Comprehensive Analysis of Web Privacy and Anonymous Web Browsers: Are Next Generation Services Based on Collaborative Filtering?

Gábor Gulyás, Róbert Schulcz, Sándor Imre

Budapest University of Technology and Economics, Department of Telecommunications, Mobile Communication and Computing Laboratory (MC^{2}L) Magyar Tudósok krt.2, H-1117, Budapest, Hungary
{gulyasg, schulcz, imre}@hit.bme.hu

Abstract. In general, networking privacy enhancing technologies are better on larger user bases - such criteria that can be enhanced by combining them with community based services. In this paper we present main web privacy issues and today's complex preventive solutions, anonymous web browsers, in several aspects including a comprehensive taxonomy as a result of our inquiry. Also, we suggest a next generation anonymous browser scheme based on collaborative filtering concerning issues on semantic web. Finally we analyze the benefits and drawbacks of such services, also examining the possible investors and raised moral considerations.

Keywords: anonymous web browsers, user tracking, web privacy, collaborative filtering

1 Introduction

The web has become a generic platform and takes a serious place in the everyday life of the digital age's citizens. Several life-like transactions can be done on the web such as browsing items in a web shop, executing financial transactions, booking hotel rooms, while users require a high level of privacy, meaning as strong as they were committing these actions in real life.

However, privacy on the web is not as strong as it is desired to be. Browsing items on web shops, or reading on-line magazines should be done anonymously if desired, but in many cases users are being observed and information is collected for profiling purposes. In most cases these profiles are later being used for direct marketing implying targeted advertising, dynamic pricing. Although user profiles can also be useful in determining content relevancy or in creating customized services.

Privacy enhancing technologies (PET) are the solution against privacy vulnerabilities. The necessity of privacy enhancing technologies for the Internet emerged in the early beginnings [1] and since solutions evolve, however, there are still a lot of open questions.

On the web anonymous web browsers represent the complex solution for sustaining anonymity and defending privacy. In this paper after outlining the current problems of web privacy and analysis of anonymous web browsers, we recommend a new solution based on collaborative filtering. This next generation service does not presume the existence of a semantic web, instead offering the possibility to create it, while it also strengthens user privacy by providing anonymous web surfing.

We structure this paper as follows. In order to determine how seriously user privacy is endangered on the web, in Section 2 we discuss web privacy issues by inspecting participants concerned in violating user privacy and primal techniques. As a summary at the end of the section we propose a criterion determining the proper conditions for achieving anonymity.

Anonymous web browsing services provide preceding solutions for the yielding privacy vulnerabilities. In Section 3 we present the architecture of today's anonymous web browsing services, and publish a short taxonomy for classifying such service types, including a comparison as well.

In Section 4 we suggest a solution describing how collaborative filtering should be applied to anonymous web browsers. In this section we analyze possible investors and examine moral questions raised as well. Finally, we give a conclusion about our work in this paper.

2 Web Privacy

Web privacy issues can be divided in two main categories, correspondingly to the categorization of passive and active attacks in security: information leaking and technologies used to compromise privacy. However, information shared inadvertently can also result in compromising privacy (for instance, tracking) which raises the importance of total user control over shared or leaked information as well, not only preventing and detecting active attacks.

Since several services rely on their advertising incomes, some privacy-friendly altering methods should be considered. For example instead of animated advertising, text based should be used, which is more audio-visual privacy friendly. Alternatively for tracking user activities and profiling, user preferences should be guessed by analyzing the web context in which the advertisement is shown.. Using this method users are classified into general preference groups instead of creating personal profiles. Otherwise, requesting the users' consent is also a privacy-friendly approach if individual profiles needed to be created.

2.1 Participants, Goals and Motivation

We divided the participants into two main groups: the users and others possibly compromising their privacy. However, in another aspect participants could be classified to be neutral, supportive or endangering user privacy. Intrinsically, actual participants can have several roles at the same time.

The *users*' objective is to have *total control over all their data*: any information sent and received, and preserving anonymity. A user should also be aware of the

information shared with the service provider or a third party any time, and should be able to defend herself against advertising and the leak of private information like e-mail addresses or login names.

Neglecting the way the profile was acquired, the *advertisers*' goal is to achieve precise *targeted advertising*: to get the proper advertisements to the proper users (in large numbers). In some cases advertising is used together with profiling by tracking user activity and storing profile information on contextual or click-through bases. Advertisements, besides overloading system resources, can violate audio-visual privacy, by expanding over their designated area and playing sound effects or music.

Web shops and *stores* might be using targeted advertising and profiling, however, they might use profiles for *dynamic pricing*, for extra profit they offer desired products more expensive and uninteresting ones cheaper. The user's profile can be easily updated accordingly to her purchase statistics.

Data collectors use special tracking techniques and often collaborate with service providers for *profiling* purposes. Their goal is to create accurate databases for *merchandising* or for some previously mentioned activities.

The category of *service providers* includes Internet Service Providers (ISP) and web services providers as well. The IPS-s' proxies are the bottleneck of the users' whole traffic, which is ideal for *logging user activities* and *blocking access* to web service providers (politically motivated censorship).

Web service providers are often the link between different participants by applying auditor services, placing third-parties' advertisements on their pages or could be *collaborating with other web service providers* for merging logs or creating wired networks for tracking purposes.

Censoring activities can be motivated by corporate policies or political regulations. In the world of the web the main goal of censorship is to *block access* to websites with certain URL addresses or any other sites providing specific content. Free Internet service providers may also be censoring web content or several URL addresses containing forbidden words or phrases (for instance Internet access available in libraries).

2.2 Passive Attacks: Public Information and Abuses

Most of the information shared with websites, such as user agent or display properties are intended to be used for customizing services, but this information can also be used to create comprehensive profiles. Information like exact browser agent version, list of installed plug-ins can be used to check the existence of specific vulnerabilities, which can be used to install spyware on the user's computer. There are several websites demonstrating severity of information leak by listing public information available of the computer which the user uses to access the web, like in [2].

Revealing the network address is a technical need due to the networking mechanisms and architecture of the Internet, however, these addresses are almost unique and allow tracking. The IP address can also be used for geo-locating users quite precisely, narrowing down the possibilities to the most likely country and city. For a visual demonstration, visit [3]. Since IP addresses can change and might be referring to several users and devices, other mechanism are used for tacking purposes,

which are considered to be active attacks against user privacy as they require tracking identifiers bound to the user.

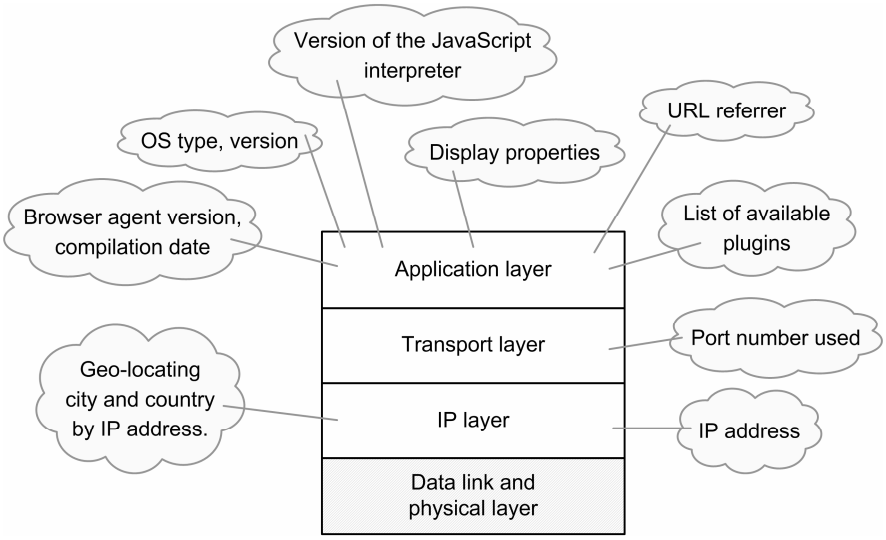

Fig. 1. TCP/IP stack model and information can be used to abuse privacy.

Different types of public information can be sorted by network layers as described in Fig. 1. This classification is required later for defining anonymity criterion (network and application level anonymity should be preserved in a different but related way).

2.3 Active Attacks: Techniques Violating Web Privacy

The main purpose of active attacks is profiling, however, censorship should not be left out. Profiling is the method of mapping user activities by time and logging preferences plus interests altogether. This is mainly done by tracking user activity throughout the web, but due to caching and history preserving mechanisms built in the browsing agents there are other methods as well. In addition, we should consider the possibility of collaborating service providers.

Our review on active attacks includes furthermore procedures for profiling (to create colorful profiles, for example including daily routine information), and also censorship activities.

2.3.1 Tracking Web Activities

The principle of tracking is simple: in every context the user visits the profiling party (perhaps a third party) tries to uniquely identify the user and if this process is successful it creates entries in the profile, based on contextual information.

IP tracking is the simplest method for tracking, since IP addresses are revealed every time a web service is visited. However, IP addresses might not be correctly

denoting users, since addresses can refer to network devices or groups of users, for example due to the use of Network Address Translation (NAT) techniques. Identifying users by their browser agent is a better idea, because several users might be using even a single computer which only has one IP address (assuming that every user on the same computer has an own profile and thus can be identified personally). Following techniques realize browser-based user tracking.

Cookies are used to store the user's settings on her computer for web services, and to do so the browser agent sends all cookies belonging to the visited website (so the site only accesses its own cookies, and cookies cannot be created for foreign sites). Sometimes cookies only store session identifiers which refer to resources (or database entries) stored at the web service provider.

However, cookies can also store tracking identifiers, which are called *tracking* or *third party cookies*. Since service providers cannot read each others' cookies they use web bugs or advertisements placed on the others' site to detect users visiting a tracked website (see Fig. 3. for better explanation). Web bugs are small, transparent 1x1 pixel sided images hidden on pages, especially for creating statistics or tracking purposes. On Fig. 2. we demonstrate how tracking is done by web bugs.

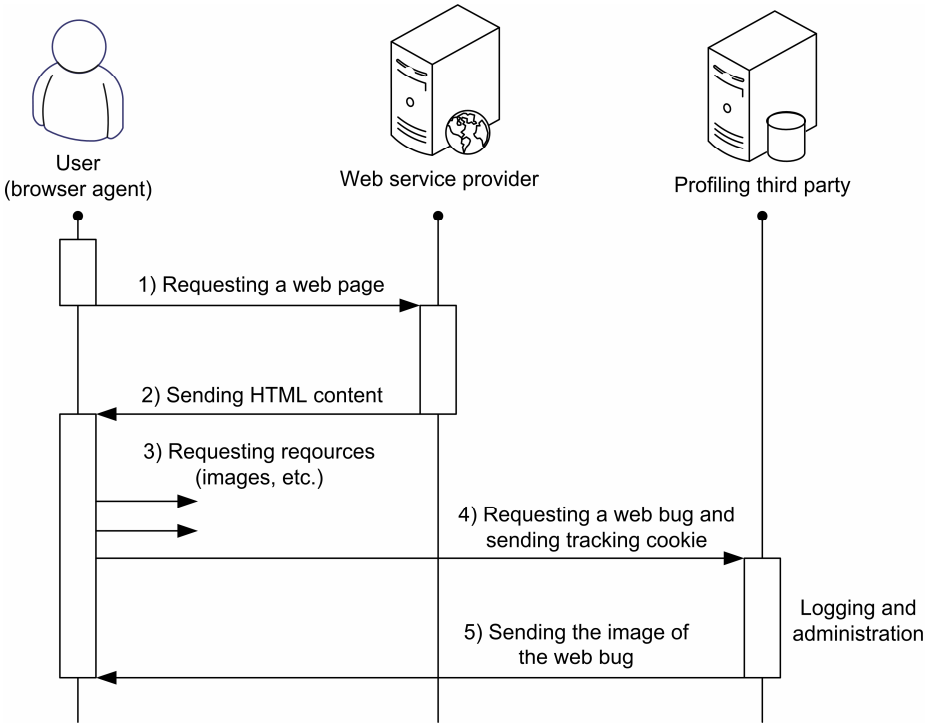

Fig. 2. Sequence diagram of web bug based tracking mechanism.

The visited website's content is downloaded in two steps: the browser agent downloads the content descriptor file in Hypertext Markup Language (HTML) format and then downloads images and other resources marked in the page's descriptor

which might have to be downloaded from elsewhere, from a third party, setting the basic idea for web bugs.

Modern browser agents offer the possibility for privacy-aware users to manage, and also delete cookies. Possibly this was the reason why *Flash Persistent Identification Element* (PIE) was introduced. PIE-s are based on a cookie-like client-side storage element called Local Shared Object (LSO). These objects are harder to check and detect changes, and even to delete, however, tracking possibilities are limited, too. PIE elements are utilized with Flash advertisements accordingly to web bugs.

Furthermore, there are alternative methods, like exploiting vulnerabilities in the browser agent's cache mechanism to use script variables (like JavaScript) storing tracking identifiers among several websites.

2.3.2 Filling Profiles

Collaborating websites can create comprehensive profiles *merging web activity logs* and *analyzing context*: visited pages, downloaded files, followed links, click-through statistics of advertisements. Statistics audit provider services might be behind these collaborations and permanently tracking users promising personalized content and services in return.

The *URL-referrer* string carries the previous URL that the user visited before following a link. Certain information can be extracted from URL-referrers besides the acknowledgement of referring sites if the user is tracked: the time she visited the referring site, possibly the content the user visited and most importantly, if the referrer was a search engine, the key words the user was using to locate the site in question.

E-mail addresses can be attached to profiles by sending links or the URL of images in e-mail, embedding a special identifier into the URL referring to the recipients address. If the user opens the mail and decides to download the images or opens a link her IP address will be instantly revealed and by opening an URL in a browser her tracking identifier will be linked to her e-mail address. Also, if a user registers for a malicious website's service, registration information can be attached to the profile.

Besides the list of preferences, information about the user's *daily routine* can be stored in profiles. The use of start pages in browser agents and subscribing to web feeds disclose such information and on the long run statistics reveal the outline of the user's daily routine. Using browser agents for reading web feeds bears the threat of being tracked, since during the check-out session of a feed channel, cookies can be set and read. This also means automatic resolution of tracking identifiers to IP addresses at the first time of the day when the user starts the browser agent that checks out the web feed.

2.3.3 Analyzing Databases Off-line: Spyware Activities

Spyware activities' goal is to collect information about the user, generate profiles and compile list of preferences based on the analysis of off-line databases: *file cache*, *URL history* and *cookie database* (and optionally PIE database). Practically available time and other resources are unlimited for processing these databases.

In the file cache database spyware agents can reveal the exact content the user viewed, creating a preference profile. However, if the previously mentioned script

caching vulnerabilities were exposed these tracking identifiers can be revealed. Primarily, processing the file caches is used together with creating tracks by URL history and cookie databases.

Cookie and PIE databases can be accessed without any restrictions off-line, and complex queries can be executed. In this way spyware agents do have the possibility of linking several tracking identifiers altogether using data and text mining techniques, even from separate databases (including script based identifiers).

Spyware protection in the prevention phase can be done by educating users, prohibiting downloads by and limiting information leak of browser agents. However, if the user's computer gets infected removal can only be done off-line which is beyond the scope of networking services. Although, the expansion of these databases should be prevented.

2.3.5 Censorship for Blocking Services and On-line Surveillance

Censoring activities are usually done by *blocking* IP address, domain names or filtering available content by keywords, patterns. Censorship often includes *surveillance*, even involving the process of tracking and identifying users sharing or accessing blocked content. Observing users also supports the management of blacklists of web service providers and content.

2.4 Criteria for Web Privacy Enhancing Technologies

We define the criteria of anonymity in two steps. First, we give a theoretical criterion listing properties, and then a practical approach for designing anonymous web browsers.

Guaranteeing the state of anonymity for web users requires the following properties:

- *Unobservability*: unobservibility of requests and content sent is required for anonymity. This equals to the criteria of confidentially, practically meaning that sent messages should be ciphered.
- *Unlinkability*: neither a web service provider, nor an observer should be able to tell if two messages sent by the same anonymous user. This also applies for pseudonyms used through the communication.
- *Pseudonymity*: the user is pseudonymous if she is referred by an identifier string, which cannot be related to any personal information, for example like a tracking identifier.
- *Anonymity*: the user is anonymous if it is not possible to identify her in a set of users identified by pseudonyms and also activities cannot be linked to users within this set.

Relationship of these properties is illustrated on Fig. 3. Unlinkability of messages or pseudonyms requires the unobservability of message content, since cleartext messages do not hide changes of pseudonyms, or message header information, which can be useful to link messages to a user, or to follow identity changes. Anonymity

property requires a set of pseudonyms which cannot be linked together or to users (a user might have multiple pseudonyms).

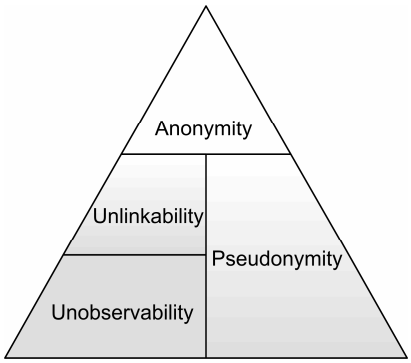

Fig. 3. Anonymity property's relationship and dependence on other properties.

In practice, anonymity needs to be guaranteed on two separate levels: network level and application level. On these levels different types of information is leaking as it was mentioned previously (see Fig. 1.), and also different types of active attacks have to be prevented and detected when securing the related layers.

In the transport and IP layer port numbers and IP addresses have to be obscured. Applying mix networks[1] [4] anonymous communication over secure channels can be granted (serving confidentiality, integrity), which not only dissolves the possibility of network surveillance but is necessary to fulfill criterion for anonymity property by terminating the chance of interaction or surveillance in application layer protocols for observers.

This leaves the only way for observing users by using application layer protocols which we discussed in previous subsections. On the web, regulations in the application layer are solved by using filtering mechanisms, run on client or proxy side.

3 Anonymous Web Browsers

Anonymous web browsers offer complex preventive solutions to previously reviewed privacy issues. Using these services, the state of anonymity can be preserved, and in some cases certain undesirable contents, like advertisements, can be filtered out, too.

Basically there are two types of anonymous browsers: web based and regular proxies with client side filtering functions. The main difference between them is suggested by their names: web based anonymous browsers can be reached through websites (their control panel embeds into the visited pages), while regular proxies do not have that much of transparency: a certain intermediary agent needs to be installed

[1] Using MIX networks is the basic technique for granting sender anonymity. A MIX node outputs messages in random order, and uses cryptographic methods for preserving linkability of messages received and sent. Usually, MIXes are used in cascades for stronger privacy.

or settings have to be changed in the web browser agent. Both have special filtering systems to remove malicious code from the downloaded content, also narrowing the scope of revealed information about the user.

3.1 Architecture

In general, anonymous web browsers are based on two basic functions accordingly to the criterion in Section 2.4: MIX services and a proxy serving filter functions. In practice filtering can be implemented client side as well, and MIX may not be utilized leaving a simple anonymous proxy (service types are conferred in the next section). However, for quality privacy enhancing service MIX services should not to be left out. For general architecture see Fig. 4.

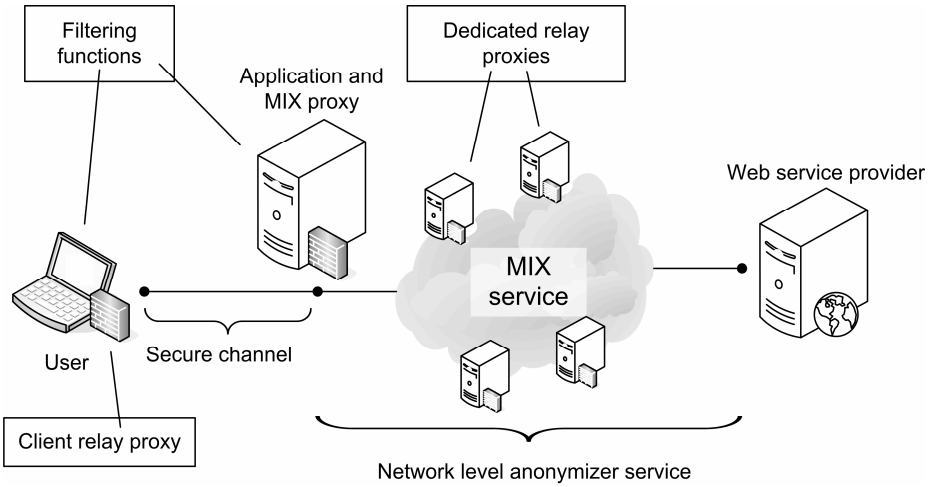

Fig. 4. General architecture of anonymous web browsers.

There are several types of mix services in numerous aspects; in [5] there is a comprehensive review of web privacy enhancing services including comparison of mix services. However, most anonymous web browsers use onion routing technology[2] [6], varying mainly in security parameters and architecture issues such as dedicated or users-based mix nodes. Due to the client-server architecture of web applications anonymous routing protocols providing only sender anonymity can be accepted. For preserving unobservability the traffic between the user and the first proxy should be secured.

[2] Onion routing is an advanced MIX technique, named according to its messages' inner structure: the original message is embedded into several encrypted layers, like an onion. Every node removes its layer from the messages by decrypting it, and send the inner onion forward.

3.2 Service Type Taxonomy and Comparison

Anonymous web browsing services can be classified into two types: *anonymous proxies* and *anonymous web browsers*. The proper taxonomy is visualized on Fig. 5. Anonymous proxies usually have filtering functions and only grant poor network level anonymity by masking IP addresses, used port numbers and using no encryption (or traffic analysis protection).

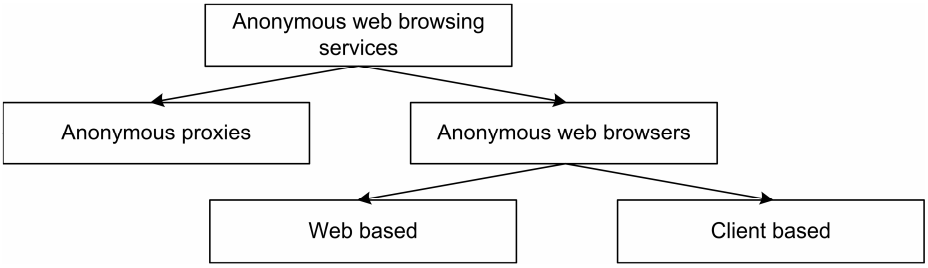

Fig. 5. Taxonomy for anonymous web browsing services.

Furthermore, anonymous web browsers can be sorted into two groups: *web based* and *client based*. Web based services can be accessed through their websites and no client side settings need to be done, all filtering functions takes place server-side. In the contrary by using client based services filtering functions take place locally, and in some cases local proxies might need to be installed. Also, in some cases service parameters need to be configured, but pre-configured client based services does exist.

Although all service types' goals are the same, realizations are quite dissimilar, even on bases of functionality; see comparison in Table 1.

Table 1. Several privacy-related and usability functions featured for comparison of the main service types.

	Anonymous proxies	Web based anonymous web browsers	Client based anonymous web browsers
Network level anonymity	IP and port masking	Secure channel, mix services	
Filtering functions	(Server-side)	Server-side	Client-side
Cookie Management	-	Stored server-side, filtering, blocking	Filtering, blocking
Cache, history protection	-	Server side protection (bypass)	Client side management
HTTPS relay	-	Possible	-
Censorship bypass	-	Dedicated relays	Dedicated and client relays
Transparency	Setting browser agent	Web proxy	Local proxy has to be installed and set
Portability	No dependency	Browser dependency	OS dependency

Though anonymous proxies have moderate server-side filtering functions, however, users might install client-side plugins for substituting such functions, but anonymous proxy services integrating server- and client-side filtering are not common. For client based anonymous web browsers filtering functions are not required. Filtering functions may include: object filtering (Java, Flash and ActiveX), scripts, browser agent and operating system properties, URL referrer, malicious content (pop-up and pop-under windows, advertisements).

Web based anonymous web browsers offer a special and useful option: storing cookies server side, allowing users to only use certain cookies while resorting anonymous web browsing services. Server side cookie management extended with cookie-profile management might allow users to harden tracking even more by switching or removing profiles.

For evaluating existing services usability aspects should be verified. Free services often have strict quotas of bandwidth and total traffic, and might be inserting their advertisements into visited pages. Terms of use should be reviewed, and also whether for how long the service logs user activities.

4 Next Generation Services Based on Collaborative Filtering

We know about work related to the semantic web studying how it might bring a new era for web privacy by letting browser agents and web service providers negotiate privacy parameters and conditions [7]. However, semantic web is yet to come. In our opinion collaborative efforts creating a semantic web could strengthen privacy by utilizing anonymous web browsing services. By using these anonymizing services server-side applications need not to be modified, leaving the web's architecture unaffected which makes it easier to introduce new technologies client-side or in the anonymous web browsers' architecture.

4.1 Anonymous Web Browsers and Collaborative Features

Today's anonymous web browsers use preset features composed by the service provider these are being applied instantly without granting fine-tuning for any part of any site the user visits. Databases supporting filtering functions are often out-dated and poorly maintained. We reckon that using community based techniques to maintain filter databases is a possible solution. Also, these techniques offer fine-tuning of content filtering by allowing users to mark content in several way in pages and in addition, the shared database is up-to-date anytime and accessible for anyone.

Among several techniques we propose *tagging* which can be used for content tagging to aid filtering in several categories like marking privacy violating content, security guidelines, warning for adult content, etc., and also numerous units of the service might be tagged like services providers, websites, pages or even partial page contents creating the possibility to fine-tune filter mechanisms. Certain supposedly cooperating sites grouped into a virtual network by tagging can be filtered out together or, similarly, parental locks can be applied to them. Tagging also provides *categorical and keyword based filtering*.

Complementary to visual content tagging script codes, web bugs, cookies and other types of malicious semi-hidden content can be marked for suggested filtering. Even more, the extension of tagging features by letting users to *vote* for tags will result a democratic service. Filtering can also be extended by applying a special threshold function customized by the user herself. Not all the users have the same preferences or level of trust in collaborative filtering. To improve the suggested model all users should be able to define a simple threshold value function or a more sophisticated method to strain out presumably invalid, low rated tags.

Some of today's anonymous web browsers support *URL based* features like ad filtering or warning for malicious websites. Supervised collaborative management of URL pattern filters would be considerably enhancing user privacy. However, fraud detection and cheat prevention should also be considered.

However, only in case of a client based anonymous web browser is possible for users to nominate themselves for offering relay services to others. Not by default but for installing proxy relay software it is possible for the users of web based services to act as relays to other clients.

4.2 Technological Basics and Architecture

We recommend web based services for high portability, compatibility and easy of use (see Section 3.2). However, a few concepts concerning the architecture need to be modified (see Fig. 6.).

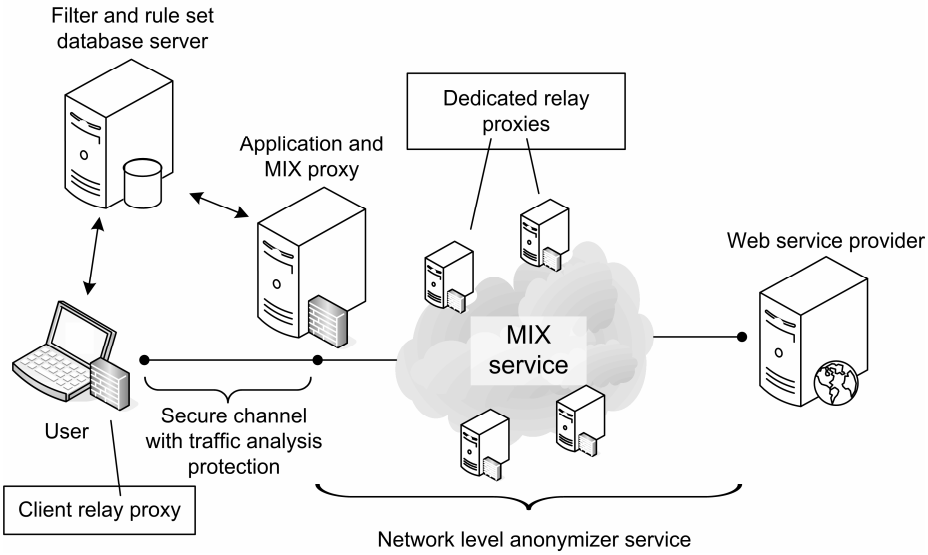

Fig. 6. Next generation anonymous web browser architecture.

Nowadays great developer tools are available dissolving the difficulty of creating browser independent services. In our vision, these tools can help to unfold the

previously introduced taxonomy since filtering functions can be placed on client-side by using scripting techniques; however, server-side implementations are also possible.

In today's anonymous web browsers the communication between the user and entry proxy is only protected by a secure channel, however, it should be traffic analysis protected as well. Another modification required is introducing an independent database server (or servers if needed) for storing filter and rule sets.

The client-side management system can be implemented by using of JavaScript technology and filtering functions can be supported by using Document Object Model (DOM) for analyzing and filtering web content. DOM is a standard object model for representing HTML (and some other formats), which can be accessed from JavaScript scripts and in such way the websites structure can be accessed and manipulated on client-side. Also, JavaScript can also be used to dynamically place buttons into the content to achieve the management of tags, votes and other collaborative features. Changes committed can be saved through using Asynchronous JavaScript and XML (AJAX) which allows the web browser agent to communicate with websites without reloading a page.

Since DOM represents page elements in a hierarchical tree structure, filtering and tagging elements means corresponding actions to all child elements recursively. This means the ease of management issues, for example by tagging a section element on a site all contents included are tagged as well.

4.4 Possible Investors and Motives

Anonymous web browsers, like Privacy Enhancing Technologies (PET), serve both individual and democratic values and rights. In many cases these aims do not osculate with business goals, and since it is hard to find financial support for these projects, the implementation phase cannot be initiated or, if initiated, it fails. In other cases financial problems, marketing purposes or other business objectives affect the result of the project.

Anonymous web browsers serve democratic rights, so it seems to be natural to have *governments* or other *democratic organizations* taking over the responsibilities of developing these services. However, even democratic governments are often counter-interested in providing such services to their citizens because governments claim control over the behaviour of their citizens even on the Internet.

It is not completely unlikely that once there will be a Europe-wide project supporting the designing and creating of a next generation anonymous web browser, or at least providing professional and financial support for a PET system including an integrated anonymous browser. The PRIME project [8] might be a viable host for researching or creating a prototype version. The project aims to demonstrate privacy enhancing identity management which is required to provide anonymous web browsing. If the prototype is successful a standalone version might be brought to life independently. According to a recent Communication of the Commission of the European Communities the Commission expressed its intention to support the development of PET technologies [9].

Another group, *online companies hosting search engines* and *pursuing direct marketing* might also be interested. Experimental search engines gather results by

interpreting the search query and the documents. This process can be helped by creating semantic description of sites, pages or even other kind of partial content built by tags added by users, however, quality control of semantic content is required to avoid subjective denotation.

Also, there are collateral benefits. By serving next generation anonymous web browsers the practice of online direct marketing could be done possible in a lawful way: all users should be informed and warned on what is observed and logged about them, and — similarly to other existing PET solutions — either they consent to forwarding their personal data, or only anonymous statistics would be created. The need of hidden observation would be non-existent any more (for these companies) and user would be monitored only within the consented limitations.

Since all browsing information flows through the central server activity from the first visited site to the last one can be tailed, and some information, such as time spent on sites, would be easier to monitor. Of course, these features necessitate a service that is compatible with all web services, and the user will never have to exclude the anonymizing service.

Advertising schemes would be different, since only the anonymous web browsing service provider's ads would be shown, others removed. Furthermore, the service provider's ads could be show in a frame of the service instead of websites.

4.4 Moral Considerations

It is worth mentioning that by building this system, the service provider would be in an advantageous position compared to its competitors. These huge corporations providing a lot of services are sometimes called informational superpowers. Introducing next generation anonymous web browsing services into their portfolio, or additionally integrating their services into the anonymous browser would exponentially increase their power regarding the possibilities mentioned in previous sections.

The basic features like creating unlimited (theoretically anonymous based on users' consent) statistics on user activities, filtering out their competitors' advertisements, restructuring the advertising policy raise the question: would it be right to let such a huge corporation extend its possibilities this way? These changes alone could kill smaller regional competitors.

In this context we should also consider our trust in these companies. Possibly they cannot be trusted at all, but we should be prepared for the worst case scenario. However, technically it is possible that different providers are involved in the process: the filter and rule set database server is run by a search engine company and other parts of the architecture including the front-end system and anonimizing services are run by someone else.

5 Conclusion

Due to the co-evolutional nature of web privacy present anonymous browsers are out dated. In this paper we suggested a new, community based solution, regarding

financial issues and moral considerations besides technical problems. Hopefully, one day symbiosis of anonymous web browsers and community based services will strengthen the democratic nature of the Internet, granting anonymity. We think user-centric identity management combined other management possibilities (for example cookie management) should be integrated into these next generation services.

Acknowledgement

This paper was made in the frame of Mobile Innovation Centre's integrated project Nr. 3.1 supported by the National Office for Research and Technology (Mobile 01/2004 contract).

References

1. Ian Goldberg, David Wagner, Eric Brewer: Privacy-enhancing Technologies for the Internet. In: the Proceedings of the 42nd IEEE Spring COMPCON, 1997.
2. Project IP, http://projectip.com
3. IP Tracer & IP Locator, http://www.ip-adress.com
4. D. Chaum: Untraceable electronic mail, return addresses, and digital pseudonyms. In: the Communications of the ACM 24, pp. 84--88, 1981.
5. S. Gritzalis: Enhancing Web privacy and anonymity in the digital era. In: Information Management & Computer Security, pp. 255--288, 2004.
6. R. Dingledine, N. Mathewson, Paul Syverson: Tor: The Second-Generation Onion Router. In: the Proceedings of the 13th USENIX Security Symposium, 2004.
7. A. Rezgui, A. Bouguettaya, M. Eltoweissy: Privacy on the Web: Facts, Challenges, and Solutions. In: IEEE Security & Privacy, pp. 40--49. 2003.
8. Privacy and Identity Management for Europe (PRIME) Project, https://www.prime-project.eu
9. Commission of the European Communities: Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs), http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0228en01.pdf