MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF:	2008-5-INF-310 V1	Created:	CERT8
Distribution:	Public	Reviewed:	CALIDAD
Date:	07.11.2008	Approved:	JEFEAREA

CERTIFICATION REPORT FOR SECURITY OPERATING SYSTEM v4.1.0.276

Dossier: 2008-5 SECURITY OPERATING SYSTEM v4.1.0.276

References:

EXT-482	Certification Request of Security Operating System V4.1.0.276.
EXT-654	Evaluation Technical Report of Security Operating System V4.1.0.276, 08/09/2008, v2.0, Epoche & Espri
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

Certification Report of the product Security Operating System (SOS), version 4.1.0.276, with certification request reference [EXT-482], of January 14th 2008, and evaluated by the laboratory Epoche & Espri, according to [CCRA], as described in the evaluation technical report [EXT-654] received on September 8th 2008.

Table Of Contents

Summary

This document represents the Certification Report for certification dossier of product Security Operating System, version 4.1.0.276.

Secuware Security Operating System (SOS) is a software product to securely transport and access confidential information (payload) in even untrusted environments.

Secuware's security technology completely isolates resources of the physical host machine, ensuring that payload and SOS sensitive information cannot be accessed or modified by Internet-borne malware or unauthorised users.

Developer/manufacturer: Secuware

Sponsor: Secuware

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Epoche & Espri.

Protection Profile: none.

Evaluation Level: CC v3.1 EAL2.

Evaluation end date: 08/09/2008.

Taking into account the results obtained in the Security Analysis performed in every aspect covered by the evaluation activities, and the verdicts assigned to each class; it has been concluded that:

The TOE Security Operating System (SOS) 4.1.0.276 does fulfil all the requirements specified in its Security Target, and therefore, the laboratory Epoche & Espri assigns the verdict PASS to the evaluation.

Therefore, the Spanish Certification Body proposes the approving resolution of the requested certification.

TOE Summary

The TOE comprises the GUI tool, called SOS Generator, and the resulting SOS image. SOS image can be considered as a security operating system based on a full encryption floppy-size image which allows authorised users to transport and access the payload in a secure manner. SOS image has been designed to be loaded under a physical environment. For instance, and due to its small size, SOS image can be encapsulated on a floppy R/O image.

Every time SOS boots, a new and completely clean environment is created, effectively preventing any malware from entering into the system.

TOE guarantees the integrity and confidentiality of the payload as well as the integrity of the TOE itself. Any change in the content of the SOS image (including the payload) will lead to a rejection of the booting. The TOE relies in the enciphering of the binary image of the secured operating system and a CRC 32-bit verification mechanism to protect SOS from unauthorized modifications.

Pre-boot authentication mechanism (PBA) assures that only the authorised user can load SOS and therefore access the payload it contains, guaranteeing its confidentiality. In case of configuring the SOS image for requiring user authentication, the user must authenticate to the SOS presenting his/her credentials. The credentials include the smart card **eDNI** (Spanish electronic Identification Card) and a user password.

In case of using a configuration based on an external user secret (password), the security of the product is highly increased. SOS configurations that imply the knowledge of a user password are the configurations recommended by Secuware and certified under CC EAL2 requirements, as well as the configurations that completely assure the integrity of SOS at the same time that the access to the payload is controlled.

The TOE does not rely on its IT environment to achieve any of its required security properties. However, it is supposed that the platform where SOS is loaded is free from any keylogger or malware that could compromise the password provided by the user. Therefore, it is assumed the existence of a secure communication channel between the user and the TOE for the password transference.

The asset of this TOE is the integrity and confidentiality of the user data (payload) and the integrity of the TSF itself.

- TOE guarantees the integrity and confidentiality of the payload. TOE guarantees also that the payload does not compromise the overall security of the TOE, even if it has malicious behaviour.
- TOE guarantees the integrity of the TOE itself, assuring that only unmodified SOS images can be launched.

- Pre-boot Authentication (PBA) ensures that only authorised users can load the SOS image and access the payload.
- SOS can run from a floppy disk – due to its small size – on an insecure environment or PC.
- The TOE originally doesn't have any default user definition. During SOS image creation stage, the authorised user (s) credentials can be configured for future authentication processes and TOE image encryption.

Security Assurance Requirements

The product was evaluated with all the evidences needed to satisfy the extent defined by the evaluation assurance level EAL2, according to the section 3 of CC v3.1 r2.

ASE_INT.1 ST Introduction
ASE_CCL.1 Conformance claims
ASE_SPD.1 Security problem definition
ASE_OBJ.2 Security objectives
ASE_ECD.1 Extended components definition
ASE_REQ.2 Derived security requirements
ASE_TSS.1 TOE summary specification

AGD_OPE.1 Operational user guidance
AGD_PRE.1 Preparative procedures

ALC_CMC.2 Use of a CM system
ALC_CMS.2 Parts of the TOE CM coverage
ALC_DEL.1 Delivery procedures

ADV_ARC.1 Security architecture description
ADV_FSP.2 Security-enforcing functional specification
ADV_TDS.1 Basic design

ATE_COV.1 Evidence of coverage
ATE_FUN.1 Functional testing
ATE_IND.2 Independent testing - sample

AVA_VAN.2 Vulnerability analysis

Security Functional Requirements

The security functionality of the product Security Operating System satisfies the following functional requirements according to the section 2 of CC v3.1 r2:

FPT_FLS.1 Failure with preservation of secure state
FDP_SDI.2 Stored data integrity monitoring and action
FIA_UID.1 Timing of identification
FIA_UAU.1 Timing of authentication
FMT_SMF.1 Specification of Management Functions
FDP_ACC.2 Complete access control
FMT_MSA.1 Management of security attributes
FMT_MSA.3 Static attribute initialisation
FDP_ACF.1 Security attribute based access control
FDP_ITC.1 Import of user data without security attributes

Identification

Product: Security Operating System (SOS) v4.1.0.276.

Security Target: SOS Security Target EAL2. v1.8. 31-08-2008.

Protection Profile: none.

Evaluation Level: CC v3.1 r2 EAL2.

Security Policies

This product does not implement any organizational policy.

Assumptions and operational environment

The following assumptions constrain the conditions over which the security properties and functionality referred in the security target is assured. In case of any of this assumptions couldn't be assumed it wouldn't be possible to assure the secure operation of the TOE.

Assumption 01: < AS.SECCHANNEL >

It is assumed that the environment where the TOE is loaded is free from any keylogger or malware that could compromise the password provided by the user. Therefore, it is assumed the existence of a secure communication channel between the user and the TOE for the password transference.

Threats

The following threats don't mean an exploiting risk to the product Security Operating System; even against attackers with EAL2 "BASIC" attack potential while complaining with the assumptions and the security policies.

The resistance to any other threat not included in this list is not assured as a result of the product properties evaluation and the corresponding certificate.

Threats covered:

Threat 01: < T.INT >

The TOE will be subject to attacks from untrusted IT elements from its IT environment. Any malware or untrusted IT element in the TOE environment, or even an untrusted user having access to the TOE may try to modify the integrity of the TOE payload or the TOE itself.

Threat 02: < T.IMP >

An unauthorized user attempts to impersonate a legitimate user, or to gain unauthorized execution of the TOE or unauthorized access to the payload. Thus, this threat is focused on compromising the confidentiality of the payload as well as subverting the access control mechanism implemented by the TOE.

Operational environment objectives

The product needs the environment collaboration to cover some of the objectives of the defined security problem.

The following objectives are covered by the environment:

Objective 01: < OE. SECCHANNEL >

The TOE Environment shall provide the user with a secure communication channel between the user and the TOE for the password transference, in order to avoid the password compromise by any keylogger or malware.

The details of either the product environment definition (assumptions, threats and security policies) or the security requirements of the TOE can be found on the Security Target.

TOE Architecture

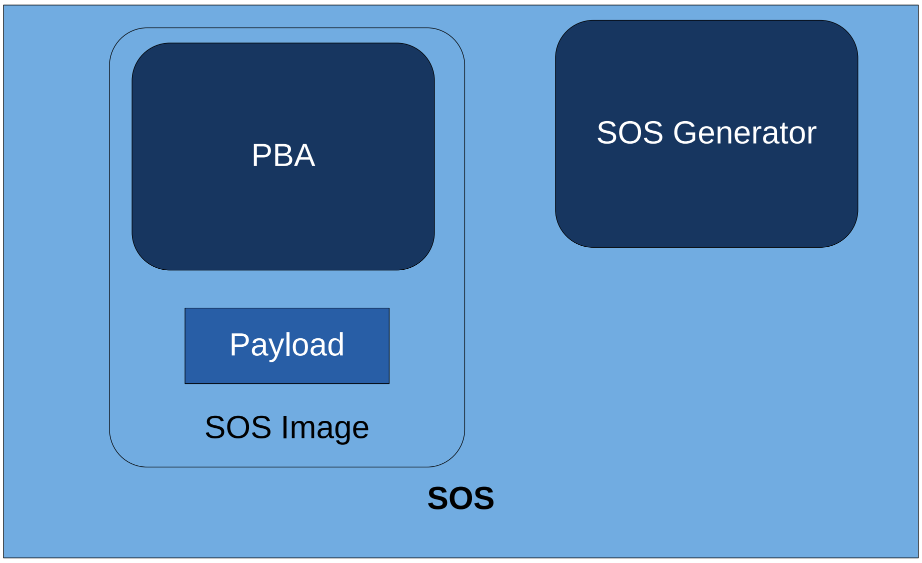
The TOE is structured in the following subsystems:

- **Preboot Authentication module**. This subsystem is in charge of authenticating the user, verifying the integrity of the SOS Image, decrypting it and, finally, making the payload available to the user.
- **SOS generator module**. This subsystem allows the security administrator to create the SOS image by using a very simple and intuitive Graphical User Interface (GUI),

called the SOS Image Creation GUI. This interface allows the administrator to select the payload and the user(s) credentials (authorised eDNIs and the user password).

- **Payload**. Payload is a user application that is securely transported inside SOS Image and which integrity and confidentiality are assured by means of the implemented SOS security mechanisms. Payload can be regarded as a subsystem which does not enforce any security property in the overall system nor is necessary for the proper execution and boot of the SOS Image.

The logical architecture in its evaluated configuration is depicted as follows:



Documents

The product includes the following documents that must be delivered jointly to the users of the evaluated version.

- Security Operating System – Security Target EAL2.
versión 1.8, 31/08/2008

- Security Operating System – Operational User Guidance.
versión 1.2, 31/07/2008

- Security Operating System – Preparative Procedures.
versión 1.2, 31/07/2008

TOE Testing

The approach defined for the developers testing plan is suitable to check the behaviour on the TOE through its interfaces. All the security interfaces TSFI defined are covered by test cases, and therefore the manufacturer test coverage is demonstrated. For all test cases, expected results match to the obtained results.

The evaluator repeated all the test cases specified and checked that the results match to those obtained by the developer.

The evaluator designed a set of test following a suitable strategy for the TOE type. The independent test plan includes test cases for all the TSFIs defined.

TOE Configuration

Following hardware requirements are needed for executing Secuware Security Operating System:

- SOS must be executed in a physical environment, like a floppy disk or by using Intel® vPro™ technology, among others. Therefore, depending on the mode of operation desired for SOS, the hardware or infrastructure requirement varies.
- Any Personal Computer or Server with basic memory and processor capabilities.

Evaluation Results

The product Security Operating System (SOS) v4.1.0.276 has been evaluated against the security target "SOS Security Target EAL2", v1.8 of August 31st 2008.

All the assurance components required in an **EAL2** evaluation have achieved the verdict "PASS". Therefore, the laboratory Epoche & Espri assigns the verdict "**PASS**" to the whole evaluation for satisfying all the evaluator actions defined in the Common Criteria and Common Evaluation Methodology version 3.1 r2.

Comments & Recommendations from the Evaluation Team

This section describes several important aspects that could influence the use of the product, taking into account the scope of the findings of the evaluation.

1. The use of virtualization Technologies allows an attacker with a moderate attack potential, to compromise the TOE integrity control mechanism. In case of disk encrypted systems with the key internally stored, the virtualisation techniques allows to install an hypervisor in the host and acquire an execution trace (and the memory content), locate the cipher loop and elicit the cipher keys allowing the replacement of the encrypted ISO parts with others.
2. The authentication with DNIe does not require the PIN allowing the possibility of user impersonation.

Certifier Recommendations

Taking into account the results obtained during the certification of the product Security Operating System (SOS) 4.1.0.276 the Spanish Certification Body proposes the approving resolution of the requested certification.

Glossary

CCN	Centro Criptológico Nacional
CB	Certification Body
PBA	Pre-boot authentication mechanism
SOS	Security Operating System
eDNI	Spanish electronic Identification Card
IT	Information Technology
PC	Personal Computer
TOE	Target of Evaluation
GUI	Graphical User Interface

Bibliography

The following rules and documents have been used during the product evaluation:

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r1, September 2007.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r1, September 2007.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r1, September 2007.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r1, September 2007.

Security Target

In addition to this report, the Security Target is available at the Certification Body:

“SOS Security Target EAL2” version 1.8, August 31st 2008.