Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0216-2003

for

SuSE Linux Enterprise Server V8
with certification-sles-eal2 package

from

SuSE Linux AG

sponsored by

IBM Corporation
Linux Technology Center

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0216-2003

SuSE Linux Enterprise Server V8

with certification-sles-eal2 package

from

SuSE Linux AG

sponsored by

IBM Corporation

Linux Technology Center

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and approved/licensed evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by CEM supplementation "ALC_FLR – Flaw remediation", Version 1.1, February 2002 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL2 augmented by** ALC_FLR.1 (Life cycle support - Basic flaw remediation)

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the Bundesamt für Sicherheit in der Informationstechnik and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 28. July 2003

The President of the Bundesamt für
Sicherheit in der Informationstechnik

IT Security Certified

SOGIS-MRA

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Telefon (0228) 9582-0 - Telefax (0228) 9582-455 - Infoline (0228) 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

This certificate is not an endorsement of the IT product by the Bundesamt für Sicherheit in der Informationstechnik or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by Bundesamt für Sicherheit in der Informationstechnik or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Bundesamt für Sicherheit in der Informationstechnik (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the Certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Bundesamt für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

---

[2] Act setting up the Bundesamt für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates based on the CC was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product SuSE Linux Enterprise Server V8 with certification-sles-eal2 package has undergone the certification procedure at BSI.

The evaluation of the product SuSE Linux Enterprise Server V8 with certification-sles-eal2 package was conducted by atsec information security GmbH which is an evaluation facility recognised by BSI (ITSEF)[6].

The sponsor is:

IBM Corporation
Linux Technology Center
11400 Burnet Road
Austin, TX 78758
USA

The developer/distributor is:

SuSE Linux AG
Deutschherrnstr. 15-19
90429 Nürnberg
Germany

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 28th July 2003.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

---

[6] Information Technology Security Evaluation Facility

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

4 Publication

The following Certification Results contain pages B-1 to B-36.

The product SuSE Linux Enterprise Server V8 with certification-sles-eal2 package has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the sponsor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] IBM Corporation - Linux Technology Center, 11400 Burnet Road, Austin, TX 78727, USA

- This page is intentionally left blank -

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is the SuSE Linux Enterprise Server V8 (also named SLES in short) with the certification-sles-eal2 package.

It is a general purpose, multi-user, multitasking Linux based operating system. It provides a platform for a variety of applications in the governmental and commercial environment. SLES is available on a broad range of computer systems, ranging from departmental servers to multi-processor enterprise servers. The SLES evaluation covers a potentially distributed, but closed network of IBM xSeries servers running the evaluated version of SLES.

SLES is based on United Linux, which is a common effort of several organisations to develop a common Linux platform designed as an enterprise platform for server applications.

The TOE includes Software components only and provides the following security functions:

- Identification and Authentication
- Discretionary Access Control
- Object reuse functionality
- Security Management
- TSF Protection

The product SuSE Linux Enterprise Server V8 is delivered by SuSE Linux AG on a CD-ROM or DVD. The following packages (rpm) as part of the product make up the evaluated TOE:

- aaa_base, aaa_skel, acl, ash, at, attr
- bash, bc, bzip2
- certification-sles-eal2, cpio, cracklib, cron, curl, cyrus-sasl
- db, devs, dialog, diffutils,
- e2fsprogs, ed
- file, filesystem, fileutils, fillup, findutils, freetype2
- gawk, gdbm, glibc, gpg, gpm ,grep, groff, grub, gzip
- hdparm, heimdal-lib, howtoenh, hwinfo
- iproute2, iputils, isapnp
- k_deflt, k_smp, kbd, ksymoops
- l2h-pngicons, less, libgcc, libstdc++, libxcrypt, libxml2, liby2util, logrotate, lprng, lukemftp
- m4, mailx, man, man-pages, mktemp, modutils

- ncurses, netcat, netcfg
- openldap-client, openssh, openssl
- pam, pam-modules, parted, pciutils, pcre, perl, permissions, popts, postfix, ps
- readline, rpm
- sed, shadow, sh-utils, sitar, sles-admin-x86+x86-en, sles-inst-x86+x86-64_en, sles-release, star, suse-build-key, sysconfig, syslogd, sysvinit
- tar, telnet, terminfo, texinfo, textutils, timezone
- UnitedLinux-buildkey, unitedlinux-release, utempter, util-linux
- vim, vsftpd
- w3m, wget
- xinetd
- yast2, yast2-bootloader, yast2-core, yast2-country, yast2-installation, yast2-mouse, yast2-ncurses, yast2-network, yast2-online-update, yast2-packager, yast2-packetmanager, yast2-pam, yast2-runlevel, yast2-security, yast2-storage, yast2-sysconfig, yast2-theme-SuSELinux, yast2-theme-UnitedLinux, yast2-trans-en_US, yast2-transfer, yast2-update, yast2-users, yast2-xml
- zlib

In addition to the packages listed above the following package has to be installed (it can be downloaded from the SuSE ftp-server):

- certification-sles-eal2

During the installation process the user has to verify the integrity and authenticity of the downloaded package as described in the Security Guide [9]. The base software installed from the CD/DVD allow the user to perform this verification by checking the digital signature of the package.

A more detailed listing which contains the exact versions of the packages can be found in chapter 11 of this report. For a detailed listing of guidance documents to be followed by a user of the TOE refer to chapter 6 of this report.

The TOE Security Functional Requirements (SFR) used in the Security Target are Common Criteria Part 2 conformant (hence all taken from the CC, part 2) as shown in the following list.

- FDP_ACC.1, FDP_ACF.1, FDP_RIP.2
- FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FIA_USB.1

- FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1, FMT_SMF.1, FMT_SMR.1
- FPT_RVM.1, FPT_SEP.1

Note that some of the SFR have been iterated in the Security Target. For details on the iteration and the required security functionality please refer to [7], chapter 5.1.

The TOE SuSE Linux Enterprise Server V8 was evaluated by:

atsec information security GmbH
Steinstraße 68-70
81667 München
Germany.

The evaluation was completed on 10th July 2003. The atsec information security GmbH is an evaluation facility recognised by BSI (ITSEF)[8].

The sponsor is:

IBM Corporation
Linux Technology Center
11400 Burnet Road
Austin, TX 78758
USA

The developer/distributor is:

SuSE Linux AG
Deutschherrnstr. 15-19
90429 Nürnberg
Germany

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report, or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL2+ (Evaluation Assurance Level 2 augmented).

The assurance level is augmented by: ALC_FLR.1 – Basic flaw remediation. For the evaluation of the CC component ALC_FLR.1 the mutually recognised CEM supplementation “ALC_FLR – Flaw remediation”, Version 1.1, February 2002 ([5]) had been used.

[8] Information Technology Security Evaluation Facility

1.2 Functionality

The TOE SuSE Linux Enterprise Server V8 provides the following Security Functions:

Name	Function
Identification and Authentication (IA)	
IA.1	User Identification and Authentication Data Management
IA.2	Common Authentication Mechanism
IA.3	Interactive Login and Related Mechanisms
IA.4	User Identity Changing
IA.5	Login Processing
Discretionary Access Control (DA)	
DA.1	Permission Bits
DA.2	Access Control Lists supported by SLES
DA.3	Discretionary Access Control: IPC Objects
Object Reuse (OR)	
OR.1	Object Reuse: File System Objects
OR.2	Object Reuse: IPC Objects
OR.3	Object Reuse: Memory Objects
Security Management (SM)	
SM.1	Roles
SM.2	Access Control Configuration and Management
SM.3	Management of User, Group and Authentication Data
TSF Protection (TP)	
TP.1	TSF Invocation Guarantees
TP.2	Kernel
TP.3	Kernel Modules
TP.4	Trusted Processes
TP.5	TSF Databases
TP.6	Internal TOE Protection Mechanisms

Note: Only the titles of the SF and a short summary are provided here because they are very granular and almost self-explanatory. Please refer for a precise definition of the SF to the Security Target of the TOE ([7], chapter 6.2)

1.3 Strength of Function

The TOE's strength of function is rated 'SOF-basic' only for the authentication function (IA) using passwords (refer to [7], chapter 6.5).

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

A summary of the threats defined in [7], chapter 3.2.1 is provided here. For the precise description of the threats please refer to [7]:

T.UAUSER

An attacker (not necessarily an unauthorised user) may try to impersonate an authorised user of the TOE without knowing the authentication information.

T.UAACCESS

An authorised user of the TOE tries to access information resources without having appropriate permissions.

The TOE has to comply to the following Organisational Security Policies (OSPs). Note that only a summary of the policies is provided here. For the detailed and precise definition refer to [7], chapter 3.3:

P.AUTHORISED_USERS

Only users who have been authorised to access information within the system may access the system.

P.NEED_TO_KNOW

The organisation using the TOE must define a discretionary access control policy on a need-to-know basis. The rules of this access control policy should base on the attributes (i) owner of object, (ii) identity of subject attempting access to an object and (iii) access rights (of a subject for the accessed object).

1.5 Special configuration requirements

The configuration requirements for the TOE are defined in chapter 2.4 and subsequent chapters of the Security Target [7] and are summarised here (please refer to the Security Target for the precise and more detailed description):

- The CC evaluated package set (refer to chapter 11.1) must be selected at install time;
- The following file systems are supported: the Ext3 journaling filesystem, the ISO 9660 file system for CD-ROM drives and the process file system, procfs.

- SLES supports the use of IPv4 and IPv6, only IPv4 is included;
- Both installation from CD and installation from a defined disk partition are supported;
- The default configuration for identification and authentication are the defined password based PAM modules. Support for other authentication options e.g. smartcard authentication, is not included in the evaluation configuration;
- If the system console is used, it must be connected directly to the workstation and afforded the same physical protection as the workstation;
- The TOE comprises a single server machine (and optional peripherals) running the system software listed in the package list of chapter 11.1 (a server running the above listed software is referred to as a “TOE server” below). Details on the allowed peripherals can be found in [7], chapter 2.4.2.
- Several TOE servers may be interlinked by a LAN, which may be joined by bridges/routers or by TOE workstations which act as routers / gateways.
- Each TOE server within this network implement its own security policy. No synchronisation function for those policies exists.
- If other systems are connected to the network they need to be configured and managed by the same authority using an appropriate security policy not conflicting with the security policy of the TOE.

Note:

A graphical user interface for system administration or any other operation is not included in the evaluated configuration.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. For example a HTTP server using a port above 1024 (e. g. on port 8080) may be used as a normal application running without root privileges on top of the TOE.

1.6 Assumptions about the operating environment

The following constraints concerning the allowed hardware and peripherals are made in the Security Target (refer to [7], chapter 2.4.2):

Hardware Platform:

- IBM xSeries Systems using Intel Pentium 4 or XEON processors

Peripherals:

- All terminals and printers supported by the TOE (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces)
- All storage devices and backup devices supported by the TOE (hard disks, CDROM drives, streamer drives, floppy disk drives) (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces)
- All Ethernet and Token-Ring network adapters supported by the TOE
- Pheripheral devices connected via PCMCIA are not supported.

The following constraints concerning the operating environment are made in the Security Target.

The following constraints are based on the assumptions defined in [7], chapter 3.4. (Please refer to the Security Target for the precise and more detailed definition):

Identifier	Summary
A.LOCATE	Location of TOE processing resources in facilities with controlled access.
A.PROTECT	Protection against physical modification (of TOE and Hardware used by the TOE).
A.MANAGE	Management of the TOE is done by competent individuals.
A.NO_EVIL_ADMIN	Administrative personnel are not careless, willfully negligent, or hostile.
A.COOP	Users are co-operative.
A.UTRAIN	Users are trained well enough to use the Security functionality of the TOE appropriately.
A.UTRUST	Users are trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their data.

Identifier	Summary
A.NET_COMP	Network components (like routers, bridges) used are assumed to pass data without modification.
A.CONNECT	All connections (to peripherals and network connections) reside within the controlled access facilities.

The following constraints are based on Security Objectives which have to be met by the TOE environment. Theses objectives are defined in [7], chapter 4.2. (Please refer to the Security Target for the precise and more detailed definition):

Identifier	Summary
OE.CREDEN	User Authentication Data has to be treated securely.
OE.INSTALL	The installation, distribution and configuration of hardware, software and firmware components has to be done in a secure manner.
OE.INFO_PROTECT	Information on security critical files (e.g. configuration files, authentication databases) shall be protected.
OE.MAINTENANCE	Diagnostic facilities shall be used periodically.
OE.RECOVER	Recovery Procedures after system failure must be available.
OE.SOFTWARE_IN	Only administrators shall be able to introduce new trusted software into the system.
OE.SERIAL_LOGIN	Clear screens before logging off (using serial login devices).
OE.HW_SEP	The underlying hardware has to provide separation mechanisms.

1.7 Disclaimers

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This certificate is not an endorsement of the IT product by the Bundesamt für Sicherheit in der Informationstechnik (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation is called:

SuSE Linux Enterprise Server V8

The following table summarises the TOE components and defines the evaluated configuration of the TOE:

Software	- CD set / DVD containing the software packages described in chapter 11.1 of this report. - certification-sles-eal2 package that can be downloaded from the SuSE ftp-server. During the installation process the integrity and authenticity of this package has to be checked.

The following guidance documents are supplied together with the TOE. The Guidance have to be followed to ensure an evaluation conformant operation of the TOE:

- SLES Security Guide, [9]
- SuSE Linux EnterpriseServer8 for X86 and AMD Hammer-based System. Administration, [10]
- SuSE Linux EnterpriseServer8 for X86 and AMD Hammer-based System. Installation, [11]

A full description of the installation and configuration process to get the evaluated configuration of the TOE can be found in [9]. The latest information on the secure configuration can be found in [12]. The user will need [10] just to obtain information on the use of the YaST user interface. All steps required to install and configure the TOE for the evaluated configuration are contained in [9].

Note that no hardware is delivered as part of the TOE.

3 Security Policy

The TOE is a Linux based multi-user multi-tasking operating system. The TOE may provide services to several users at the same time. After successful login, the users have access to a general computing environment, allowing the start-up of user applications, issuing user commands at shell level, creating and accessing files. The TOE provides adequate mechanisms to separate the users and protect their data. Privileged commands are restricted to administrative users.

The TOE uses the standard Unix model of normal (unprivileged) users and administrative users that have the capability to get full root privileges.

The TOE is intended to operate in a networked environment with other instantiations of the TOE as well as other well-behaved client systems operating within the same management domain (refer to [7], chapter 6.1.5 for more details). All those systems need to be configured in accordance with a defined common security policy.

The TOE permits one or more processors and attached peripheral and storage devices to be used by multiple users to perform a variety of functions requiring controlled shared access to the data stored on the system. Such installations are typical for workgroup or enterprise computing systems accessed by users local to, or with otherwise protected access to, the computer system.

It is assumed that responsibility for the safeguarding of the data protected by the TOE can be delegated to the TOE users.

All data is under the control of the TOE. The data is stored in named objects, and the TOE can associate with each controlled object a description of the access rights to that object.

All individual users are assigned a unique user identifier within the single host system that forms the TOE. This user identifier is used as the basis for access control decisions. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions.

The TOE enforces controls such that access to data objects can only take place in accordance with the access restrictions placed on that object by its owner or administrative users. Ownership of named objects may be transferred under the control of the access control policy.

Access rights (e.g. read, write, execute) can be assigned to data objects with respect to subjects (users). Once a subject is granted access to an object, the content of that object may be freely used to influence other objects accessible to this subject.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the personnel assumptions the following usage conditions exist. Refer to [7], chapter 3.4.2 for more details:

- The TOE is managed by competent individuals (A.MANAGE).
- Administrative personnel are not careless, wilfully negligent, or hostile (A.NO_EVIL_ADMIN).
- Users of the TOE are co-operative (A.COOP).
- Users are trained well enough to use the Security functionality of the TOE appropriately (A.UTRAIN).
- Users are trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their data (A.UTRUST).

4.2 Environmental assumptions

The following assumptions about physical and connectivity aspects defined by the Security Target have to be met (refer to Security Target [7], chapter 3.4.1 and 3.4.2):

- The TOE is located in an access controlled facility (A.LOCATE).
- The TOE (Hardware used by the TOE) is protected against physical modification (A.PROTECT).
- Network components (like routers, bridges) used are assumed to pass data without modification (A.NET_COMP).
- All connections (to peripherals and network connections) reside within the controlled access facilities (A.CONNECT).

Please consider also the requirements for the evaluated configuration specified in chapter 8 of this report.

4.3 Clarification of scope

The threats listed below have to be averted in order to support the TOE security capabilities but are not addressed by the TOE itself. They have to be addressed by the operating environment of the TOE (for detailed information about the threats and how the environment may cover them refer to the Security Target [7]).

TE.HWMF

Loss of stored data due to hardware malfunction.

TE.COR_FILE

Accidental corruption or manipulation of files relevant for the security without detection.

TE.HW_SEP

The underlying hardware functions of the hardware used by the TOE does not provide sufficient capabilities to support the self-protection of the TSF.

5 Architectural Information

General Overview

SuSE Linux Enterprise Server 8 is a general purpose, multi-user, multitasking Linux based operating system. It provides a platform for a variety of applications in the governmental and commercial environment. SLES is available on a broad range of computer systems, ranging from departmental servers to multi-processor enterprise servers.

SLES is based on United Linux, which is a common effort of several organisations to develop a common Linux platform designed as an enterprise platform for server applications.

The SLES evaluation covers a potentially distributed, but closed network of IBM xSeries servers running the evaluated version of SLES. The hardware platforms selected for the evaluation consist of machines which are available when the evaluation has completed and to remain available for a substantial period of time afterwards.

The TOE Security Functions (TSF) consist of functions of SLES that run in kernel mode plus some trusted processes. These are the functions that enforce the security policy as defined in this Security Target. Tools and commands executed in user mode that are used by an administrative user need also to be trusted to manage the system in a secure way. But they are not considered to be part of this TSF.

Also the hardware and the BootProm firmware is considered not to be part of the TOE but part of the TOE environment.

The TOE includes installation from CDROM and from a local hard disk partition.

The TOE includes standard networking applications, such as ftp and ssh. xinetd is used to protect network applications which might otherwise have security exposures.

System administration tools include the standard commands. A graphical user interface for system administration or any other operation is not included in the evaluated configuration.

The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. For example a HTTP server using a port above 1024 (e. g. on port 8080) may be used as a normal application running without root privileges on top of the TOE.

Major structural units of the TOE

The TOE is structured in much the same way as many other operating systems, especially Unix-type operating systems. It consists of a kernel, which runs in the privileged state of the processor and provides services to applications (which

those can use by calling kernel services via the system call interface). Direct access to the hardware is restricted to the kernel, so whenever an application wants to access hardware like disk drives, network interfaces or other peripheral devices, it has to call kernel services. The kernel then checks if the application has the required access rights and privileges and either performs the service or rejects the request.

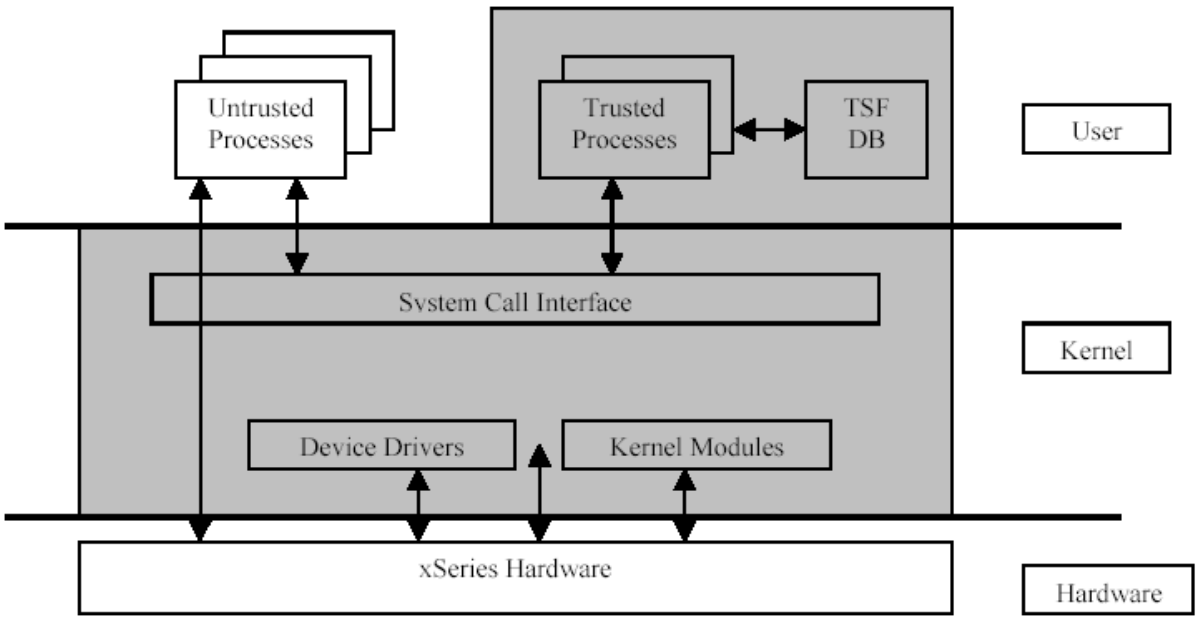
The kernel is also responsible to separate the different user processes. This is done by the management of the virtual and real memory of the TOE which ensures that processes executing with different attributes can not directly access memory areas of other processes but have to do so using the inter-process communication mechanism provided by the kernel as part of its system call interface.

The TSF of the TOE also include a set of trusted processes, which when initiated by a user with a system call operate with extended privileges. The programs that represent those trusted processes on the file system are protected by the file system discretionary access control security function enforced by the kernel.

In addition the execution of the TOE is controlled by a set of configuration files, which are also called the TSF database. Also those configuration files are protected by the file system discretionary access control security function enforced by the kernel.

Normal users – after they have been successfully authenticated by a defined trusted process – can start untrusted applications where the kernel enforces the security policy of the TOE when those applications request services from the kernel via the system call interface.

This structure is shown in the following figure:



The kernel itself is structured into a number of subsystems which are explained in detail in the high level design of the TOE. Those are:

File and I/O Subsystem

Implements all file system object related functions. Functions include those that allow a process to create, maintain, interact and delete file-system objects, such as regular files, directories, symbolic links, hard links, device special files, named pipes, and sockets.

Process Subsystem

Implements functions related to process and thread management. Functions include those that allow the creation, scheduling, execution, and deletion of process and thread subjects.

Memory Subsystem

Implements functions related to the management of a system's memory resources. Functions include those that create and manage virtual memory, including management of page tables and paging algorithms.

Networking Subsystem

Implements UNIX and internet domain sockets as well as algorithms for scheduling network packets.

IPC Subsystem

Implements functions related to inter-process communication mechanisms. Functions include those that facilitate controlled sharing of information between processes, allowing them to share data and synchronise their execution in order to interact with a common resource.

Kernel Modules Subsystem

Implements an infrastructure to support loadable modules. Functions include those that load and unload kernel modules.

Device Driver Subsystem

Implements support for various hardware devices through common, device independent interface.

Security Functions

The security functions of the TOE defined in the Security Target are (refer to Security Target [7], chapter 6.2):

- Identification and Authentication
- Discretionary Access Control
- Object reuse functionality
- Security Management
- TSF Protection

A short summary for each function is provided here. A more detailed description can be found in [7], chapter 6.2.

Identification and Authentication

The TOE provides identification and authentication using pluggable authentication modules (PAM) based upon user passwords. The quality of the passwords used can be enforced through configuration options controlled by SLES.
Other authentication methods (e. g. Kerberos authentication, token based authentication) that are supported by SLES as pluggable authentication modules are not part of the evaluated configuration.
Functions to ensure a basic password strength and limit the use of the su command and restrict root login to specific terminals are also included.

Discretionary Access Control

Discretionary Access Control (DAC) restricts access to file system objects based on Access Control Lists (ACLs) that include the standard UNIX permissions for user, group and others. Access control mechanisms also protect IPC objects from unauthorised access.
The TOE includes the ext3 file system, which supports POSIX ACLs. This allows you to define access rights to files within this type of file system down to the granularity of a single user.

Object Reuse

File system objects as well as memory and IPC objects will be cleared before they can be reused by a process belonging to a different user.

Security Management

The management of the security critical parameters of SLES is performed by administrative users. A set of commands that require root privileges are used for system management. Security parameters are stored in specific files that are protected by the access control mechanisms of the TOE against unauthorised access by users that are not administrative users.

TSF Protection

While in operation, the kernel software and data are protected by the hardware memory protection mechanisms. The memory and process management components of the kernel ensure a user process cannot access kernel storage or storage belonging to other processes.
Non-kernel TSF software and data are protected by DAC and process isolation mechanisms.
In the evaluated configuration, the reserved user ID root owns the directories and files that define the TSF configuration. In general, files and directories containing internal TSF data (e.g., configuration files, batch job queues) are also protected from reading by DAC permissions.
The TOE and the hardware and firmware components are required to be physically protected from unauthorised access. The system kernel

mediates all access to the hardware mechanisms themselves, other than program visible CPU instruction functions.

6 Documentation

The following documentation is provided with the product by the developer to the customer:

[9] SLES Security Guide, Version 1.49, 2003/05/15

[10] SuSE Linux EnterpriseServer8 for X86 and AMD Hammer-based System. Administration. Version 2002. File /usr/share/doc/packages/sles-admin-x86+x86-64_en/ sles-admin-x86+x86-64_en.pdf from SLES8 package “sles-admin-x86+x86-64_en”; also chapter 4 of the handbook supplied with SLES8

[11] SuSE Linux EnterpriseServer8 for X86 and AMD Hammer-based System. Installation. Version 2002. File /usr/share/doc/packages/sles-inst-x86+x86-64_en/ sles-inst-x86+x86-64_en.pdf from SLES8 package “sles-inst-x86+x86-64_en”; also chapter 3 of the handbook supplied with SLES8

[12] /usr/share/doc/packages/certification-sles-eal2/README-eal2.txt, 2003-05-28

7 IT Product Testing

Test Schedule

Final developer testing on the configuration defined in the Security Target [7] was performed in the time from May 16 to May 19, 2003 on two different systems (IBM xSeries 335 as a single processor machine and IBM xSeries 440 as a multiprocessor machine) at the lab of the Linux Technology Center in Austin, Texas.

Evaluator testing on the configuration defined in the Security Target was performed at the developer's facility in Nürnberg in the time from May 6 to May 7 on an IBM xSeries 335 and at the sponsor's facility in Austin, Texas on May 16 using an IBM xSeries 440.

The test systems have been installed and configured following exactly the information provided in the Security Guide [9] The constraints defined for the hardware configuration in the Security Target have been kept.

Test configuration

Tests have been performed on IBM xSeries 335 and 440 systems with the following configuration:

- **xSeries 335**: Memory 4GB, CPU 1way UP, 2 32GB SCSI drives, Onboard Broadcom 1GB Ethernet adapter
- **xSeries 440**: Memory 8GB, CPU 4way in hyperthreading mode, 2 18GB SCSI drives, Onboard Broadcom 1GB Ethernet adapter

Depth/Coverage of Testing

The developer has done substantial functional testing of all externally visible interfaces (TSFI). The evaluators repeated the developer tests (because of the highly automated testing approach of the developer) and conducted additional independent tests and penetrations tests.

Summary of Developer Testing Effort

Test configuration:

The sponsor/developer has performed the tests on the two hardware platforms defined above. The software was installed and configured as defined in the Security Guide [9]. Additional software was installed on the system to perform the tests. It was argued by the developers Test Plan that this additional software was within the boundary defined by the Security Target and did not constitute a violation of the evaluated configuration.

Testing approach:

The sponsor/developer used several test suites and manual tests to test the TOE. One of the test suites used was the LTP test suite. It is an adapted version of tests from the Linux Test Project of which the sponsor is a member.

The tests have a common framework in which individual test cases adhere to a common structure for setup execution and cleanup of tests. Each test case may contain several tests of the same function, stressing different parts (for example, base functionality, behaviour with illegal parameters and reaction to missing privileges). Each test within a test case reports PASS respectively OK or FAIL and the test case summary in batch mode reports PASS if all the tests within the test case passed, otherwise FAIL.

Tests can be executed either manually by running the test case file in the testcases/bin directory or run in batch mode by running the runalltests.sh script which is controlled by various parameters. One of them (-l) specifies the log summary file for the test cases. When the test cases are run individually no log summary is generated. The user running the test cases has to inspect stdout and stderr of the process.

Testing results:

All actual test results were consistent with the expected test results.

Summary of Evaluator Testing Effort

Test configuration:

The evaluator used the same IBM xSeries 440 machine as the developer and a different IBM xSeries 335 for testing. The machines were conformant to the Security Target requirements and setup according to in the Security Guide [9].

Testing approach:

Since the developer test are highly automated the evaluation facility decided not to choose a subset of the developer tests but to perform all developer tests again. All manual testing done by the developer were repeated by the evaluation facility as well. Additional tests were defined and executed by the evaluation facility in the following areas:

- Identification & Authentication
- Access Control
- TSF Protection
- Object Reuse

Testing results:

All actual test results were consistent with the expected test results.

Evaluator penetration testing:

The evaluators have devised a set of penetration tests based on

- common sources for vulnerabilities of the Linux Operating System,
- findings of their evaluation work examination.

In addition a widely available network scanning tool was used to check the TOE for potential vulnerabilities via network attacks taking into account that the TOE is intended to be integrated into a closed, physically protected network environment with a non-hostile user community.

The penetration testing addressed the following security functions:

- Identification and Authentication
- Discretionary Access Control
- TSF Protection

with some emphasis on the TSF Protection.

The penetration testing showed the existence of vulnerabilities but none of the vulnerabilities were exploitable in the intended environment of the TOE and/or the attack potential assumed for EAL2+ (AVA_VLA.1).

8 Evaluated Configuration

According to the Security Target the evaluated configuration of the TOE (as specified in chapter 2 of this report) is defined as follows (refer also to the Security Target [7]):

The product SuSE Linux Enterprise Server V8 is delivered by SuSE Linux AG on a CD-ROM or DVD. The packages (rpm) as specified in chapter 11.1 make up the evaluated TOE. In addition to the packages delivered on CD-ROM/DVD one package (certification-sles-eal2, refer to chapter 11.1 for more details) has to be downloaded from the SuSE ftp-server. The integrity and authenticity of this package has to be verified during the installation process.

The configuration requirements for the TOE are defined in chapter 2.4 and subsequent chapters of the Security Target [7] and are summarised here (please refer to the Security Target for the precise and more detailed description):

- The CC evaluated package set (refer to chapter 11.1) must be selected at install time;
- The following file systems are supported: the Ext3 journaling filesystem, the ISO 9660 file system for CD-ROM drives and the process file system, procfs.
- SLES supports the use of IPv4 and IPv6, only IPv4 is included;
- Both installation from CD and installation from a defined disk partition are supported;
- The default configuration for identification and authentication are the defined password based PAM modules. Support for other authentication options e.g. smartcard authentication, is not included in the evaluation configuration;
- If the system console is used, it must be connected directly to the workstation and afforded the same physical protection as the workstation;
- The TOE comprises a single server machine (and optional peripherals) running the system software listed in the package list of chapter 11.1 (a server running the above listed software is referred to as a “TOE server” below). Details on the allowed peripherals can be found in [7], chapter 2.4.2.
- Several TOE servers may be interlinked by a LAN, which may be joined by bridges/routers or by TOE workstations which act as routers / gateways.
- Each TOE server within this network implements its own security policy. No synchronisation function for those policies exists.

- If other systems are connected to the network they need to be configured and managed by the same authority using an appropriate security policy not conflicting with the security policy of the TOE.

Note: A graphical user interface for system administration or any other operation is not included in the evaluated configuration. The TOE environment also includes applications that are not evaluated, but are used as unprivileged tools to access public system services. For example a HTTP server using a port above 1024 (e. g. on port 8080) may be used as a normal application running without root privileges on top of the TOE.

For setting up / configuring the TOE all guidance documents (refer to chapter 6) especially the document [9] has to be followed.

The following constraints concerning the allowed hardware and peripherals are made in the Security Target:

Hardware Platform:

- IBM xSeries Systems using Intel Pentium 4 or XEON processors

Peripherals:

- All terminals and printers supported by the TOE
  (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces)
- All storage devices and backup devices supported by the TOE (hard disks, CDROM drives, streamer drives, floppy disk drives)
  (except hot pluggable devices connected via USB or IEEE 1394 (Firewire) interfaces)
- All Ethernet and Token-Ring network adapters supported by the TOE
- Peripheral devices connected via PCMCIA are not supported.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Common Evaluation Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE (this includes especially the methodology for flaw remediation, [5]).

The verdicts for the CC, Part 3 assurance components (according to EAL2 augmented by ALC_FLR.1 and the Security Target evaluation) are summarised in the following table:

Assurance Classes and Components		**Verdict**
Security Target	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Configuration items	ACM_CAP.2	PASS
Delivery and Operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Descriptive high-level design	ADV_HLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Tests	CC Class ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

The evaluation has shown that the TOE fulfils the claimed strength of function for the authentication function using passwords.

The results of the evaluation are only applicable to the product SuSE Linux Enterprise Server V8 with certification-sles-eal2 package in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [7] and the chapters 2, 4 and 8 of this report). The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Evaluator Comments/Recommendations

The User Guidance documentation (refer to chapter 6) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [7] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

11 Annexes

11.1 TOE software packages

The following packages include the software that is installed with the evaluated configuration (packages that are updated when installing the certification-sles-eal2 package and running the */usr/lib/eal2/bin/sles-eal2* script are marked with "yes" in the EAL2-package column):

Package Name	Version	EAL2-package
UnitedLinux-build-key	1.0	
aaa_base	2003.3.27	yes
aaa_skel	2002.10.14	
acl	2.0.19	
ash	0.2	
at	3.1.8	
attr	2.0.11	
bash	2.05b	
bc	1.06	yes
bzip2	1.0.2	
certification-sles-eal2	1.0	yes
cpio	2.5	
cracklib	2.7	
cron	3.0.1	
curl	7.9.8	
cyrus-sasl	1.5.27	
db	4.0.14	
devs	2002.10.4	
dialog	0.52	
diffutils	2.8.1	
e2fsprogs	1.28	
ed	0.2	
file	3.37	yes
filesystem	2002.9.2	
fileutils	4.1.11	
fillup	1.10	
findutils	4.1.7	
freetype2	2.0.9	yes
gawk	3.1.1	
gdbm	1.8.0	
glibc	2.2.5	yes
gpg	1.0.7	
gpm	1.20.1	
grep	2.5.1	
groff	1.17.2	
grub	0.92	yes
gzip	1.3	
hdparm	5.2	
heimdal-lib	0.4e	
howtoenh	2003.9.6	
hwinfo	5.43	yes
iproute2	2.4.7	yes

Package Name	Version	EAL2-package
iputils	ss020124	
isapnp	1.26	
k_deflt	2.4.19	yes
k_smp	2.4.19	yes
kbd	1.06	yes
ksymoops	2.4.5	
l2h-pngicons	99.2beta8	
less	376	
libgcc	3.2.2	yes
libstdc++	3.2.2	yes
libxcrypt	1.1	
libxml2	2.4.23	
liby2util	2.6.21	
logrotate	3.5.9	
lprng	3.6.12	
lukemftp	1.5	
m4	1.40	
mailx	8.1.1	
man	2.3.19deb4.0	
man-pages	1.53	
mktemp	1.5	
modutils	2.4.19	
ncurses	5.2	
net-tools	1.60	yes
netcat	1.10	
netcfg	2002.9.4	
openldap2-client	2.1.4	yes
openssh	3.4p1	
openssl	0.96g	yes
pam	0.76	
pam-modules	2002.8.28	yes
parted	1.6.3	
pciutils	2.1.10	
pcre	3.9	
perl	5.8.0	yes
permissions	2002.9.10	
popt	1.6	
postfix	1.1.11	
ps	2002.9.10	
readline	4.3	yes
rpm	3.0.6	
sed	3.02.80	
sh-utils	2.0	
shadow	4.0.2	yes
sitar	0.7.2	
sles-admin-x86+x86-64_en	8.1.0.2	
sles-inst-x86+x86-64_en	8.1.0.2	
sles-release	8	
star	1.4.2	yes
suse-build-key	1.0	
sysconfig	0.23.22	yes
syslogd	1.4.1	
sysvinit	2.82	

Package Name	Version	EAL2-package
tar	1.13.25	
telnet	1.0	
terminfo	5.2	
texinfo	4.2	
textutils	2.1	
timezone	2.2.5	yes
unitedlinux-release	1.0	
utempter	0.5.2	
util-linux	2.11u	
vim	6.1	
vsftpd	1.1.0	
w3m	0.3.1	yes
wget	1.8.2	
xinetd	2.3.6	
yast2	2.6.40	
yast2-bootloader	2.6.65	yes
yast2-core	2.6.56	yes
yast2-country	2.6.35	yes
yast2-installation	2.6.94	yes
yast2-mouse	2.6.18	
yast2-ncurses	2.6.24	yes
yast2-network	2.6.33	
yast2-online-update	2.6.15	yes
yast2-packagemanager	2.6.49	yes
yast2-packager	2.6.78	
yast2-pam	2.6.5	
yast2-runlevel	2.6.16	
yast2-security	2.6.10	
yast2-storage	2.6.56	yes
yast2-sysconfig	2.6.14	
yast2-theme-SuSELinux	2.6.8	
yast2-theme-UnitedLinux	2.6.8	
yast2-trans-en_US	2.6.7	
yast2-transfer	2.6.1	
yast2-update	2.6.23	yes
yast2-users	2.6.33	yes
yast2-xml	2.6.8	
zlib	1.1.4	1.1.4

12 Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

ACL Access Control List

AMD Advanced Micro Devices, Inc.

BSI Bundesamt für Sicherheit in der Informationstechnik

CC Common Criteria for IT Security Evaluation

CCRA Common Criteria Recognition Arrangement

DA/DAC Discretionary Access Control

EAL Evaluation Assurance Level

HTTP Hyper Text Transfer Protocol

IA Identification and Authentication

IPC Interprocess Communication

ISO International Organisation for Standardisation

IEEE Institute of Electrical & Electronics Engineers

IT Information Technology

LTP Linux Test Project

OSP Organisational Security Policy

OR Object Reuse

PCMCIA Personal Computer Memory Card International Association

PP Protection Profile

RPM Red Hat Package Manager

SF Security Function

SFP Security Function Policy

SFR Security Functional Requirement

SOF Strength of Function

SM Security Management

SLES SuSE Linux Enterprise Server

ST Security Target

TOE Target of Evaluation

TP TSF Protection

TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TST	TST mode of the DEP/PCI
USB	Universal Serial Bus
YaST	Yet Another Setup Tool

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or

organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - 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 - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[3] BSI certification: Procedural Description (BSI 7125)

[4] Applicaton Notes and Interpretations of the Scheme (AIS) as relevant for the TOE:

[5] Applicaton Notes and Interpretations of the Scheme AIS33, Version 2 – “Methodologie zur Fehlerbehebung – Flaw Remediation”, 26.07.2002

[6] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[7] SuSE Linux Enterprise Server V8, Security Target BSI-DSZ-CC-0216, Version 1.6, IBM Corporation & SuSE Linux AG, 2003-06-20

[8] Evaluation Technical Report BSI-DSZ-CC-0216, Version 1.0, atsec Information Security GmbH, 2003-07-10 (confidential document)

User Guidance Documentation:

[9] SLES Security Guide, Version 1.49, 2003/05/15

[10] SuSE Linux EnterpriseServer8 for X86 and AMD Hammer-based System. Administration. Version 2002. File /usr/share/doc/packages/sles-admin-x86+x86-64_en/ sles-admin-x86+x86-64_en.pdf from SLES8 package “sles-admin-x86+x86-64_en”; also chapter 4 of the handbook supplied with SLES8

[11] SuSE Linux EnterpriseServer8 for X86 and AMD Hammer-based System. Installation. Version 2002. File /usr/share/doc/packages/sles-inst-x86+x86-64_en/ sles-inst-x86+x86-64_en.pdf from SLES8 package “sles-inst-x86+x86-64_en”; also chapter 3 of the handbook supplied with SLES8

[12] /usr/share/doc/packages/certification-sles-eal2/README-eal2.txt, 2003-05-28

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.

Evaluation assurance level (EAL) overview (chapter 6.1)

Table 6.1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by *substitution* of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the *addition* of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation“ allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component“ is not recognised by the CC as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

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.“

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.“

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous,

do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.“

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.“

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.“

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 6.2.7)

„Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“