

A Study on Protection Profile -- Illustration of ISAAPP

Kwo-Jean Farn^a, Shu-Kuo Lin^a, Jiann-Ming Hwang^{a, b}

Abstract—In order to reach the vision “information and communication network resources can be fully used in an obstacle free and secure environment by year 2008,” TTC (Telecommunication Technology Center), a Taiwan government-funded organization, has been granted the accreditation certificate by Taiwan Accreditation Foundation (TAF) on November 15, 2005. TTC will construct a Common Criteria Testing Laboratory (CCTL) and anticipate participating in the Common Criteria Recognition Arrangement (CCRA) in a few years. In this paper we briefly introduce the recent development of CCTL in Taiwan. Furthermore, based on the standard of the Security Audit and Alarms Framework (ISO/IEC 10181-7:1996), in this paper we intend to investigate the security functional and security assurance requirements; we also propose a draft Protection Profile (PP) of ISAAPP. 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

I. INTRODUCTION

The advent of the Common Criteria (CC) for Information Technology Security Evaluation marks a significant milestone for the security community. CC is an important tool for ensuring that not only do we have truly global standards for certifying commercial software products, but that these bring real benefits for both commercial suppliers and end users in both government and the public sector. Commercial suppliers only need certification once to make their products acceptable to any member country. It cuts costs. For the end users there are also more choices. It cuts down on confusion between different schemes and makes life simpler. As the demand on trust and security in society grow, more information will be needed at all levels in society; in interest organizations (consumers, standardization, trade), governmental bodies, regulatory authorities as well as in education and training. In summary, internationally accepted criteria for IT security has and will have a major impact on the

whole security infrastructure in society- not only on a national level but world wide.

Based on CC, ISO/IEC 15408, ISO/IEC 18045, ISO/IEC 17025, international standards and guidelines, Telecom Technology Center (TTC) Information & Communication Security Testing Laboratory has been granted the accreditation certificate by Taiwan Accreditation Foundation (TAF) on November 15, 2005. This laboratory is also the first security testing/ evaluation laboratory which is accredited according to ISO/IEC 17025:2005 and ISO/IEC 15408 in Taiwan. Meanwhile, TTC also be cooperating with famous IT security product organizations for potential business. TTC has endeavored to provide the best service on testing equipments and instruments in the IT testing Lab. Furthermore, TTC will construct a Common Criteria Testing Laboratory (CCTL) and anticipate participating in the Common Criteria Recognition Arrangement (CCRA) in a few years [1-3].

TTC is in charge of technical affairs including telecommunication, broadcasting and information security. The supervision institute should be National Communication Committee (NCC), similar to Federal Communication Committee in USA. The CC conformity assessment scheme of TTC is shown in Fig. 1.1; besides, the CC evaluation and certification scheme of TTC is shown in Fig. 1.2. The first pilot target testing product will be smart card. TTC CCTL should seek help from some accredited foreign CCTL to perform a sample test for smart card and a mirror test after the sample test is performed. Then, the second target will be firewall. TTC wants to make the CCTL accredited by CCRA in two or three years. However, local certificates in Taiwan could be issued earlier before the CCRA. Basically, TTC wants to increase the competing ability of Taiwan information products in the world trade markets. Since Taiwan information products including wired and wireless communication devices, network equipments, notebooks and personal computers play an important role in the international market, the CCTL construction by TTC will make a tremendous influence in the popularity of Common Criteria Testing and Certificate in the IT industry [1-3].

Manuscript received May 17, 2007; Revised Received October 30, 2007

Kwo-Jean Farn: Institute of Information Management, National Chiao-Tung University, Taiwan (e-mail: kjf@iim.nctu.edu.tw).

Shu-Kuo Lin: Institute of Information Management, National Chiao-Tung University, Taiwan (corresponding author, Tel: +886 3 5712301; Fax: +886 3 5723792; e-mail: kuo@iim.nctu.edu.tw).

Jiann-Ming Hwang: Computer Science & Information Engineering, Ming-Chuan University, Taiwan (e-mail: jmhawang@mcu.edu.tw).

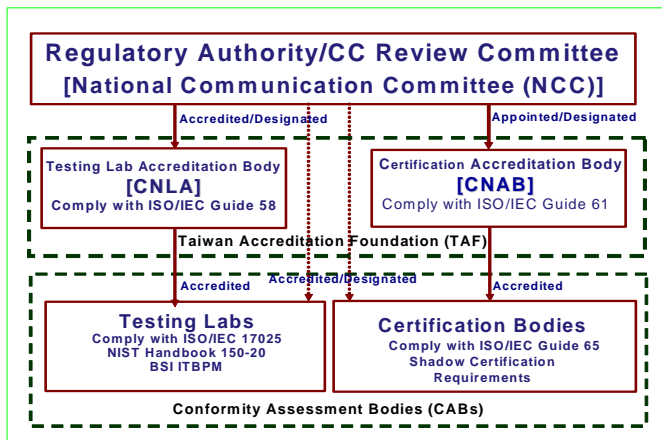


Fig. 1.1: Common Criteria Conformity Assessment Scheme in Taiwan

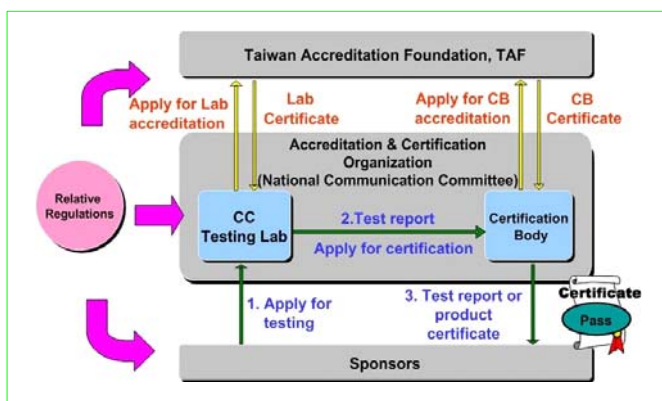


Fig. 1.2: Common Criteria Evaluation and Certification Scheme in Taiwan

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 intend to investigate the security requirements that the Information Security Audit and Alarms need to possess to protect its vulnerability [4-6]. Furthermore, in Section 2, and Section 3, we respectively explored the security infrastructure of the Information Security Audit and Alarms, and propos a draft PP so-called Information Security Audit & Alarms Protection Profile (ISAAPP) [6-8]. Finally, in Section 4, we concluded this paper.

II. 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 and 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.

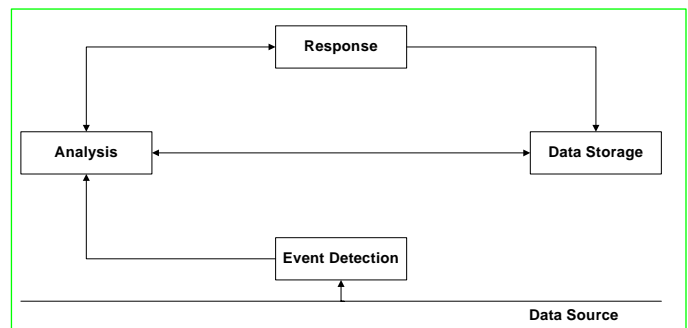


Fig. 2.1: Generic Model of Intrusion Detection [9]

To implement an information system Audit and Alarms mechanism, the following should be taken into consideration [8]:

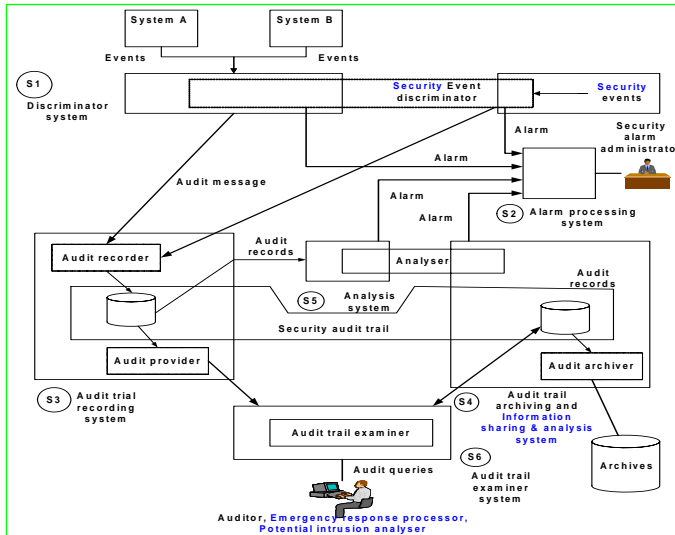
- What are the security-related events of Audit and Alarms? What are the detected security-related events?
- How to protect, analyze and report the security-related events of Audit and Alarms?
- What is the response policy to the analysis and report of the Audit and Alarms information?

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

III.DRAFT OF INFORMATION SECURITY AUDIT & ALARMS PROTECTION PROFILE (ISAAPP)

The objectives of 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, PP provides users a way to refer to given security requirements so as to make it easier for the users to process the evaluating tasks of the requirements [10-11].

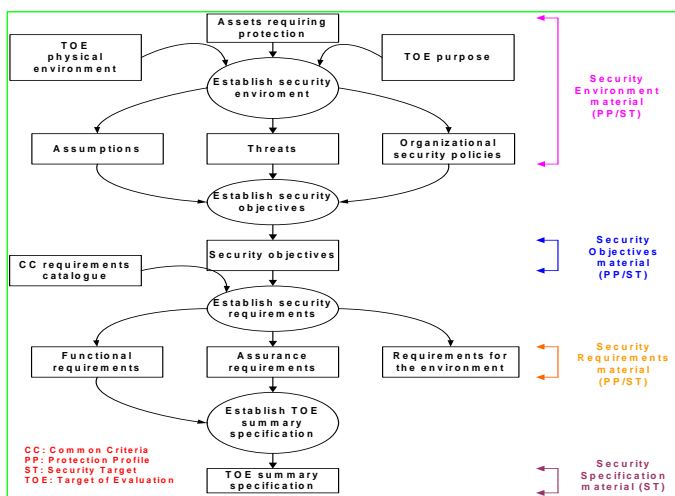
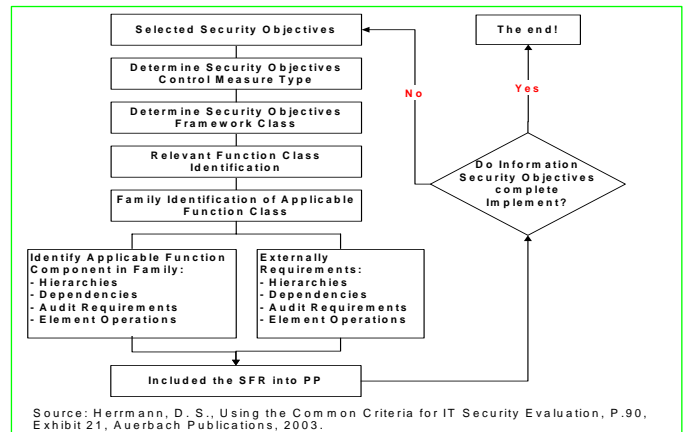


Fig. 3.1: Derivation of requirements and specification

Based on the functional architecture and its illustration from Fig. 2.2, the PP Security Function Requirements (SFR) selected process (shown in Fig. 3.2) and PP Security Assurance Requirements (SAR) selected process, we



respectively specify the security functional and assurance of ISAAPP.

Fig. 3.2: PP Security Function Requirements (SFR) Selected Process

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 [14-17], 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 [18]. 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	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_STG.1	FAU_STG.3	FAU_STG.4	FCS_COP.1	FDP_AC.C.1	FDP_AC.C.2	FDP_ACF.1	FDP_IFC.2	FDP_IFF.5	FDP_RIP.2	Note1_EX	FIA_AFL.
FAU_GEN.1	X																
FAU_GEN.2	X																
FAU_SAR.1	X																
FAU_SAR.2	X																
FAU_SAR.3	X																
FAU_STG.1	X	X															
FAU_STG.3	X																
FAU_STG.4	X	X															
FCS_COP.1									X								
FDP_AC.C.1									X								
FDP_AC.C.2																	
FDP_ACF.1									X								
FDP_IFC.2																	
FDP_IFF.5																	
FDP_RIP.2																X	
Note1_EX																X	
FIA_AFL.																	

[illegible]

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	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F	F
---------------	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

CC Identifier	F U G N . 1	F A T R	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G	F A T G
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	
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																X			

[illegible]

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].

IV. CONCLUSION

A qualified PP will capture the security requirements that are in demand by consumers. The profile will include a detailed and supportable description of the security environment for the target of evaluation and will include only the necessary functionality and assurance requirements. The security objectives will be precise and clearly linked to the security environment, perceived threat, and security policy. The rationale for each objective will clearly show why that objective was selected and which parts of the security environment are addressed. Finally, the requirements will be clearly mapped to one or more objectives. Each requirement's rationale will rest on enough evidence to establish why it is necessary. The PP will also show how each security objective has been achieved and why the overall set of requirements is sufficient [19].

The development of a PP looks simple. A PP must, at a minimum, meet the requirements in the Common Methodology for Information Technology Security Evaluation (CEM) [8]. According to CEM requirements, a PP must include:

- ◆ a description of the target of evaluation (the product or system to be evaluated), including the type of product or system and its general features
- ◆ a description of the intended security environment, including intended use assumptions, known or presumed

- ◆ threats, and organizational security policies
- ◆ a description of the security objectives for the target of evaluation and its environment. A rationale for each objective must be included and traced back to the appropriate part of the security environment. The PP must demonstrate completeness by tracing each aspect or element of the intended security environment to one or more objectives
- ◆ a set of security requirements, including functional, assurance, and environment requirements, with a rationale demonstrating all of the security objectives are addressed

In this paper we propose a draft PP of ISAAPP. This PP contains what a qualified PP needs, including the Security Environment, Security Objectives, Rationale, Dependencies, Rationale for Assurance Rating, and Rational for SOF Rating. Furthermore, the draft has been registered in the Chinese National Laboratory Accreditation (CNLA) as the security specification of relevant products and/ or systems. Furthermore, the CC 3.1 & CEM 3.1 [20] will be announced in 2007, which will provide the new guidelines for further research.

ACKNOWLEDGMENT

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

REFERENCES

- [1] <http://www.ttc.org.tw/en/ITS.asp> (2007-02-02).
- [2] <http://www.isecutech.com.tw/feature/view.asp?fid=561> (2007-02-02).
- [3] <http://www.ttc.org.tw/doc931.asp> (2007-02-02).
- [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://niap.nist.gov/cc-scheme/pp/PP_IDSYPV_V1.4.pdf (2007-02-02).
- [15] http://niap.nist.gov/cc-scheme/pp/PP_IDSAPP_V1.1.pdf (2007-02-02).

- [16] http://niap.nist.gov/cc-scheme/pp/PP_IDSSEPP_V1.1.pdf
(2007-02-02).
- [17] http://niap.nist.gov/cc-scheme/pp/PP_IDSSCPP_V1.1.pdf
(2007-02-02).
- [18] <http://www.commoncriteriaportal.org/public/files/ccusersguide.pdf> (2007-02-02).
- [19] <http://citeseer.ist.psu.edu/392722.html> (2007-02-02).
- [20] <http://www.commoncriteriaportal.org/public/consumer/index.php?menu=2> (2007-02-02).