SANDIA REPORT

SAND2000-0922
Unlimited Release
Printed May 2000

A Protection Profile for TASE.2

Rolf E. Carlson and Cheryl L. Beaver

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

SAND2000-0922
Unlimited Release
Printed May 2000

A PROTECTION PROFILE FOR TASE.2

Rolf E. Carlson
Secure Networks and Information Systems

Cheryl L. Beaver
Information Systems Surety

Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0449

Abstract

This document represents the development of a protection profile (PP) for the IEC (International Electrotechnical Commission) protocol TASE.2 (Tele-control Application Service Element.2). A protection profile states assumptions about the TOE (Target of Evaluation), identifies threats to the TOE based on the assumptions, gives security goals to counter the threats, and finally identifies security functions to satisfy the security goals. Developing protection profiles for each protocol is a significant step towards developing measurable security for electric power automation systems. As an extension of the PP, we offer a generalization to any protocol at the evaluation assurance level (EAL) 2.

Table of Contents

Background

A protection profile (PP) states assumptions about the TOE (Target of Evaluation), identifies threats to the TOE based on the assumptions, gives security goals to counter the threats, and finally identifies security functions to satisfy the security goals. A rationale section serves to explain why various decisions were made. A final section generalizes this PP to any application layer protocol.

It is expected that the TOE will be developed by a third party as a COTS solution. The customer will not be able to control the development environment. Any testing by the customer will likely be done after delivery of the TOE by the developer. Qualitatively, the level of protection that can be provided in this sort of environment is at evaluation assurance level (EAL) 2.

Objectives of EAL2 (The objectives are taken from ISO/IEC 15408-3:1999(E)):
EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

For EAL2 the profile is independent of the implementation. For a specific instance of the implementation, a Security Target is written which is more specific than the PP. The PP is meant to be a more general set of guidelines.

Protection Profile (PP) Introduction

PP ID

- *Title:* Tele-control Application Service Element (TASE.2) Protection Profile for electric power utility Environments
- *Assurance level:* <2>
- *Registration:* <To Be Determined>
- *Keywords:* tele-control, electric power, network security, information protocol, MMS

PP Overview

The purpose of the TASE.2 PP is to define the basic security requirements for electric power utilities exchanging information using the TASE.2 protocol.

Target of Evaluation (TOE) Description

The purpose of TASE.2 is to provide inter-utility real-time data exchange using a client-server model. Either the client or server utility may initiate a connection. Interactions between a client and server can consist of requests for information as well as the issuance of control directives. In this sense, TASE.2 is the extension of monitoring and control from a local, or intra-SCADA, environment to an inter-SCADA environment. Consider the following figure.

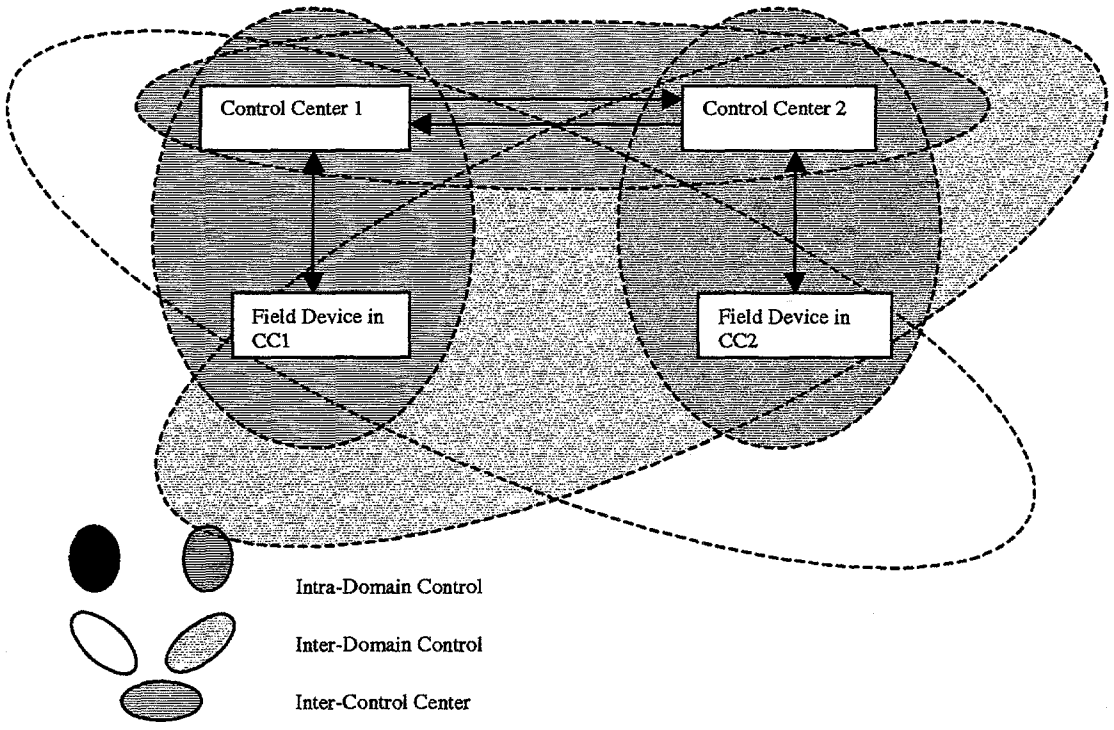

Figure 1. Field devices in the domain of control center 1 may be included in the domain of control center 2 to create an inter-domain control area.

TOE Security Environment

PP-Compliant TOEs are to be used in an electric power utility environment where business sensitive information is processed but classified information is not processed[1]. Hence, the information will be valued as proprietary to the business. Consequently, we will assume that the most likely adversary will be competitors or entities with competitive interests including professionals as well as knowledgeable amateurs. We include in the phrase "entities with a competitive interest" those whose goal is to discredit the company. Several distinguishing features between a professional and an amateur include the level of resources available as well as the systematic nature of the attack. Due to the inter-relation between business and certain governments, it is possible that a list of competitors will include government affiliates with substantial resources. Such threats require a higher level of protection than is provided in this profile. It is assumed that threats come from adversaries with only moderate resources.

In what follows an insider is defined to be an authenticated user. The insiders are authenticated prior to interaction with the TOE by some mechanism outside the TOE. Outsiders are anyone who is not an insider.

Assumptions

Assumption Name	Description	Comments
A.ADMIN	The security features of the TOE are competently administered on an on-going basis; however the administrators are capable of error.	
A.ADVERSARY	Adversaries are assumed to be outsiders with competitive interests, limited resources, and possess only publicly available information about the TOE.	
A.ADVERSARY-IMPERSONATE	Adversaries do not impersonate authorized users.	Digital signatures may mitigate this problem except when the adversary obtains the keys of an authorized user
A.BILAT	Access rights to client data objects by servers are governed by specifications in a bilateral table.	
A.BILAT-ACCESS	Authorized administrators maintain and give access to the bilateral tables.	
A.CLIENT	An entity that requests information is a client.	
A.COTS	The TOE is constructed from commercial off the shelf information technology.	

[1] Supporting more an EAL higher than 2 will require an augmentation of this PP.

Assumption Name	Description	Comments
A.INFO-FLOW	If information passes from client to server, it passes through the TOE.	
A.INFO-VALUE	The information carried by the TOE is assumed to be business proprietary.	
A.KEYS	All cryptographic keys are securely generated and distributed, and are destroyed after expiration.	
A.KEY-TRUST	Trust in the keys is established through a third party that is unconditionally trusted by the TOE. (i.e. a CA/RA).	
A.NO-DENIAL	The TOE is not expected to thwart a denial of service attack	
A.NO-INSIDER	The TOE is not expected to mitigate attacks perpetrated by insiders.	
A.PHYSEC	The TOE is physically secure.	
A.REMOTE-ACCESS	Authorized administrators may access the TOE remotely.	
A.SERVER	An entity that provides information is a server.	
A.TIME-SERVER	The TOE has access to a trusted timeserver.	
A.TRANSACTION	A transaction is defined to be an exchange of data between two entities.	
A.TRANSACTION-ENTITY	With respect to a transaction, an entity is either a client or a server.	
A.USER	All operators of the TOE are assumed to be authorized users that have been identified through some user interface, which is outside the scope of this TOE.	
A.USER-TRUST	Authenticated users are generally trusted to perform discretionary actions in accordance with security policies.	

Security Policy Issues

Policy Name	Description	Comments
P.ACCESS	Access rights to specific data objects are determined by object attributes assigned to that object, user identity, user attributes, and environmental conditions as defined by the security policy.	
P.COMPLY	The implementation and use of the organization's IT systems must comply with all applicable laws, regulations, and contractual agreements imposed on the organization.	
P.TOE-HOST	System administrators that set security policy for the system on which the TOE resides authenticate the users.	

Threats

Threat Name	Description	Comments
T.CHANGE	An adversary may modify or destroy TOE data.	
T.IMPERMISSIBLE	A user may send impermissible information through the TOE	
T.NOAUTH-VIEW	An adversary may view TOE data.	
T.REPLAY	After capturing valid data, an adversary may try to retransmit the data.	

Security Objectives

Security Objective Name	Description	Comments
O.CONFIDENTIALITY	The TOE provides services that facilitate confidentiality of data to adversaries.	
O.DATA-AUTHENTICATION	The TOE provides services to ensure the data authenticates as the original data. Note that data authentication gives data integrity.	(e.g. hash function)

Security Objective Name	Description	Comments
O.DATA-INTEGRITY	The TOE provides services that ensure data integrity.	E.g. is this acceptable data? Does it have the right format (e.g. Hamming codes, checksums, etc), etc. (not necessarily is it the original, but is it valid data?)
O.SECURITY-LEVEL	The security algorithms chosen to meet these objectives will be at a level so that it is computationally improbable for an adversary to obtain the secret hidden by the algorithm.	
O.SOURCE-AUTHENTICATION	The TOE provides services that allow the ability to validate the source of the data. Note that source integrity implicitly provides data authentication since if the data has been changed so has the source.	(e.g. signatures)
O.TRANS-INTEGRITY	The TOE provides services to ensure uniqueness and timeliness guarantees on data.	

IT Security Requirements

TOE Security Functional Requirements[2]

Functional Requirement Name	Description
FCO_NRO.1.3	The TSF shall provide a capability to verify the evidence of origin of information to [an authenticated user] given [that a trusted key and appropriate authentication algorithm was used by the originator].
FCS_COP.1.1	The TSF shall perform [digital signatures, encryption] in accordance with a specified cryptographic algorithm [DSA, RSA, 3DES, AES] and cryptographic key sizes [1024(DSA),1024(RSA), 64(2 keys for 3DES), 128(AES)] that meet the following [FIPS 186 (DSA); FIPS 81 (DES), FIPS 46-3 (3DES)].

[2] There is a concern that the security functions defined by the CC are not sufficiently resolved to meet the security objectives. The objectives include data integrity, transaction integrity, data authentication, and source authentication. Source authentication loosely maps to non-repudiation of origin (FCO_NRO), but non-repudiation is not the only reason one would want source authentication. Consequently, the two should be distinguished. Some of the objectives should apply to both static data and data in transmission even though FDP_DAU refers only to data that is static.

Functional Requirement Name	Description
FDP_DAU.1.1	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [data].
FPT_RPL.1.1	The TSF shall detect replay for the following entities [unauthenticated users].
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.

Rationale

Rationale for Assumptions:

A.ADMIN: Unless the system is administered competently in an on-going manner, security is not feasible. Therefore this assumption is both necessary and reasonable.

A.COTS: This assumption represents the key design constraint used in the development of CS2.

A.NO-INSIDER: The TOE is not expected to be able to sufficiently mitigate the risks resulting from malicious abuse of authorized privileges. It is not reasonable to expect near-term COTS products to provide sufficient protection against the malicious actions of authorized individuals.

A.USER-TRUST: The authenticated users are trusted in this manner in most organizations. The users have a fair amount of discretion and must be trusted to handle it appropriately. Therefore this assumption is both necessary and reasonable.

A.REMOTE-ACCESS: Administrators are allowed to access the system remotely to enable emergency response capability.

Rationale for Security Objectives:

O.CONFIDENTIALITY will counter the threat T.NOAUTH-VIEW.

O.DATA-INTEGRITY will counter the threat T.IMPERMISSIBLE.

O.TRANS-INTEGRITY will counter the threat T.REPLAY.

O.DATA-AUTHENTICATION will counter the threats T.CHANGE and T.IMPERMISSIBLE.

O.SOURCE-AUTHENTICATION will counter the threats T.CHANGE and T.IMPERMISSIBLE.

Rationale for Functional Security Requirements:

FCS_COP.1.1 will help to meet the security objective O.CONFIDENTIALITY as well as O.DATA-AUTHENTICATION, O.SOURCE-AUTHENTICATION, AND O.TRANS-INTEGRITY and O.SECURITY-LEVEL.

FCO_NRO.1.3 will help to meet the security objectives O.SOURCE-AUTHENTICATION.

FDP_DAU.1.1 will help to meet the security objectives O.DATA-INTEGRITY and O.DATA-AUTHENTICATION.

FPT_RPL.1.1 and FPT_STM.1.1 will help to meet the security objectives O.TRANS-INTEGRITY.

Generalization of the Protection Profile to an Arbitrary Application Layer Protocol

In order to generalize this protection profile we can remove the following assumptions specific to TASE.2: A.BILAT and A.BILAT-ACCESS. Additional assumptions and threats may be required for a specific communications protocol based on this generic PP.

DISTRIBUTION:

2	MS 0449	Cheryl L. Beaver
2	MS 0449	Rolf E. Carlson
1	MS 0449	Victoria A. Hamilton
1	MS 0449	Robert L. Hutchinson
1	MS 0449	Reynold S. Tamashiro
1	MS 0612	Review & Approval Desk, 9612 (for DOE/OSTI)
2	MS 0899	Technical Library, 9616
1	MS 9018	Central Technical Files, 8940-2