktop: "Start I2P (no window)", "Start I2P (restartable)" and "I2P router console". The same shortcuts are created in the startmenu of Windows. In addition, a shortcut to an uninstall procedure is added in the startmenu.

In order to complete CT-2, with regards to the manual, the user should simply click on the "Run I2P" button which will bring up the router console with further instructions. Because there is no button or shortcut named "Run I2P" (see above which shortcuts have been created) the user does not know how to proceed (violates G1, G2). It also cannot be assumed that a novice user knows what a router console is, so G6 is disregarded. Since a router console is mentioned in

⁶<http://www.i2p.de> (27.02.2009)

the instruction, a user might click on the “I2P router console” shortcut. On our test-system the Firefox Browser is opened with the URL `http://localhost:7657/index.jsp` which displays a connection fail error (violates G4).

Since no further documentation is available, the “Start I2P (no window)” shortcut is chosen and, as a result, the Internet Explorer (and not the default browser Firefox, as on our system) opens with the URL `http://localhost:7657/index.jsp`. The page states: “Congratulations on getting I2P installed” (conforms with G3).

If the user had managed to open the I2P configuration site, the browser presents a welcome page to the user. The page has three different parts that each contain a lot of information. Thus, the page appears (quite) complex. The first part is a sidebar on the left. The sidebar is divided in seven categories. Each presents various status information to the user, e.g. the status of the established tunnels.

The navigation bar is on the top of the page. It contains links to various services of I2P, e.g. *Susimail*, *SusiDNS*. The content area is placed under the navigation bar.

The content area itself is again divided into two scopes. The first scope shows the phrase “Congratulations on getting I2P installed!” and gives further instructions on how to proceed and configure I2P. The information is displayed in English as well as in German. The second scope of the welcome page provides instructions how to use and configure different services in the I2P net as well as the Internet. This instruction is only displayed in one language, but the user is able to pick one out of four languages. However, the confirmation of the successful installations fits G3 and signals again that CT-1 is completed.

2) *Configuration of I2P*: To complete CT-2 a user needs to read both instructions on the welcome page. The instructions of the first scope are similar with those on the download page. They may fulfil G1 and G2 in order to perform CT-2. Unfortunately, the instructions are written in a technical language. The user is asked to adjust the bandwidth, to open port 8887 on the user’s firewall and to enable “inbound TCP” on the configuration page. The instructions do clearly not address novice users (violates G6). Hence, errors in the configuration are getting more probable (violates G5). If the user had completed the tasks (adjusting the firewall and bandwidth settings), I2P neither provides feedback nor clearly states how the user can check if she has finished successfully the configuration of the first scope. This disregards G3.

The second scope of the content area deals with configuration of different applications and services. However, for a novice user the separation may not be understandable. Therefore we claim that it does not support users in achieving CT-2 (violates G1, G2)

In the part “browse the web” the instruction refers to another part. The referred part states that the user should tell the browser “to use the HTTP proxy at localhost port

4444”. Clearly, the description is not suited for a novice user: it uses technical language (violates G6) and a user might not know how to complete the task (violates G2). The same circumstance was examined for Tor in [5].

After the user finished the instructions in both scopes, she has completed CT-2. However, I2P does not present any information that the user has achieved CT-2 (violates G3). Beside the mentioned shortcomings, I2P currently also presents too many tasks and options to the user. It hinders her to use I2P comfortably (violates G7) and safe; the latter is due to the fact that the more users tweak their settings, the more likely they can be identified by an adversary because of their client’s individual behaviour.

Now, if the user finishes the configuration within a short time frame, she might receive the following error message, after she has requested a website:

```
The WWW Outproxy was not found. It is offline,
there is network congestion, or your router is not
yet well-integrated with peers. You may want to
retry as this will randomly reselect an outproxy
from the pool you have defined here (if you have
more than one configured). If you continue to have
trouble you may want to edit your outproxy list
here.
```

```
Could not find the following destination:
```

```
http://some-URL/
```

```
WWW proxy: false.i2p.
```

The message displayed is another example that the authors of I2P fail to use a non-technical language (violates G6). A novice user might not understand the message. Thus, she does not know how to proceed (violates G1, G2).

Just by waiting some minutes the user will be able to open the same website successfully. This behaviour might not be understandable for the user (violates G8).

3) *Verification and Deactivation of I2P*: Since I2P offers neither an application nor a link to the user, she can not check if her traffic is anonymized or not (CT-3). In order to check whether CT-3 was successfully finished, the user needs to compare her own (real) IP-address with the one a receiver gets together with a request of her. Again, this is probably too difficult for a novice user.

CT-4 can be performed by clicking a “shutdown” link in the configuration page. But as this just turns off I2P. The user additionally has to reverse the configuration in the browser, too. Due to the fact that the initial configuration step violated G2 and G6, it is clear that the reverse action does the same.

C. JAP/JonDo

The JAP/JonDo anonymizer [7] is known under various names: in this paper we use JonDo as name for the client software. The name was established by the commercial anonymization service *JonDonym*⁷. The service as well as

⁷<http://www.jondos.de/> (27.02.2009)

the software build upon the AN.ON project and its client. The client software of the AN.ON project is JAP. Even though JonDonym is a commercial service some of the mix cascades are freely available.

1) *Download and Installation of JonDo:* The JonDo website is available in English and German. G6 is satisfied through an explanation and an illustration of how JonDo works. The illustration can be found directly on the first website.

An issue worth mentioning is that there are no hints on possible dangers or attacks, contrary to other examined websites (violates G5).

A download button is placed clearly and visible on the left-hand side, so the user is aware of the next steps she has to do (conforms with G1, G2). With a click on the button a user can choose between different JonDo versions, namely for Windows, Linux and MacOS X. At this point an explanation is given that no registration is required and “the software and simple services it provides access for, are free of charge”. Further, it is clearly declared that payment is only required for the optional premium services. The premium services offer: a higher speed and better security by allocating enough cascades for the connection, provide longer Mix cascades which are typically spread over several countries and offer all Internet ports for usage, whereas the free services only allow web surfing.

On the download site some additional information can be found. Firstly, some installations hints and an easy to use “download button” are presented to the visitors of the website (conforms with G2). Secondly, an announcement is made that the installation process of JonDo does not make any changes that affect the user’s computer. It simply copies the JonDo packages to a default directory or to another directory the user may choose. Thirdly, an introduction to browser configuration is given for the reason that each browser used along with JonDo has to be individually configured. This declaration refers to a wizard that helps the user through such a configuration. The wizard starts when the application is executed for the first time (conforms with G1, G2). Alternatively, users have the option to use a preconfigured browser named JonDoFox instead of configuring the browser by their own. The JonDoFox browser is recommended by the JonDo provider in order to eliminate non-recoverable errors (conforms with G5). Fourthly, the website provides users with some information about the downloadable files. Fifthly, the download page provides some information how to update the JonDo software. Sixthly, a recommendation is given to the user that she should check the authenticity of the downloaded file. Beside the recommendation the download page provides the user with a reference how she can perform the authenticity check. The last part of the page briefly states that the user is allowed to distribute the software (conforms G1, G2).

The user is directed to another web page if she chooses

to install the Windows version. On this page she has the choice to install the JonDo desktop or the JonDo portable version. Both versions require Java 1.3 or higher to work. For this purpose, a link to the Java homepage (<http://java.com/>) is given. However, if the user have not installed Java, the installer will install Java 1.3 on the user’s computer. Sadly, there is no indication about the purpose of Java (violates G6). The default name for the installation package is given as “japsetup.exe”. Such a name may not be expected since JAP is the name of the client software in the AN.ON project which might be confusing for some users (violates G6). The application version number is specified above the navigation menu on the left side, but the version number is specified neither on the download page nor on the package name. This is not contradictory to any of the guidelines as presented in section III. However, more clearness on the version number can be useful for users, for example, when checking for updates.

The installation process starts with a dialogue where the installation components can be chosen. As a preselected configuration JAP, Swing and Java 1.3 are set. In the dialogue the name JAP is used five times instead of JonDo. It may bother the users and thus be in conflict with G6, because it is not necessary to know that JAP is a different name of JonDo. Moreover, it might violate G2. A clear defined name which can be used continuously will be more comprehensible. After the installation process the installer informs the user that the installation was successful. CT-1 is reached.

2) *Configuration of JonDo:* At the first start of the JonDo application a wizard starts to configure JAP/JonDo in the respective browsers. An explanation is given on how to use the JAP/JonDo proxy settings for each of the browsers. The used language is a non-technical language (conforms with G6) and offers a straight forward description of the single steps (conforms with G2). Warnings are displayed once the user tries to open a website, if JAP/JonDo is switched off.

In order to test the connection to the anonymity service, the user will be demanded to switch anonymity on and to surf the Internet. Due to the interface (see Figures 4,5) this is straight forward. In our examination, the test was not achievable because a timeout limitation had occurred. The fact that a connection was established, but no website has been presented, indicates to the user that she should choose the option “Connection established but web surfing impossible” in the configuration wizard. Subsequently, the wizard requests to choose the cascade⁸ with the name “Dresden-Dresden” and prompt browsing in the web becomes possible.

Guidance to disable Java, JavaScript, ActiveX, Flash, etc. according to the type of browses is given in the next dialogue

⁸A cascade is a sequence of mixes which are responsible for the anonymization process

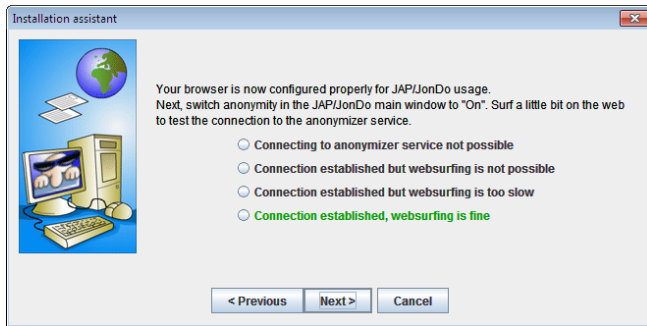


Figure 4. JAP / JonDo configuration wizard

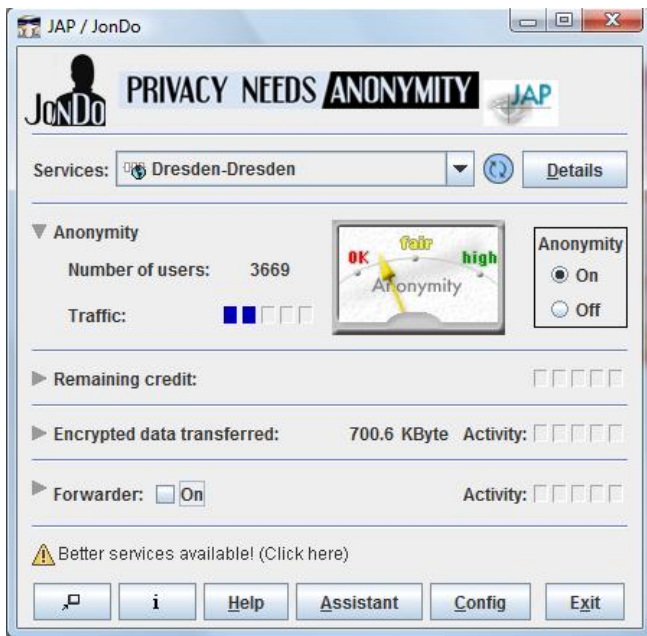


Figure 5. JAP / JonDo console

of the wizard, as these web technologies threaten the users privacy and can be used by adversaries to circumvent network layer anonymization. Next, a dialogue is presented with the option to run JonDo in either a simple or an extended view. A link is given to the JonDo FAQ and at last a confirmation screen of a successful configuration of JAP/JonDo is shown by the wizard. Thus, it gives the user a feedback that CT-2 is achieved (conforms with G3).

The step-by-step wizard has been proven as a good way to avoid users from making errors throughout the configuration of JonDo (conforms with G4, G5) and is simply to understand (conforms with G6). Further, the wizard can be restarted from the JonDo application and in this manner supports G4.

3) *Verification and Deactivation of JonDo:* An anonymity test is available on the JonDo website ⁹

⁹<https://www.jondos.de/de/anontest>

which shows several transmitted information from the visiting system (conforms with G3). CT-4 can be achieved by clicking on the “anonymity off” switch. When a user clicks on the button a message is displayed that JonDo does not support any protection further on (conforms with G1, G2, G3).

D. Mixmaster / Quicksilver

1) *Website of Mixmaster:* The Mixmaster website¹⁰ is offered in plain HTML. English is the only available language of the website. A welcome page gives a brief explanation of Mixmaster and its properties. This is followed by a link to the subversion tree of Mixmaster as well as several signatures of former Mixmaster releases. On the top of the side a simple navigation bar is given. Some links are provided to the user, among other: “FAQ” and “Download”. The style and the content as well as the technical language clearly show that the page is intended for professional users (violates G6).

The FAQ contains, among other things, the following statement¹¹:

It is possible to run a remailer on a Windows system, but due to the massive security holes and general lack of stability, this is not recommended. If one chooses to run Windows, one will probably have the most success with Windows 2000, as it is the most stable and secure of the Windows operating systems.

Again, this makes clear that Mixmaster is not intended for non professional users. Also, Windows 2000 is clearly deprecated – hence the sentence is false.

If a user clicks on the download link, she gets redirected to the Sourceforge¹² page, where she can download Mixmaster. Unfortunately, neither a manual nor helpful hints are given on that site (violates G1,G2).

The software itself is shipped within a compressed tar file. Thus, a user needs to know how to decompress the downloaded package (violates G1, G2).

If a user manages extract the files from the tar file, she sees several folders. Due to the fact that the README file does not provide any hint to the user how to install Mixmaster on Windows, the user needs to explore the folders herself. The win32 folder includes the file mixinstall.nsi in the directory win32/installer/. The file seems to be an installer. We claim that a novice (even a normal) user is not able to come that far. Therefore, we stop our evaluation at this point for Mixmaster. It is an unambiguous violation against G1, G2 and G6 and thus too distracting for normal users.

¹⁰<http://mixmaster.sourceforge.net/> (27.02.2009)

¹¹<http://mixmaster.sourceforge.net/faq.shtml> (27.02.2009)

¹²Sourceforge hosts various software projects.

2) *Download and Installation of Quicksilver*: We continue our investigation with an alternative client implementation called Quicksilver¹³. The Quicksilver website uses a simple layout and consists of pure textual content. An introduction about Quicksilver, how it works and why it is interesting to use Quicksilver is given at the beginning of the website. The author of the site states that quicksilver provides complete privacy. Therefore, a message which is sent via the Quicksilver client cannot be traced backward in order to identify the sender. The language of the website is simple and non technical (conforms with G6). The fact that Quicksilver is just a user interface for Mixmaster is explained on the website. In addition, it is stated that only one person, Richard Christman, develops the client. In order to download the package a hyperlink is given in conjunction with a hint to the read the `welcome.txt` file of the client packages. Thus, a user can determine how to perform the remaining steps (conforms with G2).

The installation process can be started after downloading the file `QS1.2.7.exe`. A dialogue pops up and by pressing the setup button a wizard installation program starts. The user has the opportunity to select an installation directory or to use the default suggestion offered by the wizard. In addition, she can select if a shortcut to her desktop should be added as well as if a program group should be created. Such a proceeding is known by users (conforms with G2).

The second dialogue demands the user to provide her email address and an SMTP host (Figure 6). To help the user to fill in the required information a text and two examples are given. The text explains for what purpose the email address and the mail server are used. In addition to the text some examples are provided. Both, the text and the two example illustrate a violation to G6 because users may feel confused (violates G6). Considering the examples alone the user cannot find out how to complete the step (violates G2).

The last dialogue of the installation process gives an overview of the options which have been chosen in the configuration. A confirmation will be given as soon as the installation is completed. Thus a user recognizes that she reached CT-1 (conforms with G3).

The wizard style installation helps to avoid non-recoverable errors. Due to the “next” and “back” buttons a user can easily change false statements she made during the installation process (conforms with G5).

3) *Configuration of Quicksilver*: As soon as Quicksilver has been started a prompt pops up in order to inform the user that Mixmaster is not installed despite being an essential component. A button labelled with non technical language (conforms with G6) “Get Mixmaster” indicates the next step (conforms with G2). If the user clicks on “Get Mixmaster” a wizard is started. In the first dialogue some information is presented to the user. The information points to the source

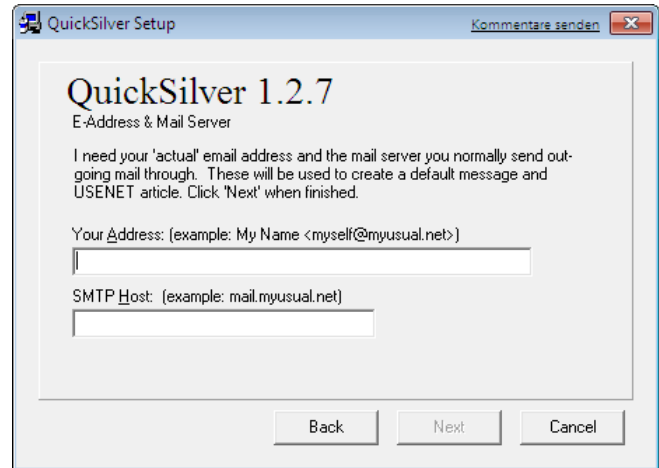


Figure 6. Installation dialogue of Quicksilver

code of Quicksilver and provides the user with an email address in case a bug is discovered by the user. The user’s only possibility is to confirm this information. Afterwards the installer asks the user to pick an FTP site from a drop-down list. If the user does not know the word FTP, she cannot make use from this point (violates G6). Once the user chooses the default site, the wizard shows a list of available updates among other Mixmaster (`Mix29b39.zip`). A user might be swamped due to the possibilities offered by the list (violates G2, G6).

After downloading the Mixmaster package of Quicksilver the user can start the install routine which is similar to the Quicksilver installer. Unfortunately, some very technical terms are used without a good explanation (violates G6):

“In actual use, this will be the directory where Mixmaster looks for ‘mix.cfg’ and QuickSilver looks for ‘mixlib.dll’ and ‘libey32.dll’ ”

In order to obtain some random data for the initialization of the random Mix pool, the install routine asks the user in the next dialogue to write her name using the mouse. This illustrates a distinct instruction even if the user does not know its purpose (conforms with G6). The user can observe the progress of the pool initialization via an indicator that displays the progress in percentage. The progress advances according to the user’s mouse writing. As soon as the indicator reaches 100% an “install” button becomes available. Once the Mixmaster setup is completed, it will be announced by a confirmation screen (conforms with G3).

Consequently, the QuickSilver interface opens and indicates that QuickSilver is ready to be used. Unfortunately, the GUI offers various buttons whose functionality is unclear (violates G7).

The help-system of Quicksilver provides a Quickstart section; sadly the steps specified in the section take a lot of time to be performed. This might appear as the opposite of quick. Chapter “I-8 Anonymous Messages” of the help-

¹³<http://www.quicksilvermail.net/> (27.02.2009)

system describes how to use QuickSilver in order to send anonymous messages. Additionally, it explains the interface “New Message”. Unfortunately, the interface has a non standard design. Thus, users are probably not familiar with its handling from other programs or applications. In essence, it contains a text field with predefined values where users have the possibility to edit or add some parameters. CT-2¹⁴ cannot be achieved with such a design. It is not intuitive to handle as usual. In addition, it does not prevent the user from making erroneous inputs (violates G5, G7).

As soon as the user has composed a test message and has pressed on the “Send” button, a dialogue appears with the note “Mixmaster Remailer Documents is missing”. This means that CT-2 is not fulfilled yet. Up to this point, the user had no chance to recognize this problem (violates G1). In order to lead the user through the configuration step a “Get documents” button is offered (conforms with G2). After a click on the button a dialogue with several other options is displayed. Here the user has the opportunity to specify URLs for the download of the missing files, e.g. “m1ist.txt”, “pubring.mix”. In addition, a reference is provided, where the user can get a brief explanation about the needed files (conforms with G2). After reading the help notes, executing the instructions (check m1ist.txt and r1ist.txt) and clicking update, the application fetches new remailers and keys. We claim that the whole procedure is too complicated and opaque for a user who has not read the complete manual.

After a user has managed to receive the files and tries to send a message, the process quits with an error messages: “No reliable remailers!”. In order to solve the problem, the user needs to seek for new sources of so-called remailer stats and keys. However, even for an average user the procedure is too demanding (violates G2, G6). Moreover, the software fails to send the message through the mail-server that was entered during the installation process. The reason for the failure was that no credentials were specified for the mail server. Thus, a user needs to enter her credentials for the outbound mail-server in order to send anonymous email. Unfortunately, there is no hint given where to enter such information. Therefore, a user has to find it herself (violates G2).

In our opinion, the whole configuration process is very complex and normal users have no chance to master this task. The configuration process violates G1, G2 and G6. Further, the interface cannot be handled in comfortable way which contradicts G7. The fact that Quicksilver is a standalone program makes it dispensable to examine CT-4.

Table I illustrates the guideline violations while trying to achieve the core tasks; table II summarizes the general guidelines violations.

¹⁴CT-2 in this context means that the user should be able to configure the application the way that anonymous email can be sent.

Anonymity network	CT-1	CT-2	CT-3	CT-4
Tor	3	2	0	0
I2P	5	9	1	2
Jap/JonDo	3	0	0	0
Mixmaster	nr	nr	nr	nr
Quicksilver	6	9	nm	nm

nr = core task not reachable; nm = metric not measurable

Table I
GUIDELINES VIOLATIONS PER CORE TASK

Anonymity network	Guidelines							
	1	2	3	4	5	6	7	8
Tor	1	2	0	0	0	1	0	1
I2P	3	4	1	1	1	4	1	2
Jap/JonDo	0	1	0	0	1	1	0	0
Mixmaster	nm	nm	nm	nm	nm	nm	nm	nm
Quicksilver	2	5	0	0	1	5	2	0

nm = metric not measurable

Table II
SUMMARY OF GUIDELINES VIOLATIONS

V. PERFORMANCE TEST

As explained in the introduction, the Quality of Service is a second important factor to maintain a large user base.

For the test we repeatedly downloaded files over the HTTP protocol using the respective anonymisation networks. However, it should be noted that these tests were only conducted as an informational addendum.

Due to the fact, that in Mixmaster the delay of messages is a core feature to achieve anonymity a performance test is obsolete. Table III presents the results of the performance tests.

VI. CONCLUSION

The main question addressed in this paper is how usability influences users’ possibility to participate in anonymization networks. Especially in this area usability plays a decisive role in order to expand a network irrespective of the other qualities of such an application.

With regards to online anonymity there are a number of software implementations of anonymous communication techniques. In this paper we examined four of them according to usability during the installation phase. Each of them has its advantages and disadvantages in terms of usability. On the one hand, strong anonymity can be reached through

Anonymity network	average bandwidth
Tor	4,2 KBytes/s
JonDo (free cascades)	3,5 KBytes/s
I2P	2,8 KBytes/s

Table III
MEASURED AVERAGE BANDWIDTH

I2P and Mixmaster/Quicksilver but both of them are difficult to use since they require deep knowledge of computer systems (not necessarily anonymity systems themselves). On the other hand, Tor and JAP/JonDo offer easy to use applications. Thus, users do not need a long period of vocational adjustment. Beside a good usability Tor as well as JAP/JonDo provide a good and well studied anonymity concept.

REFERENCES

- [1] R. Dingledine and N. Mathewson, "Anonymity Loves Company: Usability and the Network Effect," in *Proceedings of the Fifth Workshop on the Economics of Information Security (WEIS 2006)*, Cambridge, UK, June 2006.
- [2] M. Wright, M. Adler, B. N. Levine, and C. Shields, "The predecessor attack: An analysis of a threat to anonymous communications systems," in *ACM Transactions on Information and System Security TISSEC'04*, vol. 7 (4). ACM Press, November 2004, pp. 489 – 522.
- [3] A. Panchenko and L. Pimenidis, "Crowds Revisited: Practically Effective Predecessor Attack," in *Proceedings of the 12th Nordic Workshop on Secure IT-Systems (NordSec 2007)*, Reykjavik, Iceland, October 2007.
- [4] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *8th USENIX Security Symposium*, 1999. [Online]. Available: citeseer.ist.psu.edu/whitten99why.html
- [5] J. Clark, P. C. van Oorschot, and C. Adams, "Usability of anonymous web browsing: an examination of Tor interfaces and deployability," in *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. New York, NY, USA: ACM, July 2007, pp. 41–51.
- [6] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, 2004.
- [7] O. Berthold, H. Federrath, and S. Köpsell, "Web MIXes: A system for anonymous and unobservable Internet access," in *Designing Privacy Enhancing Technologies*, ser. Lecture Notes in Computer Science, vol. 2009/2001. Springer, 2001, pp. 115–129.
- [8] S. Köpsell, "Low Latency Anonymous Communication – How Long Are Users Willing to Wait?" in *ETRICS*, ser. Lecture Notes in Computer Science, G. Müller, Ed., vol. 3995. Springer, 2006, pp. 221–237.
- [9] G. Danezis and C. Diaz, "A survey of anonymous communication channels," Microsoft Research, Tech. Rep. MSR-TR-2008-35, January 2008.
- [10] C. Díaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Proceedings of Privacy Enhancing Technologies Workshop (PET 2002)*, ser. Lecture Notes in Computer Science, vol. 2482/2003. Springer, April 2003, pp. 184–188.
- [11] R. Wendolsky, D. Herrmann, and H. Federrath, "Performance Comparison of low-latency Anonymisation Services from a User Perspective," in *Proceedings of the Seventh Workshop on Privacy Enhancing Technologies (PET 2007)*, N. Borisov and P. Golle, Eds. Ottawa, Canada: Springer, June 2007.