Compucat Research Pty Limited
14 Wales St,
Belconnen ACT 2617

ACN 008 565 026

Serial Data Regulator
SDR-01

Security Target

(Abridged)

P/N 2066-0010 -02

Table of Contents

List of Tables

Introduction

This document is an abridged version of the Security Target for the Compucat Serial Data Regulator (SDR). The objectives of this document are:

- to provide a specification of the SDR security functionality;
- to relate the SDR to the environment in which it is intended to operate; and
- to provide a basis for the evaluation of the utility of the SDR.

The intended audience for this security target is:

- Potential users of the SDR who use the target to assess the suitability of the SDR for an intended application.

This security target refers to Version 1.0 of the SDR.

Definitions

Compucat	Compucat Research Pty Limited (ACN 008 565 026)
SDR	The product name used for a Serial Data Regulator device developed by Compucat
ITSEC	Information Technology Security Evaluation Criteria
SEF	Security Enforcing Function
TOE	Target Of Evaluation (the SDR)

Security Policy

The security policy for the SDR can be stated as:

> *The SDR will maintain the confidentiality of the intended receiving system by ensuring that data can only be passed to the receiving system from the sending system and that no data can be passed from the receiving system to the sending system.*

The SDR enforces this policy and therefore maintenance of the confidentially requirement of the receiving system is satisfied.

A formal model of this security policy has been evaluated.

Product Rationale

Introduction

The SDR is a hardware-based device; comprising a send unit, receive unit and an interconnecting fibre optic cable. The SDR is installed as a null modem between two serial communications ports and ensures that data can flow in only one direction, from sender to receiver, between the connected ports.

Method of Use

U1 The SDR connects to the sending system through a serial (RS-232) interface to provide a simple, single path, connection that can be verifiably configured to ensure data can only be sent from the sending system.

U2 The SDR is connected to the receiving system through a serial interface (RS-232) to provide a simple, single path, connection that can be verifiably configured to ensure data can only be received by the receiving system.

U3 Protocols used to transfer data through the SDR must be able to operate without acknowledgment from the receiving system to prevent the possible use of return signals as covert data paths.

Intended Operating Environment

Personnel

E1 The SDR should be installed by a technician who is competent in installing Information Technology terminal equipment.

E2 SDR operation is transparent to a user. No physical interaction is required for operation of the SDR once it is installed.

Physical

E3 Physical security of the SDR receive unit should be the same as that required for the computing or communication system to which the SDR receive unit is attached.

E4 The SDR receive unit is tamper-evidently sealed at the time of manufacture by chemically welding the unit cover to its base. The nature of the seal is such that it will provide a clearly visible indication if the SDR receive unit is opened. Evidence of unauthorised opening could indicate that the security mechanism of the SDR might have been tampered with.

Procedural

There are no security-related procedures required for operation of the SDR.

IT Security Measures

E5 The integrity of the tamper evident sealing of the SDR receive unit case should be checked on a regular basis. The frequency of such checks should be determined by risk assessment based on the location in which the SDR receive unit is installed.

Security Objective

O1 Maintain the confidentiality of data on the receiving system by preventing data passing from the receiving system to the sending system. This prevents compromise of data on the receiving system where:

a. The Receiving system has data that is classified at a higher level than the sending system is authorised to access;

b. The Receiving system has data with 'need-to-know' categories that the sending system is not authorised to access.

Assumed Threats

T1 Data may pass directly from the receiving system to the sending system through the SDR, which could compromise the confidentiality of data on the receiving system.

T2 Data may pass covertly from the receiving system to the sending system though control circuits of the SDR, which could compromise the confidentiality of data on the receiving system.

Specification of Security Enforcing Functions

The security enforcing functions of SDR are presented here. The formal specification of security enforcing functions, as required by ITSEC E6.2, has been evaluated.

SEF 1 The TOE shall prevent the direct flow of data from the receiving system to the sending system. This is achieved by isolating the receiving system from the sending system with an optical diode. This function prevents the compromise of data by preventing the direct transfer of data from the receiving system to the sending system.

SEF 2 The TOE shall prevent the covert flow of data from the receiving system passing to the sending system through control circuits. This is achieved by not providing control circuits from the SDR receive unit to the SDR send unit. This function prevents the compromise of data by eliminating the control circuits as a possible covert transfer path.

Correlation of SEFs to Intended Use, Operating Environment and Assumed Threats

Method(s) of Use	SEF(s)	Comment
U1, U2	SEF 1	U1 and U2 implement a serial data connection from the SDR send unit to the SDR receive unit. The TOE prevents the direct flow of data from the receiving system to the sending system by only implementing the serial data path from the SDR send unit to the SDR receive unit. The TOE ensures that data can only pass from the SDR send unit to the SDR receive unit by isolating the receiving system from the sending system with an optical diode.
U3	SEF 2	U3 requires that the SDR operate without the use of acknowledgment signals. The TOE prevents the covert flow of data from the receiving system passing to the sending system through control circuits. The TOE achieves this by not providing control circuits from the SDR receive unit to the SDR send unit.

Table 1 - Correlation between Intended methods of use and SEFs

Operating Environment	SEF(s)	Comment
E1	SEF 1	E1 requires that the SDR be installed by a technician who is competent in installing Information Technology Equipment. If the SDR was installed incorrectly, for example send and receive units transposed, then information could pass from the intended receive system to the intended send system which could result in a breach of the security objective.
E2	SEF1	E2 states that once installed, no physical interaction is required for operation of the SDR. Since no physical interaction is required, no physical procedures need be performed which could otherwise result in a breach of the security objective.
E3	SEF 1	E3 requires that the SDR receive unit should be installed in an area that has at least the same physical security as the information which the SDR is protecting. Access to the SDR receive unit will be physically restricted to at least the same level as the information which the SDR is protecting.
E4, E5	SEF1	The tamper evident sealing and regular integrity checks will identify if the SDR receive unit has been opened. If the tamper evident sealing shows evidence of having been tampered with then the SDR receive unit should be assumed compromised and should not be used.

Table 2 - Correlation between Intended Operating Environment and SEFs

Threat	SEF(s)	Comment
T1	SEF 1	The SDR is designed with an optical diode that prevents data from passing from the receive unit to the send unit.
T2	SEF 2	The SDR is designed with no control circuits between the receive unit and the send unit.

Table 3 - Correlation between Threats and SEFs

Definition of Security Mechanisms

There are no mandated security mechanisms for the SDR.

Claimed Rating of Minimum SOM

The SDR uses only Type B mechanisms. Strength of mechanism claim need not be made for these mechanisms.

Target Evaluation Level

The target evaluation level for the SDR is ITSEC E6.