

Development of Security Target for Router Based on ENISA Common Criteria Framework

Jiann-Liang CHEN*, Jian-Chang HSU**, Candra AHMADI*, Bagus Tri ATMAJA*,
Chia-Chi LIN*, Siao-He WANG*, Shu-Yu LIN**

* Department of Electrical Engineering, NTUST (National Taiwan University of Science and Technology)

** ITRI (Industrial Technology Research Institute), Taiwan

lchen@mail.ntust.edu.tw, hcc@taics.org.tw, D11007809@mail.ntust.edu.tw, M11007823@mail.ntust.edu.tw,
M11007503@gapps.ntust.edu.tw, M11007511@gapps.ntust.edu.tw, mrm@itri.org.tw

Abstract— With the development of new technologies, information and communication technologies (ICT) are everywhere in our daily life. For attackers, information and communication technology products are the entry point for attacks, so they can quickly obtain the necessary information or retrieve data to threaten users. The diversity of network devices also increases the probability of attacks, whether software, hardware, or firmware, which could be an opportunity for attackers. The EUCC is based on the ISO/IEC15408 Common Criteria for Information Technology Security Certification, an international framework agreement that provides guidelines for evaluating and certifying ICT products. When a developer submits a product for evaluation, they need to design a security target (ST) for the product, which includes an overview of the product, security features, and an assessment of potential security threats. During the development of the security target, a preliminary analysis of the possible threats on the network device is performed, the security objectives are proposed for the threats, and finally, the security functional requirements are designed. In this study, we take a router as an example and perform a gap analysis between the possible threats faced by an unregulated router and the development of a security standard document related to routers based on the Common Criteria framework. Finally, we present a list of features reported as compliant with the Common Criteria framework to improve their router products.

Keywords— Common Criteria, ENISA, Network device, Router, Security target

I. INTRODUCTION

The Internet is a rapidly developing technology worldwide, and with new technologies, information and communication technologies are becoming ubiquitous in everyday life. According to “Statista” website [1], the number of Internet users worldwide will be 4.9 billion in 2021, which means that nearly two-thirds of the world's population is currently connected to the world wide web. The diversity of network devices also increases the chance of an attack, whether it is software, hardware, or firmware.

For example, routers are the first line of defense in a network. They are devices that pass information between two or more packet-switched computer networks. Check the network protocol address (IP address) of the given packet

destination, calculate the best way to reach the destination, and forward the packets accordingly [2].

ENISA [3], the European Union Agency for Network Security, released a new version of the certification scheme in May 2021, based on the Common Criteria for European Network Security Certification (EUCC), which helps the information and communications technology industry to have a basis to produce products, to increase the security of network equipment. EUCC is based on ISO/IEC15408 Common Criteria [4] for Information Technology Security Certification, an international framework agreement. The EUCC is based on the ISO/IEC15408 Common Criteria for Information Technology Security Certification. This global framework agreement provides a standard for the assessment and verification of information and communication technology products.

In this paper, we provide an example of a network device router to develop a security target document related to the router according to the Common Criteria framework and propose a functional column that conforms to the Common Criteria framework.

II. RELATED WORK

Cybersecurity is currently an essential issue in the European Union and around the world, and the security of network devices is critical. The European Union's cybersecurity agency has proposed the certification framework to ensure the safety of designed products. It is hoped that the design of information and communication products will comply with this framework. [5]-[7]

A. ENISA [8]

ENISA, the European Network and Information Security Agency, is the European Union's information security agency established to focus on and strengthen the information security of products in the hope of achieving a high level of common network security throughout the EU. To improve network security and establish a common standard-based European network security verification specification for information and communication network products, the EUCC, ENISA has developed a policy and launched a network security

certification scheme to strengthen the credibility of information and communication product technologies and procedures.

B. Common Criteria

The Common Criteria for Information Technology Security Evaluation, mainly ISO/IEC 15408, or simply the Common Criteria (CC), is a series of standards for evaluating and certifying schemes for implementing the security of information technology used in information and communication products to ensure a certain level of assurance and security features are achieved. The Common Criteria provides a framework for information security, with three main sections introducing the Common Criteria Framework, Security Functional Requirements, and Security Assurance Requirements.

- Part 1: Introduction and general model [9]
- Part 2: Security functional requirements [10]
- Part 3: Security assurance requirements [11]

C. Protection Profile

Protection Profile (PP) is a profile of the security requirements of a particular type of information and communication product, basically related to the user's specific use. Protection Profiles are primarily produced for users or groups of users, such as government agencies.

D. Security Target

The Security Target (ST) document is mainly for evaluating specific information technology products. The Common Criteria and Protect Profile are used as references to develop security targets related to information technology products. According to different security assurance levels (EAL), the depth of evaluation and testing are different. After passing the testing and certification, the developer will release the security target to the public so that users can refer to the security characteristics of the certified security target to determine whether users require the product.

E. Related Research

The review of research that has been published in the topic of developing security target is one of the initial analysis stages in this study. The review of research is shown in Table 1.

Table 1. The review of research.

No	Title (year)	Method
1	Development of Protection Profile and Security Target for Indonesia Electronic ID Card's (KTP-el) Card Reader Based on Common Criteria V3.1:2012 / SNI ISO/IEC 15408:2014 [12]	Comparative analysis
2	A Proposal on Security Case Based on Common Criteria [13]	Security structures and threat analysis

3	Security Protection Profile on Smart Card System Using ISO 15408 Case Study: Indonesia Health Insurance Agency [5]	Risk assessment
4	Security Document for Smart Parking Gate based on Common Criteria Framework [7]	Common Evaluation Methodology (CEM)

In the first research, the study uses comparative analysis as the main method to develop a protection profile document. This method works by first creating the original Protection Profile and Security Target and comparing them with Common Criteria workflow guidelines from ISO/IEC 18045:2008.

In research 2 and 3, the researcher uses a similar method to develop a security target which is to use threat analysis and threat assessment, the research focused on analyzing the result of the security objectives and then mapped to threats, and then building security requirements that match with the security objectives.

Another case in research 4 reveals that the researcher uses the Common Evaluation Methodology (CEM), this method is used to evaluate information in the security and information technology field, also this method can be used to help compile Protection Profile (PP) documents in the application of Common Criteria (CC).

From the review of several types of research related to developing security target, it was found that most researcher uses a unique method in each study. Therefore, in this current research, we tried to design a Security Target based on analyzing the gap between regulated networking devices, in this case, the Router as the main foundation to develop a security target document.

III. METHOD

Common Criteria is an international standard framework for evaluating the security of information technology products, mainly introducing protection profiles to develop product-related security target documents. The relationship between Common Criteria (CC), Protection Profile (PP), and Security Target (ST) is shown in the Figure 1.

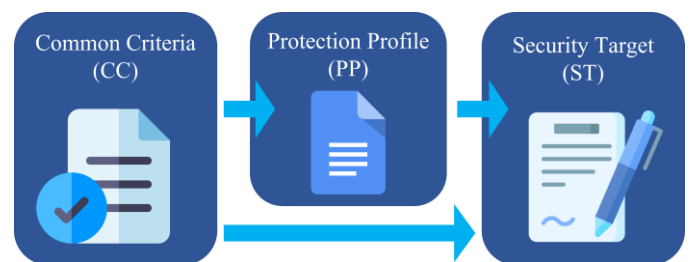


Figure 1. The ST be supported by CC and PP.

The process of developing an ST document is divided into three parts. Take routers as an example of our information technology products. First, we need to define the security problem that the router encounters and the security objectives

that this product needs to achieve. Finally, we need to achieve the required security objectives based on the security requirements in CC and PP as references. The flow chart of the ST is shown in the Figure 2.



Figure 2. The flow chart of the ST.

According to the flow chart of the ST, first, define the security problem. When the developer develops the router product and compiles the ST document, developers must first explicitly define the problems that the router may encounter, such as untrusted communication channels and weak encryption algorithms; all possible security problems should be defined first.

A. Target of Evaluation (TOE)

TOE is a type of information technology product that is evaluated, either as hardware, software, or firmware. The TOE in this study is based on the example of a router, which is a device that transmits two or more network data packet messages.

B. Security Problem

In the security target document, the security problem of TOE should be defined first. The security problem that TOE probably will face is listed in the document, which is usually divided into three categories:

- Threats
- Assumptions
- Organizational Security Polices (OSP)

C. Security Objectives

Security objectives require reference to PP to list the threats that may occur on the router. In this study, the collaborative Protection Profile for Network Devices (cPP-ND) [14] is used as the base PP reference.

D. Security Requirements

Security objectives are defined, and then the next step is the security requirements, which are mainly divided into security function requirements and security assurance requirements.

1) Security Functional Requirement (SFR): A list of security functional requirements based on the security objectives of the threat selection. The required SFR can be found in CC Part 2. The developer can find the functional class first, then the functional family, then the component; from there, the component has the functional elements, and the components are the SFRs. The list of security function requirements class is shown in Table 2. For example, the relevant FAU class, family, components and functional elements are shown in Table 3.

Table 2. Security Functional Requirements Class

Class	Description
FAU	Security Audit
FCO	Communication
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPR	Privacy
FPT	Protection of the TSF
FRU	Resource Utilisation
FTA	TOE Access
FTP	Trusted Path/Channels

Table 3. Security Function Structure

Class	Family	Component	Functional element
FAU	FAU_GEN	FAU_GEN.1	FAU_GEN.1.1

2) Security Assurance Requirement (SAR): Determining the security assurance requirements starts with selecting the assessment assurance level to be achieved. The required EAL table can be found in CC Part 3, and for this study, we select EAL1 and apply it to the router. The list of SARs required for EAL1 is shown in Table 4.

Table 4. The list of SARs required for EAL1.

Class	Component	Description
ASE	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
ADV	ADV_FSP.1	Basic Functional Specification
AGD	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
ALC	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
ATE	ATE_IND.1	Independent testing - conformance
AVA	AVA_VAN.1	Vulnerability analysis

IV. EVALUATION

The third part of the methodology describes how to complete the ST document of an information and communication technology product. The ST document defines the list of requirements the device must meet. However, this section compares all security features of compliant documents to unregulated router products. We compare the security features of non-regulated routers that have not undergone proper protection profiling with the ST documents of compliant routers that have been put together for regulatory compliance. The following document is used as the basis for comparison, as shown below.

1) User Manual Documentation: In the user manual documentation, some routers have essential features and functions built in to provide end users with information on how to use each function properly. Such as functions to enable advanced threat protection, VPN Tunnels, IP Security, and Command Line Interface (CLI) to configure the device functionality. By examining the user manual documentation, we can determine that the router device can do the same function as the device we used for comparison and writing the ST document.

2) SFR List: For router devices, to obtain more explicit information about the device's functionality, a list of security features is listed for comparison using the ST file that conforms to the specification and is associated with the router. The list of SFRs that are compliant and relevant to the router is shown in Table 5.

Table 5. The list of SFRs that are compliant and relevant to the router.

Class	Component	Compliance SFRs/Baseline
FAU	FAU_GEN.1	1/1
	FAU_GEN.2	0/2
	FAU_STG_EXT.1	2/3
FCS	FCS_CKM.1	0/1
	FCS_CKM.1/IKE	0/1
	FCS_CKM.2	1/1
	FCS_CKM.4	1/1
	FCS_COP.1/DataEncryption	1/1
	FCS_COP.1/SigGen	0/1
	FCS_COP.1/Hash	1/1
	FCS_COP.1/KeyedHash	0/1
	FCS_IPSEC_EXT.1	7/14
	FCS_RBG_EXT.1	0/2
	FCS_SSHS_EXT.1	2/8
FIA	FIA_AFL.1	0/2
	FIA_PMG_EXT.1	1/1
	FIA_PSK_EXT.1	3/4
	FIA_UIA_EXT.1	2/2
	FIA_UAU_EXT.2	1/1
	FIA_UAU.7	1/1
	FIA_X509_EXT.1/Rev	0/2
	FIA_X509_EXT.2	2/2
FMT	FMT_X509_EXT.3	0/2
	FMT_MOF.1/ManualUpdate	1/1
	FMT_MOF.1/Services	0/1
	FMT_MOF.1/Functions	1/1
	FMT_MTD.1/CoreData	1/1
	FMT_MTD.1/CryptoKeys	1/1
	FMT_SMF.1	0/1
	FMT_SMF.1/VPN	1/1
FPF	FMT_SMR.2	3/3
	FPF_RUL_EXT.1	6/6
FPT	FPT_APW_EXT.1	0/2
	FPT_FLS.1/SelfTest	0/1
	FPT_SKP_EXT.1	0/1

	FPT_STM_EXT.1	2/2
	FPT_TST_EXT.1	0/1
	FPT_TST_EXT.3	0/2
	FPT_TUD_EXT.1	2/3
FTA	FTA_SSL_EXT.1	1/1
	FTA_SSL.3	0/1
	FTA_SSL.4	1/1
	FTA_TAB.1	0/1
FTP	FTP_ITC.1	0/3
	FTP_ITC.1/VPN	2/3
	FTP_TRP.1/Admin	3/3

The list of SFRs related to routers about the CC framework specification is shown in Table 5. We propose that there are 96 security function requirements related to routers that comply with CC and PP, and the unregulated routers comply with 51 security functions, which means that the unregulated routers have a matching rate of 53.1%.

V. CONCLUSION

With the information and communication technology accompanying our daily life, to make users confident in information and communication products, ENISA has proposed the EUCC international framework agreement, which requires developers to compile relevant security target documents for their products and to comply with Common Criteria and Protect Profile. In this paper, we take an unregulated router as an example, collate the security requirements in the security target document related to the router, analyze the gap between the standard and the unregulated router, and find that the unregulated router has a 53.1% match rate. Many security requirements can be added and considered to make the router more secure.

Products developed under the Common Criteria framework assure consumers that the product has been developed and designed with international certifications, which gives consumers confidence. In the future, there will be many security threats and new security regulations, and developers should update the Security Target document to address future security issues.

ACKNOWLEDGMENT

Thanks to the ITRI (Industrial Technology Research Institute), Taiwan, for providing the security assessment criteria for information technology, Part 1 to Part 3, for our study and reference. This work was supported in part by the Department of Industrial Technology (DoIT) under the Ministry of Economic Affairs (MoEA) : The Application and Industrial Development of Sports Science and Technology. Under Grant 111-EC-17-D-11-1832.

REFERENCES

- [1] Internet usage worldwide - Statistics & Facts. The Statista website. [Online]. Available: <https://www.statista.com/topics/1145/internet-usage-worldwide/>, Oct 18, 2022.
- [2] Alissa Irei "Definition Router," The SeachNetworking website, [Online]. Available:

- <https://www.techtarget.com/searchnetworking/definition/router>, 26 October 2022.
- [3] Mandate and Regulatory Framework. The ENISA EUROPEAN UNION AGENCY FOR CYBERSECURITY website. [Online]. Available: <https://www.enisa.europa.eu/>, 2022.
 - [4] About The Common Criteria. The Common Criteria website. [Online]. Available: <https://www.commoncriteriaportal.org/ccra/index.cfm>, 2022.
 - [5] Y. A. Setyoko and R. Yasirandi, "Security Protection Profile on Smart Card System Using ISO 15408 Case Study: Indonesia Health Insurance Agency," 2018 6th International Conference on Information and Communication Technology (ICoICT), pp. 425-428, 2018.
 - [6] G. Bréda, P. J. Varga and Z. Illési, "Forensic Functional Profile of IoT Devices-Based on Common Criteria," 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), pp. 000261-000264, 2018.
 - [7] R. Yasirandi, Y. A. Setyoko and P. Sukarno, "Security Document for Smart Parking Gate based on Common Criteria Framework," 2019 7th International Conference on Information and Communication Technology (ICoICT), pp. 1-8, 2019.
 - [8] Cybersecurity Certification EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, ENISA, V1.1.1, May, 2021.
 - [9] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 5, April, 2017.
 - [10] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 5, April, 2017.
 - [11] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 5, April, 2017.
 - [12] M. E. Aminanto and S. Sutikno, "Development of protection profile and security target for Indonesia electronic ID card's (KTP-el) card reader based on common criteria V3.1:2012/SNI ISO/IEC 15408:2014," 2014 International Conference of Advanced Informatics: Concept, Theory and Application (ICAICTA), pp. 1-6, 2014.
 - [13] Yamamoto, S., Kaneko, T., Tanaka, H. "A Proposal on Security Case Based on Common Criteria," In: Mustofa, K., Neuhold, E.J., Tjoa, A.M., Weippl, E., You, I. (eds) Information and Communication Technology. ICT-EurAsia. Lecture Notes in Computer Science, vol 7804, 2013.
 - [14] Collaborative Protection Profile for Network Devices, Version 2.2e, May 23, 2020.