An intensive analysis of security and privacy browser add-ons

Nikolaos Tsalis[1], Alexios Mylonas[2], Dimitris Gritzalis[1]

[1] Information Security & Critical Infrastructure Protection (INFOSEC) Laboratory
Dept. of Informatics, Athens University of Economics & Business
76 Patission Ave., Athens, GR-10434, Greece
[2] Faculty of Computing, Engineering and Sciences, Staffordshire University
Beaconside, Stafford, ST18 0AD, United Kingdom

{ntsalis, dgrit}@aueb.gr, alexios.mylonas@staffs.ac.uk

Abstract. Browsers enable the user to surf over the Internet and access web sites that may include social media, email service, etc. However, such an activity incorporates various web threats (e.g. tracking, malicious content, etc.) that may imperil the user's data and any sensitive information involved. Therefore, web browsers offer pre-installed security controls to protect users from these threats. Third-party browser software (i.e. add-ons) is also available that enhances these pre-installed security controls, or substitutes them. In this paper, we examine the available security controls that exist in modern browsers to reveal any gaps in the offered security protection. We also study the available security and privacy add-ons and observe whether the above mentioned gaps (i.e. when a security control is unavailable) are covered or need to be revisited.

Keywords: Web browser security, privacy, add-ons, user protection, malware, phishing, controls

1 Introduction

Web browsing activities (e.g. e-commerce, online banking, social media, etc.) are accompanied by web threats that pose a direct risk towards the user, such as phishing attacks, malicious software, tracking sensitive information etc. [1]. When a user selects one of the popular web browsers (i.e. Apple Safari, Google Chrome, Internet Explorer, Mozilla Firefox or Opera) it is important to make that choice based on the features each browser provides (e.g. appearance, speed, usability, etc.). Among them there should be the available security controls provided by all modern browsers (e.g. malware/phishing protection, do-not-track service, etc.).

Pre-installed security controls aim to protect the user from web threats. Moreover, browsers offer additional software, namely add-ons, which extend the functionality of browsers. Add-ons are focused on catergories, such as *accessibility*, *news & weather*, *photos*, *productivity*, *social*, etc. One of them (that exists in some of the browsers) is *security and/or privacy*, which includes add-ons that aim to offer additional security/-privacy mechanisms to the user. However, add-ons are based on a community of developers and do not have the same popularitty in the different browser ecosystems. As a result, some add-ons that are valuable at protecting users' security and privacy (e.g. NoScript) are not available in in some of the browsers (e.g. Internet Explorer).

In this context, our work provides a comprehensive analysis of the availability of security and/or privacy controls, which are pre-installed in modern browsers. In addition, we survey the available security and/or privacy add-ons of each browser and examine whether they cover the identified gaps of the browsers' controls, when one or more security controls are not offered. Our work reveals that browsers differentiate a lot concerning both the availability of the provided security controls and the corresponding add-ons.

The rest of the paper is structured as follows. Section 2 presents the related work. Section 3 includes the methodology of our research. Section 4 depicts the results of our findings. Section 5 includes a discussion of the results and Section 6 consists of our conclusions.

2 Related work

In this paper we examine the security and privacy protection that is offered by the add-ons of the most popular desktop browsers. Former literature has examined the availability of controls in the above mentioned browsers (e.g. Safari, Chrome, etc.). Our previous work [2] surveyed the availability and manageability of the available pre-installed security controls of modern browsers, in both desktop and mobile devices. This work expands our previous one.

Botha et al. in [3] provide a simple comparison of the availability of security options in Internet Explorer 7 and Internet Explorer Mobile (for Windows Mobile 6 Professional Ed.). Furthermore, [4] focuses on the visibility of security indicators in smartphones. Carlini et al. performed a security review of 100 Google Chrome's extensions, which resulted in 70 located vulnerabilities across 40 of the total extensions examined [5].

In addition, [6] proposed a privacy preserving mechanism called "SpyShield", which enhances spyware protection by detecting malicious add-ons, that aim to monitor sensitive information. The authors tested the above mentioned mechanism on the Internet Explorer browser.

Kapravelos et al. in [7] presented similar work that focused on detecting malicious behavior of browser extensions. Such an approach included monitoring the execution phase of such extensions in corellation with the corresponding network activity, in order to detect any anomalies.

Lastly, the authors in [8] analyzed 25 of the most popular Firefox's extensions. They have found that 88% of them need less than the full set of the available privileges and they have proposed a novel extension system that enforces the least privilege principle.

3 Methodology

3.1 Security and privacy controls

The scope of our analysis includes the popular browsers for Windows desktops, i.e. Chrome (v. 41), Firefox (v. 36), Internet Explorer 11, Opera (v. 27), and Safari (v. 5.1.7). Table 1 includes the popularity of each browser, until March 2015 [9]:

Table 1. Browsers user base

Browser	User base (%)
Chrome	63.7%
Firefox	22.1%
Internet Explorer	7.7%
Opera	3.9%
Safari	1.5%

The browsers were installed in a workstation running Windows 7, which is the most commonly used operating system (52.3%) [9]. Then, we enumerated the browsers graphical interfaces and any available hidden menus (e.g. *"about:config"* in Firefox) in order to collect which security controls are offered in each browser.

3.2 Security and privacy add-ons

We visited each browser's add-on repository, so as to identify the available security and privacy add-ons. To this end, we visited the add-on repository of Safari [10], Chrome [11], Internet Explorer [12], Firefox [13] and Opera [14] and enumerated their add-ons. Then, we grouped the add-ons' categories and mapped each add-on to one category, based on the add-ons functionality. Some add-ons have been grouped in more than one categories, as they provide multiple functionality. For the mapping of the add-ons functionality we used the following taxonomy[1]:

1. **Content filtering:** Block content (advertisements, cookies, images, pop-ups, etc.)
2. **Parental control**: Includes traffic filters to block websites containing inappropriate material[2]
3. **Passwords**:
   a. **Generators**: Generation of strong passwords
   b. **Managers**: Creation of a master password and password management
4. **Plain proxy:** Simple proxy without any encryption included
5. **Privacy**: Privacy protection add-ons (e.g. privacy settings manager)
6. **Protection from rogue websites**:

[1] Categories marked with 1, 2, 3… are the 1st level categories, while those marked with a, b, c… are the 2nd level categories (i.e. sub-categories).

[2] Apart from the parental control functionality, since such sites often include malware, this control can protect users' security and privacy

a. **Antivirus blacklists**: Websites providing online antivirus scans of files for malicious software (e.g. Virus Total [15])

b. **Malware blacklists**: Websites providing blacklists blocking malicious content (e.g. MalwareDomains [16])

c. **Phishing blacklists**: Websites providing blacklists blocking phishing attacks (e.g. PhishTank [17])

d. **Reputation blacklists**: Websites providing blacklists blocking pages based on their reputation (e.g. Web Of Trust [18])

e. **Sandbox**: Analysis of downloaded files for malicious software (e.g. Dr. Web LinkChecker [19])

7. **Third-party software management**: Blocking third-party software (e.g. Flash, Java, JavaScript, etc.)
8. **Tracking**: Blocking website(s) that track user's online behavior
   a. **Social Media (SM) redirection**: Blocking the visited website from redirecting the user to a social media website
9. **Traffic encryption via proxy**: Proxy that encrypts user's traffic

4 Results

4.1 Revisiting pre-installed security controls

In our previous work [2], we examined the availability and manageability of security controls offered by popular smartphone and desktop browsers. The availability of those controls is re-examined to highlight any changes that may exist in the latest browsers' versions. The results of our work are summarized in Table 2, using the following notation: (i) ☒ is used when the security control is not offered whereas (ii) ■ is used when the browser offered the security control. Also, the following acronyms are used for the browsers: AS = Apple Safari, GC = Google Chrome, IE = Internet Explorer, MF = Mozilla Firefox and OP = Opera.

Opera modified three of its controls in its latest version: the *"master password"* and the *"SSL/TLS version selection"* controls, both of which were available in the past and are now removed. While, the same browser altered one of the available controls of this category, i.e. the *"manually update extensions"* control, which was not available in the past. Also, Chrome added a *"master password"*, which was previously unavailable. Finally, Firefox no longer provides the reporting control for rogue websites and Opera removed both *"modify user-agent"* and *"website checking"* controls.

The last two rows of Table 2 include the amount of unavailable controls in each browser from a total of 32 controls, and the percentage of those, respectively. Indicatively, Safari did not implemented 34.4% of the surveyed controls, while Firefox offered the majority of the controls that are examined herein.

The availability of a control does not offer, though, any guarantees regarding the security offered. The scope of this paper does not include the accuracy or precision of these controls. Howerver, the relevant literature has explored this area. For instance the authors in [20] and [21] evaluated the phishing and malware protection controls provided by popular mobile browsers in Android and iOS and desktop browsers in Windows.

Table 2. Availability of controls (n=32)

Browsers	**AS**	**GC**	**IE**	**MF**	**OP**
Content controls					
Block cookies	■	■	■	■	■
Block images	■	■	■	■	■
Block pop-ups	■	■	■	■	■
Privacy controls					
Block location data	■	■	■	■	■
Block referrer	☒	■	☒	■	☒
Block third-party cookies	■	■	■	■	■
Enable DNT	■	■	■	■	■
History manager	■	■	■	■	■
Private browsing	■	■	■	■	■
Browser management controls					
Browser update	☒	■	■	■	■
Certificate manager	■	■	■	■	■
Master password	☒	■	☒	■	☒
Proxy server	■	■	■	■	■
Search engine manager	■	■	■	■	■
SSL/TLS version selection	☒	☒	■	☒	☒
Task manager	☒	■	☒	☒	■
Third-party software controls					
Auto update extensions	■	■	■	■	■
Auto update plugins	☒	☒	☒	☒	☒
Disable extension	■	■	■	■	■
Disable Java	■	■	■	■	■
Disable JavaScript	■	■	■	■	■
Disable plugin	■	■	■	■	■
External plugin check	☒	☒	☒	■	☒
Manually update extensions	■	■	☒	■	■
Manually update plugins	☒	■	☒	■	☒
Web browsing controls					
Certificate warning	■	■	■	■	■
Local blacklist	☒	■	■	■	■
Malware protection	■	■	■	■	■
Modify user-agent	■	■	■	■	☒
Phishing protection	■	■	■	■	■
Report rogue Website	☒	☒	■	☒	■
Website checking	☒	☒	■	☒	☒
☒ =	11	5	7	5	8
% =	34.4%	15.65%	21.9%	15.6%	25%

4.2 Survey of browsers add-ons

The amount of add-ons offered by each browser, up to April 2015, is depicted in Table 3. We tested only a subset of the add-ons offered by Chrome (65) and Firefox (65), based on user popularity, so as to end up with almost the same amount of tested add-ons in all browsers. All the available add-ons, that were included in the rest of the browsers, were tested. Thus, we examined a total of 227 add-ons. The list of the examined add-ons is available in the paper's Appendix. Chrome did not offer a specific category, so we found relevant add-ons with the use of specific keywords for each of the proposed categories (e.g. privacy, tracking, passwords, etc.). The add-ons were selected again based on user popularity.

Table 3. Available add-ons per browser

Browser	Security and/or privacy add-ons
Safari	38
Chrome	N/A[3]
Internet Explorer	7
Firefox	1327
Opera	52

The mapping between the available categories and the add-ons is not one-to-one, as some add-ons offer mechanisms for more than one of the categories. Moreover, the tests were conducted from January to April 2015 therefore it is possible that some add-ons might have been altered (e.g. deleted or added).

Figures 1-5 summarize the results regarding the add-ons that were found in each category[4]. Each figure indicates the percentage of the total add-ons located in each category in comparison with the total add-ons in each browser. The overall sum of all add-ons exceeds 100%, since one add-on may belong in more than one category. Additionally, Table 4 (c.f. Appendix) depicts the add-ons of each category provided by surveyed browsers, while the names of the tested add-ons are included in the Appendix as well.

[3] GC does not group security add-ons in one category, which so the total number of security add-ons is unknown.

[4] 2nd level categories (e.g. password manager, etc.) are included in Table 4 of the Appendix, and not depicted in this section.

Fig. 1. Available add-ons in Safari (n=38)

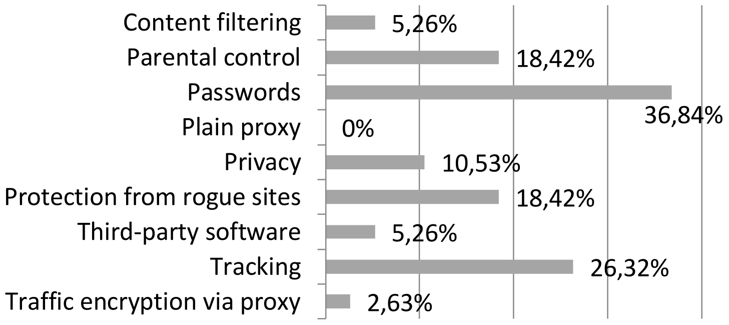


Fig. 2. Available add-ons in Chrome (n=65)

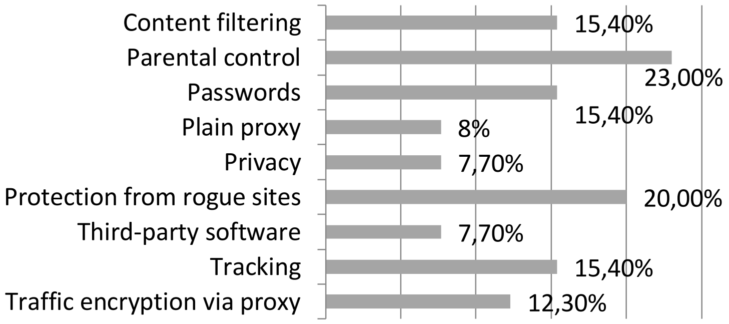


Fig. 3. Available add-ons in Internet Explorer (n=7)

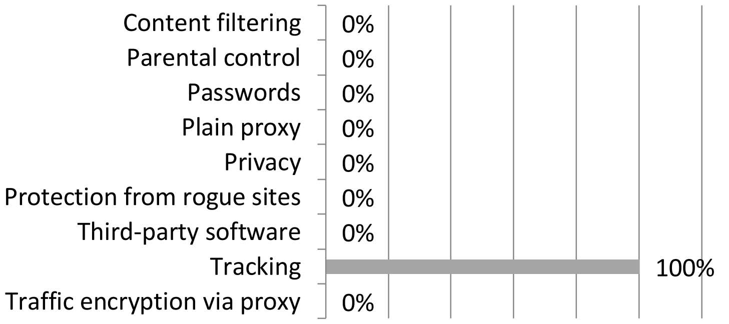


Fig. 4. Available add-ons in Firefox (n=65)

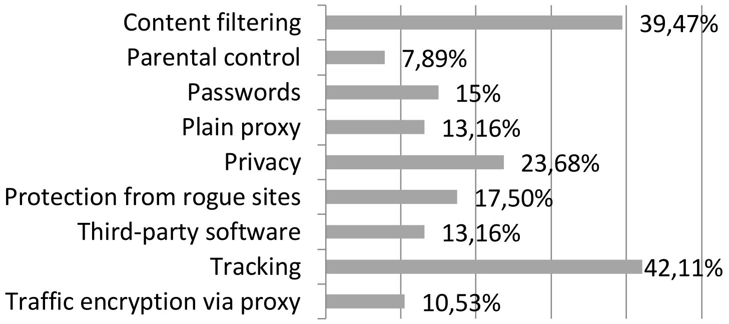
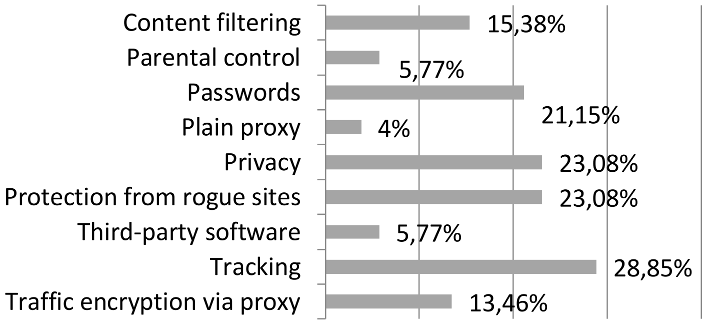


Fig. 5. Available add-ons in Opera (n=52)



5 Discussion

5.1 Revisiting pre-installed security controls

Our analysis showed that all browsers provide the content controls, while the second category (i.e. privacy controls) does not include the “block referrer” control in the majority of the tested browsers. Thus, the HTTP value in the header is most of the times transmitted and can be collected by malicious entities that aim to track users.

Browser management controls were not available in the majority of the browsers. More specifically, most of the browsers did not support the use of a master password, the selection of the SSL/TLS version and a task manager. None of them offered an auto-update function for the included plugins, while most of them failed to provide manual updates or external checks for those plugins. These are important in terms of aquiring the latest updates, which often include security patches.

Only a few browsers offered reporting rogue websites, although IE was the only one to provide a website checking control. Such an approach is clearly a major drawback, in terms of not offering a checking service for possible rogue websites and so, the user is exposed to malicious sites.

In the rest of this section, we discuss the security gaps in terms of non implemented controls, that were found in each browser:

Safari: As summarized in Table 2, 34.4% of the surveyed controls were not implemented, and thus AS does not offer an adequate level of security. From those controls, the most critical are summarized as follows: the browser lacks a master password service and thus the user cannot manage the installed passwords in the browser. Also, there is no blacklist mechanism available to filter websites based on reputation, and no reporting services if the user wants to check a visited website regarding its legitimacy. In addition, there is no SSL/TLS version selection option available, and as a result the user cannot upgrade the mechanism to its latest version.

Chrome: We had similar results to Safari. Once more, there is lack of SSL/TLS version selection and no reporting or checking mechanisms regarding the websites visited by the user. Thus, the user is unable to check a visited website whether it is malicious or not.

Internet Explorer: It does not offer a master password service and the option to block the referrer. Moreover, there were not available controls regarding the manual update of the browser's features (i.e. extensions and plugins). Finally, the user cannot use an external source to check the included plugins, a feature that is currently offered only by MF.

Firefox: As summarized in Table 2, Firefox provides the highest number of available controls. In addition, its community offers the highest amount of available add-ons, regarding security and/or privacy (i.e. 1327, April 2015). The security limitations of Firefox's were only: SSL/TLS version selection and a reputation based mechanism to filter the visited websites, as discussed in the Safari browser.

Opera: It was the second less secure browser (after IE) with regards to the availability of security controls. Almost all of the unavailable controls were similar to the AS, except the "modify user-agent" control, which was not provided by Opera.

5.2 Survey of add-ons

The analysis revealed that all browsers except for GC and IE offered a 1st level categorization dedicated for security and or privacy add-ons. More specifically, Safari provided *Security*, Firefox and Opera provided *Privacy & Security*. Chrome and IE did not, and as a result we manually searched for the security and privacy add-ons. This confusing structure/organization of add-ons may result in users unavailable any useful (with respect to the provided security) add-on. For example, Chrome classified a popular add blocker add-on (i.e. AdBlock Plus [22]) in the "search & browsing tools" category, which does not encourage the user to install the application.

Additionally, none of the browsers offered a 2nd level categorization (e.g. passwords, malware protection, VPNs, etc.). Such approach, could be proven beneficial for users, since they could be searching for specific add-ons only in.

All of the browsers provided an adequate description of each add-on, except Safari, which only provided a short paragraph. Thus, the user had to visit the developer's website to find additional information regarding the add-on(s).

In the rest of this subsection, we discuss the results of our analysis, concerning the available add-ons in each browser's repository:

Safari: As Figure 1 depicts, Safari's community clearly covers almost every one of the surveyed categories. Its main focus is two-fold: offering password services for password generation and management (36.84%), and protecting the user from tracking (26.32%). These two pose as the community's highest priorities. Note that the first category was one the browser's gap, in terms of unavailable controls. Next, Safari's add-ons focus in website filtering protection, i.e. parental control and rogue sites' filtering (both at 18.42%). Thus, they protect the user from visiting websites that contain malicious or offensive content that covers the second security gap as well. The other categories were partially covered by Safari's community, with the highest being the "privacy" category (10.53%) and the lowest being the "plain proxy", which is not covered.

Chrome: According to Figure 2, Chrome provides add-ons in each of the surveyed categories, thus, satfisfied the unavailable controls that we have been identified in this work. More specifically, the browser's community focuses on offering parental control services (23%) and rogue sites filtering mechanisms (20%), therefore succeeding in protecting the user against malicious websites. Moreover, Chrome offers add-ons that provide the user with content blocking mechanisms, password services and tracking blocking services (all with a 15.4% availability). This suggests that the Chrome communicty considers those services almost as equal of importance as the highest priorities, as discussed above. All the other categories, were partially covered by Chrome's community, with the highest being the "traffic encryption via proxy" category reaching 12.3%, while the rest of the categories have a 7.7% availability. Note that this applies only to the current tested subset, which includes a part of the most popular add-ons of the browser, based on user popularity.

Internet Explorer: Internet Explorer offers only 7 security and/or privacy add-ons. All of them focus on tracking protection and, thus, all the categories that are not covered by the browser's controls, are unprotected by the offered add-ons as well. As a result, Internet Explorer's add-ons fail to provide the unavailable security and/or privacy protection.

Firefox: According to Figure 4, Firefox browser fully covers not only the unavailable controls, but the total categories (and sub-categories) of the add-ons. More specifically, the browser's highest priorities are tracking protection (42.11%) and content filtering services (39.47%). As a result, the user is able to block both tracking websites that aim in accessing sensitive information and content elements (e.g. pop-ups) that could either annoy or harm the user (e.g. phishing content). Also, all the other categories are again adequatelly covered, while varying from 23.68% (privacy) to 7.89% (parental control). Overall, Firefox succeeds in offering almost a full set of both controls and add-ons regarding the surveyed categories.

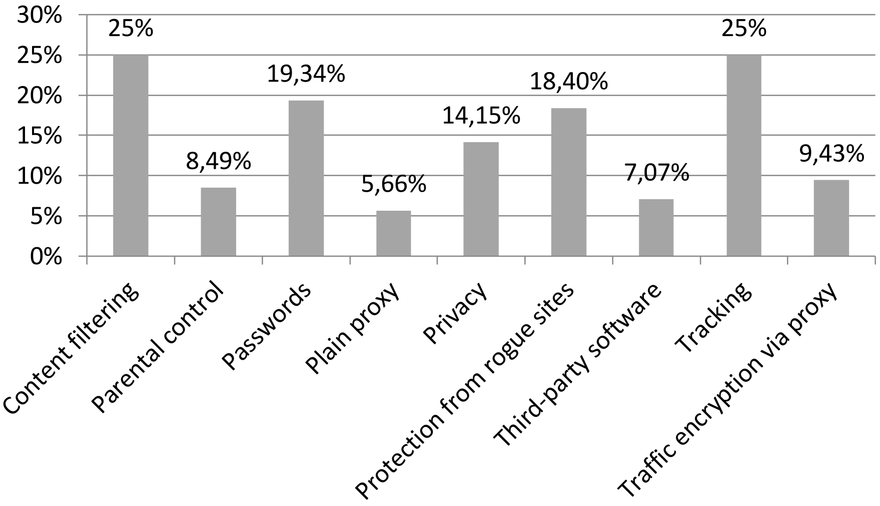
Opera: Despite the controls' unavailability, Opera offered a variety of add-ons regarding all the tested categories. Four categories clearly pose as Opera's main focus: tracking blocking services (28.85), privacy and protection from rogue sites (both at 23.08%) and password services (21.15%). The rest of categories were partially covered by Opera's community, with the highest being the "content filtering" category reaching

15.38% and the lowest being the "plain proxy" one, which is located at 3.85%. Overall, Opera may not offer a complete set of security and privacy controls, but such a feature is clearly covered by the browser's community regarding the available add-ons.

Overall availability of add-ons

Figure 6 summarizes the above. It reveals the overall focus of the community that provides security-oriented add-ons in the browser ecosystem.

Fig. 6. Overall availability of add-ons (n=227)



As Figure 6 suggests, *"tracking"* and *"content filtering"* categories include 25% of the most popular, security-oriented add-ons. This suggests that the highest priority in the browsing ecosystem is enhancing the protection of the user from malicious entities who aim to violate users' privacy. In parallel, the community aims to offer filtering services for content elements (i.e. cookies, advertisements, images and pop-ups), which could either create annoyance or include malicious software (e.g. phishing, scam) that harm the user.

After that, there are the "*passwords*" and "*protection from rogue websites*" categories, which hold 19.34% and 18.4% respectively. The former category includes password oriented services, i.e. *managers* (15.1%) and *generators* (9.43%), and covers the identified gap, since almost all modern web browsers (except Firefox) do not offer such a control. The latter, includes protection based on\against: *malware* (8.02%), *reputation* (8.02%), *phishing* (5.19%) *antivirus* (4.72%) and *sandbox* (3.77%). Such services aim in protecting the user from malicious websites.

The *"privacy"* category includes privacy oriented contents (e.g. autofill forms, cache, location, etc.). Those can either be blocked or cleared (e.g. cache cleaner), so as not to be monitored by an unauthorized entity. This category includes 14.15% of the surveyed add-ons.

The remaining four categories are located just below 10%. More specifically, in descending order: *traffic encryption via proxy* (9.43%), *parental control* (8.49%), *third-party software* (7.07%) and *plain proxy* (5.66%). The first and last category reveal the need to use a proxy service to either access any region protected content, or hide user's identity for tracking protection. The "*parental control*" category includes website filtering to block any inapropriate material[5]. Finally, the last surveyed category (i.e. *third-party software*) allows the management (i.e. blocking, enabling) of third-party software: flash, java, javascript, etc., in order to protect the user from services that are not built-in the browser, since malicious content may be included.

6 Conclusions

The paper provides a comprehensive analysis of the available security and privacy controls that are pre-installed in popular desktop web browsers. It also provided a comparative evaluation of the availability of security-oriented add-ons in each desktop browser. This paper extends our previous work [2] and examines the security controls (both, pre-installed and third-party add-ons) that are available in modern desktop browsers.

We analyzed a total of 32 pre-installed security-oriented controls and found that Firefox provided the majority of them (i.e. 84.4%). Safari offered only 65.6% of the controls and the availability of the controls in the rest of the browsers varied (from approx. 71-85%). The analysis of the available security-oriented add-ons revealed that Firefox and Chrome provided a plethora of security and/or privacy oriented add-ons. The other browsers had in total approximately 50 security-oriented add-ons only, while Internet Explorer offered only seven. Almost all browsers (except IE) provided add-ons that fill the gap for the unavailable pre-installed security controls. In addition, already existing controls (e.g. malware protection, master password, etc.) are enhanced by the availability of add-ons, if the user chooses not to only trust the browser's built-in mechanisms.

The analysis reveals that web browsers can enhance the grouping of the available security-oriented add-ons. That holds true as all browsers, except GC and IE, offered only a 1st level categorization. The absence of this add-on grouping hinders users' searches for add-ons that enhance their security. However, none of the browsers offered additional subgroups (2nd level categorization), which could further enhance user's search results when looking for a specific subcategory of an add-on (e.g. password generators). In this work, we provide such a taxonomy of add-on categories.

Our analysis focuses on the availability of security oriented controls. However, their performance is not in the scope of this paper. Another limitation of our work is that that new security controls and add-ons may be added to browsers or the popularity of the addons might change. Also, in Chrome and Firefox only the 65 most popular add-ons, in order to have a consistent comparison with the rest browser that had only approximately 35 addons on average. In future work we plan to extend our work by increaseing the number of addons that have been surveyed, as well as measure the effectiveness and performance of security controls (both, pre-installed and addons).

[5] Pornographic or gambling material.

References

1. Securelist.com (2015) Financial cyber threats in 2014: Things changed - Securelist. http://securelist.com/analysis/kaspersky-security-bulletin/68720/financial-cyber-threats-in-2014-things-changed/. Accessed 10 Apr 2015
2. Mylonas A., Tsalis N., Gritzalis D. (2013) Evaluating the manageability of web browsers controls. In: 9th International Workshop on Security and Trust Management, pp. 82-98, LNCS 8203, Springer
3. Botha R., Furnell S., Clarke N. (2009) From desktop to mobile: Examining the security experience. Computers & Security. 28(3-4), 130-137
4. Amrutkar C., Traynor P., van Oorschot P. (2012) Measuring SSL Indicators on mobile browsers: Extended life, or end of the road?. pp. 86-103, LNCS 7483, Springer
5. Carlini N., Felt A., Wagner D. (2012) An evaluation of the google chrome extension security architecture. In: 21st USENIX Conference on Security, USA
6. Li L., Wang X., Choi J. (2007) SpyShield: Preserving privacy from spy add-ons. In Conference on Recent Advances in Intrusion Detection
7. Kapravelos A., Grier C., Chachra N., Kruegel C., Vigna G., Paxson V. (2014) Hulk: Eliciting malicious behavior in browser extensions. In: 23rd USENIX Security Symposium (USENIX Security 14), USA. USENIX Association
8. Barth A., Felt A. P., Saxena P.,Boodman A. (2009) Protecting browsers from extension vulnerabilities. In: 17th Network and Distributed System Security Symposium (NDSS ’10), USA
9. W3schools.com (2015) Browser Statistics. http://www.w3schools.com/browsers/browsers _stats.asp. Accessed 10 Apr 2015
10. Extensions.apple.com (2015) Apple - Safari - Safari Extensions Gallery. https://extensions.apple.com/. Accessed 10 Apr 2015
11. Chrome.google.com (2015) Chrome Web Store. https://chrome.google.com/webstore/category/extensions. Accessed 10 Apr 2015
12. Internet Explorer Gallery (2015) Internet Explorer Gallery. http://www.iegallery.com/ PinnedSites. Accessed 10 Apr 2015
13. Addons.mozilla.org (2015) Add-ons for Firefox. https://addons.mozilla.org/en-US/firefox/. Accessed 10 Apr 2015
14. Opera add-ons (2015) Opera add-ons. https://addons.opera.com/en/. Accessed 10 Apr 2015
15. Virustotal.com (2015) VirusTotal - Free Online Virus, Malware and URL Scanner. https://www.virustotal.com/. Accessed 10 Apr 2015
16. Malwaredomains.com (2015) DNS-BH – Malware Domain Blocklist. http://www.malwaredomains.com/. Accessed 25 Apr 2015
17. Phishtank.com (2015) PhishTank | Join the fight against phishing. https://www.phishtank.com/. Accessed 25 Apr 2015
18. Ltd. W (2015) Safe Browsing Tool | WOT (Web of Trust). In: Mywot.com. https://www.mywot.com/. Accessed 25 Apr 2015
19. LinkChecker D (2013) Dr.Web LinkChecker. In: Addons.mozilla.org. https://addons. mozilla.org/en-US/firefox/addon/drweb-anti-virus-link-checker/?src=search. Accessed 25 Apr 2015
20. Virvilis N., Tsalis N., Mylonas A., Gritzalis D. (2014) Mobile devices: A phisher's paradise. In: 11th International Conference on Security and Cryptography (SECRYPT-2014), pp. 79-87, ScitePress, Austria.
21. Virvilis N., Mylonas A., Tsalis N., Gritzalis D. (2015) Security Busters: Web Browser security vs. rogue sites. Computers & Security.

22. Chrome.google.com (2015) Adblock Plus. https://chrome.google.com/webstore/detail/adblock-plus/afkdehgifkgjdcdlbfkjnmaeagepfbgp?hl=en. Accessed 25 Apr 2015

Appendix

Table 4. Number of add-ons in each browser (n=227)

1st level	2nd level	AS	GC	IE	MF	OP
Content filtering	-	7	15	0	17	18
Parental control	-	2	10	0	4	53
Passwords	-	14	10	0	6	41
	Generators	4	6	0	4	20
	Managers	14	7	0	5	32
Plain proxy	-	0	5	0	6	12
Privacy	-	4	5	0	10	30
Protection from rogue websites	-	7	13	0	8	39
	Antivirus	2	3	0	3	10
	Malware	4	5	0	3	17
	Phishing	4	2	0	2	11
	Reputation	2	7	0	3	17
	Sandbox	2	3	0	3	8
Third-party software	-	2	5	0	6	15
Tracking	-	10	10	7	17	53
	SM redirection	3	0	0	0	5
Traffic encryption via proxy	-	1	8	0	5	20
Total		**38**	**65**	**7**	**65**	**52**

Apple Safari. 1Password, AdBlock Lite, Adblock Plus, Adguard AdBlocker, Avatier Single Sign-On (SSO), Blur, Bonafeyed, Cognisec Workspace Application Helper, Cryptocat, Cryptonify, DisableGoogleRedirect, Dr.Web LinkChecker, Facebook Disconnect, Ghostery, Google Disconnect, HyprKey Authenticator, Incognito, JavaScript Blocker, Keeper - Password and Data Vault, LastPass, Mitto Password Manager, MyPermissions Cleaner, PoliceWEB.net, Redirector, RoboForm Online, SafariSGP, Safe In Cloud, SafeSurf, Search Virustotal.com, Security Plus, SID, Teddy ID Password Manager, Total Defense TrafficLight, TrafficLight, Twitter Disconnect, uBlock, URL-Filter, WOT.

Google Chrome. 1Password, AdBlock, Adblock Plus, Adblock Plus Pro, Adblock Super, Ad-blocker for Gmail, Adguard AdBlocker, Adult Blocker, Avast Online Security, AVG Do Not Track, AVG PrivacyFix, Bitdefender QuickScan, Blockfilter | The Advanced Adult Filter, Blocksi Web Filter, Blur, Browsec, Cache Killer, Clear Cache, Clear Cache Shortcut, CommonKey Team Password Manager, Cookie Manager, CyberGhost VPN, Deadbolt Password Generator, Do Not Track, DotVPN, Dr.Web Anti-

Virus Link Checker, EditThisCookie, eSafely, Falcon Proxy, FlashControl, FreeMyBrowser, Ghostery, Hide Images, HTTPS Everywhere, iNetClean porn filter - protect your family, LastPass, Parental Control App, Parental Controls & Web Filter from MetaCert, Passter Password Manager, Password Hasher Plus, PasswordBox, Privacy Badger, Privacy Guardr, Privacy manager, Proxy Auto Auth, Proxy Era, Proxy Helper, Proxy SwitchyOmega, Proxy SwitchySharp, ScriptBlock, ScriptSafe, Secure Downloader, Secure Passwords, Security Plus, Simple JavaScript Toggle, Simply Block Ads!, StopItKids parental control, Strong Password Generator, Swap My Cookies, Vanilla Cookie Manager, VTchromizer, WebFilter Pro, Webmail Ad Blocker, YouDeemIt - Parental Advice System, ZenMate Security & Privacy VPN.

Internet Explorer. EasyList Standard, EasyPrivacy, Indonesian EasyList, PrivacyChoice - all companies, PrivacyChoice - Block companies without NAI, Stop Google Tracking, TRUSTe.

Mozilla Firefox. Ad Killer, Adblock Edge, AdBlock for Firefox, AdBlock Lite, Adblock Plus, Adblock Plus Pop-up Addon, Advanced Cookie Manager, anonymoX, Anti-Porn Pro, Autofill Forms, AutoProxy, AVG Do Not Track, BetterPrivacy, Bitdefender QuickScan, BlockSite, Bluhell Firewall, Blur, BugMeNot, Censure Block, Clear Console, Click&Clean, Cookie Monster, Cookies Manager+, Disable Anti-Adblock, Disconnect, Dr.Web LinkChecker, DuckDuckGo Plus, Empty Cache Button, Facebook Disconnect, FB Phishing Protector, Flash Block, Flash Control, friGate, Ghostery, Google Privacy, Google search link fix, Hide My Ass! Web Proxy, JavaScript Deobfuscator, KeeFox, LastPass Password Manager, Lightbeam for Firefox, McAfee Security Scan Plus detection, Modify Headers, Multifox, NO Google Analytics, NoScript Security Suite, Password Exporter, Private Tab, ProCon Latte Content Filter, ProxTube - Unblock YouTube, Public Fox, QuickJava, RefControl, RequestPolicy, Saved Password Editor, Self-Destructing Cookies, SSL Version Control, Stealthy, Strict Pop-up Blocker, Tamper Data, User Agent Overrider, Web of Trust, WorldIP, YesScript, ZenMate Security & Privacy VPN.

Opera. Ghostery, ZenMate, WOT, LastPass, Dr.Web Link Checker, DotVPN, HTTPS Everywhere, History Eraser, Avira Browser Safety, Browsec, Disconnect, CyberGhost VPN, Blur, AVG PrivacyFix, VPN.S HTTP Proxy, MyPermissions Cleaner, HideMy Ass, PasswordBox, Adult Blocker, Google Analytics Opt-out, Cryptocat, History On/Off, RoboForm Lite Password Manager, µMatrix, Location Guard, Blocksi, Single-Click Cleaner, Security Plus, SimpleClear, Facebook Redirect Fixer, Stop-it, SafeBrowser, Show passwords, Local pass store, BlocksiLite, Show Password, Cobra Online Security ATD, Disconnect Privacy Icons, Cookie Jar, IvlogSafe, Blockfilter, KANOPE, Google Safe Browsing, Filter request headers, Twitter Redirect Fixer, PasswordMaker Pro, Certified Messages, Floodwatch, vPass, Limitlesslane, LogMote, PreferSafe.