Protection Profile of Web Content Protection System

Hyun-Jung Lee and Dongho Won[1]

[1] Information Security Group,
School of Information and Communication Engineering,
Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu,
Suwon, Gyeonggi-do 440-746, Korea
{hjlee, dhwon}@security.re.kr

Abstract. Since the Internet is a widely used tool in many business areas these days, a large amount of contents are offered through the Web. Almost all of them, however, are being provided to users without any protection. Anyone can copy and reuse the contents without permission by using features of the Web browser and even use them for commercial purposes. It is time to consider having countermeasures to protect the Web contents from illegal use and leakage. Therefore, this paper intends to derive necessary security functions for a Web contents protection system with the basis of the Common Criteria V3.1. It can be used as reference in the case of introduction or evaluation of the system.

Keywords: Web Content Protection System; Protection Profile; Common Criteria; PP; CC

1 Introduction

While the wide distribution of Internet enables people to share and exchange data easily, it also caused many sorts of accidents. For example, a malicious user can copy and leak Web contents of a company by using features provided on the Web. The contents lose the value as an asset after being leaked, which can cause financial loss, psychological damage, and even ruined company name.

Also many companies have been changing their work environments into a groupware system with the developing Internet technologies. In a groupware environment, confidential information of a company, such as information of client, marketing, or product, can be easily exposed to the staff. Web-based service system increases the possibility of the information being copied and leaked out of a company. Given the fact that many of the security-related accidents on the Internet happened in-house, it is necessary to protect against information leakage in a company that adopts a groupware system.

This paper intends to derive security functional requirements for a Web contents protection system based on the Common Criteria V3.1.

[1] Corresponding author: Dongho Won (dhwon@security.re.kr)

2 Related Works

2.1 Common Criteria and Protections Profile

The Common Criteria(CC) is a standard that connects evaluation criteria of a number of countries and makes mutual recognition of evaluation certificates between different evaluation authorities possible. It permits comparability between the results of independent security evaluations by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. The target audience of the CC includes consumers, developers, and evaluators. Consumers and developers can use it to decide what security functions they need a product to provide [2].

The CC provides a special construct called Protection Profile(PP) to allow consumer groups and communities of interest to express their security needs and to facilitate writing Security Target(ST)s. Whereas an ST always describes a specific TOE, a PP is intended to describe a TOE type(e.g. firewalls). The same PP may therefore be used as a template for many different STs to be used in different evaluations. A PP must contain a PP introduction, a conformance claim, a security problem definition, security objectives, extended components definition, and security requirements [2].

2.2 Introduction of Web Contents Protection System

The Web contents protection system prevents the Web contents from being copied, stored, or printed by an unauthorized user so that the Web contents can be protected from illegal use or leakage. The system is comprised of two components: one is the Web contents protection server, which controls the security of an HTML document between the Web server and the client; the other is the client agent, which controls the Web browser menu and screen capture protection for an HTML document for which the Web contents protection server enabled contents protection [5,6,7].

The Web contents protection server, which is located between the Web server and the client, takes and intermediary role between the two: It receives a request for HTTP service from the client and sends it to the Web server; When the Web server gives a response, it sends it back to the client. All contents of a Web server for which contents protection is enabled will be given to a client through the Web contents protection server. When an HTML document for a URL that an administrator specified for contents protection has to be sent to a client, the Web contents protection server encrypts the HTML document first and sends it to the client. The client agent controls the features of the Web browser such as storing/viewing HTML source, printing a Web page, and copying using clipboard to prevent copy of and link to the HTML contents provided by the Web browser. It also provides screenshot protection to prevent the Web image from being captured by an image capture program.

3. Proposed Web Content Protection System Protection Profile

3.1 Scope of the TOE

The TOE should provide the security functions required for on-line e-document issuance depending on the components of an issuance system.

- Identification and authentication: The Web contents protection server will identify and authenticate an administrator before allowing access.
- Security management: The TOE manages several aspects of the TSF, such as the security functions, TSF data, security roles, etc.
- Security audit: The TOE generates and maintains an audit log in the case of security-relevant events to ensure accountability.
- User data protection: The TOE provides the Web contents through encryption of the Web page being transmitted from the Web server to the client, Web browser cache control, and Web browser control(e.g. print control, source view control, clipboard control, etc.).
- Cryptographic support: To ensure the confidentiality of the user data and TOE data, the TOE supports the life cycle of a cryptographic key from its generation to destruction.
- Protection of the TSF: The TOE shall check the integrity of its processes and TSF data on a periodical basis for the sake of protection of the TOE. It is also for a safe transfer of the TSF data between parts of the TOE(e.g. between the Web contents protection server and the client agent).
- TOE access: The TOE terminates a session after a specified period of administrator inactivity.

This paper is intended to apply to various types of implementation. The TOE may require hardware, software, or firmware that is not explicitly stated in this paper.

3.2 Security problem definition

A security problem definition defines the threats, organizational security policies, and assumptions that should be addressed by the TOE and its operational environment. The assets that should be protected by the TOE:

- Web contents to be protected by the Web server The assets that support secure operation of the TOE:
- The TOE itself; which includes the TSF data, executable code, etc

Threats. This subsection of the security problem definition shows the threats that are to be countered by the TOE. A threat consist of a threat agent, an asset and an adverse action of that threat agent on that asset[2]. The specification of threats should include all threats detected up to now[5,6,7], if it is not done the TOE may provide inadequate protection. In other words, if the specification of threats is insufficiency, the assets may be exposed to an unacceptable level of risk. The Threats for this paper are described in Table 1.

Table 1. Threats

Threat	Description
T.SPOOFING	A threat agent can access the user data or TSF by disguising himself.
T.FAILURE	A failure in the TOE can cause the TSF data or user data to be modified by or exposed to a threat agent.
T.MODIFICATION	A threat agent can modify the TSF data in the TOE in order to access the TOE or the assets.
T.DATA_TRANSFER	A threat agent can expose or modify the Web contents or TSF data without authorization while they are being transferred between the Web server and the client.
T.WEB_BROWSER_CACHE_CONTENTS	A threat agent can expose the Web contents by using the cache of the Web browser. (* When the Web browser stores data using a cache, the data is usually stored in a specific folder of a user PC in the format of HTML document. A threat agent can always analyze the HTML document source stored in a cache and get access to the contents or copy/distribute an image without authorization.)
T.WEB_BROWSER_MENU	A threat agent can leak the Web contents by using the features of the Web browser, such as 'store HTML source', 'view source', 'print', 'copy using clipboard', etc.
T.WEB_PAGE_URL	A threat agent can get the information about the Web contents by using URL link information in the HTML page or the Web page visit history stored in the Web browser.
T.MOUSE_CONTENTS	A threat agent can leak the Web contents by using the mouse right-click menu, such as 'copy content', 'view source', 'print', 'copy script', etc.
T.SCREENSHOT	A threat agent can leak the Web contents by copying the screen using a screen capture program.
T.WebCrawler	A threat agent can leak the Web contents by making copies of all Web pages with a Web crawler.

Organizational Security Policy. An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The organizational security policies for this paper are described in Table 2.

Table 2. OSPs

Name	Description
P.AUDIT	The TOE shall generate and mainitain a record of security-related events to ensure accountability. The records shall be reviewed properly.
P.SECURE_MANAGEMENT	The TOE shall provide its authorized administrator with a means to manage the TOE securely.
P.POLICY	The TOE shall support security policy for each Web page.
P.CRYPTO_ALGORITHM	The TOE shall use the cryptographic algorithm that is reliable or specified by the organizational security policy.

Assumptions. The assumptions are made on the operational environment in order to be able to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment. The Assumptions for this paper are described in Table 3.

Table 3. Assumptions

Assumption	Description
A.PHYSICAL_SECURITY	The TOE_server is located in a physically secure environment, which will protected from an unauthorized access.
A.TRUSTED_ADMIN	An authorized administrator of the TOE has no malicious intention, is properly educated in terms of the management functions of the TOE, and follows the administrator's guidance.
A.OS_ENHANCEMENT	Unnecessary services or measures will be removed from the TOE_server system and vulnerabilities of the operating system will be fixed properly to ensure its reliability and stability.
A.SECURE_CHANNEL	Message communication between the TOE server and the administrator console will be protected through a secure channel.
A.SECURE_EXTERNAL_ENTITY	External entities containing the Web contents that should be protected by the TOE, such as the Web server, will be operated in a secure manner.

3.3 Security objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition. The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

Security Objectives for the TOE. The TOE provides security functionality to solve a certain part of the problem defined by the security problem definition. This part wise solution is called the security objectives for the TOE and consists of a set of objectives that the TOE should achieve in order to solve its part of the problem. The security objectives for the TOE for this paper are described in Table 4.

Table 4. Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE shall generate and mainitain a record of security-related events to ensure accountability. It shall provide a proper means to review the records. It shall also provide a function to deal with audit data storage exhaustion.
O.MANAGEMENT	The TOE shall provide its authorized administrator with a means to manage the TOE securely.

Name	Description
O.IA	The TOE shall uniquely identify a user and authenticate the user before allowing his access to the management functions and objects of the TOE. It shall have a countermeasure for consecutive authentication failures.
O.FAILURE_PROTECTION	The TOE shall protect the TSF data and user data from failures, such as unauthorized modification or deletion of the processes or executable files.
O.STORED_DATA_PROTECTION	The TOE shall protect the user data and TSF data from unauthorized exposure, modification, or deletion.
O.TRANSFERRED_DATA_PROTECTION	The TOE shall protect the Web contents and TSF data being transferred between the Web server and the client from unauthorized exposure or modification.
O.WEB_BROWSER_CACHE_CONTROL	The TOE specifies that, for the contents in the Web page for which contents protection is enabled, the Web browser cannot store the contents in a local cache.
O.WEB_BROWSER_MENU_CONTROL	The TOE shall control the use of menu in the Web browser related to the HTML document so that 'store HTML document in a local disk', 'send an email', 'print', and 'copy using clipboard' features cannot be used.
O.WEB_PAGE_URL_PROTECTION	The TOE shall protect the URL information and the Web page visit history by deleting the visit history, hiding the Web browser status, or controlling the address input.
O.MOUSE_CONTROL	The TOE shll control the right-click features of a mouse to prevent the Web contents leakage using those features.
O.SCREENSHOT_PROTECTION	The TOE shall provide a screenshot protection function to prevent screen capture.
O.WEBCRAWLER_CONTROL	The TOE shall be able to prevent many different types of Web crawlers from collecting Web pages.

Operational Environment of the TOE. The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality (which is defined by the security objectives for the TOE). This part wise solution is called the security objectives for the operational environment and consists of a set of statements describing the goals that the operational environment should achieve. The operational environments of the TOE for this paper are described in Table 5.

Table 5. Security objectives for the operational environment of the TOE

Name	Description
OE.PHYSICAL_SECURITY	The TOE_server shall be located in a physically secure environment, which will protected from an unauthorized access.
OE.TRUSTED_ADMIN	An authorized administrator of the TOE shall have no malicious intention, be properly educated in terms of the management functions of the TOE, and follow the administrator's guidance.
OE.OS_ENHANCEMENT	Unnecessary services or measures shall be removed from the TOE_server system and vulnerabilities of the operating system shall be fixed properly to ensure its reliability and stability.

Name	Description
OE.SECURE_CHANNEL	Message communication between the TOE server and the administrator console shall be protected through a secure channel.
OE.SECURE_EXTERNAL_ENTITY	External entities containing the Web contents that should be protected by the TOE, such as the Web server, shall be operated in a secure manner.
OE.TIMESTAMP	The TOE shall record security-relevant events accurately using the reliable timestamp provided in the operational environment.

3.4 Security Functional Requirements

The Security functional requirements substantiate the security objectives. Each security functional requirement must be related to one or more security objectives. These requirements are defined in CC part 2, and protection profile author just chooses and uses appropriate requirements. The security functional requirements for this paper are described in Table 6.

Table 6. The security functional requirements

Functional class	Functional component	
Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible audit data loss
	FAU_STG.4	Prevention of audit data loss
Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ETC.2	Export of user data with security attributes
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Security management	FMT_MOF.1	Management of security functions behavior

Functional class	Functional component	
	FMT_MSA.1	Management of securitty attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_TST.1	TSF testing
TOE access	FTA_SSL.3	TSF-initiated termination

4. Conclusion

Many companies are adopting a Web contents protection server hoping that it can solve the desperate problem they are facing, risk of data leakage. This paper intends to suggest a baseline for introducing/evaluating a Web contents protection server and eventually help protect data and prevent its theft or leakage. However, unlike the perimeter security, which is the essential aspect of IT security, data leakage protection is more about business than IT technologies because it deals with information assets, which is the most important thing to a company. That is, mere introduction of a Web contents protection server does not prevent data leakage. For a complete prevention of data leakage, not only the IT team members but all company workers should aware their roles and responsibilities.

References

1. Smith, T.F., Waterman, M.S.: Identification of Common Molecular Subsequences. J. Mol. Biol. 147, 195--197 (1981)
2. Lee, S., Shin, M.: Protection Profile for Software Development Site. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Lagan´a,A., Lee, H.P., Mun, Y., Taniar,D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3481, pp. 499–507. Springer, Heidelberg (2005)
3. Common Criteria, Common Criteria for Information Technology Security Evaluation; part 1: Introduction and general model, Version 3.1 R1, CCMB-2006-09-001(September 2006)
4. Common Criteria, Common Criteria for Information Technology Security Evaluation; part 2: Security functional components, Version 3.1 R2, CCMB-2007-09-002(September 2007)
5. Common Criteria, Common Criteria for Information Technology Security Evaluation; part 3: Security assurance components, Version 3.1 R2, CCMB-2007-09-003(September 2007)
6. Markany, WebSafer 3.0 Whitepaper Version 3(November 2003)
7. http://www.fasoo.com
8. http://www.softcamp.co.kr