A Proposal on Security Case Based on Common Criteria

Shuichiro Yamamoto, Tomoko Kaneko, Hidehiko Tanaka

A Proposal on Security Case based on Common Criteria

Shuichiro Yamamoto[1], Tomoko Kaneko[2], and Hidehiko Tanaka[3]

[1]Nagoya University
syamamoto@acm.org
[2]NTT DATA CORPORATION
knktmk204th@gmail.com
[3]Institute of Information Security
tanaka@iisec.ac.jp

Abstract. It is important to assure the security of systems in the course of development. However, lack of requirements analysis method to integrate security functional requirements analysis and validation in upper process often gives a crucial influence to the system dependability. For security requirements, even if extraction of menaces was completely carried out, insufficient countermeasures do not satisfy the security requirements of customers.
In this paper, we propose a method to describe security cases based on the security structures and threat analysis. The security structure of the method is decomposed by the Common Criteria (ISO/IEC15408).

Key Words: Security Case, Security Requirements Analysis, Common Criteria

1 Introduction

It is important to show how a request such as “The system is acceptably secure” is supported by objective evidence for customers. We show the description method by using Assurance Case and Common Criteria as the objective evidence.

In Chapter 2 “Related work,” we explain assurance case [1-4] and security case approaches [6-8], as well as an overview of common criteria (CC) [5]. In Chapter 3, we show security case reference patterns based on CC. In Chapter 4, some considerations on the method are described. Chapter 5 explains future issues.

2 Related work

2.1 Assurance case

Security case is an application of Assurance case, which is defined in ISO/IEC15026 part 2. Security cases are used to assure the critical security levels for target systems. Standards are proposed by ISO/IEC15026 [2] and OMG’s Argument Metamodel

(ARM) and [3] Software Assurance Evidence Metamodel (SAEM) [4]. ISO/IEC 15026 specifies scopes, adaptability, application, assurance case's structure and contents, and deliverables. Minimum requirements for assurance case's structure and contents are: to describe claims of system and product properties, systematic argumentations of the claims, evidence and explicit assumptions of the argumentations; to structurally associate evidence and assumptions with the highest-level claims by introducing supplementary claims in the middle of a discussion. One common notation is Goal Structuring Notation (GSN) [1], which widely used in Europe for about ten years to verify system security and validity after identifying security requirements.

2.2 Security case

Goodenough, Lipson and others proposed a method to create Security Assurance case [6]. They described that the Common Criteria provides catalogs of standard Security Functional Requirements and Security Assurance Requirements. They decomposed Security case by focusing on the process, such as requirements, design, coding, and operation. The approach did not use the Security Target structure of the CC to describe Security case.

Alexander, Hawkins and Kelly overviewed the state of the art on the Security Assurance cases [7]. They showed the practical aspects and benefits to describe Security case in relation to security target documents. However they did not provide any patterns to describe Security case using CC.

Kaneko, Yamamoto and Tanaka recently proposed a security countermeasure decision method using Assurance case and CC [8]. Their method is based on a goal oriented security requirements analysis [9-10]. Although the method showed a way to describe security case, it did not provide Security case graphical notations and the seamless relationship between security structure and security functional requirements.

2.3 Common criteria

Common Criteria (CC: equivalent to ISO/IEC15408) [5] specifies a framework for evaluating reliability of the security assurance level defined by a system developer. In Japan, the Japan Information Technology Security Evaluation and Certification Scheme (JISEC) is implemented to evaluate and authenticate IT products (software and hardware) and information systems. In addition, based on CC Recognition Arrangement (CCRA), which recognizes certifications granted by other countries' evaluation and authorization schemes, CC accredited products are recognized and distributed internationally. As an international standard, CC is used to evaluate reliability of security requirements of functions built using IT components (including security functions). CC establishes a precise model of Target of Evaluation (TOE) and the operation environment. And based on the security concept and relationship of assets, threats, and objectives, CC defines ST (Security Target) as a framework for evaluating TOE's Security Functional Requirement (SFR) and Security Assurance Requirement (SAR). ST is a document that accurately and properly defines security functions

implemented in the target system and prescribes targets of security assurance. ST is required for security evaluation and shows levels of adequacy in TOE's security functions and security assurance.

3 Security case reference patterns

3.1 Issues to describe Security case

Product and process are both important to assure system security. In this paper we propose a hierarchical method to describe Security case. We decompose Security case based on Security Target structure in the upper part. And then we describe bottom part of the Security case based on security analysis process.

3.2 Security case based on Security Target structure

Fig.1. describes an example pattern for Security case based on CC.

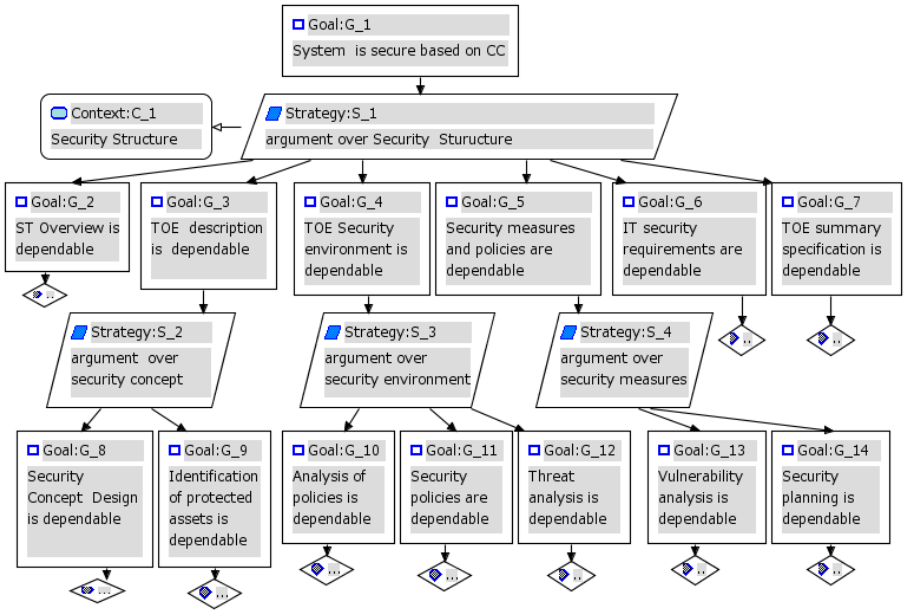

Fig.1. Security case pattern for CC based Security Structure

The figure shows the Security Target structure and security analysis process consists of the two decomposition layers. In the first decomposition, ST overview, TOE description, TOE security environment, Security measures and policies, IT security requirements, and TOE summary specification are described. For each decomposed

claim, arguments are also attached to decompose it by security analysis process. For example, to assure the dependability of the TOE security environment, the security analysis process is decomposed by three claims, i.e., Analyzing protection policies, Clarifying security policies, and threat analysis.

3.3 Security case to assure security requirements against threats

Fig.2. describes security case to assure security functional requirements. It consists of the following hierarchical layers, Threats category, Activity of threats, and Security function layers. The security case can be considered as the decomposition of the claim G_6 in Fig.1.

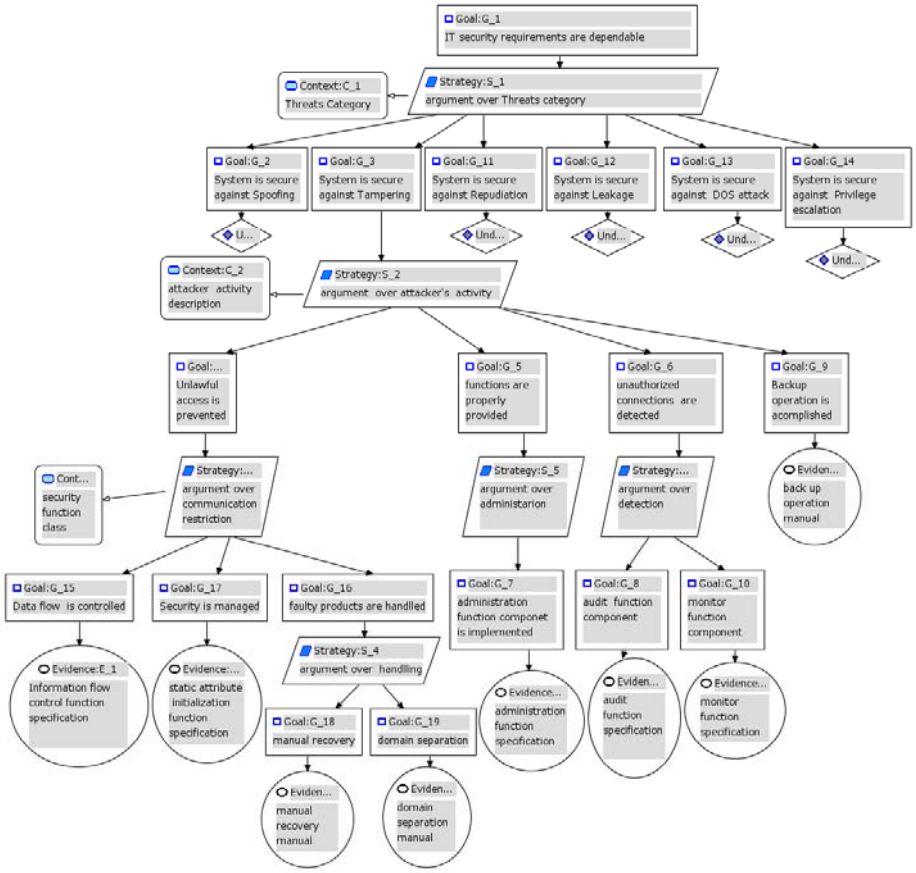

Fig.2. Security case pattern for security function specification based on CC

The sample case is created based on PP [13] provided by IPA (Information-technology Promotion Agency) and is not the example of actual specific system. Thus, the sample case should be regarded as a reference model of Security case.

4 Considerations

Describing Security case according to ST structure of CC has an advantage in validating objective assurance levels based on an international standard notation. It is possible to properly define and implement security functions in line with ST structure and appropriate threat analysis. We also can implement negotiated security functions based on structured way of Security case and international standardized terminologies in CC of catalogued security function levels.

The relationship between security structure of CC and Security case structure is mandatory for compatibility. As shown in the examples of section 3, the Security case structure is seamlessly correspondent to CC.

We also confirmed a way to integrate Security cases between Security Target structure and Security functional requirements as shown in the goal relationship of two figures.

5 Future issues

There are some unsolved issues in security case development presented in this paper.

Our study is still in a preliminary phase and further evaluation needs to be done in future. It is necessary to evaluate the proposed method for designing actual system development. The proposed approach provides a reference Security case structure. Therefore, it can also be used to effective validation of the target systems compatibility to CC. This kind of application of our method will provide a simple integration process between security design and validation.

We also have a plan to develop Security case patterns based on this paper. This will ease to reuse Security cases based on CC. This research is an extension of Safety case pattern proposed by Kelly and McDermid [11].

In terms of CC based security requirement analysis, goal oriented methods and use-case based methods are proposed [12]. Therefore, it is desirable to verify effectiveness of our method by comparing our method with these methods.

6 References

1. Kelly, T. & Weaver, R., The Goal Structuring Notation – A Safety Argument Notation, Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases(2004)
2. ISO/IEC15026-2-2011,Systems and Software engineering-Part2:Assurance case
3. OMG, ARM, http://www.omg.org/spec/ARM/1.0/Beta1/
4. OMG, SAEM, http://www.omg.org/spec/ SAEM/1.0/Beta1/
5. Common Criteria for Information Technology Security Evaluation, http://www.commoncriteriaportal.org/cc/
6. Goodenough, J., Lipson, H., and Weinstock, C., Arguing Security - Creating Security Assurance Cases, https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/assurance/643-BSI.html(2007)

7. Alexander, T., Hawkins, R., and Kelly, T., Security Assurance Cases: Motivation and the State of the Art, CESG/TR/2011 (2011)
8. Kaneko, T., Yamamoto, S., Tanaka, H., Proposal on Countermeasure Decision Method Using Assurance Case And Common Criteria, ProMAC 2012(2012)
9. Kaneko, T., Yamamoto, S., Tanaka, H., SARM -- a spiral review method for security requirements based on Actor Relationship Matrix ,ProMAC2010, P1227-1238 (2010)
10. Kaneko, T., Yamamoto, S., Tanaka, H., Specification of Whole Steps for the Security Requirements Analysis Method (SARM)- From Requirement Analysis to Countermeasure Decision - ,ProMAC2011(2011)
11. Kelly, T. and McDermid, J A, *Safety Case Construction and Reuse using Patterns*, in Proceedings of 16th International Conference on Computer Safety, Reliability and Security (SAFECOMP'97), Springer-Verlag, September(1997)
12. Saeki, M., Kaiya, H., Security Requirements Elicitation Using Method Weaving and 3 Common Criteria, Lecture Notes in Computer Science, Volume 5421/2009, 185-196, DOI:0.1007/978-3-642-01648-6_20(2009)
13. http://www.ipa.go.jp/security/fy13/evalu/pp_st/pp_st.html