SWEPT

Securing Websites through malware dEtection and attack Prevention Technologies

Deliverable title

User requirements

Deliverable ID:

D1.1

Preparation date:

16th June 2014

Milestone: Final Revised

Editor/Lead beneficiary (name/partner):

Carlos Bracero/Arsys

Internally reviewed by (name/partner):

Bachar Wehbi/Montimage

Abstract:

The main goal of this deliverable is to define in detail the requirements and functionalities of the SWEPT security solutions that will be offered to the different types of users as a result of the SWEPT project. This description will allow the project members to obtain a common understanding of the project framework from the earliest stage, and have a clear idea about the platform architecture and the services that will be validated within it. Moreover, a matching between the user requirements and the implementation will ensure the future system and satisfaction of the user.

In order to reach a pack of solutions that fits the user expectations, SWEPT members will work with the philosophy that the product/service developed must suit the user, rather than making the user suit the product/service.

Therefore, this document will serve as a common starting point in order to establish the foundations of the project, taking into account from the very beginning of the project that the final solution must fulfil diverse group of users’ requirements and expectations.

Project co-funded by the European Commission within the ICT Policy Support Programme

Dissemination level

PU	Public	X
CO	Confidential, only for members of the consortium and the Commission Services	

SWEPT project is funded by the European Community's Competitiveness and Innovation Framework Programme (CIP/2007-2013) under grant agreement n° 621056

SWEPT consortium

Fundación Tecnalia Research & Innovation (TECNALIA, Spain) www.tecnalia.com/en	**Project manager:** Erkuden Rios erkuden.rios@tecnalia.com +34 664 100 348
EUROHELP Consulting SL (EUROHELP, Spain) www.eurohelp.es	Contact: Aritz Rabadan arabadan@euro-help.es
Montimage EURL (MONTIMAGE, France) www.montimage.com	Contact: Edgardo Montes de Oca edgardo.montesdeoca@montimage.com
Everis Aerospacial y defensa SL (EAD, Spain) http://www.everis.com	Contact: Maria Pilar Torres Bruna maria.pilar.torres.bruna@everis.com
IVARX LIMTED (CYBERDEFCON, UK) https://cyberdefcon.com/	Contact: Jart Armin jart@cyberdefcon.com
Emaze networks SPA (EMAZE, Italy) www.emaze.net	Contact: Davide Varesano davide.varesano@emaze.net
S21Sec Information security labs SL (S21SEC, Spain) www.s21sec.com/	Contact: Irene Eguinoa ieguinoa@s21sec.com
AMIS druzba za telekomunikacije D.O.O. (AMIS, Slovenia) www.amis.net	Contact: Arton Lipaj arton.lipaj@amis.net
CSIS security group AS (CSIS, Denmark) www.csis.dk/en/	Contact: Rasmus Larsen rln@csis.dk
ARSYS Internet S.L. (ARSYS, Spain) www.arsys.es/	Contact: Carlos Bracero cbracero@arsys.es
ARIMA software design S.L.L (ARIMA, Spain) www.arima.eu	**Technical manager**: Roberto Velasco roberto@arima.eu

Table of contents

SWEPT consortium iii
Table of contents v
List of figures vii
List of tables vii
Executive summary 1
1 Introduction 3
1.1 SWEPT motivation and background 3
1.2 Structure of this document 3
1.3 Relationships with other deliverables 3
1.4 Contributors 4
1.5 Acronyms and abbreviations 4
1.6 Revision history 4
1.7 Statement of originality 4
1.8 Change log 5
2 User requirements objective 7
3 Working methodology 9
4 End users of SWEPT platform 11
5 Questionnaire and major conclusions of the analysis 15
6 SWEPT platform requirements 17
7 Conclusion 26
References 27
Appendix A. User requirements gathering questionnaire 29

List of figures

Figure 1: SWEPT concept ... 3
Figure 2: Relation of end users and stakeholders with the SWEPT concept ... 12

List of tables

Table 1: Explanation of Requirements Repository ... 17
Table 2: SWEPT platform requirements ... 20

Executive summary

The main goal of this deliverable is to define in detail the requirements and functionalities of the SWEPT security solutions that will be offered to the different types of users as a result of the SWEPT project. This description will allow the project members to obtain a common understanding of the project framework from the earliest stage, and have a clear idea about the platform architecture and the services that will be validated within it. Moreover, a matching between the user requirements and the implementation will ensure the future system and satisfaction of the user.

Therefore, this document will serve as a common starting point in order to establish the foundations of the project, taking into account from the very beginning of the project that the final solution must fulfil diverse group of users’ requirements and expectations.

This deliverable complements the D1.3 Technical specification of the set of SWEPT services, which explains the SWEPT platform architecture and services. These will be designed taking into account the result of the requirements gathering phase.

The document explains the different SWEPT stakeholders and analyses the requirements of each group over the SWEPT platform. The deliverable includes a description of the methodology used for the requirements gathering. Finally, the document provides the whole set of requirements extracted in this early stage of the project and which will drive the design and development of the platform in the future phases.

1 Introduction

1.1 SWEPT motivation and background

The main goal is to develop a new multifaceted approach to mitigate malicious attacks on websites by maximizing the security posture of websites with a minimum of intervention needed by website owners and administrators. In addition, the project aims to define a de facto standard and good practice for securing websites.

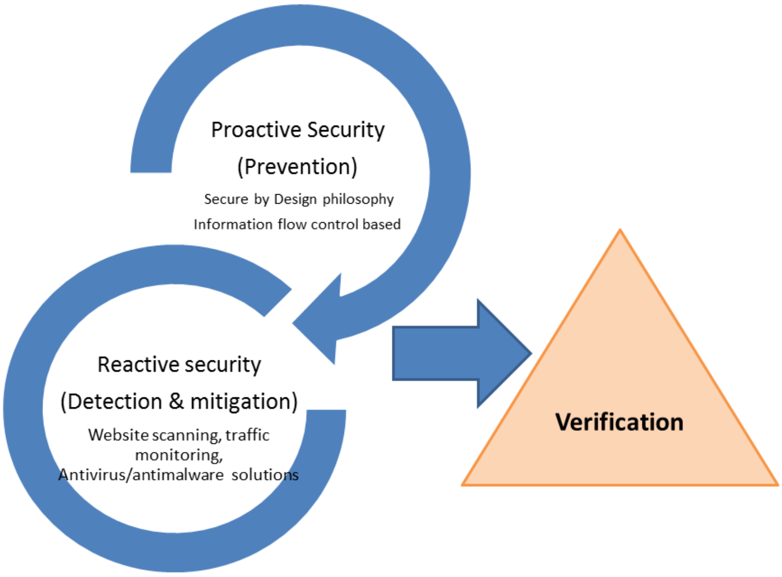
Proactive Security
(Prevention)
Secure by Design philosophy
Information flow control based
Reactive security
(Detection & mitigation)
Website scanning, traffic monitoring,
Antivirus/antimalware solutions
Verification

Figure 1: SWEPT concept

The proposed SWEPT security solution will incorporate prevention and detection security mechanisms and tools for automatically preventing and mitigating web site attacks. The project also proposes a certification model that will certificate the security level of a web application based on SWEPT security mechanisms.

1.2 Structure of this document

This document is structured as follows. After this introductory section, in Section 2 we describe the objectives of the user requirements gathering process. Section 3 explains the approach methodology followed for the requirements gathering and analysis. Section 4 describes the different SWEPT stakeholders that we have identified for the project and their intended use of the platform, and Section 5 describes the questionnaire used in the requirements gathering process and the major conclusions of their analysis. The Section 6 describes the set of user requirements obtained for the SWEPT platform. Finally, Section 7 provides major conclusion remarks. The document includes in Appendix A the Questionnaire used to elicit the requirements from the different stakeholders.

1.3 Relationships with other deliverables

The D1.1 User requirements presented in this document relates to the following deliverables:

- D1.3 Technical specification of the set of SWEPT services, which describes the SWEPT platform architecture and services. These will be designed taking into account the results of the requirements gathering phase.

1.4 Contributors

The following partners have contributed to this deliverable:

- TECNALIA
- EUROHELP
- MONTIMAGE
- EAD
- CYBERDEFCON
- EMAZE NETWORKS
- S21SEC LAB
- AMIS
- CSIS
- ARSYS
- ARIMA

1.5 Acronyms and abbreviations

API	Application Programming Interface
CMS	Content Management System
CSRF	Cross-Site Request Forgery
DNS	Domain Name System
DoW	Description of Work
HTML	Hyper Text Markup Language
IDS	Intrusion detection system
IPS	Intrusion prevention system
ISP	Internet Service Provider
PHP	Personal Home Page
SIEM	System Information Event Management
SSL	Secure Sockets Layer
UML	Unified Modelling Language
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAF	Web Application Firewall

1.6 Revision history

Version	Date issued	Author	Organisation	Description
V0.1	30/03/2014	Arton Lipaj	AMIS	TOC Proposed
V1.0	28/04/2014	Carlos Bracero	ARSYS	Intermediate Proposed
V1.1	28/05/2014	Carlos Bracero	ARSYS	Intermediate Revised
V1.4	09/06/2014	Carlos Bracero	ARSYS	Final Proposed
V2.0	16/06/2014	Carlos Bracero	ARSYS	Final Revised

1.7 Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

1.8 Change log

No change log entries.

2 User requirements objective

Currently, website security is one of the main concerns in the cybersecurity field. All web applications have some kind of vulnerability, a fact that cyber criminals exploit to carry out their malicious activities.

This is not an easy threat to fight as the foundational software currently used to develop and create web applications (such as web frameworks and content management systems (CMSs)) within the most commonly-used platforms (Java EE, .NET, PHP) are not equipped with adequate or easy-to-implement security mechanisms. The result is that the development of a secure web application depends, to a great extent, on the developer. For this reason, the majority of developed applications are not secure by design and have to be secured afterwards via custom, complex and error-prone security measures that depend on each business domain. In addition, the web security solutions offered by traditional cybersecurity providers (such as application firewalls or intrusion detection systems) are usually made completely ineffective by complex solution implantation issues and hardware overheads which are prone to generating delayed response times.

In all cases, a great deal of effort and investment from website owners and administrators is required (e.g. security audits, continuous software, license or component updates, etc.). This is feasible for organizations with the necessary resources, but presents a difficult problem to cope with for individual website owners and administrators, or small organizations with limited resources.

In order to overcome the current situation, SWEPT project will provide a software platform comprised of the integration of a set of already-available tools and technologies provided by the project partners. Some of these tools are proprietary and others are based on open source developments. These components will be extended and adapted and afterwards integrated onto the SWEPT platform which will offer website security purposes (protection, detection, mitigation) either as a whole, individually, or as a combination of tool features.

With the aim of clarifying which are the main user requirements the future platform should fulfil, the project has undertaken the initial requirements gathering process. The collected requirements come from a number of sources: the contractual description of work (DoW), the needs of the tools to be integrated in the platform, particular requirements of the end-users in the case studies of the project, and partner inputs that build from their expertise in the security, with the aim of ensuring the exploitation of the future platform.

This collection of requirements will allow the project members to obtain a common understanding of the project framework from the project beginning and will drive the architecture and the services offered by the platform. Moreover, a matching between the user requirements and the implementation will ensure the future system and satisfaction of the user.

In order to reach a pack of effective solutions that fits the user expectations, SWEPT members have worked with the philosophy that the product/service developed must suit the user, rather than making the user suit the product/service.

Therefore, this document will serve as a common starting point in order to establish the foundations of the project, taking into account from the very beginning of the project that the final solution must fulfil different group of users´ requirements and expectations.

3 Working methodology

The work methodology chosen for the creation of the collection of user requirements has the objective to guide the project by continuous validation of what we are building in the SWEPT platform.

The methodology includes the following sequential processes:

1. **gathering** user needs and expectations on the SWEPT platform functionalities,
2. **analysing** the collected information,
3. **defining and refining** the set of requirements into clear functional and non-functional statements which fulfilment can be tracked.

For the **gathering phase**, the requirements originated from the following sources:

- Answers of end-users to direct questions prepared in the project to learn about their needs,
- Requirements extracted from the DoW,
- Particular requirements of the tools to be integrated in the SWEPT platform,
- Particular requirements of the 4 case studies in the project,
- Stock taking of security reports on website risks,
- Partner ideas coming from their previous experiences in security and web application protection,
- Partner ideas for ensuring that the future product is exploitable.

The collection of the end-users needs and expectations was performed through the following steps:

1. Identifying the types and profiles of intended SWEPT end-users as described in Section 4,
2. Mapping between the end-user profiles and SWEPT partners expertise, and assigning to SWEPT partners the responsibility for collecting the views and needs of particular end-user profiles.
3. Creation of a dedicated questionnaire to gather end-user current problems and needs. The questionnaire is explained in Section 5 and the template for the questionnaire is provided in Appendix A.
4. Distribution of the questionnaire to different stakeholders covering the defined end-users profiles. A total number of 22 end-users of different profiles answered the questionnaire.

The **analysis phase** included the rationalisation of collected information from the different sources, particularly the answers received in the questionnaires on the existing security solutions in the companies and the identified issues that could be solved by SWEPT platform.

The major conclusions of the analysis are described in Section 5.

For the **defining and refining phase**, the analysed information was transformed into the definition of requirements which have undergone a refinement process involving WP leaders and the technical manager.

With all the requirements obtained, we have created a dedicated requirements repository which will allow detailed tracking of requirements' fulfilment throughout the project life. The explanation of the repository and the complete list of requirements are provided in Section 6.

4 End users of SWEPT platform

The end users targeted by the SWEPT platform are, in some way or another, all the stakeholders and actors of the web applications value chain. All of them are targeted by the project as the project addresses the particular needs of each of them:

- **Website administrators and website owners**: The owners need to keep their websites secure and protected from threats and attacks. At the same time, website administrators need effective means to achieve this protection. SWEPT makes available for website administrators and owners an innovative set of measures for the protection of websites to be applied at the web application level. When applied in this comprehension way, these measures, based on the security by design concept, will raise website security to known levels with the minimum of administration and maintenance effort.
- **Web hosting service providers**: These stakeholders provide web hosting services to all manner of clients but especially to website owners with small resources. The types of services are varied: web hosting, cloud hosting, hosting services for resellers, managed hosting, etc. They need to offer the best possible service to their clients (website owners and administrators), and this implies providing a secure service. Therefore, keeping the hosted websites as safe as possible from attacks and free from malware that could damage their reputation is one of the added values of their service. The same set of security measures offered to the website administrators and website owners (to be applied at the web application level), will be offered to these stakeholders but additionally the SWEPT project will offer additional measures to be applied externally to the web application level (proxy web level and web server level).
- **ISPs (Internet service providers)**: ISPs play an important role in the internet value chain in terms of limiting and mitigating the impact of website attacks and website infections. They are intermediate stakeholders between the users and the website hosting providers (or the website owners and administrators), and the traffic related to the use of the websites goes through them and they can provide an intermediate interception point for website security. The SWEPT project will provide a set of security measures for this type of stakeholder.
- **Cybersecurity service providers**: They provide security services and products on demand. They need security guidelines and regulations to improve the services offered to clients. They are interested also in security standards and security regulations that could be implemented by their products, and therefore SWEPT solutions will provide them with the means to achieve higher security levels for their customers.
- **Software development providers (particularly website and web application developers)**: They develop web applications for business and they need to assure the security of developed web applications. They will be able to apply SWEPT outcomes at the design and development phase.
- **Foundational software providers (such as web frameworks and CMSs)** whose software frameworks are used to create web applications. They are interested in offering to their users a secure by default foundational software that is integrated with solutions offered by the cybersecurity industry.
- **Any internet end user**, who is interested in avoiding the consequences of malware and therefore interested in minimizing the risk of infection. SWEPT will offer a range of security measures that check that the websites they visit are secure. Additionally, the project proposes a new security certification based on the SWEPT security measures that will be useful for internet end users to identify secure web sites.

- **Governments:** they are the responsible of cybersecurity policies and regulations. They need understandable and measurable security best practices and standards to raise awareness, and create and enforce effective and long-term regulations.

In summary, the way the different services and tools are envisaged to be used by the different stakeholders is the following:

- **Website administrators and website owners**: They will be able to download and install in their websites the security measures proposed at the web application level.
- **Web hosting service providers**: They will be able to download and apply in their systems (websites, web servers, web proxies) the complete set of security measures proposed by SWEPT.
- **Internet service providers**: They will be able to download and apply to their systems (web servers and web proxies principally) the set of security measures proposed by SWEPT to be applied externally to the web application level.
- **Cybersecurity service providers**: They will be able to make use of part of the SWEPT tools and measures to complement their own security tools.
- **Software development providers**: Thanks to the integration point provided by SWEPT to foundational software providers and the security industry, this type of user will be able to create secure web applications more efficiently, avoiding the complexity and high costs of current approaches based on hand-coded and proprietary security measures.
- **Foundational software providers** will be able to integrate the security measures proposed by SWEPT with solutions available in the security industry in order to offer more particular software for creating web applications.
- **Any internet end user** will be able to access the SWEPT platform and make use of and download several tools that check the security levels of websites (scanners, plugins for web browsers etc.).
- **Governments**: they will be able to use the security standards developed in SWEPT project as a foundation for future security regulations.

The next figure illustrates the relation between the most important potential end users of SWEPT project:

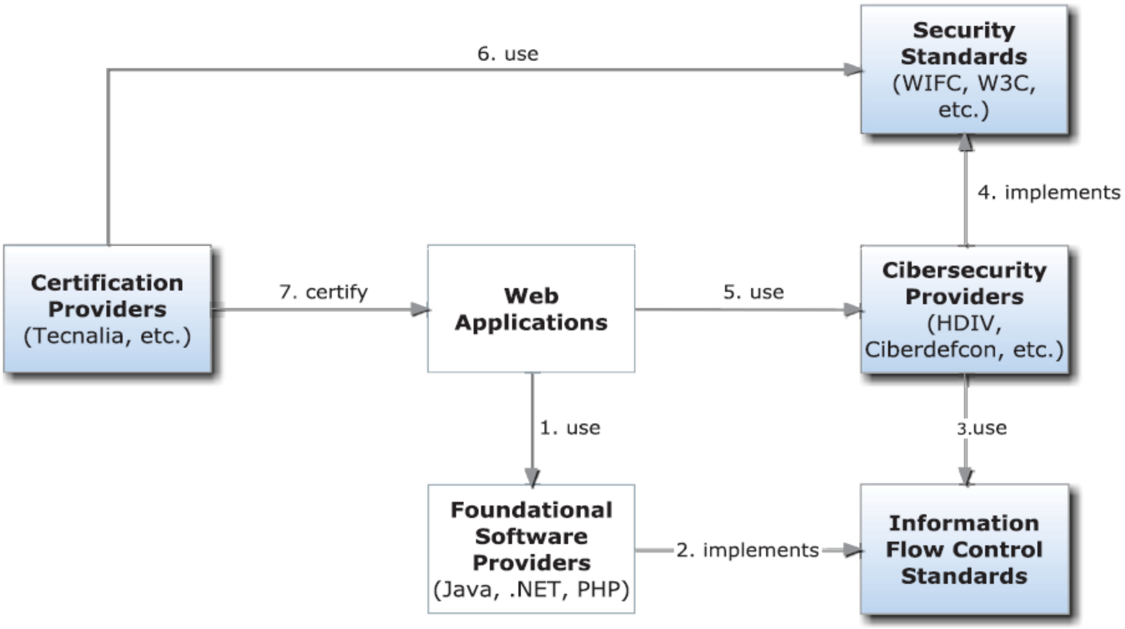
Security Standards (WIFC, W3C, etc.)
6. use
4. implements
Certification Providers (Tecnalia, etc.)
7. certify
Web Applications
5. use
Cibersecurity Providers (HDIV, Ciberdefcon, etc.)
1. use
3.use
Foundational Software Providers (Java, .NET, PHP)
2. implements
Information Flow Control Standards

Figure 2: Relation of end users and stakeholders with the SWEPT concept

As it can be seen in Figure 2, the different stakeholders do interact with the SWEPT platform in diverse ways:

1. Web developers use foundational software because it is hard to implement web applications from scratch.
2. Foundational software providers implement or accomplish the requirements defined at information flow control standards, who define how to access to the data exchange between the client and the server.
3. Using the integration point offered by information flow control standards, cybersecurity providers implement security requirements.
4. Security requirements are defined in Security Standards.
5. Web applications use the solutions offered by cybersecurity providers (as libraries) in order cover security standards automatically.
6. Certification providers use the security standards as input to configure their tools and define their methodologies.
7. Certification providers certify that the web applications comply with defined security standards. In order to increase user confidence, it is essential that high reputation third parties provide the certification service. In order to increase user confidence, it is essential that high reputation third parties provide the certification service.

5 Questionnaire and major conclusions of the analysis

With the aim of gathering the problems and needs from the different stakeholders with respect to website protection, we developed both a document and an on-line questionnaire. See in Appendix A the complete questionnaire or found it in this link: https://www.surveymonkey.com/s/7N95Z8Q.

The on-line version of the questionnaire was developed with the aim of making it available to a wider public in the future, in order to follow the gathering of the visions and needs of SWEPT community, and their intended participation in our workshops.

The questionnaires sent to the end-users, have been divided into five sections with different questions:

1. Contact user information
    - 1.1. General contact info.
    - 1.2. Which is the privacy policy the user wants for the information provided in the questionnaire.
    - 1.3. Whether the user is interested to participate in the SWEPT workshop to be organized in 2016.
2. Profile information
    - 2.1. With what type of websites are you dealing during your daily duties?
    - 2.2. Which website technologies do the websites you deal with use?
    - 2.3. Please, indicate your relationship with websites
    - 2.4. Please, indicate your relationship with website security tools and measures
    - 2.5. Please indicate which profile you think best suits you
3. Current status of website security
    - 3.1. Safeguards
    - 3.2. Top current security incidents
    - 3.3. Top current vulnerabilities
    - 3.4. State of the art shortcomings
        - 3.4.1. What threats do you think are not properly addressed by the state of the art security solutions?
        - 3.4.2. How do you think it is possible to solve these shortcomings?
4. Requirements for the SWEPT platform
    - 4.1. What aspects should be covered by a comprehensive and effective solution for website protection?
5. Additional comments or suggestions

Each section allowed us to gather valuable information, both for the current status of security problems in the organisation and for the possible help SWEPT platform can bring to solve them. The questions intended to characterise the respondent according to each profile, and learn about the main challenges faced by that end user.

As explained before, each partner was responsible for distributing the questionnaire among its customers and partners in order to learn about the needs and problems of the different target profiles.

After a thorough **analysis** of the 22 received questionnaires, and discussions with some of the stakeholders for clarifications on their answers, we identified the relevant expectations and needs expressed repeatedly by different stakeholders.

The key results of this information gathering process are the following:

- The vast majority of respondents navigate all kinds of web pages, but basically often blogs, e-commerce, social networking sites and search engines, monopolize 75% of the total.
- Regarding the languages used in the websites visited/developed, they include PHP, HTML5 and JAVA, with 80% of the total, and if we consider .NET, this percentage exceeds 90%.
- Concerning safeguards used, the degree of awareness that exists in security is very high. 95% of respondents have firewalls installed, 86% use some antivirus, 86% use SSL/VPN, 60% have antimalware, 59% use WAF, 59% use antispam/antimalware, and only 40% of them use complex protection system as IDS or IPS systems and SIEM.
- As for security incidents, the collected answers highlighted especially those related to unavailability of service, identity spoofing, loss of information, phishing and fraud.
- In connection with the vulnerabilities, user answers mainly referred to problems with: OWASP-A1- Injection, OWASP - A3 - Cross Site Scripting, OWASP - A9- Using components with known vulnerabilities, OWASP - A10 - Unvalidated redirect and forwards, OWASP - A5- Security misconfiguration and OWASP- A2- Broken authentication and session management.
- Users consider very important to them the following measures:
  - The detection tools include vulnerability detection mechanisms.
  - The detection and prevention tools are integrated.
  - Mechanisms are provided to support the preventive analysis to be performed during the early stages of the website design.
  - A certification system or model is established to allow easy understanding of the protection level of websites.

These key points were combined with the other requirements gathered from different sources (DoW, partners previous experiences, stock taking of security reports, etc.) and were transformed into definitions of SWEPT platform requirements stored in the repository for their tracking (see below).

6 SWEPT platform requirements

The SWEPT platform requirements were defined through the analysis of inputs from the following sources:

- Surveyed end-users on their needs through the use of the questionnaire explained in Section 5.
- Requirements extracted from the DoW,
- Particular requirements of the background tools by the SWEPT partners to be integrated in the SWEPT platform,
- Particular requirements of the 4 case studies in the project,
- Stock taking of security reports on website risks, e.g. [2], [3] and [4].
- Partner inputs based on their experience in security and web application protection,
- Partner inputs for ensuring that future SWEPT platform is exploitable.

All these inputs were analysed by the technical manager and the WP leaders by summarizing the objectives of the ideas, categorizing them with respect to functional and non-functional aspects, comparing them to identify relationships, duplicates and gaps, and prioritizing them in the timeframe of the project. Then, the analysis finalizes with identifying the target phase and WP within the project that should be made responsible for the fulfilment of the requirement, together with the identification of the best indicators or means for verification of the requirement fulfilment.

As a result of the previous analysis, we obtained a set of **74 requirements** which give us the actual overview of the needs of potential stakeholders over the SWEPT solution.

This list of requirements serves as a starting point for the development of the SWEPT platform and the services provided through it. The fulfilment of the requirements will be mastered by the technical manager and the different work package leaders.

We will follow an iterative approach to make updates to the requirements repository in order to improve the requirements and to track their progress. The updates will reflect needs of reprioritization, additions due to progress in platform technology development, as well as needs and expectations from the industry. This way, we will always have a detailed control of the situation of the fulfilment of each requirement, from the early development until the end of the pilot tests.

In this repository, the requirements are defined though the following major attributes:

Table 1: Explanation of Requirements Repository

Field/column name	Explanation	Format
ReqID	The ID of the requirement.	Unique ID. Has to be manually inserted
Title	The title should be short and give a simple idea about what the requirement is about.	Free text
Description	A brief but understandable description of the requirement. It should be unambiguous and testable	Free text
Type	It identifies whether this is a functional requirement, or non-functional requirement (efficiency, maintainability, reliability and usability).	Drop-down list

Source	It identifies the origin of the requirement identification.	Free text, typical value: questionnaire answered by X
Target WP	It indicates which WP must work to achieve the requirement, and the WP leader will be responsible for its fulfilment.	Drop-down list
Target phase	It indicates in which phase of SWEPT project is possible to verify the requirement is achieved or not.	Drop-down list
Related to	It indicates which other requirement/s (partly) address similar needs.	Free text to indicate the related ReqID/ReqIDs.
Priority	It indicates how important the requirement is in order the SWEPT project can achieve its objectives. The possible values are: 1 (more important) to 3 (less important)	Drop-down list

In addition to the attributes shown above, we have included in the master description of the requirements information relating to:

- *Author:* It indicates which SWEPT partner suggested/identified the requirement.
- *Verification method*: In this field we will indicate which method or mechanism will be used to check if a requirement is met. The options are:
    - Inspection/review – A solution is textually described in a deliverable (e.g. an algorithm) that a person is able to evaluate.
    - Runtime testing – The fulfilment will be verified through testing/demo of running software.
    - Formal proof – A formal method of verification is applied.
    - User feedback – End-users provide their evaluation/opinion on the fulfilment of the requirement.
- *How addressed*: This field is related to the previous one, and provides a free-text explanation on how the requirements have been fulfilled.
- *Target*: This field indicates which part (document, component, etc.) is the one that shall fulfil the requirement.
- *Fulfilment status*: This attribute will indicate whether the requirement was achieved or not in the current phase of the project. The field can take the following values:
    - Not achieved phase 1 - (M1-M24),
    - Achieved phase 1 - (M1-M24),
    - Not achieved phase 2 - (M25-M36),
    - Achieved phase 2 - (M25-M36),
    - Rejected,
    - Obsolete,
    - Redundant,
    - Deferred post-SWEPT.
- *Changelog/comments:* Free text with comments or explanations to the changes that occur in the requirements description.

In the table below, we provide an extract of the requirements repository, including all the requirements, but major attributes (fields) only.

Table 2: SWEPT platform requirements

ReqID	Title	Description	Type	Source	Target WP	Target phase	Related to	Priority
1	Support for PHP	SWEPT prevention mechanisms should be useful for PHP websites.	Functionality	DoW	2	1		1
2	Not intrusive prevention	SWEPT prevention mechanisms should be the less intrusive as possible.	Functionality	DoW	2	1		1
3	Dynamic website scanning	SWEPT detection should serve for blogs or dynamic websites.	Functionality	DoW	3	1		2
4	HTTP response speed	HTTP response times will be less than 3 seconds	Efficiency	ARSYS	3	1		1
5	Service independency	The SWEPT services must be independent so that if one fails it does not affect the rest.- Fault tolerance	Reliability	ARSYS	5	1	73	1
6	Available documentation	Documentation must be kept current and available at all times.	Maintainability	ARSYS	5	1		3
7	Multi-language	SWEPT platform must be able to be configured in different languages easily	Usability	ARSYS	5	1		3
8	Easily installable	SWEPT platform should be easily installable in both Windows and Linux environments	Usability	ARSYS	5	1		1
9	Easily configurable	SWEPT platform should be easily configurable in both Windows and Linux environments	Usability	ARSYS	5	1		1
10	Commercial exploitation	Solutions and tools that make up the SWEPT solution must be commercially exploitable, separately or together.	Usability	DoW	5	1		1
11	User groups to cover	The different security mechanisms, tools and service incorporated to the SWEPT platform will be marketed to a wide variety of clients over many delivery channels	Usability	DoW	5	1		1
12	Automatic and manual detection	The SWEPT platform should include both automatic and manual detections tools/mechanisms	Functionality	DoW	2	1		1
13	External and internal scans	SWEPT platform should provide tools that allows for external and internal scans	Functionality	DoW	2	1		1

14	Certification Model	SWEPT certification Model to measure the security level of websites. Independent of the business domain, verifiable automatically by using tools and Integrated with existing foundational software and web environments	Functionality	DoW	4	1		1
15	Flexible and cost effective solution	It will be a flexible and cost effective solution, addressing the needs of the different end users.	Usability	DoW	2	1		1
16	Integrated with the ACDC	SWEPT platform shall be integrated with the ACDC clearing house, so that the information gathered by ACDC platform related to the latest detected threats is incorporated to SWEPT system and used for the protection, detection and mitigation purposes.	Functionality	DoW	3	1		1
17	Verification tool for websites	To provide a verification tool for websites based on the technologies underlying in SWEPT project.	Functionality	DoW	4	1	14	1
18	Control the user’s actions	Control the user’s actions in the websites in order to avoid the exploitation of web security risks	Functionality	DoW	3	1		1
19	Support different foundational software	SWEPT must support different foundational software such as PHP, JAVA, .NET	Functionality	DoW	2	1		1
20	Definition updates	The definition updates of malware, viruses, etc., should be performed at a minimum once a day, ideally once every hour.	Reliability	ARSYS	3	1		1
21	Common web attacks shall be detected.	Common web risks in OWASP Top 10 shall be covered by SWEPT detection.	Functionality	ARIMA	2	1		2
22	Network traffic analysis:	Tools should be learning algorithms Tools for identification and statistical analysis of network flows and the detection of unexpected behaviour and security flaws.	Functionality	DoW	3	1		1
23	Reputation analysis:	SWEPT should be able to control the blacklisting and report to the owner	Functionality	DoW	4	1		1
24	Binary file analysis:	The tool should have a system that allows scanning binary files, such as antivirus or anti-malware tools.	Functionality	DoW	3	1		3
25	Alert system	Web site owners and administrator must be aware of the risk detected at their web. Must have a configurable alert system (SMS, email,…)	Functionality	DoW	3	1		2
26	Vulnerability fixes	The solution should provide solutions to any identified vulnerabilities.	Functionality	DoW	2	1		3

27	Network & port scanning	the tool will allow to detect servers or machine within a network and scan different ports	Functionality	DoW	3	1		1
28	Outdated software detection	SWEPT should provide a tool to detect outdated software.	Functionality	DoW	3	1		2
29	Guide recommendations.	A guide that recommends for every type of site, the set of technologies that should be used to protect it.	Maintainability	DoW	4	1		3
30	Access to the reactive security tools	A central server connected to the decentralized servers of the different technology and product providers in order to execute and correlate the results of each tool	Usability	DoW	5	1		1
31	False positives	A protection system with low false positives is needed.	Reliability	Questionnaire by ACK STORM SL	3	1		1
32	Low impact	Should have low impact on protected services/servers. Low resource consumption on the computers installed (memory, cpu ..)	Functionality	ARSYS	5	1		1
33	Independent from services	Must be independent of services without dependencies of system libraries, if there was an error on swetp protection the rest of the services must be running	Functionality	ARSYS	5	1		1
34	easily detachable	Should be easyly to set on or off to a server/service	Usability	ARSYS	5	1		1
35	Powerful reporting tool	Powerful report tool from low level reports (web page) to high level server/platform detail. Granularity. Easily configurable, multiple formats export possibility, (XML, CSV, TXT, …)	Functionality	ARSYS	5	1		1
36	Remotely configurable	Should be remotely configurable	Usability	ARSYS	5	1		2
37	API required	You must have an API that allows to control tools and platform services	Functionality	ARSYS	5	1		2
38	Small network impact	Must have a small impact on the network	Functionality	ARSYS	5	1		1
39	IPv6 ready	IPv6 ready	Functionality	ARSYS	4	1		2
40	Backup compatible	Must be compatible with the backup systems	Usability	ARSYS	5	1		3

41	Users/Roles	Must have different roles for different users (admin, operator, reports, read-only, etc)	Functionality	ARSYS	4	1		2
42	Modularity	Choice of packages to deploy	Functionality	ARSYS	5	1	9	1
43	Console	Centralized console to manage deployment, operation, configuration, reports…from the server side	Usability	ARSYS	5	1		2
44	Cloud	Must be able to be used in cloud environments	Functionality	ARSYS	5	1		1
45	Access from any device	The users will be able to access the services globally, from any device with an internet connection	Usability	DoW	5	1		1
46	Scanning techniques	Website scanning techniques will be used to detect and clean infections	Functionality	DoW	3	1		1
47	Monitoring techniques	Network and business activity monitoring techniques will be used to prevent the transmission of infections	Functionality	DoW	3	1		1
48	Change management	SWEPT should have a system to report on possible file changes to a website	Functionality	ARSYS	5	1		2
49	Control Panel	SWEPT should have a single dashboard where final users can control all functions and reports, as well as showing a series of activity indicators	Usability	ARSYS	5	1		1
50	Predict threats in analysis phase	SWEPT to be able to predict threats to an application during its analysis phase.	Functionality	Question naire by EVERIS	4	1		2
51	Processing rules for each type of business	Must provide information processing rules, so that it can adapt to the logic of each type of business.	Functionality	Question naire by EVERIS	4	1		2
52	Protect from attacks from social networks, IRC…	should be able to protect from attacks from social networks, IRC, blogs, …	Functionality	Question naire by Zink Security	3	1	3	1
53	Protect against DoS attacks	Should be able to detect and protect against DoS attacks	Functionality	Question naire by ARSYS	3	1		1
54	Authentication mechanisms	Must support different authentication methods	Functionality	Question naire by ARSYS	4	1		2

55	Scanning for wireless and wired network	Should provide tools to perform network scans of all kinds (wireless and wired) for threats or suspicious equipment	Functionality	Questionnaire by ARSYS	3	1	13	2
56	Unification of tools on different OS	The different tools that make SWEPT should operate similarly in different Operating Systems	Usability	Questionnaire by ARSYS	5	1		2
57	Heuristic analysis	Must have some advanced Heuristic analysis system, capable of detecting unknown threats at the moment of the analysis.	Functionality	Questionnaire by EVERIS	3	1		1
58	Global coordination	Improve global coordination and security research with economic media and global laws regarding information security	Functionality	Questionnaire by EVERIS	5	1	16	1
59	Standardized solution of communication between tools	Standardized security solutions, able to communicate among each other, instead of multiple proprietary protocol and technology, hard to interoperate	Functionality	Questionnaire by EVERIS	5	1		1
60	Vulnerability Analysis	A tool that has a holistic view of our environment, be able to perform vulnerability analysis and based on that can give a view of what kind of attack we are vulnerable	Functionality	Questionnaire by COOP	4	1		1
61	Artificial intelligence in log monitoring	Artificial intelligence in log monitoring that can see all attacks and miss-happenings, something that parses this as well as humans, and sees connections and patterns.	Functionality	Questionnaire by COOP	4	1		1
62	Detect and fix vulnerabilities in CMS	Must be able to detect and fix vulnerabilities in CMS	Functionality	Questionnaire by SWITCH	3	1		1
63	Strength of FTP passwords	Must be able to analyze the strength of passwords of FTP, in order to avoid or easily guessable passwords accessible by brute force.	Functionality	Questionnaire by SWITCH	4	1		3
64	Self awareness	Must be able to assess the own SWEPT platform or use the existing information to identify vulnerabilities in the SWEPT platform.	Functionality	S21SEC	5	1		1
65	Environment integration	Must be able to integrate with analysed scenarios (e.g. connect the active directory or LDAP) to fulfil reporting information such as users, timeshifts etc.	Functionality	S21SEC	5	1		2
66	Detect rogue clients	Must detect and deny access from untrusted devices	Functionality	S21SEC	5	1		1

67	HTTP security	Must be able to identify threats, weakness and vulnerabilities in the HTTP protocol and server application.	Functionality	S21SEC	2	1		1
68	Ciphered communications	Must support ciphered and secure (e.g. SSL) communications between platform components and client devices	Reliability	S21SEC	5	1		1
69	Detection of malicious URLs	Must be able to detect malicious URLs injected on the analyzed website	Functionality	S21SEC	3	1		1
70	Heartbleed bug solution	The platform should provide a solution to Open SSL Heartbleed bug, easily deployable by SMEs.	Functionality	Project Officer	2	2		1
71	Validation of WIFC	SWEPT verification tool automates validation of WIFC	Functionality	DoW	4	2	17	1
72	Web risks repository	SWEPT verification tool will contain a repository of most common web risks	Functionality	DoW	4	2	17	1
73	Scalable architecture	Unforeseen issues within one module will not affect the work of other modules	Maintainability	DoW	1	2	5	1
74	Modular design	SWEPT architecture shall be modular	Maintainability	DoW	1	2		1

7 Conclusion

This deliverable describes the objectives and methodology for end-users requirements gathering in SWEPT project and provides the initial collection of the user requirements over the SWEPT platform. The user requirements gathered in this early phase of the project will be stored and tracked through a live repository that will evolve throughout the project and will be kept aligned with the design and the implementation activities in the other technical tasks.

By having an early set of requirements in the initial project months, and by involving all partners in the WP1 End user needs, platform requirements and design, we have set the foundations for a common understanding of the project members and a single project-wide vision on what the SWEPT platform should look like and offer.

The main idea is to pursue an effective solution that fits the user expectations, rather than making the users suit the final product/service.

References

[1] SWEPT EU CIP project, Securing Websites through malware dEtection and attack Prevention Technologies.2014-2017. Available at: http://www.swept.eu/ (Retrieved June 2014)

[2] OWASP Top 10–2013–The Ten Most Critical Web Application Security Risks. The Open Web Application Security Project, 2013. Available at: http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf

[3] Symantec internet security threat report 2014. White Paper, Symantec Corporation, 2014, vol. 19. Available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[4] 2014 Data breach investigations report. Verizon, 2014. Available at: http://www.verizonenterprise.com/DBIR/2014/

Appendix A. User requirements gathering questionnaire

Securing Websites through malware dEtection and attack Prevention Technologies

SWEPT User requirements gathering questionnaire

SWEPT project is funded by the European Community's Competitiveness and Innovation Framework Programme (CIP/2007-2013) under grant agreement n° 621056

1. Introduction

This questionnaire is part of a requirements collection process for **SWEPT: Securing Websites through malware dEtection and attack Prevention Technologies**, a project under the financial support of the European Union's ICT Policy Support Programme within the Competitiveness and Innovation Framework Programme (CIP) (www.swept.eu). The project's main objective is to develop a new multifaceted approach to mitigating malicious attacks on websites by maximizing their security posture with a minimum of intervention required from website owners and administrators.

The SWEPT consortium - particularly all those organisations involved in gathering, processing and analysing end-user needs - fully understand the sensitive nature of the subject and will not include any information arising during an inquiry, being it a questionnaire or an interview, that is not suitable for the public domain.

Please note that we would like you to answer the questions with as many details as you are able to share and that we fully accept that certain information might be confidential. You should indicate in the first question whether you wish to share the information in this questionnaire only with the SWEPT person that contacted you, only with the whole SWEPT consortium, or publicly but always keeping the source of information anonymous.

At the same time, all interviewees' personal details will remain anonymous and 'firewalled'.

Data and information obtained from the filled questionnaires will be exploited only for the project purposes (defined in description of work / Grant Agreement) and within the project duration.

2. User information

2.1 Personal data of person answering the questionnaire:

Please fill with your data:

Name

Organization

Position

- Do you want your data be kept private by the SWEPT person that contacted you? (Choose one option)

  □ Yes

  □ No, I do not mind sharing it with the SWEPT consortium.

  □ No, I do not mind sharing it publicly, but always keep the source of information anonymous.

- Would you like to participate in a SWEPT workshop with stakeholders for the presentation of the project results and the SWEPT solution, to take place in 2016? (Choose one option)

  □ Yes

  □ No

2.2 Profile information:

Please mark the answers to the questions below.

1. With what type of websites are you dealing during your daily duties? (Multiple choices are allowed)

□ social networks

□ blogs

□ newspapers and other communication media

□ retail

□ e-commerce portals

□ search engines

□ Other

2. Which website technology do the websites you deal with use? (Multiple choices are allowed)

□ PHP

□ Java

□ HTML5

□ Other

3. Please, indicate your relationship with websites. (Multiple choices are allowed)

□ User

□ Administrator

□ Service provider

□ Security officer

□ Infrastructure / hardware provider

□ Other

4. Please, indicate your relationship with website security tools and measures. (Multiple choices are allowed)

□ Novel user

□ Senior user

□ Junior security researcher

□ Senior security researcher

□ Junior security officer

□ Senior security officer

□ Security infrastructure/hardware provider

□ Other

5. Please indicate which profile you think best suits you: (Choose one option)

□ Website administrators and website owners.

□ Webhosting service providers.

□ Internet service providers.

□ Cyber-security services' providers.

□ Software development providers.

□ Foundational software providers.

□ Internet end-user.

□ Governments or public authorities.

3. Current status of website security

3.1 Safeguards

- What kind of security safeguards are you using to protect your websites or IT systems?

Safeguard	Are you using?	Name of the tool used
Network Firewall	Yes/No	
Application Firewall (WAF)	Yes/No	
IDS (intrusion detection system)	Yes/No	
IPS (intrusion prevention system)	Yes/No	
Antivirus	Yes/No	
AntiMalware	Yes/No	
AntiSpam	Yes/No	
Digital certificates	Yes/No	
SSL	Yes/No	
VPN	Yes/No	
SIEM	Yes/No	
Custom solutions	Yes/No	
Others	Yes/No	

3.2 Top current security incidents

- Did you have any of the following incident types in your IT systems in the last 2 years? And which safeguards did you apply to prevent or tackle with them?

Incident Type	How many times?	Safeguards installed
Service unavailable	0	e.g. Network firewall
Espionage	0	
Fraud		
Information Theft		
Loss of information		

Spoofing identity		
Others		

3.3 Top current vulnerabilities

- How many times has any of the following OWASP top ten vulnerabilities been exploited (Column 1) and/or detected (Column 2) in your IT systems?
- Which detection tools did you apply to learn if the vulnerability existed? (Answer in Column 3).
- Which prevention tools did you apply to avoid the vulnerability been exploited? (Answer in Column 4).

Vulnerability	**Exploited**	**Detected**	**Detection tools used**	**Prevention tools used**
OWASP-A1- Injection				
OWASP- A2- Broken authentication and session management				
OWASP - A3 - Cross Site Scripting				
OWASP - A4 - Insecure object reference				
OWASP - A5- Security misconfiguration				
OWASP - A6 - Sensitive data exposure				
OWASP - A7 - Missing Function Level access control				
OWASP - A8- CSRF				
OWASP - A9- Using components with known vulnerabilities				
OWASP - A10 - Unvalidated redirect and forwards				

3.4 State of the art shortcomings

- What threats do you think are not properly addressed by the state of the art security solutions? (Please explain).

- How do you think it is possible to solve these shortcomings?

4. Requirements for the SWEPT platform

- What aspects should be covered by a comprehensive and effective solution for website protection?

Please rate them (give them a score from 1 to 4) with regard to their importance (4 for the most important aspect).

Website security aspect	**Priority (1 less to 4 most)**
Tools to prevent security incidents at website design phase	
Detection tools to detect security vulnerabilities	
Integration of prevention and detection mechanisms	
Certification model to measure the security level of websites	

5. Additional comments or suggestions

- Please write here any comments or suggestions you want to add to your answers.