Privacy-enabled Communities Demonstrator

Editors:	Stefanie Pötzsch, (TUD)
Reviewers:	Carine Bournez, (W3C)
	Leif-Erik Holtz, (ULD)

Identifier:	D1.2.2
Type:	Deliverable
Class:	Public
Date:	February 23, 2010

Abstract

This deliverable document is an addition to the three parts of the software for privacy-enabled communities that have been developed by different partners within PrimeLife work package 1.2.

To support users of social networking sites we created the first tool called Scramble! that allows encryption of texts on users' profile sites. Clique, an extension of the popular social networking site software Elgg is the second tool. It enables users to segregate between different audiences for their data. For users and providers of phpBB forums we developed a phpBB extension as the third tool. The extension upgrades the access control features of the forum software so that users instead of administrators can define who should have access to their own contributions.

This text document provides an overview about the key features of the three tools and explains how to install the software that is the core part of this deliverable.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 216483 for the project PrimeLife.

Members of the PrimeLife Consortium

1.	IBM Research GmbH	IBM	Switzerland
2.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany
3.	Technische Universität Dresden	TUD	Germany
4.	Karlstads Universitet	KAU	Sweden
5.	Università degli Studi di Milano	UNIMI	Italy
6.	Johann Wolfgang Goethe – Universität Frankfurt am Main	GUF	Germany
7.	Stichting Katholieke Universiteit Brabant	TILT	Netherlands
8.	GEIE ERCIM	W3C	France
9.	Katholieke Universiteit Leuven	K.U.Leuven	Belgium
10.	Università degli Studi di Bergamo	UNIBG	Italy
11.	Giesecke & Devrient GmbH	GD	Germany
12.	Center for Usability Research & Engineering	CURE	Austria
13.	Europäisches Microsoft Innovations Center GmbH	EMIC	Germany
14.	SAP AG	SAP	Germany
15.	Brown University	UBR	USA

Disclaimer: *The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. Copyright 2008 - 2010 by K.U.Leuven, TILT, TUD.*

List of Contributors

This *deliverable document and the software demonstrator* have been jointly developed by multiple PrimeLife partner organisations. The following list presents the contributors for the individual parts of this deliverable and the software demonstrator.

Chapter	**Author(s)**
Introduction	Stefanie Pötzsch (TUD)
Scramble!	Filipe Beato (K.U.Leuven)
Clique	Joeri de Ruiter (TILT), Ronald Leenes (TILT)
phpBB extension	Hagen Wahrig (TUD), Stefanie Pötzsch (TUD), Katrin Borcea-Pfitzmann (TUD)

Contents

List of Figures

Chapter 1

Introduction

In these days' information society, individuals communicate via Internet and share a lot of personal data with each other using social software like forums or social networking sites. However, in these communities not everything is intended to be shared with everyone. An analysis of social software from a privacy perspective in H1.2.2 [4] revealed that especially the lack of support for audience segregation leads to privacy issues. We want to address these problems and therefore, as a first step, we derived a set of high-level requirements for selective access control in social networking sites and collaborative workspaces, in H1.2.4 [6]. Based on this preliminary work, three concrete ideas for web-based tools that enhance users' possibilities to protect their privacy through different mechanisms for audience segregation were pursued and protoyped.

The first tool, called *Scramble!*, allows encryption of texts on social networking sites. Therefore, only other users who have the right key are able to decrypt and access the plain texts. *Clique*, the second tool, is an extension of the social networking site software *Elgg*. It supports users in realising the segregation of different audiences for their social networking activities by configuring different *faces* (e.g. *family*, *personal*, *professional*) that they can use for interactions with other users. As a third tool, we developed a *phpBB extension* that upgrades the access control features of the phpBB forum software so that users, instead of administrators, can define who should have access to their own contributions. Since in a forum users do not necessarily know each other by name, the access control setting is done based on the other users' properties (e.g. *is over 18* or *lives in Dresden*). The three tools are prototypes that demonstrate how existing, popular social software like Elgg and phpBB can be modified and extended in order to support not only the building of communities, but of *privacy-enabled* communities. They are not optimised with regard to usability yet, however usability testing and experiments with real end users will be conducted in the near future. A more elaborated insight in the theoretical background and concepts underlying the demonstrator for privacy-enabled communities is provided in deliverable D1.2.1.

This deliverable document is a complement to the three parts of the software for privacy-enabled communities. The document provides an overview about the key features of the single tools, describes the target groups and explains how to install the software. It starts with Scramble! in the next chapter 2. Chapter 3 introduces Clique and in chapter 4 the phpBB extension is presented.

Chapter 2

Scramble!

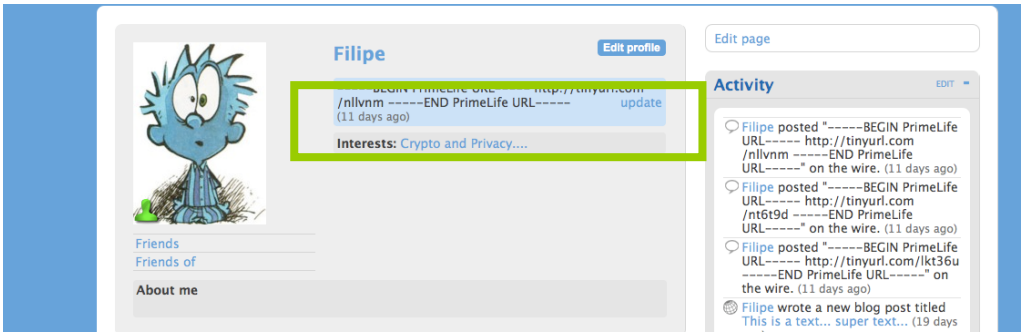

Figure 1: Encrypted text on a web site, viewed without Scramble!

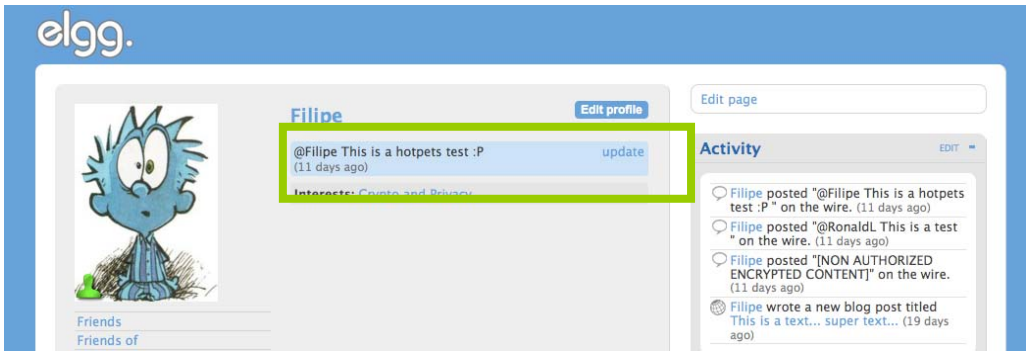

Figure 2: Same text viewed with Scramble! (and the right decryption key)

2.1 Objective and key feature of Scramble!

Scramble! provides mechanisms for users to enforce access control over their own data. Its main objective is to protect users to share sensitive information with providers of social networking sites. The tool allows the creation of a web of friends and by means of encryption to enforce access rights.

Scramble! uses the *OpenPGP* standard [5] as the encryption mechanism, and therefore builds further on the existing public key infrastructure and key management model, allowing also *broadcast* encryption for multiple recipients. *GnuPG* [3] also allows performing anonymous recipient encryption by omitting the public key IDs from the encrypted piece, but is still vulnerable for active attacks. Apart from storing large amounts of encrypted data in a social networking site, it is also possible to only list shortened URIs using a URI shortening service[1], that refer to the encrypted data into a third server. In this way the problem of the large ciphertext size that currently grows linear in the number of users that are granted access is minimised, as well as the visual contamination of the social networking site.

2.2 Target group

The target group of Scramble! are all social networking site users, who are concerned about privacy with regard to. the confidentiality of their personal data.

2.3 System requirements

Scramble! is platform independent and requires the following software to be installed on a system.

- GnuPG: version 1.4.5 or higher
  - Linux http://www.gnupg.org/download
  - Mac http://macgpg.sourceforge.net
  - Win32 http://www.gnupg.org/download
- Java: version 1.6 or higher
  - Linux & Mac installed by default, use the Win32 link to update
  - Win32 JVM http://www.java.com/en/download/index.jsp
- Mozilla Firefox: version 3.5.* or higher
  - http://www.mozilla.com/en-US/firefox/personal.html

2.4 Download Scramble!

The software is composed by only one component, *scramble.xpi*. However, the software is dependent on external software, such as Firefox and GnuPG, as explained in the previous section. Scramble! can be downloaded at

- https://svn.ercim.eu/primelife/src/branches/scramble/xpi/scramble-1.105-SNAPSHOT.xpi

[1] It is strongly recommended to use only third party services where the author is assured that privacy policies are acceptable (e.g. no logs are sold for commercial purposes). Another option would be to store the data on a third server that is controlled by the user. *TinyURL* [8] is a popular URI shortening service, however it needs to be mentioned that this service is logging access to the data, which may introduce new privacy concerns.

2.5 Scramble! installation guide

In order to install Scramble! the following steps need to be performed:

1. If not installed, install Mozilla Firefox
2. If not installed, install GnuPG
3. Open the scramble.xpi file with Firefox
4. Use the Initialisation dialog (run for first installation) to configure the main preferences
5. Run Settings dialog to change any extra settings
6. Scramble! is up and running (Figure 3)

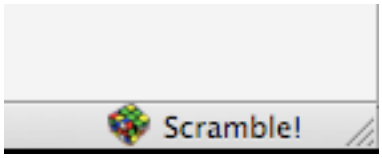

Figure 3: Browser icon when Scramble! is running

2.6 License

Scramble! will be licensed under an appropriate open source license, as soon the quality of the code has been reviewed within the PrimeLife consortium. After a positive internal review, we foresee that the exact license and the open source software hosting facility to expose it to the general public can be decided upon, in the beginning of Q2 2010.

Chapter 3

Clique

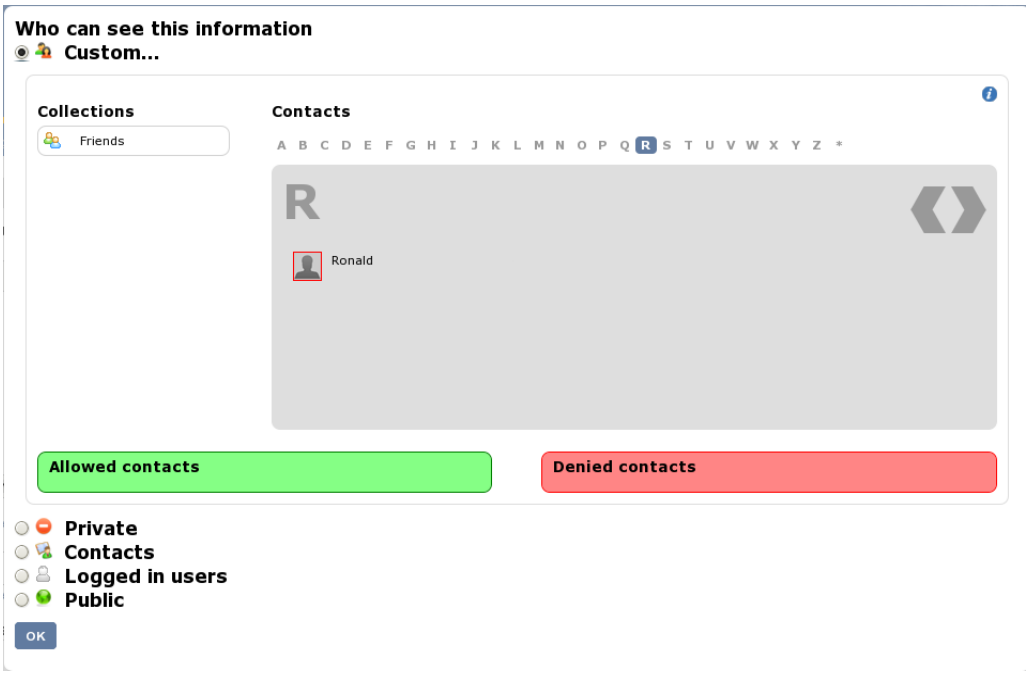

Figure 4: Clique – Audience customisation dialogue

3.1 Objective and key feature of Clique

Clique is a modification of the *Elgg* social networking platform [1]. Clique provides users with a social network platform that enables them to keep control over their privacy. This includes, for example, fine grained access control and configuration of multiple *faces* (e.g. *family*, *personal*, *professional*) that can be used for interactions with other users. When posting a data item, e.g., name, birthday or profile photo on the site, the user can define for every single other user whether they should be able to see it or not.

3.2 Target group

The main target group of Clique are providers of social networking sites.

3.3 System requirements

The basic software Elgg runs on a combination of the *Apache web server*, *MySQL* database system and the *PHP* interpreted scripting language. This is one of the most popular web server environments. Due to Elgg's advanced functionality, there are some extra configuration requirements that are explained in the following.

- The Apache web server needs to be installed with the following modules:
  - mod_rewrite
  - PHP 5
- MySQL 5+ is needed for data storage PHP 5.2+ needs to be installed as an Apache module (not in CGI mode or safe mode) with the following libraries:
  - GD (for graphics processing, e.g. user icon rescaling and Captcha)
  - JSON (for API functionality)
  - XML (not installed/compiled by default on all systems)
  - Multibyte String support (for internationalisation)

It is recommended that you increase the memory available to PHP threads beyond the standard 8 or 12MB, and increase the maximum uploaded filesize (which defaults to 2MB). By default, these settings have been set for you in the *.htaccess* file in the base Elgg directory.

3.4 Download Clique

Clique as an extension of Elgg consists of a single web application written in PHP. Clique can be downloaded at

- https://trac.ercim.eu/primelife/attachment/wiki/Clique/clique-1.0.tgz

3.5 Clique installation guide

Clique is based on the Elgg social networking platform. The installation procedure is the same as for Elgg. Therefore, the Elgg installation instructions from [2] are provided below.

1. Upload Elgg

Unzip Elgg and upload it to your site's document root.

2. Create a data folder

Elgg needs a special folder to store uploaded files, including profile icons and photos. You will need to create it.

We recommend that this folder is called data, and is stored outside of your document root. For example, if Elgg is installed in */home/elgg/html/*, you might create it in */home/elgg/data*.

Once this folder has been created, you'll need to make sure Elgg has permission to write to it. This shouldn't be a problem on Windows-based servers, but if your server runs Linux or a UNIX variant, you'll need to type something like:
chmod 777 /home/elgg/data/

If you use a graphical client to upload files, you can usually set this by right or shift-clicking on the folder and selecting *properties*.

3. Create a database

Using your database administration tool of choice (if you're unsure about this, ask your system administrator), create a new database for Elgg. Make sure you know the username and password necessary to access this.

4. Install your crontab (UNIX ONLY)

Cron is a UNIX command which allows programs to be run at set times of the day.

If you want to take advantage of some of the maintenance functions such as log rotation or garbage collection, you must install a cron tab to trigger these events.

We have provided an example crontab as */crontab.example*. Edit this with a text editor to provide the details of your site, rename it to another filename (e.g. *crontab.mine*) and install it with the following command:
crontab crontab.mine

Substitute your filename for *crontab.mine*.

5. Visit your Elgg site

Once you've performed these steps, visit your Elgg site in your web browser. Elgg will take you through the rest of the installation process from there.

6. A note on settings and .htaccess

The Elgg installer will try and create two files for you:

- *engine/settings.php*, which contains the database settings for your installation
- *.htaccess*, which allows Elgg to generate dynamic URLs

If these files can't be automatically generated, for example because you don't have the correct directory permissions, Elgg will tell you how to create them. If, for some reason, this won't work, you will need to:

- Copy *engine/settings.example.php* to *engine/settings.php*, open it up in a text editor and fill in your database details
- Copy */htaccess_dist* to */.htaccess*

3.6 Existing Clique

At http://clique.primelife.eu a running version of Clique can be tested from a user's perspective.

3.7 License

Clique is licensed under GPLv2. The text of the license is available at http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt.

Chapter 4

phpBB extension

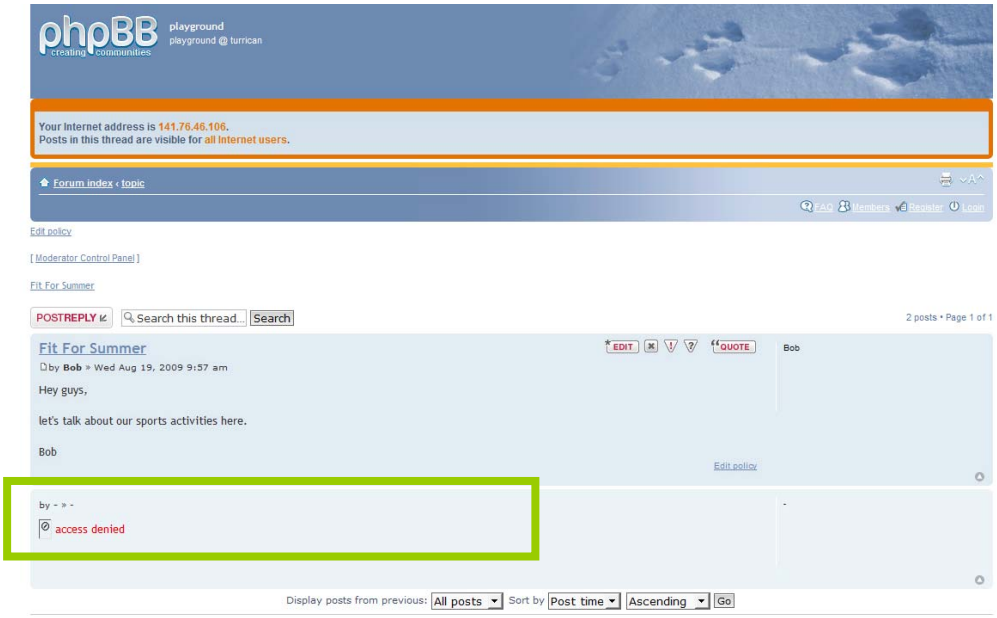

Figure 5: phpBB forum with extension for privacy-enhanced access control

4.1 Objective and key features of the phpBB extension

The software extends a phpBB forum with privacy-enhancing access control. The privacy-enhancing access control works with technical building blocks provided by the project PRIME [7], namely credentials and access control policies (in short: ACPs). The phpBB extension modifies and upgrades the original access control features of the forum, so that they work together with the access control components that were developed in the project PRIME. These components encompass:

- Creating and editing access control policies
- Issuing anonymous credentials

- Checking access control rights

In a PRIME-enabled forum with extended access control features, each user is allowed to specify which properties someone has to possess in order to access that user's contribution. With this privacy-enhancing extension, it is not only possible to set ACPs for the whole forum or topics, but also on a more fine grained level for threads and even single postings. This means, the user is able to define a particular audience for each single contribution and, thus privacy-enhancing identity management is realised by audience segregation based on the properties of the audience.

Technically, the process of creating a new resource (e.g. a thread) includes that the originator of that resource receives the corresponding credential (e.g. *cred:Owner-Thread-ID*). Further, a set of default access control policies is created, which ensure that only administrators who show an *administrator credential* or moderators who possess a *moderator credential* get the required access granted to fulfill their roles. The owner of a resource possessing the *owner credential* always has access to that resource and can modify the access control policies to, e.g., allow also users who live in Dresden and who can show a *LivesInDresden credential* read and write access to the resource.

In addition to the extended access control, the phpBB extension also contains a *privacy-awareness panel* as a new visual interface component. The privacy-awareness panel gives feedback about the access control settings of the currently displayed forum element (e.g. *Posts in this thread are visible for Internet users with the specified provable properties.*) and shows also a user's current IP address. The display of the IP address should remind the user that she is not totally anonymous when browsing the forum or, if an anonymisation service is used, the user will know whether the service works.

4.2 Target groups

The extension for phpBB is targeted to providers of phpBB forums and to users of those forums, who have an interest in protecting their privacy. For further instructions and explanations in the sections below it is distinguished between these two target groups.

4.3 System requirements

In this section the different system requirements for forum providers and forum users are stated.

4.3.1 phpBB forum providers

- Web server
  - Tested with Apache 2.2.9 http://archive.apache.org/dist/httpd
- PHP5
  - Tested with version 5.2.6 http://www.php.net/downloads.php
- SQL database, e.g.: MySQL
  - Tested with MySQL 5.0 http://dev.mysql.com/downloads
- Java 6 http://java.com/de/download/manual.jsp
- phpBB3
  - Tested with 3.0.4 http://www.phpbb.com/files/archive/3.0.4 (other 3.x versions may also work, but are not tested)

- PRIME server http://turrican.inf.tu-dresden.de/download/cw/server.zip

Note: In general, the PRIME server and the PRIME client consist of the same source code, however they contain different configurations. The *server.zip* and *client.zip* already have the according configurations set, e.g., the server already knows the relevant credential issuing categories. Providers who run a PRIME server and who want to check the configuration can go to https://localhost:9907/debug/configIssuer (user: debug / pw: debug).

4.3.2 phpBB forum users

- Java 6 http://java.com/de/download/manual.jsp
- PRIME client http://turrican.inf.tu-dresden.de/download/cw/client.zip
- Web browser

4.4 Download the phpBB extension

The phpBB extension is designed as a modification (in short: mod) for phpBB3. It consists of several php files that can be downloaded as zipped package at http://turrican.inf.tu-dresden.de/download/cw/phpBB_prime_extension.zip. After unpacking, the file structure of the folder looks as shown in Figure 6 .

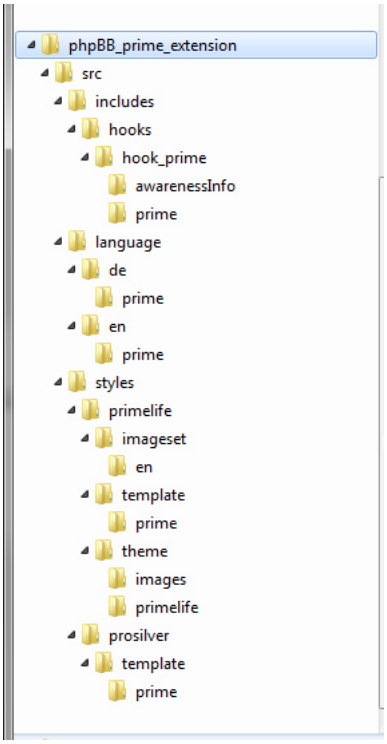

Figure 6: File structure of the phpBB extension

4.5 phpBB extension installation guide

This installation guide starts with detailed support for forum providers on how to install the required software in order to run a phpBB forum with the extension for privacy-enhancing access control. The second subsection explains which components forum users need to install and

configure. Finally, a link to an already running test forum with the extension is provided. This allows for testing the functionalities of the extension from the user perspective without installing an own phpBB forum first.

4.5.1 phpBB forum providers

System requirements:

- Make sure to have a web server running and that PHP5, Java6 and MySQL are installed
- Install the phpBB3 forum on your web server, for detailed instructions see http://www.phpBB.com
  - Select *prosilver* as style template
- Install and run PRIME server software on your web server
  - Unpack the downloaded server.zip
  - Open your command line and go to the directory where you have stored the unzipped file
  - Start the PRIME server by entering the following line in your command line: *java -jar prime.jar --configfile=config/prime.properties*

phpBB extension:

- Unpack phpBB_prime_extension.zip
- Merge the folders named *includes*, *languages* and *styles* from *phpBB_prime_extension > src* with the similarly named folders of your forum installation (some files in folders and subfolders will be replaced or added)
- *Alternatively* is also possible to do the merge manually and step-by-step:
  - Open the folder *includes* of your installed forum and replace the original folder named *hooks* by the similarly named folder from *phpBB_prime_extension > src > includes > (hooks)*
  - Open the folder *languages > en* of your installed forum and copy the folder named *prime* from *phpBB_prime_extension > src > languages > en > (prime)* into that folder (and repeat this procedure for other available languages (e. g. *de*) if you want)
  - Open the folder *styles* of your installed forum and copy the folder named *primelife* from *phpBB_prime_extension > src > styles > (primelife)* into that folder
  - Open folder *styles > prosilver > template* of your installed forum and copy the folder named *prime* from *phpBB_prime_extension > src > styles > prosilver > template > (prime)* into that folder
  - Open the folder *styles > prosilver > template* of your installed forum and replace seven original html files with the similarly named ones from *phpBB_prime_extension > src > styles > prosilver > template > (wildcard.html)*
- Open the folder *cache* and delete all php files
- It is recommended to use either the *prosilver* or the *primelife* style template for the phpBB forum with privacy-enhancing access control including the privacy-awareness panel (otherwise the privacy-awareness panel will not be shown)
- It is useful to deactivate *captchas* in the forum
  - Go to *Administrator Control Panel > General > Visual Confirmation Setting* and disable *visual confirmation for guest postings*

4.5.2 phpBB forum users

System requirements:

- Make sure to have Java6 installed
- Install and run prime client software on your device
  - Unpack client.zip
  - Open your command line and go to the directory where you have stored the unzipped file
  - Start the PRIME client by entering the following line in your command line *java -jar prime.jar --configfile=config/prime.properties*
- Set proxy in your web browser to *localhost*, port *9909*
  - See Figure 6 for configuration dialogue using the example of opera

The phpBB extension has no client-side component that has to be installed.

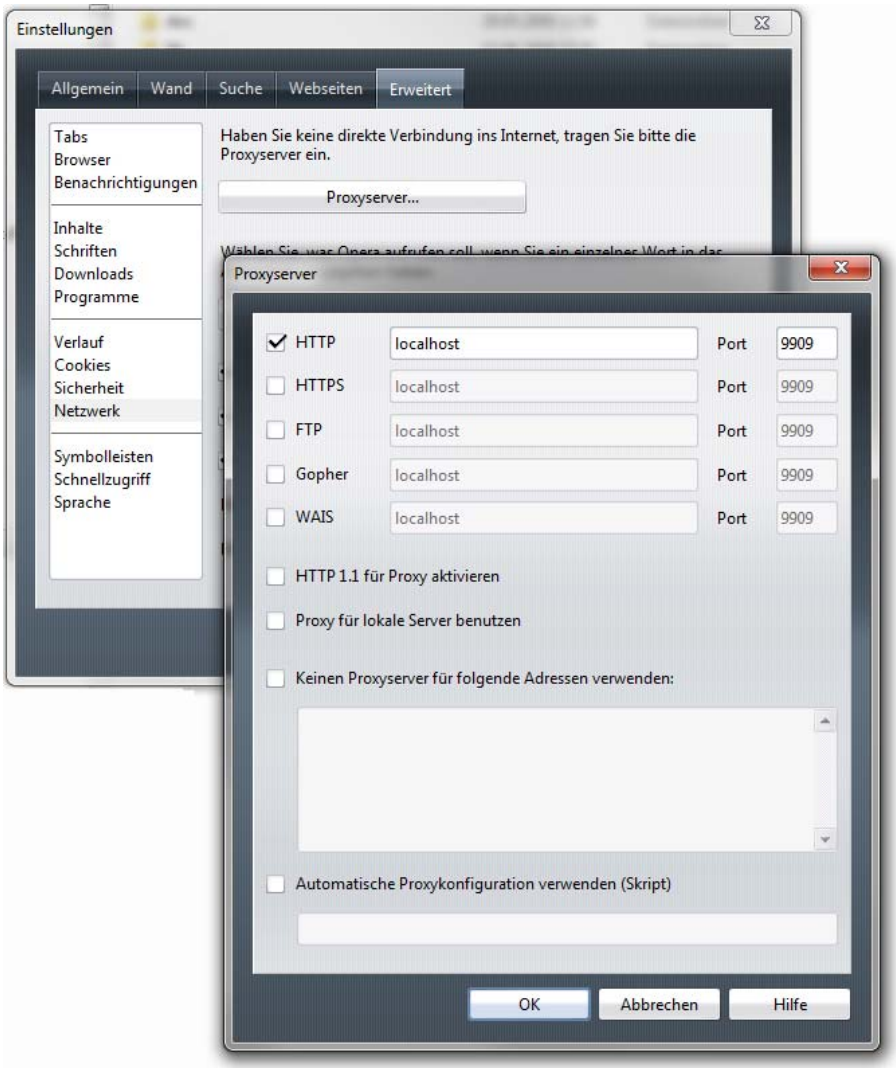

Figure 7: Setting localhost as web proxy in Opera

4.6 Preconfigured packages for testing on a local machine

In order to allow interested users to easily test the phpBB extension on their computers locally, two preconfigured packages are avalaible. Both packages already include an Apache web server, a MySQL database, PHP5, a phpBB3 forum and the phpBB extension. The preconfigured packages can be downloaded here:

- Mac http://turrican.inf.tu-dresden.de/download/cw/MAMP.zip
- Windows http://turrican.inf.tu-dresden.de/download/cw/xampp.zip

A short list with detailed instructions and hints is contained in the *readme.txt* of each zip file.

Please note that in addition to the mamp or xampp package a PRIME server and a PRIME client must be downloaded and run on the local machine as it is explained in section 4.5.1 and 4.5.2 Further, Java6 is required and a web browser with proxy set to localhost/9909 (cf. section 4.5.2).

4.7 Existing phpBB forum with extension

At http://turrican.inf.tu-dresden.de/playground/phpbb/index.php a running phpBB forum including PRIME server and the phpBB extension can be visited. In order to test the privacy-enhancing access control functionalities as a user, it is still required to install the PRIME client and set the proxy configurations in the web browser.

A document that illustrates a few workflows and that provides a step-by-step explanation of what a user can do in particular in this forum due to the phpBB extension is available at http://turrican.inf.tu-dresden.de/download/cw/phpBB_extension_workflow.pdf.

4.8 License

The phpBB extension is licensed under GPLv2. The text of the license is available at http://www.gnu.org/licenses/old-licenses/gpl-2.0.txt.

References

[1] Elgg. http://elgg.org

[2] Elgg installation. http://community.elgg.org/pg/pages/view/24

[3] GnuPG. http://www.gnupg.org/

[4] Kuczerawy, Aleksandra; Pekárek, Martin; Pötzsch, Stefanie; Roosendaal, Arnold. Privacy and Access Control in Social Software. Heartbeat H1.2.2, PrimeLife - Privacy and Identity Management in Europe for Life, November 2008.

[5] Open PGP. http://www.openpgp.org

[6] Pekárek, Martin; Pötzsch, Stefanie. Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces. Heartbeat H1.2.5, PrimeLife - Privacy and Identity Management in Europe for Life, July 2009.

[7] PRIME. https://www.prime-project.eu

[8] TinyURL. http://www.tiny.cc