Application Software Extended Package for Web Browsers

Version: 2.0
2015-06-16
National Information Assurance Partnership

Revision History

Version	Date	Comment
v 1.0	2014-03-31	Release - Protection Profile for Web Browsers
v 2.0	2015-06-16	Update as Extended Package of the Protection Profile for Application Software
v 2.0	2015-06-16	Application Software Extended Package for Web Browsers
v 1.0	2014-03-31	Initial release - Protection Profile for Web Browsers

Contents

1 Overview

Web browsers are client applications that retrieve and render content provided by web servers, primarily using the hypertext transfer protocol (HTTP) or HTTP Secure (HTTPS). Browsers have grown in complexity over the years, starting as tools used to display simple, unchanging web pages and becoming sophisticated execution environments for web content. The use of browsers to administer accounts, servers or embedded systems remotely requires them to handle sensitive information securely. Innovations such as tabs, extensions and HTML5 have not only increased browser functionality, but also introduced new security concerns. Being the principal method for accessing the Internet, and due to their complexity and the information that they process, browsers are a natural target for attackers. As a result, it is paramount that the security of web browsers be improved to reduce the risk to client machines and enterprise networks. This Extended Package (EP) along with the Protection Profile for Application Software () provide a baseline set of Security Functional Requirements (SFRs) for web browsers running on any operating system regardless of the composition of the underlying platform. The requirements are intended to improve the security of browsers by encouraging the use of operating system security services and requiring the use of sandboxing technologies and environmental mitigations provided by the underlying platform. Additionally, these requirements define security functionality that browsers must provide.The terms web browser, browser, and TOE are interchangeable in this document.

2 Terms

The following sections list Common Criteria and technology terms used in this document. The following sections provide both Common Criteria and technology terms used in this Extended Package. CC Common Criteria for Information Technology Security Evaluation. EP An implementation-independent set of security requirements for a category of products, which extends those in a Protection Profile. PP An implementation-independent set of security requirements for a category of products. ST A set of implementation-dependent security requirements for a specific product. TOE The product under evaluation. In this case, a web browser and its supporting documentation. TSF The security functionality of the product under evaluation. TSS A description of how a satisfies the SFRs in a . SFR A requirement for security enforcement by the . SAR A requirement to assure the security of the . Add-on Capabilities or functionality added to an application. This term includes plug-ins, extensions, and other controls. Administrator The Administrator is responsible for management activities, including setting the policy that is applied by the enterprise on the browser. This administrator is likely to be acting remotely. If the platform is unmanaged by an enterprise, the user can act as the administrator. CSRF Cross Site Request Forgery - Vulnerability where an attacker gets a target user to execute a script with that user's privileges. Domain A realm of administrative autonomy, authority or control on the Internet (e.g., cnn.com). Extension Bundle of code added to the browser to add specific functionality that the browser does not provide by default. HTML HyperText Markup Language - Language used by web servers to present content to browsers. HTML5 HyperText Markup Language version 5, a new version of HTML that incorporates many new features that enrich the browsing experience. HTTP HyperText Transfer

Protocol - Protocol for communicating on the web. HTTPS HyperText Transfer Protocol Secure; secure version of HTTP that runs over an encrypted channel (SSL/TLS). JavaScript Scripting language commonly integrated into web pages to generate dynamic, interactive content. Mobile Code Software transmitted from a remote system for execution within a limited execution environment on the local system. Typically, there is no persistent installation and execution begins without the user's consent or even notification. Examples of mobile code technologies include Java applets, Adobe ActionScript, and Microsoft Silverlight. Note: JavaScript is not included in references to mobile code in this browser . Plug-in Browser add-on to handle specific types of web content. Pop-up Piece of web code that causes a browser to open a window outside the window that is currently in focus. Port An application-specific construct that functions as a communications endpoint in a computer's host OS; in a web environment, port 80 is the default port for HTTP communications, although other ports can be used. In a web address, the port follows the domain or sub-domain name (e.g., http://www.cnn.com:80). Protocol A system of digital rules for data exchange within or between computers; in a web environment, the typical protocols are HTTP and HTTPS. Sandbox Security mechanism for separating running processes, most often used to run untrusted or vulnerable processes by reducing their privileges to such an extent that they should not be able to harm the host system. Sensitive Data Sensitive data may include all user or enterprise data or may be specific application data such as data transferred to submit a form or complete a transaction. Sensitive data must minimally include personally identifiable information (PII), credentials, and keys. Sensitive data shall be identified in the application's by the author. Sub-domain An Internet domain which is part of a primary domain, denoted by a prefix before the primary domain (e.g., news.cnn.com). Tabs Allow the browsers to display content from multiple web sites in the same window. Web Browser Application that retrieves and renders content provided by a web server. The terms web browser, browser, and TOE are interchangeable in this document. XSS Cross Site Scripting - Injection of untrusted content into a vulnerable web application to render or execute that content on a victim's system.

3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) in this is any web browser client capable of running on any operating system or platform and rendering web content using HTTP and HTTPS. This describes the extended security functionality of web browsers in terms of . As an extension of the App PP, it is expected that the content of this will be appropriately combined with the App PP to include selection-based requirements in accordance with the selections and/or assignments made, and any optional and/or objective components to include: FCS_CKM.1.1, FCS_CKM.2.1, FCS_COP.1.1(*), FCS_DTLS_EXT.1.*, FCS_HTTPS_EXT.1.*, FCS_RBG_EXT.2.*, FCS_TLSC_EXT.1.*, FIA_X509_EXT.1.*, FIA_X509_EXT.2.*. An must identify the applicable version of the App PP and this in its conformance claims.

4 Use Cases

Requirements in this extended package are designed to address the security problems in the use cases below. These use cases are intentionally very broad, as web browsers can be used to perform many tasks.

[USE CASE 1] Surfing the Web

Browsers are used to retrieve, display and render content from the web, such as web pages, streaming media, images and specialized formats (e.g., Java, Flash, PDF). They can also be used to write content to web sites (web 2.0 – e.g., Facebook). Web surfing can be done over the Internet or within an Intranet.

[USE CASE 2] Remote Administration Client

Browsers are used to provide remote administration interfaces for systems such as servers, network devices and embedded systems, to include supervisory control and data acquisition (SCADA) systems, smart TVs and thermostats. As opposed to surfing the web, where the browser may be interacting with untrusted content, the browser, acting as a Remote Administration Client, is connecting to a server that the user trusts.

[USE CASE 3] Content Creation

Browsers are used to create content via an increasing number of Software as a Service (SaaS) offerings, including Microsoft Office 365, Google Drive, and Adobe Creative Cloud, where user data and records are stored online.

The Protection Profile for Application Software () defines the baseline Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for application software products. This serves to extend the App PP baseline with additional SFRs and associated Assurance Activities specific to a web browser. Assurance Activities are the actions that the evaluator performs in order to determine a web browser's compliance to the SFRs. This conforms to Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4. It is CC Part 2 extended and CC Part 3 conformant. In order to be conformant to this , the must include all components in this and the associated App PP that are: unconditional (which are always required) selection-based (which are required when certain selections are chosen in the unconditional requirements) and may include optional and/or objective components that are desirable but not required for conformance. In accordance with CC Part 1, dependencies are not included when they are addressed by other SFRs. The assurance activities provide adequate proof that any dependencies are also satisfied.

The security problem is described in terms of the threats that the web browser is expected to address, assumptions about the operational environment, and any organizational security policies that it is expected to enforce. This Extended Package does not repeat the threats, assumptions, and organizational security policies identified in the App PP, though they all apply given the conformance and hence dependence of this on it.

Together the threats, assumptions and organizational security policies of the App PP and those defined in this describe those addressed by a web browser as the Target of Evaluation. Notably, browsers are particularly at risk from the Network Attack threat identified in the App PP. Attackers can use phishing or another social engineering technique to persuade a user to visit a malicious site. Users may also unintentionally visit malicious sites in the course of web browsing. Such sites then present malicious content to the user's browser to exploit it and perform installation of malware, often with no indication to the user.

5 Threats

The following threats are specific to web browsers, and represent an addition to those identified in the App PP.

Web browser functionality can be extended through the integration of third-party utilities and tools. Malicious or vulnerable add-ons could result in attacks against the system. Such attacks can allow unauthorized access to sensitive information in the browser, unauthorized access to the platform's file system, or even privilege escalation that enables unauthorized access to other applications or the operating system.

Violating the same-origin policy is a specialized type of network attack (covered generally as T.NETWORK_ATTACK in the App PP) which involves web content violating access control policies enforced by a web browser to separate the content of different web domains. It is specifically identified as a threat to web browsers, since they implement the access control policies that are violated in these attacks. Attacks which involve same origin violations include: Insufficient protection of session tokens can lead to session hijacking, where a token is captured and reused in order to gain the privileges of the user who initiated the session. Cross-site scripting (XSS) and Cross-Site Request Forgery (CSRF) attacks are methods used to compromise user credentials (usually by stealing the user's session token) to a web site. These attacks are more likely a result of server security problems, but some browsers incorporate technologies that try to detect the attacks. Inadequate sandboxing of browser windows/tabs or a faulty cross domain communications model can lead to leakage of content from one domain in one window/tab to a different domain in a different window/tab. Such attacks leverage the ability of browsers to display content from multiple domains simultaneously.

This Extended Package adds security objectives to those identified in the Protection Profile for Application Software (App PP).

6 Security Objectives for the TOE

To address the network attack associated with content leakage between different web domains, the browser must ensure that content originating from different domains (e.g., in a tab or iFrame) is properly isolated.

To address issues associated with malicious or flawed add-ons, conformant browsers implement mechanisms to ensure their integrity. This includes verification and validation at installation time and update.

7 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

7.1 TOE Security Functional Requirements

This PP-Module does not define any mandatory SFRs.

8 Consistency Rationale

Appendix A - Optional SFRs

Appendix B - References

[CC]Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012. Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012. Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012. [AppPP] Protection Profile for Application Software

Appendix C - Acronyms

CRL Certificate Revocation List CSRF Cross Site Request Forgery GPU Graphics Processing Unit HTML HyperText Markup Language HTML5 HyperText Markup Language version 5 HTTP HyperText Transfer Protocol HTTPS HyperText Transfer Protocol Secure IETF Internet Engineering Task Force IPC Inter-process communication OCSP Online Certificate Status Protocol PDF Portable Document Format RFC Request for Comment (IETF) SaaS Software as a Service SSL Secure Sockets Layer TLS Transport Layer Security W3C World Wide Web Consortium XSS Cross Site Scripting

Appendix D - Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
OE	Operational Environment
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification

Appendix E - Bibliography

Identifier	Title
[AppPP]	Protection Profile for Application Software
[CC]	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012. Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012. Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.