International Journal of Security and Its Applications
Vol.7, No.6 (2013), pp.373-384
http://dx.doi.org/10.14257/ijsia.2013.7.6.37

Protection Profile for Unidirectional Security Gateway between Networks

Hyun-Jung Lee and Dongho Won

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

Development of hacking techniques demands more and more network security. For this reason, Major facilities as well as government agencies divide the Protected Network from Internet Network Physically. However, if Internal/external network is divided, file transfer and work efficiency is reduced. To solve this problem and to transfer data between the Internet Network and protected Network, Unidirectional Security Gateway System was born. This paper analyzes unidirectional Security Gateway and suggests a protection profile based on the CC V3.1 to help develop and evaluation of unidirectional Security Gateway.

Keywords: Unidirectional Security Gateway, One-way flow, Protection Profile, Common Criteria, Security Requirement

1. Introduction

Communication is intended to be used in a bidirectional matter, where sender and receiver exchange information without any hassle. The problem is that communication between two differently classified networks is submitted to strict security rules. Specifically rules regarding the declassification of information i.e. before it is allowed to leave the classified network. In classified environments Data Diodes are used to transport information from the unclassified network to the classified network securely. However, when information is declassified it is still transported manually using a media carrier like USB or CD to the unclassified network.

The disadvantage of manual transporting (declassified) information is that it' s not real-time, it's time consuming and it introduces additional security risks since information is transported in an uncontrolled matter (humans). In order to solve this problem, Unidirectional Security Gateway System was born.

This paper derives necessary security functions of a Unidirectional Security Gateway based on the Common Criteria v3.1 and intends to suggest how to improve the functionality of currently used privacy protection system.

2. Related Work

2.1. CC(ISO/IEC 15408) and Protection Profile

The Common Criteria for Information Technology Security Evaluation (Common Criteria or CC) is an international standard (ISO/IEC 15408) established with the objectives to integrate various evaluation standards from different countries and allow mutual recognition

ISSN: 1738-9976 IJSIA

of the evaluation results between the countries that agrees on the idea. 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. Consumers, developers, and evaluators can use the CC. Consumers and developers can use it to enumerate and describe the security functions they need from a product [2].

The CC is presented as a set of distinct but related parts as identified below [2][3].

- Part 1: The part 1 is the introduction to the CC. It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation [2].
- Part 2: The part 2 establishes a set of security functional components that serve as standard templates upon which to base functional requirements for TOEs[3]. CC Part 2 catalogues the set of functional components and organizes them in families and classes[3].
- Part 3: The part3 establishes a set of security assurance components that serve as standard templates upon which to base assurance requirements for TOEs. CC Part 3 catalogues the set of assurance components and organizes them into families and classes. Furthermore, CC Part 3 describes seven assurance package and evaluation criteria for PPs and STs.

To allow consumer groups and communities of interest to express their security needs, and to facilitate writing STs, the CC provides a special construct called Protection Profile (PP). 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, conformance claim, security problem definition, security objectives, extended components definition, and security requirements.

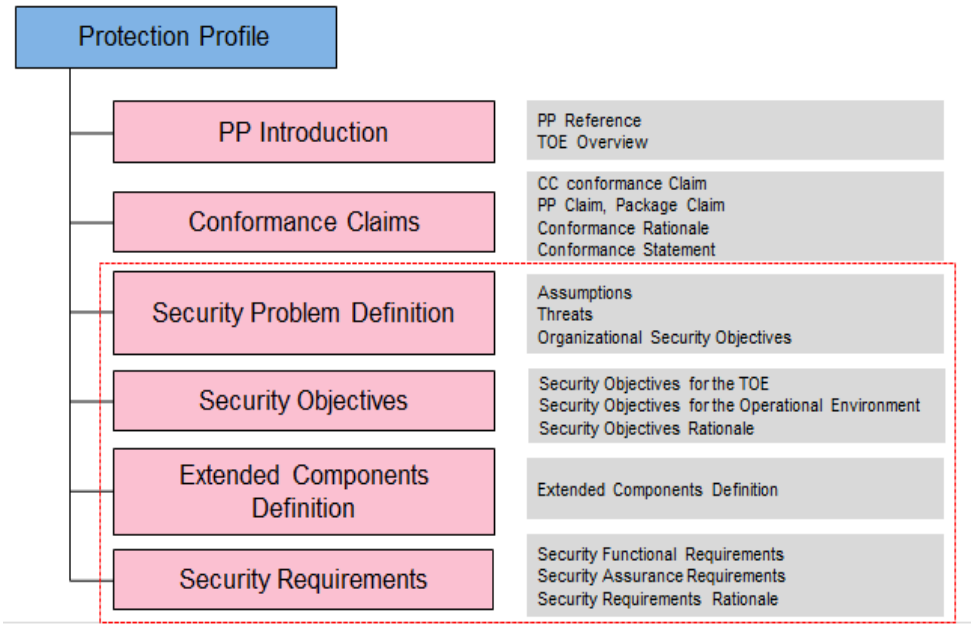

Figure 1. Architecture of Protection Profile

To see what kinds of security functions are needed to operate a Unidirectional Security Gateway, this paper intends to draw out security functional requirements for Unidirectional Security Gateway using the CC v3.1.

2.2. Unidirectional Security Gateway

A unidirectional network (also referred to as a unidirectional security gateway or data diode) is a network appliance or device allowing data to travel only in one direction, used in guaranteeing information security. They are most commonly found in high security environments such as defense, where they serve as connections between two or more networks of differing security classifications. This technology can now be found at the Industrial Control level for such facilities as nuclear power plants, and electric power generation [4].

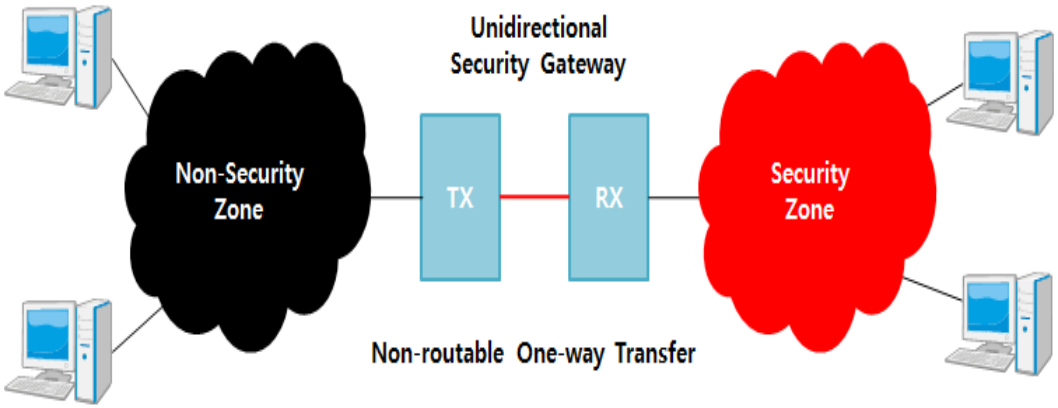

Figure 2. Unidirectional Security Gateway

Unidirectional Security Gateway is installed between two separate networks. And it cuts off all communication data and relays the response/request data using data copy.

3. Security Problem Definition

The security problem definition is statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address[1-3].

This statement consists of a combination of:

- threats to be countered by the TOE,
- the OSPs enforced by the TOE, and
- the assumptions that are upheld for the TOE and its operational environment.

3.1 Threats

This subsection of the security problem definition shows the threats that are to be countered by the Unidirectional Security Gateway. A threat consist of a threat agent, an asset and an adverse action of that threat agent on that asset[8-16]. The specification of threats should include all threats detected up to now; if it is not done the Unidirectional Security Gateway 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[5-7].

Table 1. Threats

Threat	Description
T. Inflow of unauthorized traffic	Threat agents can attack the internal network zone as unauthorized traffic (e.g. malware, unauthorized information) flows in the Security Zone.
T.Outflow of data to the unauthorized Security Zone	Users in the Security Zone can take unauthorized data to the unauthorized Security Zone through networks.
T.User Impersonation	Threat agents can access the Transmission Control Server as impersonating authorized users.
T.Administrator Impersonation	Threat agents can access the Transmission Control Server as impersonating the authorized administrator.
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.Continuous Authentication Attempt	Threat agents can get authentication of the authorized administrator as attempting authentication continuously to access the Transmission Control Server.
T.Reuse Attack	Threat agents can access the Transmission Control Server as reusing the administrator’s authentication data
T.Outflow and Damage of transmission data	Threat agents can flow out, change and delete transmitted data between elements of the product by unauthorized methods.
T.Damage of Storage data	Threat agents can flow out, change and delete important operating data stored in product by unauthorized methods.

3.2 OSP

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. We identified Organizational Security Policies (OSPs) which are to be met by the security objectives in Table 2[5-7].

Table 2. Organizational Security Policy

Policies	Description
P.Audit	The TOE must audit every auditable event and keep the audit record secure. This audit record is protected from unauthorized access.
P.Secure Management	An authorized administrator shall manage the TOE, audit log, and so on in a secure way.

3.2 Assumption

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[5-7].

Table 3. Assumption

Assumptions	Description
A.Trusted Administrator	It is assumed that the administrators are non-hostile, well trained and follow all administrator guidance.
A.Timestamp	It is assumed that the TOE environment provides a secure timestamp that fulfills RFC 1305.
A.Physical Security	The e-document issuing system is located in a physically secure environment that can only be accessed by an authorized administrator.
A.Secure Installation and Operation	The TOE will be distributed and installed on a user PC in a secure manner.
A.Network	Any traffic flow required by the TOE services will always be allowed.
A.OS Enhancement	Services or means not required by the e-document issuing system will be removed from the operating system and vulnerabilities of the operating system will be fixed properly to ensure its reliability and stability.

4. Proposed Security Objective

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 [8-16].

4.1 Security Objectives for the TOE

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 Unidirectional Security Gateway form a high-level solution to the security problem. Table II identifies the security objectives for the Unidirectional Security Gateway.

Table 4. Security Objectives for the TOE

Security Objectives	Description
O.Secure Communication	TOE must protect the distributed IT entity through secure communication channel.

Table 4. *(Continued)*

Security Objectives	Description
O.Residual Information Clearing	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.Unidirection	The Communication Request shall consist of a connect which is from the Transmission Control Server in the Security Zone to the Transmission Control Server in the Non-Security Zone and the Communication Request shall provide a function of One-direction Maintenance which does not permit any other Communication Requests.
O.Audit	The TOE shall generate and maintain 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.
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.TSF Protection	The TOE shall protect itself from unauthorized access or tampering to its functionality and data in order to maintain the integrity of the system data and audit records. And The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.
O.Stored DATA Protection	The TOE shall protect the user data and TSF data from unauthorized exposure, modification, or deletion.
O.Data Inspect	Before transmitting data from Non-Security Zone to Security Zone, a function shall be provided when malwares are not found after finishing a compulsory Malicious Code testing.

4.2 Security Objective for the Operational Environment

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 Objective for the Operational Environment

Security Objectives	Description
OE.Trusted Administrator	Authorized administrator must be trained as to establishment and maintenance of security policies in practice.

Table 5. *(Continued)*

Security Objectives	Description
OE.Timestamp	The TOE environment shall provide a secure timestamp that fulfills RFC 1305.
OE.Physical Security	The e-document issuing system shall be located in a physically secure environment that can only be accessed by an authorized administrator.
OE.Secure Installation and Operation	The TOE shall be distributed and installed on a user PC in a secure manner.
OE.OS Enhancement	Services or means not required by the e-document issuing system shall be removed from the operating system and vulnerabilities of the operating system shall be fixed properly to ensure its reliability and stability.
OE.Network	Any traffic flow required by the TOE services shall always be allowed.

4.3. Security Objective Rationale

The Rationale proves that the requirements are specified completely. According to the rationale, it is possible to determine that security requirements are correct, complete and both protection profile author and potential developer can verify security of the proposed TOE. Table 6 describes the rationale.

Table 6. Security Objective Rationale

Security Objectives / Security Problem Definition	Security Objectives for the TOE									Security Objective for the Operational Environment					
	O.Secure Communication	O.Residual Information Clearing	O.Unidirection	O.Audit	O.Management	O.IA	O.TSF Protection	O.Stored DATA Protection	O.Data Inspect	OE.Trusted Administrator	OE.Timestamp	OE.Physical Security	OE.OS Enhancement	OE.Secure Installation and Operation	OE.Network
T. Inflow of unauthorized traffic			X						X						
T.Outflow of data to the unauthorized Security Zone			X						X						
T.User Impersonation						X									

Table 6. (Continued)

Security Objectives / Security Problem Definition	Security Objectives for the TOE									Security Objective for the Operational Environment					
	O.Secure Communication	O.Residual Information Clearing	O.Unidirection	O.Audit	O.Management	O.IA	O.TSF Protection	O.Stored DATA Protection	O.Data Inspect	OE.Trusted Administrator	OE.Timestamp	OE.Physical Security	OE.OS Enhancement	OE.Secure Installation and Operation	OE.Network
T.Administrator Impersonation						X									
T.FAILURE							X	X							
T.Continuous Authentication Attempt						X									
T.Reuse Attack						X									
T.Outflow and Damage of transmission data	X														
T.Damage of Storage data		X													
P.Audit				X											
P.Secure Management					X										
A.Trusted Administrator										X					
A.Timestamp											X				
A.Physical Security												X			
A.Secure Installation and Operation	X													X	
A.Network		X													X
A.OS Enhancement				X									X		

5. 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 7[1-3].

Table 7. Security Functional Requirements

Security functional class	Security functional component	
Security audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_SEL.1	Selective audit
	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)	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)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_ITT.1	Basic internal transfer protection
Identification and authentication (FIA)	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action

Table 7. (Continued)

Security functional class	Security functional component	
Security management (FMT)	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_ITT.1	Inter-TSF detection of modification
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
Trusted Path/Channel (FTP)	FTP_ITC.1	Inter-TSF trusted channel

6. Conclusions

This paper proposes security requirements which can be used as a request for a proposal to procure a unidirectional Security Gateway, a guideline for developers to develop a unidirectional Security Gateway, and criteria with which evaluators can evaluate the completeness of a developed system. Thus, the unidirectional Security Gateway was analyzed, a threat was modeled, and CC based security requirements were deduced.

Acknowledgements

Corresponding author: Dongho Won.

References

[1] Common Criteria, Common Criteria for Information Technology Security Evaluation; part 1: Introduction and general model, Version 3.1 R1, CCMB-2006-09-001, **(2006)** September.
[2] Common Criteria, Common Criteria for Information Technology Security Evaluation; part 2: Security functional components, Version 3.1 R2, CCMB-2007-09-002, **(2007)** September.
[3] Common Criteria, Common Criteria for Information Technology Security Evaluation; part 3: Security assurance components, Version 3.1 R2, CCMB-2007-09-003, **(2007)** September.
[4] hwikipedia, ttp://en.wikipedia.org/.
[5] K. Rhee, W. Jeon and D. Won, "Security Requirements of a Mobile Device Management System", International Journal of Security and Its Applications, **(2012)** April.
[6] K. Lee, Y. Lee, D. Won and S. Kim, "Protection profile for secure E-voting systems", ISPEC 2010, LNCS 6047, **(2010)**, pp. 386-397.
[7] Waterfall, Waterfall Unidirectional Security Gateway WF-400 Security Target, V0.72, 2012.6.29.
[8] J. Slay and B. Turnbull, "The Uses and Limitations of Unidirectional Network Bridges in a Secure Electronic Commerce Environment", paper presented at the INC 2004 Conference, Plymouth, UK, **(2004)** July 6-9.

[9] M. W. Stevens and M. Pope, "Data Diodes", DSTO Electronics and Surveillance Research Laboratory, Adelaide, **(1995)**.
[10] M. W. Stevens, "An Implementation of an Optical Data Diode", DSTO Electronics and Surveillance Research Laboratory, Adelaide, **(1999)**.
[11] M. Anderson, C. North, J. Griffin, R. Milner, J. Yesberg and K. Yiu, "Starlight: Interactive Link", San Diego, CA, USA, **(1996)**.
[12] H. K. Myong, I. S. Moskowitz and S. Chincheck, "The Pump: A Decade of Covert Fun", **(2005)**.
[13] C. A. Nilsen, "Method for Transferring Data from an Unsecured Computer to a Secured Computer", U.S. Patent 5,703,562, **(1997)** December 30.
[14] Australian Government Information Management Office 2003, Securing systems with Starlight, Department of Finance and Administration, viewed, [1][dead link], **(2011)** April 14.
[15] C. Wordsworth, "Media Release: Minister Awards Pioneer in Computer Security", viewed 14 April 2011, [2], **(1998)**.
[16] D. W. Jones and T. C. Bowersox, "Secure Data Export and Auditing Using Data Diodes", Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop, Vancouver, **(2006)** August 1.

Authors

HyunJung Lee, received B.S. degree in Computer Science form SungShin women's University in 2002. After working at KISA from 2002 to 2007, she joined KOSYAS in 2008 and is currently a member of engineering staff of KOSYAS. She interests are information security, information assurance, and security evaluation

Dongho Won, received M.S and Ph.D. degrees in electronic Engineering form Sungkyunkwan University in 1978 and 1988, respectively. After working at ETRI from 1978 to 1980, he joined Sungkyunkwan University in 1982, and is currently a Professor of the College of Information and Communication Engineering. His interests are cryptology and information security.