Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D7.5

Open tool portal – accompanying document

Document Identification	
Due date	31 May 2022
Submission date	08 June 2022
Revision	1.00

Related WP	WP7	Dissemination Level	Public
Lead Participant	BRNO	Lead Author	Vashek Matyáš (BRNO)
Contributing Beneficiaries	UMU, VAF, TDL	Related Deliverables	D7.2, D7.3, D7.4, D7.7

Abstract:
This document carries information related to and largely also taken from the deliverable D7.5 – Open tool portal (https://cybersec4europe.eu/open-tool-portal), with a proposal of the taxonomy of open source security and privacy tools for end-users, with a particular focus on the Firefox web browser and its ecosystems of extensions. The portal primary aim is to provide a secure and usable desktop environment for the two defined user types - beginner and intermediate user. The secondary aim is to present 5 expert tools developed during the project course.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This is an accompanying document to the deliverable D7.5 Open tool portal – the portal itself is the ultimate deliverable, which you find at https://cybersec4europe.eu/open-tool-portal.

The portal section "Open tools for professional use" presents 5 expert tools developed within the project, these tools are briefly described in the following sections. The main tool here is the Cyber Sandbox Creator – the deliverable D7.2 (Virtual lab for open-source tools education and research) of the project, and was also accompanied by D7.4 (Common virtual lab with open-source tools for research and development), where it was integrated with parts of the expert tools described in the following sections.

The set of open-source tools and operating systems in the Open tool portal forms a secure and usable desktop environment for the two defined user types – *beginner* and *intermediate* users. CyberSec4Europe consortium evaluated multiple candidate open tools in each of the categories, and we provide specifications of ideal candidate traits and test evaluations for each individual tool category.

This document also provides the taxonomy of open source security and privacy tools for end-users. This taxonomy was developed to support end-users in navigating through the portal of open source security and privacy tools that is provided as one of the outputs of the CyberSec4Europe project. We consider the end-user view with respect to two levels of security/privacy skills and knowledge - end-users not experienced in these areas at all, who have moderate general IT skills and can install applications and undertake their basic settings according to instructions and users with moderate security/privacy skills and knowledge, who are keen to explore advanced settings of relevant tools and applications and are willing to undertake their advanced settings by given instructions. The taxonomy is presented in more detail/depth in one particular dimension, the web browser and its ecosystems of extensions (a.k.a. plugins or add-ons). This work was undertaken with a particular focus on the Firefox browser.

Document information

Contributors

Name	Partner
Vashek Matyáš	BRNO
Tamara Čierniková	BRNO
Alexandre Le Clanche	BRNO & INSA Centre Val de Loire
Milan Brož	BRNO
Irene Cocco	BRNO & University of Cagliari
Lukáš Němec	BRNO
Lydia Kraus	BRNO
Guilherme Alves Carvalho	BRNO & Universidade Federal de Uberlândia
Antonio Skarmeta	UMU

Jozef Vyskoč kindly reviewed chapters 4-7 of this document, and the preceding sections are derivatives of the portal itself.

History

Version	Date	Authors	Comment
0.01	2022-05-27	All contributors as stated above	1st draft
0.99	2022-05-29	All contributors as stated above	2nd & final draft – internal review
1.0	2022-05-31	Vashek Matyas	Final release
1.0	2022-06-08	Ahad Niknia	Final check, preparation and submission

Table of Contents

1 Introduction

The purpose of this document is rather simple – it is not a deliverable, but an accompanying text to the deliverable D7.5 – Open tool portal of the CyberSec4Europe project – https://cybersec4europe.eu/open-tool-portal.

This document roadmap is as follows: Chapter 2 and 3, respectively, describe the two pivotal sections of the Open tool portal – expert user and end-user, respectively. Chapter 4 presents the taxonomy work undertaken in the start of our effort and provides a sort of introduction to the following chapters. Chapters 5 and 6 both carry the first section that describes the most important related work discovered during our research, and then we describe the development of the taxonomy and the taxonomy itself. Chapter 5 outlines the baseline taxonomy of open source security and privacy tools for end-users. Chapter 6 presents our taxonomy in one important (if not the most important) category – web browser and its ecosystems of extensions (a.k.a. plugins or add-ons). As agreed during the discussions of the CyberSec4Europe project in 2020, we focus on the Firefox browser in particular, as it is not just an open source system, but is also corporate neutral.

2 Open tool portal section for expert users

The portal section "Open tools for professional use" presents 5 expert tools developed by the CyberSec4Europe consortium members and associate partners. These tools are briefly described in the following sections.

2.1 Cyber Sandbox Creator: A tool for creating lightweight virtual labs

Cyber Sandbox Creator (CSC) is an open-source tool for building lightweight virtual laboratories for cybersecurity education, testing, and certification. Since February 2020, CSC has been used in practice numerous times and has been continuously improved to address the needs of a broad range of users. We identified six target user roles that can benefit from the tool: Educator, Trainee, Researcher, Developer, Specialist, and Auditor.

CSC is the deliverable D7.2 (Virtual lab for open-source tools education and research) of the project, and was also accompanied by D7.4 (Common virtual lab with open-source tools for research and development), where it was integrated with parts of the expert tools described in the following sections.

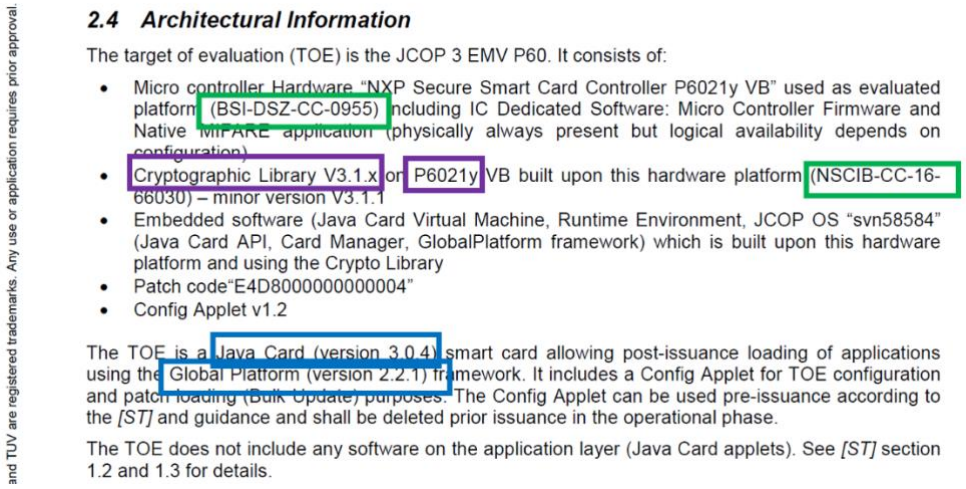
To create a virtual lab environment, a knowledgeable user first writes a sandbox definition: semi-structured text files describing virtual machine parameters and configuration of network topology. Then, CSC uses these files as input to generate an intermediate definition for Vagrant and Ansible. Finally, the result is distributed to regular users, who execute CSC to instantiate the actual virtual lab.

2.2 Seccerts.org: Analysis of security certification reports (CC EAL, FIPS140-2)

The sec-certs set of tools download, process, and analyse security certificates issued under Common Criteria and NIST FIPS 140-2 schemes and turn these into computer-searchable and analysable datasets. As a result, the following and other questions can be answered:

- What chips are impacted by flaw found in certified library X? Which certificates are relevant for my certified product Z? What products are affected by specific CVE vulnerability?
- Which devices were analysed for timing side-channel leakage? Is ECC 521-bit curves supported?
- What are the trends of whole certification ecosystem regarding the archival rate, achieved security levels, usage of protection profiles and others?

The certification reports are the most detailed publicly available documents, yet currently available as pdf report in non-standardized format with only some metadata extracted (e.g., FIPS140-2 extracts referenced certificates). The sec-certs downloads source documents (pdf describing certified configuration and security target, csv and html with additional metada) and extract relevant information using regular expressions created for specific areas like certificate references, cryptographic algorithms, security assurance levels and many others. The information extracted is stored in open format (json) and futher used to analyze certificates, map them to other sources like CVE vulnerability database and construct aggregate visual presentation available at https://seccerts.org. The sec-certs tools also allows to process all data locally including additional own, non-public documents.



and TUV are registered trademarks. Any use or application requires prior approval.

2.4 *Architectural Information*

The target of evaluation (TOE) is the JCOP 3 EMV P60. It consists of:

- Micro controller Hardware "NXP Secure Smart Card Controller P6021y VB" used as evaluated platform (BSI-DSZ-CC-0955) including IC Dedicated Software: Micro Controller Firmware and Native MIFARE application (physically always present but logical availability depends on configuration)
- Cryptographic Library V3.1.x on P6021y VB built upon this hardware platform (NSCIB-CC-16-66030) – minor version V3.1.1
- Embedded software (Java Card Virtual Machine, Runtime Environment, JCOP OS "svn58584" (Java Card API, Card Manager, GlobalPlatform framework) which is built upon this hardware platform and using the Crypto Library
- Patch code"E4D8000000000004"
- Config Applet v1.2

The TOE is a Java Card (version 3.0.4) smart card allowing post-issuance loading of applications using the Global Platform (version 2.2.1) framework. It includes a Config Applet for TOE configuration and patch loading (Bulk Update) purposes. The Config Applet can be used pre-issuance according to the *[ST]* and guidance and shall be deleted prior issuance in the operational phase.

The TOE does not include any software on the application layer (Java Card applets). See *[ST]* section 1.2 and 1.3 for details.

Figure 1 Example of interesting strings extractable via regular expressions, later stored in database (excerpt taken from NXP JCOP3 P60 CC certificate).

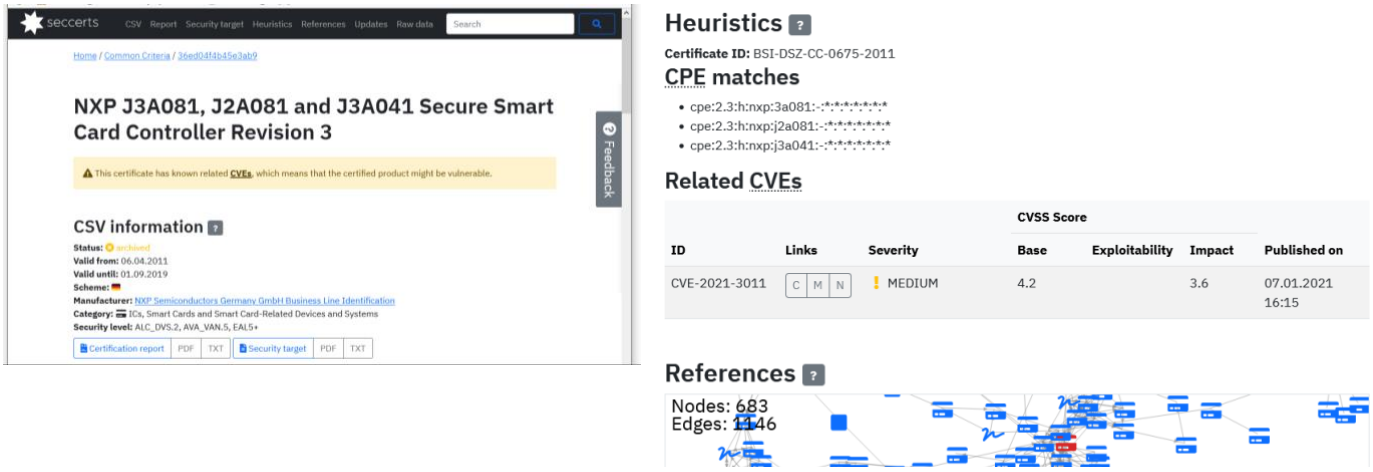


Figure 2 Example generated visualization for aggregated data extracted from CC certificate including matched CVE vulnerabilities and cross-certificate references graph.

2.3 SCRUTINY: Tool for quick similarity assessment of certified devices

Set of tools allowing to verify that all devices (e.g., cryptographic smartcards cards) are matching the expected forensic profile to detect chips of different revision, malfunctioning, or even counterfeited one.

Currently, the user is dependent on the trusted distribution channel established with vendor. Basic chip identification like ATR or CPLC is insufficient as can easily be modified during the card personalization. SCRUTINY tool orchestrates a suite of other open tools analysing target device and provide human-readable summary.

The typical procedure when applied to cryptographic smartcards is following:

- A card is inserted to reader, fingerprinted using suite of tools like JCAlgTest and compared with the expected profile.
- The device fingerprinting is based on the ATR, CPLC, supported algorithms, performance of selected crypto algorithms or power consumption traces for common cryptographic operations. The processing is configurable and may omit some of the analysis tool (e.g., power analysis which requires more elaborate measurement setup).
- The computed fingerprint is compared with expected one or optionally with the public database of results of already analysed cards and html report with visualized similarities and differences is generated.

The forensic profile can be created either by the end-users or by (preferably) by the device vendor or evaluation facility and included as authorized certification artefacts later verifiable by end-users.

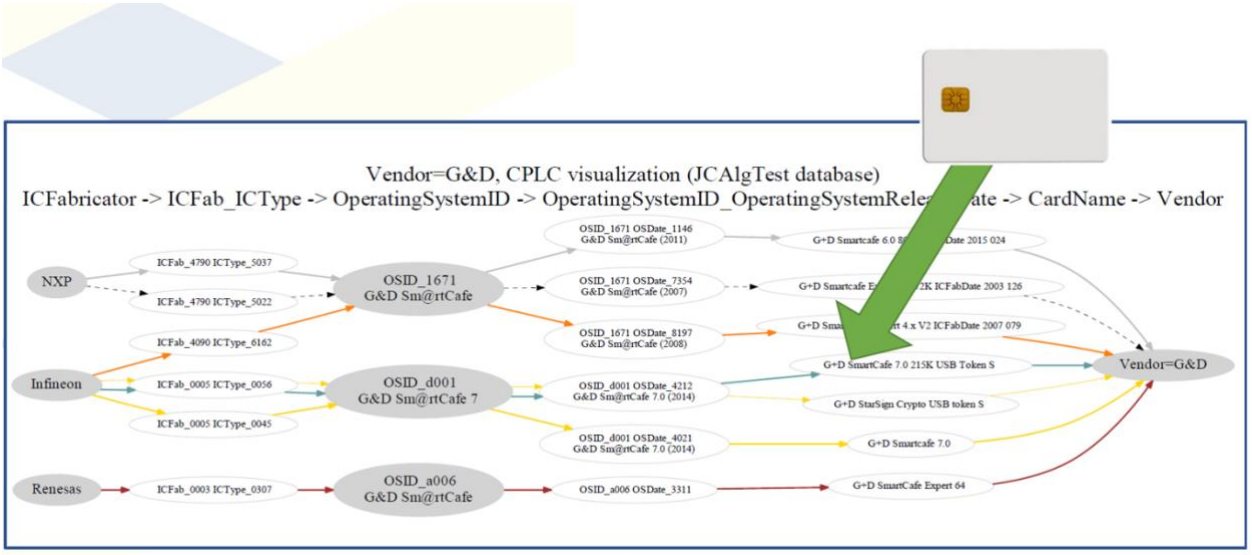


Figure 3 Example matching of target card fingerprint to database of known cards fingerprint (only CPLC matching is shown).

Figure 4 Example visualization of SCRUTINY summary report comparing two somewhat similar, but distinct types of smartcards.

2.4 Tool for high-performance, easy testing of (pseudo-)random data generators

Provides easy to use assessment of the randomness properties of data generated by truly random data generator (e.g., physical TRNG) or pseudo-random generator (e.g., AES ciphertext, PRNG). The typical use-case scenarios are:

- Detailed analysis of truly random data generators (on-card, dedicated entropy sources…),
- Continuous analysis of the randomness data used or produced,
- Continuous verification of the correct application of encryption on the outgoing encrypted data (shall be undistinguishable from random data).

The RTT consist of the following components:

- Multiple, well-known randomness statistical testing tools (NIST STS, TestU01, Dieharder, BoolTest) implemented with unified interface,
- Randomness testing performed as testing service (deployable as hosted or on-premises), parallelized computation of tests from the batteries for faster overall computation time,
- Easy end-user interface via local folders synchronized via suitable cloud-storage (OwnCloud, Dropbox…) and tested by the service.

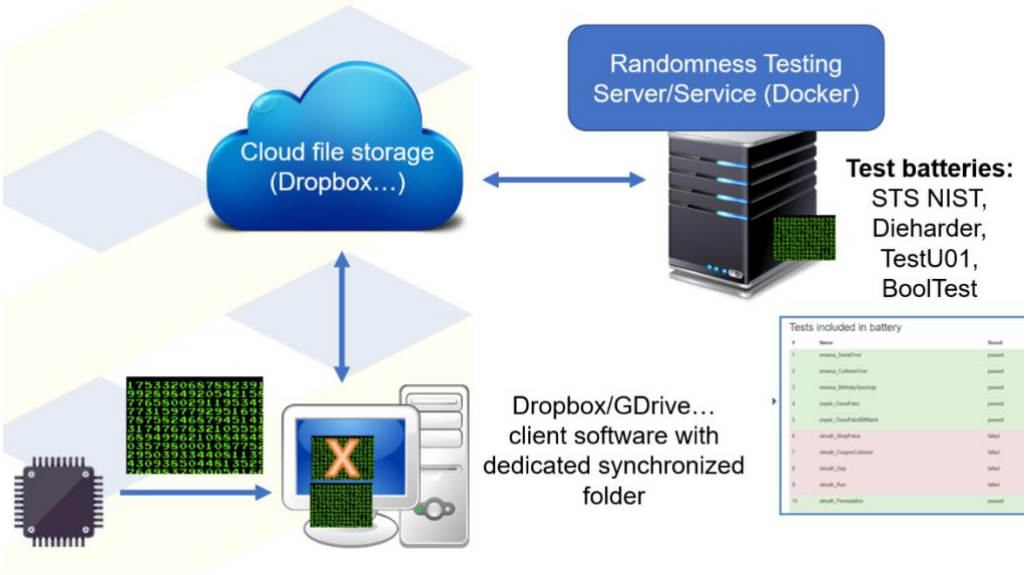


Figure 5 Overview of the randomness testing service workflow.

2.5 Tool for security analysis of RSA and ECC implementations in crypto libraries and cards

Set of tools for exhaustive implementation testing of existing RSA and ECC implementations and verify that the required security-relevant checks like known invalid inputs tested (EC point not on curve, invalid curve parameters…) are performed. Automatic analysis of library output artefacts (generated keys, side-channel leakage...) is collected and any deviances (even if not directly exploitable) from the common behaviour are searched for detected. A black-box analysis is performed, allowing for analysis also on the closed, proprietary devices. The typical use-case scenarios are:

- Automatic testing during development (e.g., Continuous Integration),
- Initial thorough analysis of a specific card or library.

• Generation of behavioural forensic profiles for later comparison of the libraries including the closed, proprietary ones.

3 Open tool portal section for standard users

3.1 Background

This portal section "Tools for end-users" contains recommendations for open-source tools focused on regular end-users. Within the portal, regular users are divided into two categories: *beginner* and *intermediate*. These user types are precisely described in Section "User definitions" below.

The set of open-source tools and operating systems in the Open Tool Portal forms a secure and usable desktop environment for the defined user types. A *beginner* or an *intermediate* user should be able to perform desired tasks within the environment effectively and securely.

The portal contains following sections:

- Data-at-rest encryption – disk and filesystem encryption,
- Password management – password managers and suggestions for secure password management,
- Email communication – email encryption,
- Firefox web browser with a set of privacy-enhancing plugins,
- Operating systems – suitable operating systems for deploying the tools.

These sections include specifications of ideal candidate traits and test evaluations for each individual tool category. The core of each section describes only recommended tools. Other tools were evaluated as inappropriate and their descriptions can be found on the portal.

The tool categories were selected according to the Open tool taxonomy described later in this document. Some members of the team then also worked with Irene Cocco on the evaluation of the selected web browser and its set of browser plugins from April 2020 till May 2022. The selection was based on Firefox taxonomy and Browser plugin taxonomy.

The rest of the results on this portal were supported by previous research of Maxime Faure and Flavien Ehret in 2019. This research was conducted during their internship in cooperation with the CRoCS laboratory research group at the Faculty of Informatics, Masaryk University. Faure and Ehret searched for available security-focused open tools and operating systems and provided a list of potential candidates for further testing. Milan Brož reviewed and summarized their results regarding open-source operating systems as of May, 2022[1]. Other supporting materials were also provided by Daniel Pecuch and Andrej Hulina in their bachelor theses.

The final suggestions for this portal were provided by Tamara Čierniková as results of her bachelor thesis in May 2022, with cooperation of Václav Matyáš and Milan Brož. This thesis updated and extended previous research with direct focus on the specific user types.

3.2 Methodology

The final delivery of suggested tools for the Open Tool Portal was preceded by several steps:

- Previous work on the CyberSec4Europe project was collected and other related information sources were analysed.

[1] The overview of internship results can be found at https://docs.google.com/document/d/13hHt1-7Rwd-St4GbSWOmv3d5L7buUbhFRjpfGXZbnpY/edit#heading=h.i302a31hcbyc.

- We defined the *beginner* and *intermediate* categories precisely for the scope of the Open Tool Portal since previous definitions within the CyberSec4Europe internal working documents were too informal and vague.
- We conducted extensive research on available tools to select candidates for further testing. A possible candidate should be issued under a license approved by the Open Source Initiative. The development of the tool should be active with regular releases and security patches. The selection criteria were also influenced by the specific needs and skills of the custom user types.
- We described the ideal properties and features for each tool category with respect to the custom user types.
- The candidates were tested with the focus on usable security and compliance with the latest best security practices.
- We evaluated the candidates by comparing previously defined ideal properties and features to populate the final set of suggested tools. The conclusions for each tool category include recommendations on configuration to yield secure settings where necessary.

Testing of these categories was realized by the *cognitive walkthrough* method. The *cognitive walkthrough* method is a technique based on cognitive theory of exploratory learning used for evaluation of software usability.

We managed to select at least one solution for each user type from all candidate sets, including basic comparative reviews of tested applications. Additional results of the testing show persisting problems with usable security and insufficient focus on inexperienced audiences in the documentation of open-source projects.

3.3 User definitions

3.3.1 General user categorization

Two end-user categories are considered in the scope of this document: a *beginner* and an *intermediate* user. The categorization is based on knowledge and experience in the usage of an operating system and applications on top. There is no focus on security experts and in-depth knowledge in information security is not expected.

The goal of this categorization is to provide accurate documentation adjusted for a particular user type to maximize its utility. Descriptions below define general differences between a beginner and an intermediate; they do not define them across the whole documentation, rather are used as a basis of further categorization for each internal section.

3.3.2 Beginner

A beginner user is defined as a person with moderate technical skills in terms of running an operating system, developed by common everyday use. Their understanding of the operating system is superficial - they can use the basic features, but do not understand processes below the user interface. Due to a lack of information security and privacy knowledge, their system needs to be secured by default.

Beginners are able to install, launch, use and terminate desktop applications. They are capable of adjusting simple properties of the system and applications, like colour themes or the desktop background. The environment is accessed solely through the GUI.

Users at this level of skills are not experienced in working with the command line at all. However, some commands may be executed directly on the command line when following provided clear and simple instructions on further configuration of the environment or troubleshooting.

3.3.3 Intermediate

Skills of an intermediate user form a superset of beginner skills. They are interested in information technology and developed a deeper knowledge in specific areas needed to accomplish non-trivial tasks. Information security and privacy knowledge of an intermediate is moderate- they are aware of basic threats they might encounter.

Besides beginner system employment, intermediate users are confident with adjusting some system properties and trying new features and applications. Since they are interested in possible different experiences and want to make use of any available flexibility, they tend to explore and alter available options and settings. They are not always satisfied with defaults.

To either change the environment or solve problems, they can search for, read and understand standard documentation. Intermediate users also possess basic command-line skills. They are able to handle the filesystem using the CLI, read manual pages, execute commands with administrator privileges and even write simple scripts to automate processes.

3.4 Data-at-rest encryption

Data-at-rest is persistent data stored on a physical storage device – hard disks or external storage devices – used by the operating system and applications.

Keeping this data unencrypted exposes information of the user to be accessed in a fully readable form - either if the device is stolen or discarded without a proper data erasure. A potential adversary is thus able to gain various types of confidential data that can be commonly found on personal computers, like credit card numbers, medical reports or demographic information.

There are three main aspects determining the quality of data-at-rest encryption: the underlying encryption cipher, key strengthening and key management.

More information on these tools is provided the within the portal itself.

3.5 Password management

Passwords remain the main form of user authentication despite the inconvenient trade-off between security and usability. Since passwords are firmly rooted in many areas of information security, future usage is expected, and better care needs to be taken to support the security without usability degradation.

Regular users prefer using simple, easy-to-remember passwords to using secrets with better security guarantees. Even the simplest password-retrieving attacks, like brute-force or dictionary attacks, are effective when targeted on this group of users. Creating and remembering passwords capable of withstanding these attacks requires an additional effort, and letting this responsibility to users yields secure passwords only rarely.

More information on these tools is provided the within the portal itself.

3.6 Email communication

Electronic mail (email) is currently a standard and necessary medium in the daily life of people in most countries. An email address is a common part of contact information not only in personal areas of life, but also in business, education or government.

The long-term intensive usage of email yielded many additional features besides pure text communication. Some of these, like email attachments, introduced a lot of potential attack vectors.

Common threats of email communication include:

- eavesdropping due to lack of data-in-transit encryption,
- unauthorized data access on servers or server data leaks,
- malicious email content,
- man-in-the-middle attacks due to lack of authentication or
- modification of data in transit.

The basic practice is to encrypt data during its transport over the Internet. There are two encryption layers of electronic communication: transport-level and end-to-end encryption.

More information on these tools is provided the within the portal itself.

3.7 Firefox web browser

The last version of Firefox 100.0, was released on May 3 2022. Firefox released security bug fixes in its latest version, regarding on bypass vulnerabilities, but since 93.0 some security and privacy updates still remain, specifically concerning:

- Protection against insecure downloads:
  - Block insecure HTTP downloads on a secure HTTPS page.
  - Block downloads in sandboxed iframes, unless the iframe is explicitly annotated with the allow-downloads attribute.
- Private Browsing and Strict Tracking Protection:
  - Firefox developed a mechanism called “SmartBlock 3.0”, which compensates the issue related to the content blocking (missing images or bad performance), already provided by the previous versions, and It basically loads local, privacy-preserving alternatives to the blocked resources that behave just enough like the original ones to make sure that the website works properly.
- HTTP Referrer Protections:
- Trims the HTTP referrer for cross-site requests. In fact, the referrer not only allows a website to learn which other website the user was visiting before, but also the full URL may reveal sensitive user data included in the URL itself.

The user can benefit from these additional security mechanisms by simply installing the Firefox latest version.

More information on these tools is provided the within the portal itself.

3.8 Operating systems

We aim to recommend a stable, usable and secure open-source operating system for deploying tools recommended in previous chapters of this work. The ideal operating system shall hold an appropriate level of usability within a well-secured environment.

Essential functionality shall be available for direct use with the particular operating system. For the scope of this work, the essential functionality of a workspace running on the given operating system consists of:

- a web browser,
- an office suite,
- a media viewer,
- a document viewer,
- a software manager, and
- GUI-integrated settings of Wi-Fi, BlueTooth, sound, notifications, input devices and workspace customization.

The operating system should also provide detailed documentation, user support and have a regular release cycle.

To achieve both usability and security of the operating system, it shall come with a quality desktop environment and a minimized attack surface by application of essential system hardenings.

More information on these tools is provided the within the portal itself.

4 Introduction to the taxonomy

The goal of the proposed taxonomy of open source security and privacy tools for end-users is to support end-users in navigating through the portal of open source security and privacy tools (Deliverable D7.5, due M40) that is provided as one of the outputs of the CyberSec4Europe project. We consider the end-user view with respect to two levels of security/privacy skills and knowledge - end-users not experienced in these areas at all, who have moderate general IT skills and can install applications and undertake their basic settings according to instructions and users with moderate security/privacy skills and knowledge, who are keen to explore advanced settings of relevant tools and applications and are willing to undertake their advanced settings by given instructions. Our portal targets these two levels of end-users, and does not target security/privacy experts.

To quickly navigate through the portal, end-users need to understand the items presented in the taxonomy. Navigation is easy whenever designers use a language that users understand and when the presented items overlap with users' mental models of the domain. The portal should also provide end-users with the option to explore new tools of which they are not yet aware. Subsequently, the taxonomy should meet two requirements: covering a wide variety of available tools, including those that are newly developed or not yet widely known and adopted and overlapping with end-users' mental models of security and privacy as indicated in related work.

5 Taxonomy of open source security and privacy tools for end-users

The taxonomy design eventually encompassed the following steps:

- We first conducted an open search of open source security and privacy tools for end-users. We broadly focused on standard end-user tools such as password managers, disc encryption programs, web browsers, web browser plug-ins (e.g., cookie trackers), and anonymous browsers. Additionally, we searched for already existing portals of security and privacy tools for end-users (see section 5.1.1) to see whether we missed any tool categories.
- Based on these two steps, we created a first draft of the taxonomy.
- We then shared the first draft of the taxonomy with a handful of security and usable security professionals to obtain comments on the taxonomy's completeness and consistency. Based on these experts' feedback, we created a second draft of the taxonomy, which we then shared with the CyberSec4Europe community to obtain comments on completeness and consistency. Altogether, we received 14 comments hinting at additional taxonomy items and tools, as well as other security ontologies, which we considered as presented in the discussion in section 5.1.2.
- After being sufficiently sure that the taxonomy covers all relevant tool categories, we reviewed the literature on end-users' mental models of internet security and security and privacy-protective measures (see sections 5.1.3 and 5.1.4) to find out how to best arrange the taxonomy items.

The third and final version of the taxonomy is presented later on in this chapter.

5.1 Related work

5.1.1 Existing portals for security and privacy tools

The Electronic Frontier Foundation [3] maintains a repository of "tips, tools, and how-to's for safer online communication", available to everybody, though especially targeting security scenarios for

higher-risk groups such as activists and journalists. Within their tool section[2], EFF distinguishes between tools for different kinds of mobile (Android and iOS) and desktop operating systems (Linux, macOS, Windows). How-To instructions on this website include tools, tips, and technologies related to standard instant messaging tools (IM), secure IM tools, anonymous browsers, two-factor authentication, data deletion, secure communication, disc encryption, and end-to-end encryption. The portal provided a valuable reference point for the taxonomy design. It hinted us at a few categories that we hadn't considered that far, although it does not explicitly focus on open source tools.

5.1.2 Efforts to map security and privacy knowledge

Several standardization bodies, governmental agencies, and research projects have published cybersecurity and privacy-related taxonomies, ontologies, and other documents.

The European Union Agency for Cybersecurity (ENISA) has published an incident classification taxonomy [4], a study on online tracking and user protection mechanisms [5], and an overview of smartphone risks, opportunities, and recommendations for users [6].

The Distributed Management Task Force (DTMF) maintains a Common Information Model (CIM) that also features a Security Event Schema [7] and an IP Security Policy Schema [8].

The SELFNET project has designed a framework for self-organized network management in virtualized and software-defined networks [9]. Within this framework, they created a Security Ontology For Inter-Cloud (SOFIC) [10].

The Cyber Security Body Of Knowledge (CyBOK) is a project that brings together international experts to map the existing cybersecurity knowledge to provide a resource for educational and professional training [11]. The project's knowledge base[3] encompasses 19 knowledge areas in five categories: Human, Organisational & Regulatory Aspects, Attacks & Defences, Systems Security, Software Platform Security, and Infrastructure Security.

The described taxonomies and ontologies present an invaluable in-depth overview of the cybersecurity and privacy domain. Yet, they target an audience of experts rather than an audience of lay users.

5.1.3 Users' mental models of security and privacy

The literature distinguishes two groups of end-users [12] [13] [14]. The vast majority are those who do not have in-depth knowledge about the technology and technical processes underlying the devices, tools, and services they are using. The second (and minor) group of users is those who possess this knowledge, often through formal education or work experience in computer science, IT, engineering, and similar technology-affine professions. In the remainder of this section, we will refer to the first group of users as "lay users" and to the second group as "expert users".

Research hints at the fact that the security and privacy-related mental models of lay users differ from those of expert users [15] [13]. This difference applies as well to mental models of the Internet, with lay users having simpler and more service-oriented models [12].

Apart from that, end-users distinguish mobile and computer security in their mental models [16] [13]. In the context of mobile security, researchers even found that the mental models of iPhone users differ from those of Android users [17].

5.1.4 What tools do end-users' mental models encompass?

In general, end-users rely on both tools and protective actions, when it comes to protecting themselves from security and privacy-related threats.

[2] https://ssd.eff.org/en/module-categories/tool-guides

[3] https://www.cybok.org/knowledgebase/

Kang et al. [12] found four categories of protection measures that users deploy to protect their information when using the Internet: proactive risk management, event-based risk management, controlling digital data traces, and securing connections. All categories, except for event-based risk management, include the use of security and privacy tools including antivirus tools, data back-up, encryption, anonymous search engines, cookie trackers, browser-related settings (e.g., private browsing mode, cookie deletion), and browser indicators (HTTPS).

In the context of smartphones, Kraus et al. [18] found four categories of threats that users perceive: device loss or theft, resource drainage and service abuse, network attacks, and privacy invasion. The tool-related protective measures that the users in their study suggested to counteract these threats were password locks, firewalls, data encryption, end-to-end encryption, and permission management.

5.2 Taxonomy overview

As our taxonomy targets mainly end-users from the laypeople area, the items should be arranged in a simple and service-oriented manner (cf. Kang et al. [12]). Furthermore, the taxonomy should distinguish between mobile and computer security and related operating systems (cf. Muslukhov et al. [16], Volkamer & Renaud [13], and Benenson et al. [17]), and list the tools mentioned in the mental models of end-users (cf. Kang et al. [12] and Kraus et al. [18]).

Following users' mental models of security and privacy and protective measures (see sections 5.1.3 and 5.1.4), we arranged the taxonomy items along with two major categories: *Mobile* and *Computer*. We then split both categories into two subcategories: *Secure device and data* and *Secure usage*. The S*ecure device and data* category encompasses tools meant to protect the device. The *Secure usag*e category contains activities that end-users typically entangle during the usage of the device: *Authentication*, *Connection security*, *Internet security*, *Email security*, *App security*, *Encrypted/secure instant messaging*, and *Secure file transfer* (see Table 1 and Figure 1).

The proposed taxonomy eventually encompasses the following items:

MAIN	SUB-1	SUB-2	SUB-3
Mobile	Secure device and data	Data-at-rest encryption	Encrypted filesystem or user storage
		Antivirus	--
		Firewall	--
		Secure OS (and kernel modules)	--
		Secure data deletion	--
		Remote management	--
		Back-up management	--
		Endpoint detection and response (EDR) tools	--
	Secure usage	Authentication	Password managers
			2FA
			Lockdown
			Smart locking
		Connection security	VPN
			Host-based proxy
		Internet security	Browsers (standard, anonymous)
			Browser plug-ins / extensions
		E-Mail	Encryption/signing
			Phishing protection
		App security	Permission management
			Update management
		Encrypted/secure instant messaging	--
		Secure file transfer	--
Computer	Secure device and data	Data-at-rest encryption	Encrypted filesystem or user storage
		Antivirus	--
		Firewall	--
		Secure OS (and kernel modules)	SELinux
		Secure data deletion	--
		Remote management	--
		Back-up management	--

		Endpoint detection and response (EDR) tools	--
	Secure usage	Authentication	Password managers
			2FA
			Lockdown
			Smart locking
		Connection security	VPN
			Host-based proxy
		Internet security	Browsers
			Browser plug-ins / extensions
		E-Mail	Encryption/signing
			Phishing protection
		App security	Permission management
			Update management
		Encrypted/secure instant messaging	--
		Secure file transfer	--

Table 1: Taxonomy of open source security and privacy tools for end-users.

6 Taxonomy of Firefox web browser security and privacy features and extensions

This chapter provides a short recapitulation of the methodology and research work undertaken to build the taxonomy of *Security and privacy extensions and features of the Firefox browser* during Spring 2020.

The taxonomy was built incrementally, through a bottom-up approach. First, we collected information on all available security and privacy extensions (for the Firefox web browser) and then grouped these according to their features in functional categories.

The security and privacy extensions and features of the Firefox browser taxonomy is presented later in this chapter.

Firefox is usually described as the best browser for security and privacy (behind TOR Browser [19], which is Firefox-based). Indeed, most of the new features on these topics are implemented in Firefox and not in the other, even in Google Chrome [20], which is used by 60 % of end-users [21].

Firefox is state-of-the-art about security and privacy. Brave Browser [22], which is also open-source, is also interesting with respect to these aspects. Brave includes a private navigation mode using Onion Router Network [23] and automatically blocks ads by default [24].

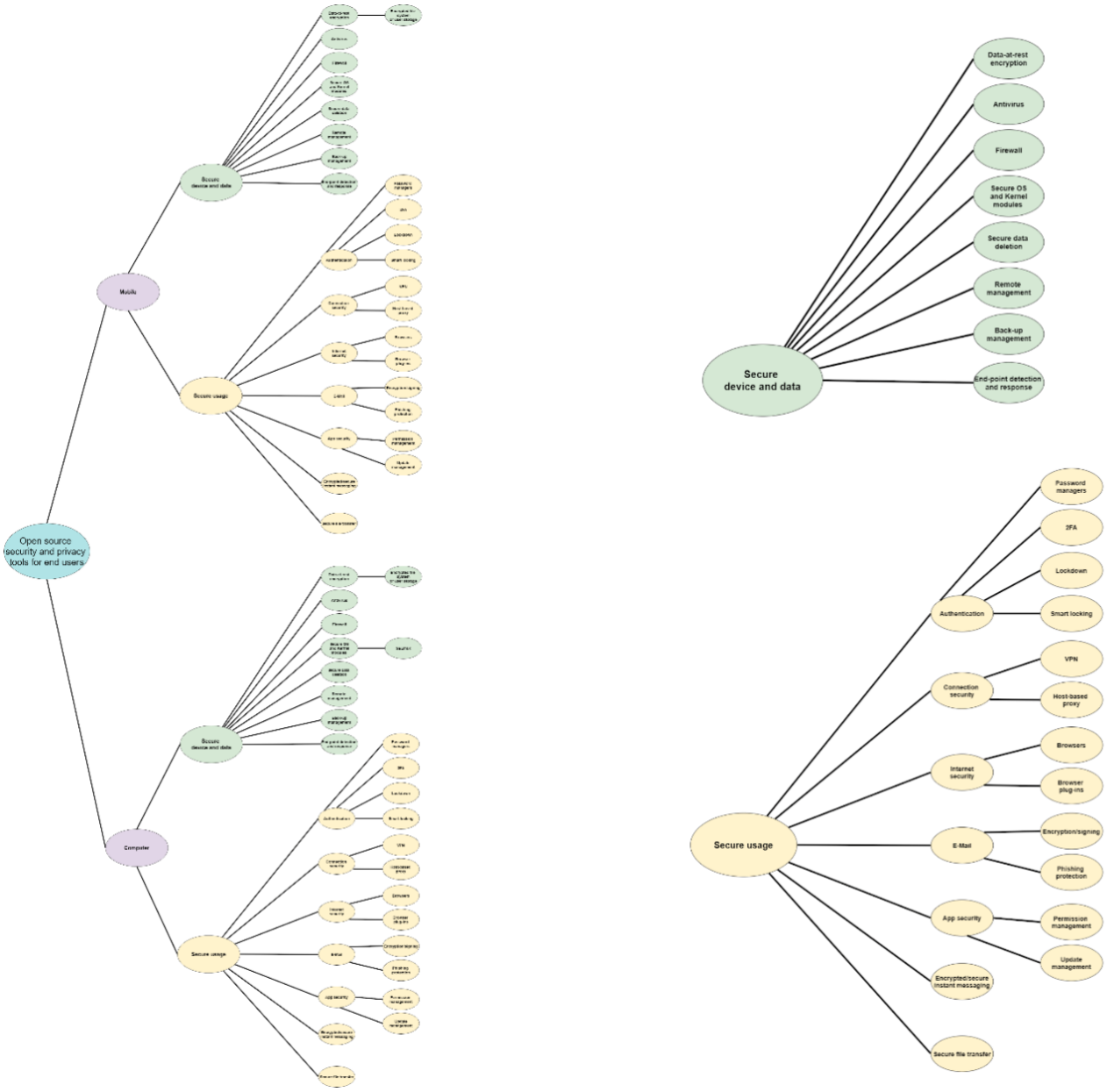


Figure 1: Full taxonomy of open source security and privacy tools for end-users (left). Magnified *Secure device and data* sub-category (right, top). Magnified *Secure usage* sub-category (right, bottom).

6.1 Related work

While researching the Firefox ecosystem and web browser taxonomies in general, we found a research article from Nikolaos Tsalis et al. [25] This article describes a taxonomy for web browsers extensions, not only for Firefox. Our taxonomy is same for browser settings and extensions. We also get the same kind of categories, yet our work concerned only on Firefox and its ecosystem, while they worked on more browsers. We reviewed numerous web articles that advise how to configure Firefox and what extensions should be used. The Mozilla Organization also explains new features for end-users in [26, 27, 28].

6.2 Development of the taxonomy

6.2.1 Collection of Firefox extensions

We collected as many extensions as possible, to get the most relevant taxonomy. We collected recommended extensions on Firefox blog posts, from articles on specialized security and privacy websites. Obviously, most of extensions in our collection come from the Firefox Add-ons Store [29].

Indeed, the Firefox Add-ons Store provides search functionality to select extensions according to some keywords (“Security” [30], “Privacy” [31]). In addition, the result of the research can be sorted, especially by “Relevance” [32, 33], or “Most Users” [34, 35]. Hence, we collected extensions from this store through these sorted lists, and according to two criterions. The extension has more than 10,000 users, or the extension is marked as “Recommended” by the Firefox Add-ons Store [36].

Then, while building the taxonomy, some categories appeared. We completed a little bit the collection of Firefox extensions by searching more extensions for some categories (for example “VPN” [37]).

For each extension, we also collected its features. It is thanks to these features that we created categories and subcategories in the taxonomy. Each extension has been reviewed to consider a category refinement. At the end of this collection of extensions for the Firefox browser, there are around 140 extensions focused on security and privacy, with all the main extensions of these domains. Some of them have functions somewhat similar, and that is why it is also useful to have this taxonomy.

6.2.2 The open-source definition problem and Firefox extensions

During the collection process, we selected some extensions that are not open-source, even though the main project is to map the landscape of open-source tools in information security. We choose this approach to create a complete taxonomy, since it is not easy to gain an assurance whether an extension is open-source or not.

The open-source problem is complex because of the Firefox extension mechanism. To install an extension, the browser downloads a .xpi file. This file is equivalent to an archive (The .xpi file [38] can be renamed as a .zip file to extract the extension structure and the different files which compose the extension). Extensions are usually JavaScript codes that are executed by the browser. While the end-user browses online, the extension is executed. JavaScript is an interpreted language. Hence, to execute the application, the browser must access some sources.

However, it does not mean the browser executes the original source code, and that the executed code is open-source. First, there is the licence problem. Sometimes, the executed source code is available in the .xpi file and is readable, but a licence claims the code is all right reserved [39, 40].

Then, some executed codes are the result of transpiling, for example, from TypeScript to JavaScript [41]. Hence, the JavaScript code is available, but it is not the source code. Finally, some JavaScript codes are obfuscated [42].

We followed the Open Source Initiative definition of open-source software [43].

6.2.3 Built-in Firefox security and privacy features

Firefox claims to be one of the best web browsers from security and privacy purposes. This is not only thanks to the multiple extensions that are available in its Firefox Add-ons Store, but also because Firefox developers implement many tools to ensure security and privacy for the user while browsing online [44].

Research about these features are hard because of the Firefox complexity and the size of the project. There are the Firefox ads and blog posts [45, 46, 47], but they are not accurate.

Most of the features we found were thanks to our experiment of the Firefox browser and the browsing experience as a common user. There is not a balance between this user information [45, 46, 47] and technical details in Bugzilla discussions [48]. In addition, Firefox design is not well explained and only

few developers know how the browser works. We would like to thank Martin Stransky, Red Hat Czech, for his help on this topic.[4]

Firefox security and privacy features are integrated at each level of the browser, from the networking to the rendering part. The security also relies, of course, on the code review, bug tracking, and all the development cycle [49, 50, 51]. Hence, there are some features which are integrated for security and privacy purposes, but which are not like an extension, because it is mostly defence in depth principles and practices.

From the taxonomy perspective, security and privacy features for the end-users can most often be also achieved by some extensions, for example, about the networking security (certificates [52], DNS-over-HTTPS [53]). It was also thanks to this analysis we realize Firefox extensions can be a way for the user to take control on its browser settings [54, 55], because they are too hard to configure ("about:config" [56] hidden settings is a good example of this obscurity).

6.2.4 Taxonomy structure

Some extensions can be found in more than one category, because they provide more than one feature. Categories and subcategories are described by the combinations of a name and a brief description. The taxonomy is available in two forms. The first one is a textual description, with multi-layers. The second one is a graph of bubbles (subcategories) connected to their categories by an edge.

We sorted categories and subcategories in the textual taxonomy by relevance and importance for the end-user. Some categories are more important than others to achieve end-user security or privacy, but the trade-off between both characteristics is hard, and even harder when usability or performance should be considered.

6.3 Taxonomy of security and privacy extensions and features of the Firefox web browser

The taxonomy consists of 7 categories, which are divided into subcategories. These categories are sorted according to the impact on end-user security. The category "Other" groups all extensions and subcategories that do not fit in any other categories.

The "Tracking/Privacy Protection" category is the most extensive since there are a lot of ways to identify the user, and to track her behaviour.

The taxonomy is made thanks to some extensions that are open-source, and some others that are not. All the categories and subcategories have at least one open-source solution or extension, except for the "Temporary Virtual Cards and Secure Payments" subcategory.

The taxonomy is outlined in the form of a basic table below, its graphical depiction follows and the same taxonomy with some additional comments w.r.t. categories is provided in Annex A.

[4] Martin Stransky is a developer of the Firefox browser. He works on the compatibility between Firefox browser and Wayland. He helps us to understand how Firefox components interact and the overall architecture of the project.

MAIN	SUB-1	SUB-2
Connection Security	Firefox Networks Features	
	VPN/Proxies	
	DNS over HTTPS	
	HTTP to HTTPS	
	New TLS Version Enforcer	
Content and Scripts Blockers	Ads Blockers	
	Scripts and Malwares Blockers	
	Cookies and Local Data Storage Blockers	
	Secure Downloads	
	Websites Blockers	
	Ads Blockers Protectors	
	Security Suite (NoScript only)	
	WebRTC Blockers	
Cleaners	History Cleaners	
	Cookies Cleaners	
	Cache Cleaners	
Browser Settings Controllers	Cookies Cache History Proxy Managers	
	Browser Updates	
	Session Lockers and Guest Sessions	
	Easy Security and Privacy Settings Managers	
Authentication and Reputation	Passwords Managers	
	Reputation and Blacklists for Rogue Websites	
	Temporary Virtual Cards and Secure Payments	
	Third-Party Authentication Systems	
Tracking/Privacy Protection	Privacy-based Search Engines	
	Easy Privacy Settings Managers	
	Cookies and Local Data Storage Blockers	
	Tracking Parameters Link Cleaners	
	Containers/Sandboxes	
	Cookies Cache History Cleaners	
	Location	Location Spoofers
		Location Blockers
	Fingerprints	Fingerprinting Spoofers
		Fingerprinting Blockers
	Header Tracking Parameters	Header Tracking Parameters Spoofers
		Header Tracking Parameters Blockers
		Header Do Not Track (DNT) Flag
	Local CDNs	
	Random Email Generators	
	Cookies Cache History Managers	
	WebRTC Blockers	
	Policy Privacy (GDPR) Decoders	
Others	PGP Mails Encryption	
	TOR Solutions	

Table 2: Firefox browser security and privacy functions, extensions.

The taxonomy of security and privacy extensions and features of the Firefox web browser is provided in a graphical depiction on the following page and the same taxonomy with some additional comments w.r.t. categories comes in Annex A.

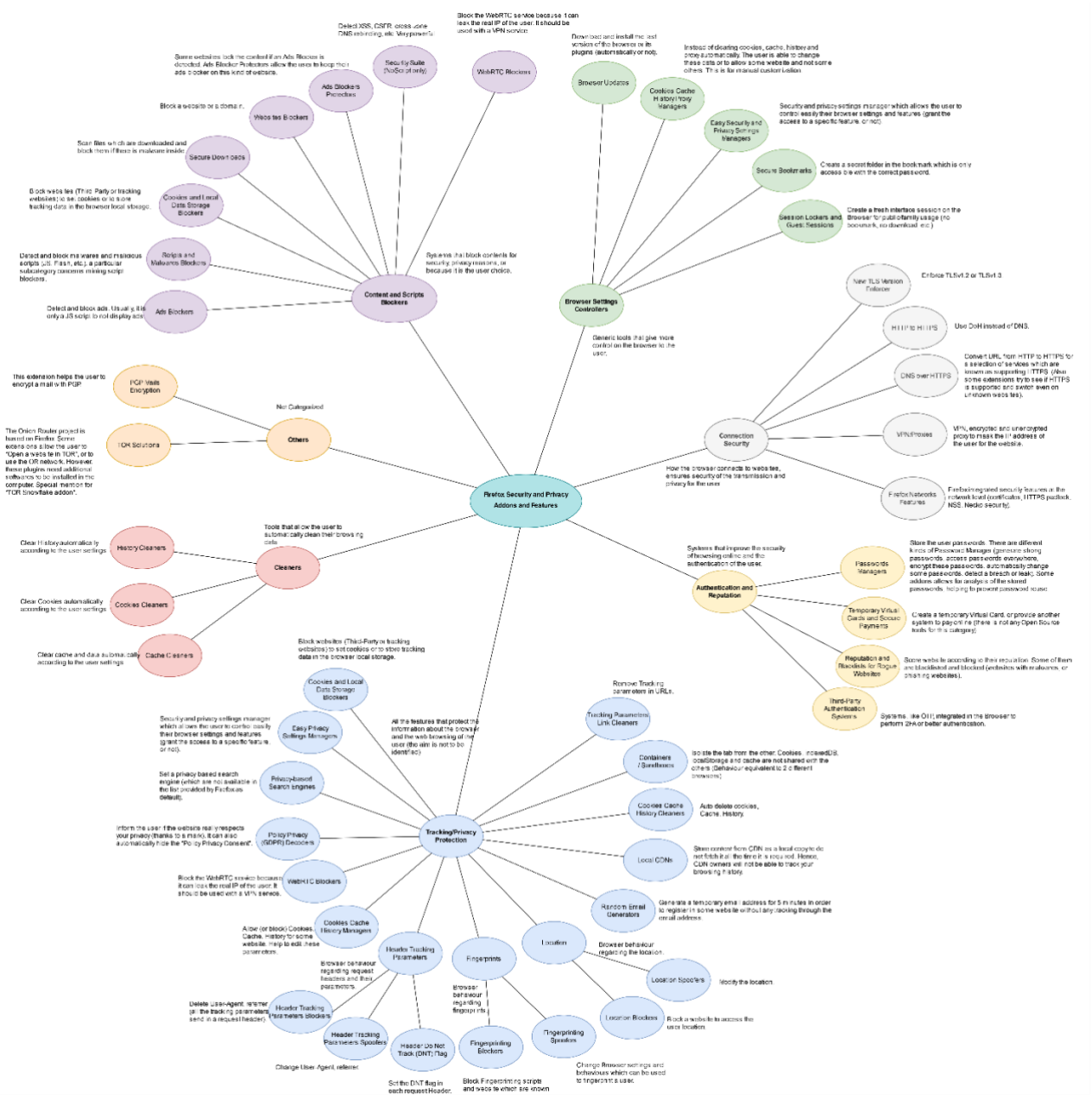


Figure 2: Graph with the full taxonomy of Firefox browser security and privacy functions, extensions.

7 Conclusions and future work

This document provided some accompanying information to the deliverable D7.5 of the CyberSec4Europe project – Open tool portal.

We shall carry on updating the portal during the remainder of the project work.

8 References

[1] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 1990.

[2] D. A. Norman, The psychology of everyday things, Basic books, 1988.

[3] Electronic Frontier Foundation (EFF), "Surveillance Self-Defense Tips, Tools and How-tos for Safer Online Communications," [Online]. Available: https://ssd.eff.org/. [Accessed 19 June 2020].

[4] European Union Agency for Network and Information Security (ENISA), "Reference Incident Classification Taxonomy - Task Force Status and Way Forward," 2018. [Online]. Available: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy. [Accessed 18 May 2020].

[5] European Union Agency for Network and Information Security (ENISA), "Online Tracking and User Protection Mechanisms - A study on the technical implementation of user consent and Do Not Track (DNT)," 2017. [Online]. Available: https://www.enisa.europa.eu/publications/online-tracking-and-user-protection-mechanisms. [Accessed 18 May 2020].

[6] G. Hogben and M. Dekker, "Smartphones: Information security risks, opportunities and recommendations for users," European Network and Information Security Agency, 2010.

[7] Distributed Management Task Force (DTMF), "CIM Schema: Version 2.53.0., Security Event Version 2.48.0.," 2020. [Online]. Available: https://www.dmtf.org/sites/default/files/cim/cim_schema_v2530/Visio-CIM_SecurityEvents.pdf. [Accessed 19 June 2020].

[8] Distributed Management Task Force (DMTF), "CIM Schema: Version 2.53.0., IPSecPolicy Overview CIM 2.48.0.," 2020. [Online]. Available: https://www.dmtf.org/sites/default/files/cim/cim_schema_v2530/Visio-CIM_IPsecPolicy.pdf. [Accessed 19 June 2020].

[9] "The SELFNET Project," 2020. [Online]. Available: https://selfnet-5g.eu/. [Accessed 19 June 2020].

[10] The SELFNET Project, "SOFIC (Security Ontology For Inter-Cloud)," [Online]. Available: http://selfnet.inf.um.es/sofic/. [Accessed 19 June 2020].

[11] "CyBOK – The Cyber Security Body of Knowledge," [Online]. Available: https://www.cybok.org/. [Accessed 19 June 2020].

[12] R. Kang, L. Dabbish, N. Fruchter and S. Kiesler, ""My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015.

[13] M. Volkamer and K. Renaud, "Mental models–general introduction and review of their application to human-centred security," in *Number Theory and Cryptography*, Berlin, Heidelberg, 2013.

[14] S. M. Furnell, P. Bryant and A. D. Phippen, "Assessing the security perceptions of personal Internet users," *Computers & Security*, vol. 26, no. 5, pp. 410-417, 2007.

[15] F. Asgharpour, D. Liu and L. J. Camp, "Mental models of security risks," in *International Conference on Financial Cryptography and Data Security*, Berlin, Heidelberg, 2007.

[16] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester and K. Beznosov, "Understanding users' requirements for data protection in smartphones," in *IEEE 28th International Conference on Data Engineering Workshops*, 2012.

[17] Z. Benenson, F. Gassmann and L. Reinfelder, "Android and iOS users' differences concerning security and privacy," in *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, 2013.

[18] L. Kraus, T. Fiebig, V. Miruchna, S. Möller and A. Shabtai, "Analyzing end-users' knowledge and feelings surrounding smartphone security and privacy," in *Mobile Security Technologies (MoST), IEEE S&P Workshops.*, 2015.

[19] "TOR Project," [Online]. Available: https://www.torproject.org/. [Accessed 25 June 2020].

[20] "Google Chrome," [Online]. Available: https://www.google.com/intl/en-us/chrome/. [Accessed 25 June 2020].

[21] "Browser & Platform Market Share May 2020," w3Counter, [Online]. Available: https://www.w3counter.com/globalstats.php?year=2020&month=5. [Accessed 25 June 2020].

[22] "Brave browser," [Online]. Available: https://brave.com/. [Accessed 25 June 2020].

[23] "What is a Private Window with Tor?," [Online]. Available: https://support.brave.com/hc/en-us/articles/360018121491-What-is-a-Private-Window-with-Tor-. [Accessed 25 June 2020].

[24] "Accurately Predicting Ad Blocker Savings," [Online]. Available: https://brave.com/accurately-predicting-ad-blocker-savings/. [Accessed 25 June 2020].

[25] M. A. G. D. Tsalis N., "An Intensive Analysis of Security and Privacy Browser Add-Ons," in *Lambrinoudakis C., Gabillon A. (eds) Risks and Security of Internet and Systems. CRiSIS 2015. Lecture Notes in Computer Science, vol 9572. Springer, Cham*, 2016.

[26] "Make your Firefox browser a privacy superpower with these extensions," 9 August 2018. [Online]. Available: https://blog.mozilla.org/firefox/make-your-firefox-browser-a-privacy-superpower-with-these-extensions/. [Accessed 2020 June 25].

[27] "Encryption and tools to protect against global mass surveillance," [Online]. Available: https://www.privacytools.io/browsers/. [Accessed 25 June 2020].

[28] "5 Firefox extensions to protect your privacy," 9 July 2018. [Online]. Available: https://opensource.com/article/18/7/firefox-extensions-protect-privacy. [Accessed 2020 June 2020].

[29] "Firefox Add-ons Store," [Online]. Available: https://addons.mozilla.org/en-US/firefox/. [Accessed 25 June 2020].

[30] "Search for : Security," [Online]. Available: https://addons.mozilla.org/en-US/firefox/search/?q=security. [Accessed 25 June 2020].

[31] "Search for : Privacy," [Online]. Available: https://addons.mozilla.org/en-US/firefox/search/?q=Privacy. [Accessed 25 June 2020].

[32] "Search for : "Security", sorted by relevance," [Online]. Available: https://addons.mozilla.org/en-US/firefox/search/?q=Security&sort=relevance. [Accessed 25 June 2020].

[33] "Search for : "Privacy", sorted by relevance," [Online]. Available: https://addons.mozilla.org/en-US/firefox/search/?q=Privacy&sort=relevance. [Accessed 25 June 2020].

[34] "Search for : "Security", sorted by number of users," [Online]. Available: https://addons.mozilla.org/en-US/firefox/search/?q=Security&sort=users. [Accessed 25 June 2020].

[35] "Search for : "Privacy", sorted by number of users," [Online]. Available: https://addons.mozilla.org/en-US/firefox/search/?q=Privacy&sort=users. [Accessed 25 June 2020].

[36] "Recommended Extensions program—where to find the safest, highest quality extensions for Firefox," 3 September 2019. [Online]. Available: https://blog.mozilla.org/firefox/firefox-recommended-extensions/,. [Accessed 25 June 2020].

[37] "Search for : VPN," [Online]. Available: https://addons.mozilla.org/en-US/firefox/search/?q=VPN. [Accessed 25 June 2020].

[38] "XPI File Explanation," 23 March 2019. [Online]. Available: https://developer.mozilla.org/en-US/docs/Mozilla/XPI. [Accessed 25 June 2020].

[39] "PureVPN: VPN Proxy to Unblock Internet Privately, PureVPN," [Online]. Available: https://addons.mozilla.org/en-US/firefox/addon/purevpn-for-privacy-security/?src=search. [Accessed 25 June 2020].

[40] "Custom License for Malwarebytes Browser Guard, Malwarebytes Browser Guard Extension," [Online]. Available: https://addons.mozilla.org/en-US/firefox/addon/malwarebytes/license/?src=search. [Accessed 25 June 2020].

[41] "Github Repository of Bitwarden," [Online]. Available: https://github.com/bitwarden/browser. [Accessed 25 June 2020].

[42] "NordVPN – The #1 VPN Proxy Extension for Firefox, NordVPN," [Online]. Available: https://addons.mozilla.org/fr/firefox/addon/nordvpn-proxy-extension/. [Accessed 25 June 2020].

[43] "Open Source Definition," [Online]. Available: https://opensource.org/osd. [Accessed 25 June 2020].

[44] "Firefox protects your privacy in every product," [Online]. Available: https://www.mozilla.org/en-US/firefox/privacy/products/. [Accessed 25 June 2020].

[45] "Firefox Lockwise, Take your passwords everywhere," [Online]. Available: https://www.mozilla.org/en-US/firefox/lockwise/. [Accessed 25 June 2020].

[46] "Support for Firefox Monitor," [Online]. Available: https://support.mozilla.org/en-US/kb/firefox-monitor. [Accessed 25 June 2020].

[47] "Support for Enhanced Tracking Protection," [Online]. Available: https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop. [Accessed 25 June 2020].

[48] "Bug 1320222 Review FxA client-side key stretching parameters," 24 November 2016. [Online]. Available: https://bugzilla.mozilla.org/show_bug.cgi?id=1320222. [Accessed 25 June 2020].

[49] "Code Review FAQ," 23 March 2019. [Online]. Available: https://developer.mozilla.org/en-US/docs/Mozilla/Developer_guide/Code_Review_FAQ. [Accessed 25 June 2020].

[50] "Code Review," 24 July 2013. [Online]. Available: https://wiki.mozilla.org/Code_Review. [Accessed 25 June 2020].

[51] "Firefox/Code Review," 14 September 2017. [Online]. Available: https://wiki.mozilla.org/Firefox/Code_Review. [Accessed 25 June 2020].

[52] "How do I tell if my connection to a website is secure?," [Online]. Available: https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure. [Accessed 25 June 2020].

[53] "Firefox DNS-over-HTTPS," [Online]. Available: https://support.mozilla.org/en-US/kb/firefox-dns-over-https. [Accessed 25 June 2020].

[54] "FoxyProxy Standard Extension," [Online]. Available: https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/?src=search. [Accessed 25 June 2020].

[55] "Privacy Settings, by Jeremy Schomery," [Online]. Available: https://addons.mozilla.org/en-US/firefox/addon/privacy-settings/?src=search. [Accessed 25 June 2020].

[56] "Configuration Editor for Firefox," [Online]. Available: https://support.mozilla.org/en-US/kb/about-config-editor-firefox. [Accessed 25 June 2020].

Annex A: Taxonomy of security and privacy extensions and features of the Firefox web browser with notes

I. **Connection Security:** How the browser connects to websites, ensures security of the transmission and privacy for the user.
   1. **Firefox Networks Features**: Firefox integrated security features at the network level (certificates, HTTPS padlock, NSS, Necko security).
   2. **VPN/Proxies**: VPN, encrypted and unencrypted proxy to mask the IP address of the user for the website.
   3. **DNS over HTTPS**: Use DoH instead of DNS.
   4. **HTTP to HTTPS**: Convert URL from HTTP to HTTPS for a selection of services which are known as supporting HTTPS. (Also, some extensions try to see if HTTPS is supported and switch even on unknown websites).
   5. **New TLS Version Enforcer**: Enforce TLSv1.2 or TLSv1.3.

II. **Content and Scripts Blockers:** Systems that block contents for security, privacy reasons, or because it is the user choice.
   1. **Ads Blockers**: Detect and block ads. Usually, it is only a JS script to not display ads.
   2. **Scripts and Malwares Blockers**: Detect and block malwares and malicious scripts (JS, Flash, etc.), a particular subcategory concerns mining script blockers.
   3. **Cookies and Local Data Storage Blockers**: Block websites (Third-Party or tracking websites) to set cookies or to store tracking data in the browser local storage.
   4. **Secure Downloads**: Scan files which are downloaded and block them if there is malware inside.
   5. **Websites Blockers**: Block a website or a domain.
   6. **Ads Blockers Protectors**: Some websites lock the content if an Ads Blocker is detected. Ads Blocker Protectors allow the user to keep their ads blocker on this kind of website.
   7. **Security Suite (NoScript only)**: Detect XSS, CSFR, cross-zone DNS rebinding, etc. Very powerful.
   8. **WebRTC Blockers**: Block the WebRTC service because it can leak the real IP of the user. It should be used with a VPN service.

III. **Cleaners:** Tools that allow the user to automatically clean their browsing data.
   1. **History Cleaners**: Clear History automatically according to the user settings.
   2. **Cookies Cleaners**: Clear Cookies automatically according to the user settings.
   3. **Cache Cleaners**: Clear cache and data automatically according to the user settings.

IV. **Browser Settings Controllers:** Generic tools that give more control on the browser to the user.
   1. **Cookies Cache History Proxy Managers**: Instead of clearing cookies, cache, history and proxy automatically. The user is able to change these data or to allow some website and not some others. This is for manual customization.
   2. **Browser Updates**: Download and install the last version of the browser or its plugins (automatically or not).
   3. **Session Lockers and Guest Sessions**: Create a fresh interface session on the Browser for public/family usage (no bookmark, no download, etc.).
   4. **Secure Bookmarks**: Create a secret folder in the bookmark which is only accessible with the correct password.

5. **Easy Security and Privacy Settings Managers:** Security and privacy settings manager which allows the user to control easily their browser settings and features (grant the access to a specific feature, or not).

V. **Authentication and Reputation:** Systems that improve the security of browsing online and the authentication of the user.
   1. **Passwords Managers**: Store the user passwords. There are different kinds of Password Manager (generate strong passwords, access passwords everywhere, encrypt these passwords, automatically change some passwords, detect a breach or leak). Some addons allows for analysis of the stored passwords, helping to prevent password reuse.
   2. **Reputation and Blacklists for Rogue Websites**: Score website according to their reputation. Some of them are blacklisted and blocked (websites with malwares, or phishing websites).
   3. **Temporary Virtual Cards and Secure Payments**: Create a temporary Virtual Card, or provide another system to pay online (there is not any Open Source tools for this category).
   4. **Third-Party Authentication Systems**: Systems, like OTP, integrated in the Browser to perform 2FA or better authentication.

VI. **Tracking/Privacy Protection:** All the features that protect the information about the browser and the web browsing of the user (the aim is not to be identified).
   1. **Privacy-based Search Engines**: Set a privacy-based search engine (which is not available in the list provided by Firefox as default).
   2. **Easy Privacy Settings Managers:** Security and privacy settings manager which allows the user to control easily their browser settings and features (grant the access to a specific feature, or not).
   3. **Cookies and Local Data Storage Blockers**: Block websites (Third-Party or tracking websites) to set cookies or to store tracking data in the browser local storage.
   4. **Tracking Parameters Link Cleaners**: Remove Tracking parameters in URLs.
   5. **Containers/Sandboxes**: Isolate the tab from the other. Cookies, indexedDB, localStorage and cache are not shared with the others (Behaviour equivalent to 2 different browsers).
   6. **Cookies Cache History Cleaners**: Auto delete cookies, Cache, History.
   7. **Location**: Browser behaviour regarding the location.
      a. **Location Spoofers**: Modify the location.
      b. **Location Blockers**: Block a website to access the user location.
   8. **Fingerprints**: Browser behaviour regarding fingerprints.
      a. **Fingerprinting Spoofers**: Change Browser settings and behaviours which can be used to fingerprint a user.
      b. **Fingerprinting Blockers**: Block Fingerprinting scripts and website which are known as provider for these scripts.
   9. **Header Tracking Parameters**: Browser behaviour regarding request headers and their parameters.
      a. **Header Tracking Parameters Spoofers**: Change User-Agent, referrer.
      b. **Header Tracking Parameters Blockers**: Delete User-Agent, referrer (all the tracking parameters send in a request header).
      c. **Header Do Not Track (DNT) Flag**: Set the DNT flag in each request Header.
   10. **Local CDNs**: Store content from CDN as a local copy to do not fetch it all the time it is required. Hence, CDN owners will not be able to track your browsing history.
   11. **Random Email Generators**: Generate a temporary email address for 5 minutes in order to register in some website without any tracking through the email address.

12. **Cookies Cache History Managers**: Allow (or block) Cookies, Cache, History for some website. Help to edit these parameters.
13. **WebRTC Blockers**: Block the WebRTC service because it can leak the real IP of the user. It should be used with a VPN service.
14. **Policy Privacy (GDPR) Decoders**: Inform the user if the website really respects your privacy (thanks to a mark). It can also automatically hide the "Policy Privacy Consent".

VII. Others: Not Categorized.

1. **PGP Mails Encryption**: This extension helps the user to encrypt a mail with PGP.
2. **TOR Solutions**: The Onion Router project is based on Firefox. Some extensions allow the user to "Open a website in TOR", or to use the OR network. However, these plugins need additional softwares to be installed in the computer. Special mention for "TOR Snowflake addon".