Intrusion Detection System Analyzer

Protection Profile

Version 1.2

April 27, 2005

Prepared for
National Security Agency
9800 Savage Road
Fort Meade MD, 20755

Prepared by
Science Applications International Corporation
7125 Gateway Drive, Suite 300
Columbia, MD 21046

Foreword

This publication, Intrusion Detection System Analyzer Protection Profile, is issued by the National Security Agency as part of its program to promulgate security standards for information systems.

Comments on this document should be directed to Stephen Belcher, National Security Agency, V55, 9800 Savage Road, Ft. Meade, MD 20755.

TABLE OF CONTENTS

List of Tables

Intrusion Detection System Analyzer Protection Profile

1 PROTECTION PROFILE (PP) INTRODUCTION

1.1 INTRODUCTION

This section contains document management and overview information necessary to allow a Protection Profile (PP) to be registered through a Protection Profile Registry. The identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The overview can also be used as a stand-alone abstract for PP catalogues and registers. The Conventions section provides an explanation of how this document is organized. The Terms section gives a basic definition of terms, which are specific to this PP. Finally, the Related Profiles section identifies profiles directly related to this profile and may be of interest to those interested in this profile.

1.2 IDENTIFICATION

Title: Intrusion Detection System Analyzer Protection Profile, Version 1.2

Registration: (TBD)

Evaluation Assurance Level (EAL) – EAL 2

Common Criteria Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

International Standard – ISO/IEC 15408:1999

Keywords: intrusion detection, intrusion detection system, analyzer, sensor, scanner

1.3 OVERVIEW

The Common Criteria (CC) Intrusion Detection System Analyzer Protection Profile (IDSAPP) specifies a set of security functional and assurance requirements for Information Technology (IT) products. An

Intrusion Detection system (IDS) monitors an IT System for activity that may inappropriately affect the IT System's assets. An IT System may range from a computer system to a computer network. An IDS consists of Sensors, Scanners and Analyzers. Sensors and Scanners collect information regarding IT System activity and vulnerabilities, and they forward the collected information to Analyzers. Analyzers perform intrusion analysis and reporting of the collected information.

IDSAPP-conformant products support the ability to receive IDS Sensor or Scanner data and then apply analytical processes and information to derive conclusions about intrusions. IDSAPP-conformant products also provide the ability to protect themselves and their associated data from unauthorized access or modification and ensure accountability for authorized actions.

The IDSAPP provides for a level of protection which is appropriate for IT environments that require detection of malicious and inadvertent attempts to gain inappropriate access to IT resources, where the IDS can be appropriately protected from hostile attacks. Though products that are IDSAPP-conformant can be used to derive analytical conclusions about a system or network in a hostile environment, they are not designed to resist direct, hostile attacks. The IDSAPP does not fully address the threats posed by malicious administrative or system development personnel. This profile is also not intended to result in products that are foolproof and able to identify intrusion attempts by hostile and well-funded attackers. IDSAPP-conformant products are suitable for use in both commercial and government environments.

The IDSAPP was constructed to provide a target and metric for the development of Analyzers. This protection profile identifies security functions and assurances that represent the lowest common set of requirements that should be addressed by a useful Analyzer product.

The IDSAPP is generally applicable to products regardless of whether they are embedded, stand-alone, centralized, or distributed. However, it addresses only security requirements and not any special considerations of any particular product design.

It should be noted that just because an Analyzer may be conformant with this Protection Profile, that Analyzer should not be assumed to be interoperable with any other IDS component evaluated against a Protection Profile in the Intrusion Detection System family of Protection Profiles. There are no requirements for interoperability within the Protection Profiles.

1.4 CONVENTIONS

The requirements in this document are divided into assurance requirements and two sets of functional requirements. The first set of functional requirements is designed to address the core Analyzer requirements for self-protection. The second set, which were invented and categorized by the short name, IDS, is designed to address the requirements for the Analyzer's primary function, that is, IDS analysis and reactions based upon derived conclusions.

The CC permits four functional component operations—assignment, refinement, selection, and iteration —to be performed on functional requirements. This PP will highlight the four operations in the following manner:

- assignment: allows the specification of an identified parameter. Indicated with bold text and italics if further operations are necessary by the Security Target author;
- refinement: allows the addition of details. Indicated with bold text and italics if further operations are necessary by the Security Target author;
- selection: allows the specification of one or more elements from a list. Indicated with underlined text; and
- iteration: allows a component to be used more than once with varying operations. Not used in this PP.

In addition, this PP has explicitly stated requirements. These new requirements are indicated in bold text and contain the text (EXP) in the title.

1.5 TERMS

This section describes terms that are used throughout the IDSSPP and other Protection Profiles in the Intrusion Detection System family. The same terms section is used among all Protection Profiles to maintain consistency. When possible, terms are defined as they exist in the *Common Criteria for Information Technology Security Evaluation* or the *NSA Glossary of Terms Used in Security and Intrusion Detection*[2] provided by the NSA Information Systems Security Organization. The definitions were modified only to provide consistency with the IDSSPP. For example, occurrences of *computer system* or *network* were replaced with IT System. The authors of the IDSSPP defined all other terms as necessary.

- **Analyzer data** – Data collected by the Analyzer functions
- **Analyzer functions** – The active part of the Analyzer responsible for performing intrusion analysis of information that

may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.

- **Assets** - Information or resources to be protected by the countermeasures of a TOE.
- **Attack** - An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.
- **Audit** - The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.
- **Audit Trail** - In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.
- **Authentication** - To establish the validity of a claimed user or object.
- **Authorized Administrator** – A subset of authorized users that manage an IDS component
- **Authorized User** - A user that is allowed to perform IDS functions and access data
- **Availability** - Assuring information and communications services will be ready for use when expected.
- **Compromise** - An intrusion into an IT System where unauthorized disclosure, modification or destruction of sensitive information may have occurred.
- **Confidentiality** - Assuring information will be kept secret, with access limited to appropriate persons.
- **Evaluation** - Assessment of a PP, a ST or a TOE, against defined criteria.
- **IDS component** - a Sensor, Scanner, or Analyzer.
- **Information Technology (IT) System** - May range from a computer system to a computer network
- **Integrity** - Assuring information will not be accidentally or maliciously altered or destroyed.
- **Intrusion** - Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.
- **Intrusion Detection** - Pertaining to techniques which attempt to detect intrusion into an IT System by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.
- **Intrusion Detection System (IDS)** - A combination of Sensors, Scanners, and Analyzers that monitor an IT System for activity

that may inappropriately affect the IT System's assets and react appropriately.

- **Intrusion Detection System Analyzer (Analyzer)** – The component of an IDS that accepts data from Sensors, Scanners and other IT System resources, and then applies analytical processes and information to derive conclusions about intrusions (past, present, or future).
- **Intrusion Detection System Scanner (Scanner)** – The component of an IDS that collects static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
- **Intrusion Detection System Sensor (Sensor)** - The component of an IDS that collects real-time events that may be indicative of vulnerabilities in or misuse of IT resources.
- **IT Product** - A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.
- **Network** - Two or more machines interconnected for communications.
- **Packet** - A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
- **Packet Sniffer** - A device or program that monitors the data traveling between computers on a network
- **Protection Profile (PP)** - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.
- **Scanner data** – Data collected by the Scanner functions
- **Scanner functions** – The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data)
- **Security** - A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.
- **Sensor data** – Data collected by the Sensor functions
- **Sensor functions** – The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data)
- **Security Policy** - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
- **Security Target (ST)** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

- **Target of Evaluation (TOE)** - An IT product of system and its associated administrator and user guidance documentation that is the subject of an evaluation.
- **Threat** - The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security
- **TOE Security Functions (TSF)** - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
- **TOE Security Policy (TSP)** - A set of rules that regulate how assets are managed, protected, and distributed within a TOE.
- **Trojan Horse** - An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data.
- **TSF data** - Data created by and for the TOE, that might affect the operation of the TOE.
- **TSF Scope of Control (TSC)** - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.
- **User** – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
- **Virus** - A program that can "infect" other programs by modifying them to include a, possibly evolved, copy of itself.
- **Vulnerability** - Hardware, firmware, or software flow that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

1.6 RELATED PROTECTION PROFILES

Intrusion Detection System Scanner Protection Profile
Intrusion Detection System Sensor Protection Profile
Intrusion Detection System System Protection Profile

2 TARGET OF EVALUATION (TOE) DESCRIPTION

This Protection Profile specifies the minimum security requirements for a TOE that is an Analyzer. The purpose of an Analyzer is to accept data from Sensors and/or Scanners and to apply analytical processes and information to reach conclusions about potential intrusions, past, present, or future. Conclusions are acted upon according to the response functions included in the analyzer. Response functions can vary greatly from a simple display of a running list of analysis conclusions to actually reconfiguring system components to stop or prevent intrusions. This Protection Profile specifies the minimum-security requirements for TOEs composed of an Analyzer.

In general, the Analyzer is expected to collect relevant information from one or more Sensors and Scanners and derive conclusions based on the information it receives. Response functions built into the Analyser determine what actions are taken. Possible actions may range from a simple display of conclusions to an automated reconfiguration of the IT System or IDS to stop or prevent intrusions. The Analyzer is not required to perform any collection of the information. A Sensor or Scanner is responsible for performing collection functions An Analyser must be able to:

- Receive data from identified Sensors and Scanners.
- Protect itself and its data from tampering.
- Process specified data to make intrusion/vulnerability determinations.
- Respond to identified intrusions/vulnerabilities. Such responses may include report generation, visual signals/alarms, audible signals/alarms, configuration changes, and/or invocation of remote warnings.
- Be configured by an authorised user.
- Produce an audit trail (e.g., configuration changes, Analyser and data accesses).

An Analyser is a component of an IDS. Any IT System that needs to be aware of vulnerabilities and cyber attacks should deploy an IDS with one or more Analysers. The IDS monitors itself as well as its target IT System. The IT System must provide adequate protection for the Analysers so that the Analysers operates in a non-hostile environment. The following diagrams illustrate examples of how an IDS (represented by a star) may be utilised by IT Systems ranging from a computer system to a computer network. Figure-1 illustrates that an IDS may monitor and exist in a computer system that is not necessarily part of a larger network. Figure-2 illustrates that an IDS may monitor and exist within a computer

network. The arrows represent the monitoring functionality of the IDS as opposed to the implementation of the computer network.

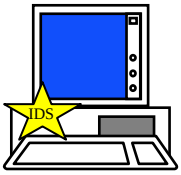

Figure-1. Computer System

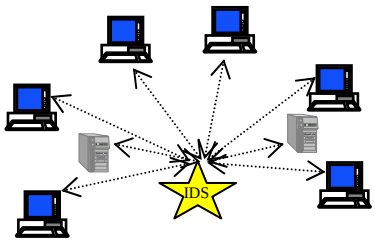

Figure-2. Computer Network

This PP makes a distinction between the Analyzer and TOE. The term Analyzer is used when the PP is referring to the ID analysis and response mechanisms. When the term TOE is used, the PP is referring to the Analyzer and the mechanisms necessary to ensure accountability and protection for the Analyzer.

3 TOE SECURITY ENVIRONMENT

3.1 ASSUMPTIONS

This section contains assumptions regarding the security environment and the intended usage of the TOE.

3.1.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System resources necessary to perform its functions.

3.1.2 Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.1.3 Personnel Assumptions

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

3.2 THREATS

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The

assumed level of expertise of the attacker for all the threats is unsophisticated.

3.2.1 TOE Threats

T.COMINT An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.

T.NOHALT An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

3.2.2 Analytical Threats

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

3.3 ORGANIZATIONAL SECURITY POLICIES

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the IDSAPP.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data analyzed and generated by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data analyzed and generated by the TOE shall be protected from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

4 SECURITY OBJECTIVES

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 INFORMATION TECHNOLOGY (IT) SECURITY OBJECTIVES

The following are the TOE security objectives:

O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.

O.IDACTS The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

O.RESPON The TOE must respond appropriately to analytical conclusions.

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.

O.OFLOWS The TOE must appropriately handle potential audit and Analyzer data storage overflows.

O.AUDITS The TOE must record audit records for data accesses and use of the Analyzer functions.

O.INTEGR The TOE must ensure the integrity of all audit and Analyzer data.

O.EXPORT When the TOE makes its Analyzer data available to other IDS

components, the TOE will ensure the confidentiality of the Analyzer data.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

The TOE's operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

O.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

O. PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Analyzer.

O.INTROP The TOE is interoperable with the IT System it monitors and other IDS components within its IDS.

5 IT SECURITY REQUIREMENTS

This section defines the functional requirements for the TOE. Functional requirements in this PP were drawn from Part 2 of the CC. These requirements are relevant to supporting the secure operation of the TOE. Functional requirements pertaining to the Analyzer analysis and response mechanisms were invented and are identified by the short name IDS.

The functional security requirements for the PP consist of the following components, summarized in Table 1 TOE Functional Components.

Functional Components	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_SEL.1	Selective audit
FAU_STG.2	Guarantees of audit data availability
FAU_STG.4	Prevention of audit data loss
FIA_UAU.1	Timing of authentication
FIA_ATD.1	User attribute definition
FIA_UID.1	Timing of identification
FMT_MOF.1	Management of security functions behaviour
FMT_MTD.1	Management of TSF data
FMT_SMR.1	Security roles
FPT_ITA.1	Inter-TSF availability within a defined availability metric
FPT_ITC.1	Inter-TSF confidentiality during transmission
FPT_ITI.1	Inter-TSF detection of modification
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation
FPT_STM.1	Reliable time stamps
IDS_ANL.1	Analyzer analysis
IDS_RCT.1	Analyzer react
IDS_RDR.1	Restricted data review
IDS_STG.1	Guarantee of analyzer data availability
IDS_STG.2	Prevention of Analyzer data loss

Table 1 TOE Functional Components

5.1 SECURITY AUDIT (FAU)

5.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the basic level of audit; and

c) **Access to the Analyser and access to the TOE and Analyser data**. FAU_GEN.1.1

Application Note: The auditable events for the basic level of auditing are included in Table 2 Auditable Events.

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to Analyser	
FAU_GEN.1	Access to the TOE Analyser data	**Object ID, Requested access**
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU. 1	All use of the authentication mechanism	**User identity, location**
FIA_UID.1	All use of the user identification mechanism	**User identity, location**
FMT_MOF.1	All modifications in the behaviour of the functions of the TSF	
FMT_MDT.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	**User identity**

Table 2 Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) **For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,** the additional information specified in the **Details** column of Table 2 Auditable Events. FAU_GEN.1.2

5.1.2 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide ***[assignment: authorised users]*** with the capability to read ***[assignment: list of audit information]*** from the audit records. FAU_SAR.1.1

Application Note: This requirement applies to authorised users of the TOE. The requirement is left open for the writers of the ST to define which authorised users may access what audit data.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information. FAU_SAR.1.2

5.1.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.2.1

5.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform sorting of audit data based on date and time, subject identity, type of event, and success or failure of related event. FAU_SAR.3.1

5.1.5 FAU_SEL.1 Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) event type;

b) ***[assignment: list of additional attributes that audit selectivity is based upon].*** FAU_SEL.1.1

Application Note: The ST must state any additional attributes that are available for audit selectivity.

5.1.6 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion. FAU_STG.2.1

FAU_STG.2.2 The TSF shall be able to detect modifications to the audit records. FAU_STG.2.2

FAU_STG.2.3 The TSF shall ensure that ***[assignment: metric for saving audit records]*** audit records will be maintained when the following conditions occur: ***[selection: audit storage exhaustion, failure, attack]***. FAU_STG.2.3

5.1.7 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall ***[selection: 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records']*** and send an alarm if the audit trail is full. FAU_STG.4.1

The ST must define what actions the TOE takes if the result log becomes full. Anything that causes the Analyser to stop analysing events may not be the best solution, as this will only affect the Analyser and not the system on which it is analysing data (e.g., shutting down the Analyser).

5.2 IDENTIFICATION AND AUTHENTICATION (FIA)

5.2.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow ***[assignment: list of TSF mediated actions]*** on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.1

Application Note: The ST must define any mediated actions that are permitted before a user is authenticated. Actions must be limited to aiding a user in accessing the TOE. An acceptable action before authentication is using the help facility.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.1.2

5.2.2 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **a settable, non-zero number** of unsuccessful authentication attempts occur related to **external IT products attempting to authenticate**. FIA_AFL.1.1

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **prevent the offending external IT product from successfully authenticating until an authorised administrator takes some action to make authentication possible for the external IT product in question**. FIA_AFL.1.2

5.2.3 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) **User identity**;

b) **Authentication data**;

c) **Authorisations**; and

d) ***[assignment: any other security attributes]*.** FIA_ATD.1.1

Application Note: At a minimum, there must be sufficient user information for identification and authentication purposes. That information includes maintaining any authorisations a user may possess.

5.2.4 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow ***[assignment: list of TSF-mediated actions]*** on behalf of the user to be performed before the user is identified. FIA_UID.1.1

Application Note: The ST must define any mediated actions that are permitted before a user is identified. Actions must be limited to aiding a user in accessing the TOE. An acceptable action before identification is using the help facility.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.1.2

5.3 SECURITY MANAGEMENT (FMT)

5.3.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of the functions **of analysis and reaction** to **authorised Analyser administrators**. FMT_MOF.1.1

Application Note: The TOE may have administrative roles for the operating system that do not have permissions to change the configuration options of the Analyser.

5.3.2 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to query **and add Analyser and audit data**, **and shall restrict the ability to query and modify all other TOE data** to ***[assignment: the authorised identified roles]***. FMT_MTD.1.1

Application Note: The ST should define which roles are permitted to access the Analyser data and all other TOE data. The ST may define any number of roles to meet this requirement.

5.3.3 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the **following** roles: **authorised administrator**, **authorised Analyser administrators, and** ***[assignment: other authorised identified roles]***. FMT_SMR.1.1

FMT_SMR.1.2 The TSF shall be able to associate users with roles. FMT_SMR.1.2

5.4 PROTECTION OF THE TOE SECURITY FUNCTIONS (FPT)

5.4.1 FPT_ITA.1 Inter-TSF availability within a defined availability metric

FPT_ITA.1.1 The TSF shall ensure the availability of **audit and Analyser data** provided to a remote trusted IT product within ***[assignment: a defined availability metric]*** given the following conditions ***[assignment: conditions to ensure availability]***. FPT_ITA.1.1

Application Note: The ST should state what the TOE does to promote availability to the audit and Analyser data.

5.4.2 FPT_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission. FPT_ITC.1.1

5.4.3 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: ***[assignment: a defined modification metric].*** FPT_ITI.1.1

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform ***[assignment: action to be taken]*** if modifications are detected. FPT_ITI.1.2

5.4.4 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_RVM.1.1

Application Note: The policies enforced by the TOE include identification and authentication, roles, and audit access.

5.4.5 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.1

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.1.2

5.4.6 FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

5.5 IDS COMPONENT REQUIREMENTS (IDS)

5.5.1 IDS_ANL.1 Analyser analysis (EXP)

IDS_ANL.1.1 **The TSF shall perform the following analysis function(s) on all IDS data received:**

a) **[selection: *statistical, signature, integrity*]; and**

b) **[assignment: *other analytical functions*]. (EXP)** IDS_ANL.1.1

Application Note: Statistical analysis involves identifying deviations from normal patterns of behaviour. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a system. For example, patterns of system settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing system settings or user activity at some point in time with those of another point in time to detect differences.

IDS_ANL.1.2 **The TSF shall record within each analytical result at least the following information:**

a) **Date and time of the result, type of result, identification of data source; and**

b) **[assignment: *other security relevant information about the result*]. (EXP)** IDS_ANL.1.2

Application Note: The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.

5.5.2 IDS_RCT.1 Analyser react (EXP)

IDS_RCT.1.1 **The TSF shall send an alarm to [assignment: alarm destination] and take [assignment: appropriate actions] when an intrusion is detected. (EXP)** IDS_RCT.1.1

Application Note: There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The Analyser may optionally perform other actions when intrusions are detected; these actions should be defined in the ST. An intrusion in this requirement

applies to any conclusions reached by the analyser related to past, present, and future intrusions or intrusion potential.

5.5.3 IDS_RDR.1 Restricted Data Review (EXP)

IDS_RDR.1.1 **The Analyser shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of Analyser data*] from the Analyser data. (EXP)** IDS_RDR.1.1

Application Note: This requirement applies to authorised users of the Analyser. The requirement is left open for the writers of the ST to define which authorised users may access what Analyser data.

IDS_RDR.1.2 **The Analyser shall provide the Analyser data in a manner suitable for the user to interpret the information. . (EXP)** IDS_RDR.1.2

IDS_RDR.1.3 **The Analyser shall prohibit all users read access to the Analyser data, except those users that have been granted explicit read-access. . (EXP)** IDS_RDR.1.3

5.5.4 IDS_STG.1 Guarantee of Analyser Data Availability (EXP)

IDS_STG.1.1 **The Analyser shall protect the stored Analyser data from unauthorised deletion. (EXP)** IDS_STG.1.1

IDS_ STG.1.2 **The Analyser shall protect the stored Analyser data from modification. (EXP)** IDS_STG.1.2

Application Note: Authorised deletion of data is not considered a modification of Analyser data in this context. This requirement applies to the actual content of the Analyser data, which should be protected from any modifications.

IDS_ STG.1.3 **The Analyser shall ensure that [assignment: *metric for saving Analyser data*] Analyser data will be maintained when the following conditions occur: [selection: *Analyser data storage exhaustion, failure, attack*]. (EXP)** IDS_STG.1.3

Application Note: The ST needs to define the amount of Analyser data that could be lost under the identified scenarios.

5.5.5 IDS_STG.2 Prevention of Analyser data loss (EXP)

IDS_STG.2.1 **The Analyser shall [selection: 'ignore Analyser data', 'prevent Analyser data, except those taken by the authorised user with special rights', 'overwrite the oldest stored Analyser data '] and send an alarm if the storage capacity has been reached. (EXP)** IDS_STG.2.1

Application Note: The ST must define what actions the analyser takes if the result log becomes full. Anything that causes the Analyser to stop analysing events may not be the best solution, as this will only affect the Analyser and not the system on which it is analysing data (e.g., shutting down the Analyser).

6 ASSURANCE REQUIREMENTS

This chapter defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 with no augmentation. Table 3 Assurance Components summarizes the components.

	Assurance components
Class ACM: Configuration management	ACM_CAP.2 Configuration items
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.1 Descriptive high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 3 Assurance Components

6.1 CONFIGURATION MANAGEMENT (ACM)

6.1.1 Configuration Items (ACM_CAP.2)

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all the requirements for content and presentation of evidence.

6.2 DELIVERY AND OPERATION (ADO)

6.2.1 Delivery Procedures (ADO_DEL.1)

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2 Installation, Generation, and Start-up Procedures (ADO_IGS.1)

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

6.3 DEVELOPMENT (ADV)

6.3.1 Informal Functional Specification (ADO_FSP.1)

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

6.3.2 Descriptive High-Level Design (ADV_HLD.1)

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

6.3.3 Informal Correspondence Demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.4 GUIDANCE DOCUMENTS (AGD)

6.4.1 Administrator Guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.4.2 User Guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.5 TESTS (ATE)

6.5.1 Evidence of Coverage (ATE_COV.1)

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.5.2 Functional Testing (ATE_FUN.1)

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.5.3 Independent Testing (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

6.6 VULNERABILITY ASSESSMENT (AVA)

6.6.1 Strength of TOE Security Function Evaluation (AVA_SOF.1)

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level of SOF-basic.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric of SOF-basic.

> Application Note: While this PP does not require a particular SOF for any mechanism, any SOF claims that the Security Target makes must be at least SOF-basic.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements

for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

6.6.2 Developer Vulnerability Analysis (AVA_VLA.1)

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

7 RATIONALE

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

7.1 RATIONALE FOR IT SECURITY OBJECTIVES

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose the IDSAPP. Table 4 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

	O.PROTCT	O.IDACTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP
A.ACCESS															X
A.PROTCT												X			
A.LOCATE												X			
A.MANAGE														X	
A.NOEVIL											X	X	X		
A.NOTRUST												X	X		
T.COMINT	X				X	X			X						
T.COMDIS	X				X	X				X					
T.LOSSOF	X				X	X			X						
T.NOHALT		X			X	X									
T.PRIVIL	X				X	X									
T.IMPCON				X	X	X					X				
T.INFLUX							X								
T.FALACT			X												
T.FALREC		X													
T.FALASC		X													
P.DETECT		X						X							
P.MANAGE	X			X	X	X					X		X	X	
P.ACCESS	X				X	X									
P.ACCACT						X		X							
P.INTEGR									X						
P.PROTCT				X								X			

Table 4 Security Environment vs. Objectives

A.ACCESS The TOE has access to all the IT System resources necessary to perform its functions.

The O.INTROP objective ensures the TOE has the needed access.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The O.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The O.PHYCAL provides for the physical protection of the TOE.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST The TOE can only be accessed by authorized users.

The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

T.COMINT An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.COMDIS An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.LOSSOF An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDACTS objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.IMPCON The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.

The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

The O.IDACTS objective requires analytical processes be applied to data collected from Sensors and Scanners.

P.MANAGE The TOE shall only be managed by authorized users.

The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective provides for TOE self-protection.

P.ACCESS All data analyzed and generated by the TOE shall only be used for authorized purposes.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective provides for TOE self-protection.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.

P.INTGTY Data analyzed and generated by the TOE shall be protected from modification.

The O.INTEGR objective ensures the protection of data from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

The O.OFLOWS objective requires the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications.

7.2 RATIONALE FOR SECURITY OBJECTIVES FOR THE ENVIRONMENT

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

7.3 RATIONALE FOR SECURITY REQUIREMENTS

This section demonstrates that the functional components selected for the IDSAPP provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

	O.PROTCT	O.IDACTS	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT
FAU_GEN.1								X		
FAU_SAR 1				X						
FAU_SAR.2					X	X				
FAU_SAR.3				X						
FAU_SEL.1				X				X		
FAU_STG.2	X				X	X	X		X	
FAU_STG.4							X	X		
FIA_UAU.1					X	X				
FIA_ATD.1						X				
FIA_UID.1					X	X				
FMT_MOF.1	X				X	X				
FMT_MTD.1	X				X	X			X	
FMT_SMR.1						X				
FPT_ITA.1										X
FPT_ITC.1									X	X
FPT_ITI.1									X	X
FPT_RVM.1	X			X		X		X	X	
FPT_SEP.1	X			X		X		X	X	
FPT_STM.1								X		
IDS_ANL.1		X								
IDS_RCT.1			X							
IDS_RDR.1				X	X	X				
IDS_STG.1	X				X	X	X		X	
IDS_STG.2							X			

Table 5 Requirements vs. Objectives Mapping

The following discussion provides detailed evidence of coverage for each security objective.

O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage

exhaustion, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1].

O.IDACTS The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

O.RESPON The TOE must respond appropriately to analytical conclusions.

The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

The TOE must provide the ability to review and manage the audit trail of an Analyzer [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The Analyzer must provide the ability for authorized administrators to view the Analyzer data [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1].

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer is required to restrict the review of Analyzer data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The Analyser is required to protect the Analyzer data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the

TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].

O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The Analyzer is required to restrict the review of collected Analyzer data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from unauthorized deletion as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the Analyzer may query and add Analyzer and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE [FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1]

O.OFLOWS The TOE must appropriately handle potential audit and Analyzer data storage overflows.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event the its audit trail is full [FAU_STG.4]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The Analyzer must prevent the loss of audit data in the event the its audit trail is full [IDS_STG.2].

O.AUDITS The TOE must record audit records for data accesses and use of the Analyzer functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which

security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event the its audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

O.INTEGR The TOE must ensure the integrity of all audit and Analyzer data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The Analyzer is required to protect the Analyzer data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the Analyzer may query or add audit and Analyzer data [FMT_MTD.1]. The Analyzer must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1].

O.EXPORT When the TOE makes its Analyzer data available to other IDS components, the TOE will ensure the confidentiality of the Analyzer data.

The TOE must make the Analyzer data available to other IT products [FPT_ITA.1]. The TOE must protect the Analyzer data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1].

7.4 RATIONALE FOR EXPLICITLY STATED REQUIREMENTS

A family of IDS requirements was created to specifically address the data collected and analysed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

7.5 RATIONALE FOR STRENGTH OF FUNCTION

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in section 4.

7.6 RATIONALE FOR ASSURANCE REQUIREMENTS

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the Analyzer may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the Analyzer will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

7.7 RATIONALE FOR SATISFYING ALL DEPENDENCIES

The IDSAPP does satisfy all the requirement dependencies of the Common Criteria. Table 6 Requirement Dependencies lists each requirement from the IDSAPP with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	YES
FAU_SAR.1	FAU_GEN.1	YES
FAU_SAR.2	FAU_SAR.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	YES
FAU_STG.2	FAU_GEN.1	YES
FAU_STG.4	FAU_STG.1	YES
FIA_UAU.1	FIA_UID.1	YES
FMT_MOF.1	FMT_SMR.1	YES
FMT_MTD.1	FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.1	YES

Table 6 Requirement Dependencies

References

[1] *Common Criteria for Information Technology Security Evaluation*, CCIMB-99-031, Version 2.1, August 1999.

[2] *NSA Glossary of Terms Used in Security and Intrusion Detection*, Greg Stocksdale, NSA Information Systems Security Organization, April 1998.

Acronyms

CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
IDSAPP	Intrusion Detection System Analyzer Protection Profile
IT	Information Technology
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Errata Sheets

As stated in the Introduction, the Intrusion Detection System (Analyzer) Protection Profile is intended to be generally applicable to products regardless of whether they are embedded, stand-alone, centralized, or distributed. However, some of the security functional requirements do not support the stated applicability. This section identifies several areas that have been identified as problematic for software vendors to claim conformance to this PP. Software vendors can follow the guidance in this Errata Section and claim conformance to this PP.

[1] FPT_STM.1

CCEVS guidance with respect to this requirement is only TOEs that include hardware can meet this requirement. In order to be consistent with the intent to permit software products to claim conformance to this PP, this requirement may be moved to the IT Environment. Additionally, a security objective for the IT Environment needs to be added to correspond to this IT Security Requirement – OE.TIME *The IT Environment will provide reliable timestamps to the TOE*. This additional security objective should be mapped to the P.ACCACT and P.DETECT policies which require audit and system data to be generated and include a timestamp.

[2] FPT_SEP.1

CCEVS guidance with respect to this requirement is only TOEs that include hardware can meet this requirement. In order to be consistent with the intent to permit software products to claim conformance to this PP, this requirement may be moved to the IT Environment. Additionally, a security objective for the IT Environment needs to be added to correspond to this IT Security Requirement – OE.PROTECT *The IT environment will protect itself and the TOE from external interference or tampering*. This additional security objective should be mapped the P. PROTECT security policy that addresses protection of the TOE from external entities.

[3] FPT_RVM.1

CCEVS guidance with respect to this requirement is only TOEs that include hardware can meet this requirement. In order to be consistent with the intent to permit software products to claim conformance to this PP, this requirement may be moved to the IT Environment. The OE.PROTECT security objective for the IT Environment added for the previous requirement, FPT_SEP.1, can also be used to address this requirement. This security objective should be mapped to T.COMINT and T.COMDIS

which address the threat of TOE's security functions being vulnerable to bypass attacks.

[4] FAU_STG.2

CCEVS guidance with respect to this requirement is only TOEs that provide the actual storage mechanism (e.g., file system) can meet this requirement. In order to be consistent with the intent to permit various types of software products to claim conformance to this PP, this requirement may be moved to the IT Environment. Additionally, a security objective for the IT Environment needs to be added to correspond to this IT Security Requirement – OE.AUDIT_PROTECTION *The IT Environment will provide the capability to protect audit information*. This additional security objective should be mapped to the P.ACCESS policy which limits who may access TOE data.