A Study on Information Wrapper Protection Profile

Kwo-Jean Farn [a], Shu-Kuo Lin [a], Jiann-Ming Hwang [a, b]
[a] Institute of Information Management, National Chiao-Tung University, Taiwan
[b] Computer Science & Information Engineering, Ming-Chuan University, Taiwan

Abstract: - How to help the end-users to identify and analyze the attacks in cyberspace has become extremely important to the information security task. Based on the standard of the Information Security Audit and Alarms Framework published by ISO, in this paper we intend to investigate the security functional and security assurance requirements of the so-called Information Wrapper. Besides, in this paper we also propose a draft Protection Profile (PP) of Information Wrapper. The draft has been registered in the Chinese National Laboratory Accreditation (CNLA) as the security specification of relevant products and/ or systems.

Keywords: Common Criteria (CC), Protection Profile (PP), Information Security Audit and Alarms, Security Assurance, Security Functional

1. Introduction

On February 5, 2001, the Executive Yuan of Republic of China (R.O.C) sent out the "Plan for Establishing the Construction of Basic Information and Communication Security Mechanisms in Taiwan" to each of its subordinate authorities, requesting active cooperation [1]. That's how a brand new era of information security began in Taiwan. To embrace the global e-trend and head on with all the challenges that are overclouding the future of Taiwan's IT industry - the impact of global knowledge based economy, out-moving business and decreasing total revenue, the National Information & Communication Initiative (NICI) of the Executive Yuan has formulated a plan "e-Taiwan project" to counter all these issues. The "e-Taiwan project" has been formally approved by the Executive Yuan in June of 2002 and is further combined with nine other plans to form the so-called "Challenge 2008: the 6-Year National Development Plan" [2].

There are five integral parts in this plan, e.g., '6 million broadband users', 'ez Life', 'e-Industry', 'e-Government' and 'e-Transportation'. The "Plan for Establishing the Information Security Product Certification and Accreditation Scheme in Taiwan" is one of the 'ez Life' sub-plan, and hopes to reach the vision "information and communication network resources can be fully used in an obstacle free and secure environment by year 2008." [3].

The information systems in the cyberspace offer attractive targets. Therefore, they should be resistant to such as Passive, Active, Close-in, Insider, and Distribution attacks from the full range of threat-agents -- from hackers to nation states -- and they must limit damage and recover rapidly when attacks do occur [4].

The management of information security must take the following three phases into consideration -- the secure management of information asset (ISO/IEC TR 13335, ISO 19011, ISO/IEC 17799, ISO/IEC 27001), the security functional and assurance of information techniques to prevent from attack and threat (ISO/IEC 15408, ISO/IEC 17025, ISO/IEC 18045), and the security assurance of vulnerability caused by the exposure of incomplete information weakness in the operational process (ISO/IEC 15408, ISO/IEC TR 15443, ISO/IEC TR 19791). Based on those three phases, in this paper we intended to investigate the security requirements that the Security Audit and Alarms [4-6] ought to possess to protect its vulnerability. Furthermore, in Section 2, and Section 3, we respectively explored the security infrastructure of the Information Security Audit and Alarms [4-6], and proposed Draft of Security Audit and Alarms Protection Profile (so-called "Information Wrapper Protection Profile (IWPP)") [6-8]. Finally, in Section 4, we concluded this paper.

2. Security Framework for Information System Audit & Alarms

Information System Audit & Alarms is a kind of complex conclusion that includes the accountability of active, passive and insider attacks, feature extraction, response, and special non-repudiation. The techniques of Audit & Alarms are based on the development of audit log, anti-virus, and the intrusion detection, which results in robustness nowadays. Although the techniques are still improving, the field remains to depend on the high stuff of operations and analysts.

A generic model of intrusion detection [9] can be defined by a set of functions. These functions include: raw data sourcing, event detection, analysis, data storage, and response. These functions can be implemented by separate components or be software packages as part of a larger system. The following Fig. 2.1 [9] shows the manner in which these functions relate to each other.

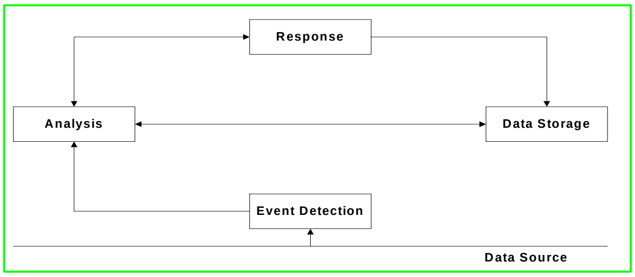

Fig. 2.1: Generic Model of Intrusion Detection [9]

To implement an Information System Audit & Alarms mechanism, the following should be taken into consideration [8]:

- What are the security-related events of Audit and Alarms? What are the detected security-related events?
- How to protect, analyze and report the security-related events of Audit and Alarms?
- What is the response policy to the analysis and report of the Audit and Alarms information?

The functional architecture of Information System Audit & Alarms is indicated in Fig. 2.2. The architecture of Fig. 2.2 could be set up in any network node, when supporting Network operation, Forensic subsystem, Alarm processing subsystem, Audit log reporting subsystem, and supplying subsystem. Among them, the service provided by audit architectures, information sharing, and analysis subsystem is so-called "Information Sharing and Analysis Center (ISAC)". The following phrases may occur in audit procedures [6, 9]:

- Detection Phase: in which a security-related event is detected.
- Discrimination Phase: in which an initial determination is made as to whether it is necessary to record the event in the security audit trail or to raise an alarm.
- Alarm Processing Phase: in which a security alarm or security audit message may be issued.
- Analysis Phase: in which a security-related event is evaluated together with, and in the context of, previously detected events as logged in the audit trail, and a course of action determined.
- Aggregation Phase: in which distributed security audit trail records are collected into a single security audit trail.
- Report Generation Phase: in which audit reports are built from security audit trail records; and
- Archiving Phase: in which records from the security audit trail are transferred to the security audit trail archive. The storage used for archiving must maintain the confidentiality, integrity, and availability of the original records.

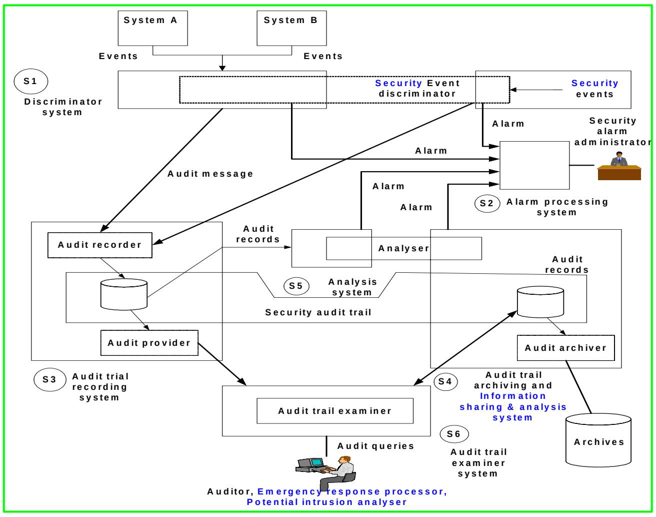

Fig. 2.2: An example of realization of Audit & Alarms service

3. Draft of Information Security Audit & Alarms Protection Profile (ISAAPP)

The objectives of Common Criteria (CC) (ISO/IEC 15408) aim to provide the criteria for security evaluation of information techniques so as to offer the assurance of reliable basis. CC is required to enhance the width, depth, and strength of the security evaluation of the foregoing IT, and to investigate the effectiveness of IT products or system security testing. As shown in Fig. 3.1, Protection Profiles (PP) provide users a way to refer to given security requirements so as to make it easier for the users to process the evaluating tasks (shown in Fig. 3.2) of the requirements [10-11].

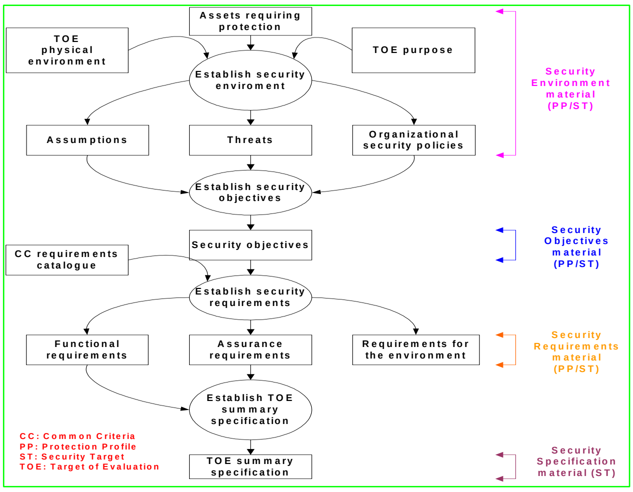
Assets requiring protection
TOE physical environment
TOE purpose
Establish security enviroment
Assumptions
Threats
Organizational security policies
Establish security objectives
Security objectives
CC requirements catalogue
Establish security requirements
Functional requirements
Assurance requirements
Requirements for the environment
Establish TOE summary specification
TOE summary specification
Security Environment material (PP/ST)
Security Objectives material (PP/ST)
Security Requirements material (PP/ST)
Security Specification material (ST)
CC: Common Criteria
PP: Protection Profile
ST: Security Target
TOE: Target of Evaluation

Fig. 3.1: Derivation of requirements and specification

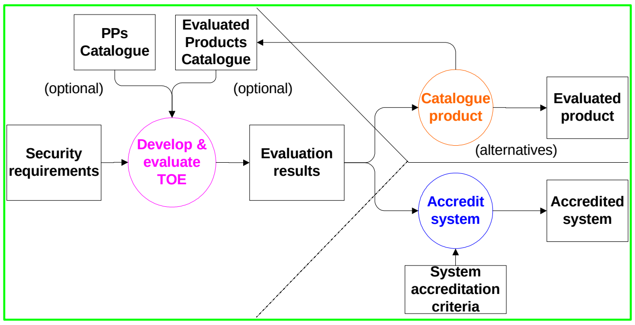

Fig. 3.2: Use of TOE evaluation results

3.1 Security Environment

3.1.1 Threats

The ISAAPP has derived all security objectives from the statement of Organizational Security Policy. After we compare the Controlled Access Protection Profile (CAPP) [12] with the Threats to Security of Windows 2000 Security Target (ST) [13], and Intrusion Detection System (IDS) related PP [14], the threats that the ISAAPP might encounter can be specified as follows (NOTES: Owing to the page limitation, in Section 3 we omit all the detailed description of Threats, Policies, Assumptions, Objectives, Rationale, etc.): **T.AUDIT_CORRUPT, T.CONFIG_CORRUPT, T.DENIAL_MALWARE, T.OBJECTS_NOT_CLEAN, T.SPOOF, T.SYSACC, T.UNAUTH _ACCESS, T.UNAUTH _MODIFICATION, T.UNDETECTED_ACTIONS, T.USER_CORRUPT**

3.1.2 Organizational Security Policies

An Organizational Security Policy is a set of rules or procedures imposed by an organization upon its operations to protect its sensitive data. The organizational security policies described below are addressed by ISAAPP: **P.ACCOUNTABILITY, P.ADD_IPSEC, P.AUTHORIZATION, P.AUTHORIZED_USERS, P.NEED_TO_KNOW, P.WARN**

3.1.3 Security Usage Assumptions

An ISAAPP-conformant TOE is assured to provide effective security measures in a cooperative non-hostile environment only if it is installed, managed, and used correctly. The operational environment must be managed in accordance with assurance requirements documentation for delivery, operation, and user/administrator guidance. The following specific conditions are assumed to exist in an environment where ISAAPP-conformant TOEs are employed.

3.1.3.1 Physical Assumptions

ISAAPP-conformant TOEs are intended for application in user areas that have physical control and monitoring. It is assumed that the following physical conditions will exist: **A.LOCATE, A.PROTECT**

3.1.3.2 Personnel Assumptions

It is assumed that the following personnel conditions will exist: **A.COOP, A.MANAGE, A.NO_EVIL_ADM**

3.1.3.3 Connectivity Assumptions

The ISAAPP contains no explicit network or distributed system requirements. However, it is assumed that the following connectivity conditions exist: **A.CONNECT, A.PEER**

3.2 Security Objectives

3.2.1 IT Security Objectives

The following are the ISAAPP IT security objectives: **O.ALERT, O.AUDITING, O.AUDIT_PROTECTION, O.AUTHORIZATION, O.DENIAL_MALWARE, O.DISCRETIONARY_ACCESS, O.ENCRYPTED_DATA, O.ENFORCEMENT, O.IPSEC, O.LEGAL_WARNING, O.LIMIT_AUTHORIZATION, O.MANAGE, O.PROTECT, O.RESIDUAL_INFORMATION,**

O.TRUSTED_PATH

3.2.2 Non-IT Security Objectives

The TOE is assumed to be complete and self-contained and, as such, is not dependent upon any other products to perform properly. However, certain objectives with respect to the general operating environment must be met. The following are the ISAAPP Non-IT Security Objectives: **O.CREDEN, O.INSTALL, O.PHYSICAL**

3.3 Rationale

3.3.1 Security Objectives Rationale

Each objective counters or addresses at least one assumption, organizational security policy, or threat. Table 3.1 and Table 3.2 present the mapping of objectives to the security environment.

Table 3.1: IT Security Objectives Rationale Mapping

IT Security Objectives	Threats and Organizational Policies
O.ALERT	T.UNDETECTED_ACTIONS P.ACCOUNTABILITY P.AUTHORIZED_USERS P.NEED_TO_KNOW
O.AUDITING	T.UNDETECTED_ACTIONS P.ACCOUNTABILITY
O.AUDIT_PROTECTION	T.AUDIT_CORRUPT
O.AUTHORIZATION	T.SYSACC T.UNAUTH_ACCESS P.AUTHORIZED_USERS
O.DENIAL_MALWARE	T.DENIAL_MALWARE
O.DISCRETIONARY_ACCESS	T.USER_CORRUPT P.NEED_TO_KNOW
O.ENCRYPTED_DATA	T.USER_CORRUPT T.UNAUTH_ACCESS
O.ENFORCEMENT	P.ADD_IPSEC P.ACCOUNTABILITY P.AUTHORIZED_USERS P.NEED_TO_KNOW
O.IPSEC	P.ADD_IPSEC
O.LEGAL_WARNING	P.WARN
O.LIMIT_AUTHORIZATION	P.AUTHORIZATION
O.MANAGE	P.ACCOUNTABILITY P.AUTHORIZED_USERS P.NEED_TO_KNOW
O.PROTECT	T.CONFIG_CORRUPT T.UNAUTH_ACCESS T.UNAUTH_MODIFICATION T.USER_CORRUPT
O.RESIDUAL_INFORMATION	T.OBJECTS_NOT_CLEAN P.NEED_TO_KNOW
O.TRUSTED_PATH	T.SPOOF

Table 3.2: Non-IT Security Objectives Rationale Mapping

Non-IT Security Objectives	Environmental Assumptions
O.CREDEN	A.COOP
O.INSTALL	A.MANAGE A.NO_EVIL_ADM A.PEER
O.PHYSICAL	A.CONNECT A.LOCATE A.PROTECT

3.3.2 Security Requirements Rationale

3.3.2.1 Internal Consistency of Requirements

The functional components were selected from pre-defined CC components. The use of component refinement was accomplished in accordance with CC guidelines [15]. An additional component was included to clarify the relationship of objects and security attributes.

Assignment, selection, and refinement operations were carried out among components using consistent computer security terminology. This helps to avoid the ambiguity associated with interpretations of meanings of terms between related components.

Multiple instantiation of identical or hierarchically-related components was used to clearly state the required functionality that must exist in a TOE conformant with this profile.

3.3.2.2 Complete Coverage - Objectives

The Functional Components selected for this profile provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the Table 3.3.

Table 3.3: Requirement to Security Objective Correspondence

Requirement	O.ALERT	O.AUDITING	O.AUDIT PROTECTION	O.AUTHORIZATION	O.DENIAL MALWARE	O.DISCRETIONARY ACCESS	O.ENCRYPTED DATA	O.ENFORCEMENT	O.IPSEC	O.LEGAL WARNING	O.LIMIT AUTHORIZATION	O.MANAGE	O.PROTECT	O.RESIDUAL INFORMATION	O.TRUSTED PATH
FAU_GEN.1		X													
FAU_GEN.2		X													
FAU_SAR.1		X										X			
FAU_SAR.2		X													
FAU_SAR.3		X										X			
FAU_STG.1		X	X												
FAU_STG.3		X										X			
FAU_STG.4		X	X									X			
FCS_COP.1							X								
FDP_ACC.1						X									
FDP_ACC.2					X										
FDP_ACF.1						X									
FDP_IFC.2					X										
FDP_IFF.5					X										
FDP_RIP.2														X	
Note1_EX														X	
FIA_AFL.1				X											
FIA_ATD.1				X		X					X				
FIA_SOS.1				X											
FIA_UAU.2				X											
FIA_UAU.7				X											
FIA_UID.2				X											
FIA_USB.1_EX		X				X									
FMT_MOF.1				X					X			X			
FMT_MSA.1						X						X			
FMT_MSA.3						X						X			
FMT_MTD.1		X		X						X		X	X		
FMT_MTD.2				X								X			
FMT_REV.1						X					X	X			
FMT_SAE.1				X								X			
FMT_SMR.1											X	X			
FMT_SMR.3												X			
FPT_ITC.1	X														
FPT_ITI.1	X														
FPT_ITI.2	X														
FPT_RVM.1	X							X							
FPT_SEP.1	X							X					X		
FPT_STM.1		X													
FPT_TST.1	X														
REPLICATION_EX												X			
TRANSFER_PROT_EX									X				X		
FRU_RSA.1				X											
BANNERS_EX										X					
FTA_SSL.1				X											
FTA_SSL.2				X											
FTA_TSE.1				X											
FTP_TRP.1															X

3.4 Dependencies

The Table 3.4 shows the dependencies which exist. A box with an “X” in it indicates a dependency which has been satisfied. A box with an “O” in it indicates an optional dependency where one of the options has been satisfied.

Table 3.4: Dependency Rationale Mapping

CC Identifier	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FAU_STG.2	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_IFC.1	FDP_IFF.1	FDP_ITC.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	TRANSFER_PROT	FMT_MTD.1	FMT_SMR.1	FPT_STM.1
FAU_GEN.1																					X
FAU_GEN.2	X													X							
FAU_SAR.1	X																				
FAU_SAR.2		X																			
FAU_SAR.3		X																			
FAU_STG.1	X																				
FAU_STG.3			X																		
FAU_STG.4			X																		
FCS_COP.1					O	X					O					X					
FDP_ACC.1								X													
FDP_ACC.2								X													
FDP_ACF.1							X										X				
FDP_IFC.2										X											
FDP_IFF.5									X												
FDP_RIP.2																					
Note 1_EX																					
FIA_AFL.1													X								
FIA_ATD.1																					
FIA_SOS.1																					
FIA_UAU.2														X							
FIA_UAU.7													X								
FIA_UID.2																					
FIA_USB.1_EX												X									
FMT_MOF.1																				X	
FMT_MSA.1							O		O											X	
FMT_MSA.3															X					X	
FMT_MTD.1																				X	
FMT_MTD.2																			X	X	
FMT_REV.1																				X	
FMT_SAE.1																				X	X

CC Identifier	FAU GEN.1	FAU SAR.1	FAU STG.1	FAU STG.2	FCS CKM.1	FCS CKM.4	FDP ACC.1	FDP ACF.1	FDP IFC.1	FDP IFF.1	FDP ITC.1	FIA ATD.1	FIA UAU.1	FIA UID.1	FMT MSA.1	FMT MSA.2	FMT MSA.3	TRANSFER PROT	FMT MTD.1	FMT SMR.1	FPT STM.1
FMT_SMR.1														X							
FMT_SMR.3																				X	
FPT_ITC.1																					
FPT_ITI.1																					
FPT_ITI.2																					
FPT_RVM.1																					
FPT_SEP.1																					
FPT_STM.1																					
FPT_TST.1																					X
REPLICATION_EX																		X			
TRANSFER_PROT_EX																			X		
FRU_RSA.1																					
BANNERS_EX																			X		
FTA_SSL.1													X								
FTA_SSL.2													X								
FTA_TSE.1																					
FTP_TRP.1																					

3.5 Rationale for Assurance Rating

This PP has been developed for a generalized environment with a moderate level of risk to the assets. It is intended that products used in these environments will be generally available, without modification to meet the security needs of the environment. As such it was determined the Evaluation Assurance Level (EAL) 4 was the most appropriate [8].

4. Conclusion

In this paper, according to the essential security requirements for the Wrapper to fight against the specialized opponents, we propose the PP of Information Security Audit & Alarms products as the reference for investigating the security specification of relevant products.

In our country, people begin to concern the relevant concepts of CC. But due to the little time and experience, we are probing for the value, concept and systems that need to be established. Furthermore, the CC 3.1 & Common Methodology for Information Technology Security Evaluation (CEM) 3.1 [16] will be announced in 2007, which will provide the new guidelines for further research.

Acknowledgements

The authors would like to express our appreciation to Mr. Kung-Yu Lu for his invaluable help.

References

[1] The Executive Yuan of Republic of China (R.O.C), February 5, 2001 (90) MOE document no. 007431, 2001, Taipei, Taiwan.

[2] http://www.cepd.gov.tw/2008/challenge2008.pdf (2004-10-10).

[3] http://www.nicst.nat.gov.tw/template/nics/content.pdf, (2004-08-01).

[4] National Security Agency, Information Assurance Technical Framework, Release 3.1, September 2002.

[5] Sherwood, J.E., The Security Certification Criteria Project, Proceedings of the 3rd International Common Criteria Conference, May 13~14, 2002, Ottawa, Canada.

[6] ISO, Information technology - Open Systems Interconnection - Security Frameworks for Open System: Security Audit and Alarms Framework, ISO/IEC 10181-7:1996.

[7] Katake, S., Protecting Federal Information Systems and Networks, Proceedings of the 4th International Common Criteria Conference, Sept. 7~9, 2003, Stockholm, Sweden.

[8] ISO, Information technology - Security techniques - Evaluation Criteria for IT Security (All parts), ISO/IEC 15408:2005(E).

[9] ISO, Information technology - Security techniques - IT Intrusion Detection Framework, ISO/IEC TR 15947:2002(E).

[10] ISO/IEC, Information technology - Security techniques - Guide for the Production of Protection Profiles and Security Targets, ISO/IEC TR 15446:2004(E).

[11] Herrmann, D. S., Using the Common Criteria for IT Security Evaluation, Auerbach Publications, 2003.

[12] http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.pdf, (2007-02-02).

[13] http://niap.nist.gov/cc-scheme/st/ST_VID4002-ST.pdf, (2007-02-02).

[14] http://www.commoncriteriaportal.org/public/consumer/index.php, (2007-02-02).

[15] http://www.commoncriteriaportal.org/public/files/ccusersguide.pdf, (2007-02-02).

[16] http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2 (2007-02-02).