Swedish Certification Body for IT Security

Certification Report - Canonical Ubuntu Server 18.04 LTS

Issue: 1.0, 2020-Dec-11

Authorisation: Jerry Johansson, Lead Certifier , CSEC

SWEDAC ACKREDITERING
Accred. no. 1917
Certification of Products
ISO/IEC 17065

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is a Linux-based general-purpose operating system. The TOE also includes a virtualization environment based on the Linux KVM technology, where Ubuntu implements the host system for the virtual machine environment and management of the virtual machines. The TOE is intended to operate in a networked environment with other instantiations of the TOE as well as other well-behaved peer systems operating within the same management domain.

The TOE has been evaluated on the following two hardware platforms:

- IBM s390x (z architecture mainframe) with IBM z14 processors
- Supermicro SYS-5018R-WR server with Xeon processor.

The TOE is delivered via download in the form of an ISO image. A SHA-256 checksum is calculated and signed, by several trusted entities within Canonical Group Limited, using a GPG signing key. These values are made publicly available and are to be used for verification of the TOE.

As the TOE is a general purpose operating system, there are many possible configurations and modifications that can be made in the Linux kernel. The evaluation only covers a subset of all possible operational modes of Ubuntu, which is described in chapter 8 Evaluated configuration.

The ST do not claim conformance to any protection profiles. The ST does however derive its security functional requirements from the Operating System Protection Profile v2.0 with the extended package for virtualization.

There are ten assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the eleven threats and comply with the four organisational security policies (OSPs) in the ST. The assumptions, the threats and the OSPs are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden, and to some extent in the approved foreign location in Austin, Texas, USA, and was completed on the 19th of November 2020.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 2, augmented by ALC_FLR.3 Systematic flaw remediation.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 2 + ALC_FLR.3.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.
This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2019029
Name and version of the certified IT product	Ubuntu 18.04.4 LTS
Security Target Identification	Security Target for Ubuntu 18.04 LTS, 2020-12-02, version 1.0
EAL	EAL 2 + ALC_FLR.3
Sponsor	Canonical Group Ltd.
Developer	Canonical Group Ltd.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	1.24
Scheme Notes Release	17
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2020-12-11

3 Security Policy

The TOE provides the following security services:

- Auditing
- Cryptography
- Packet Filter
- Identification and Authentication
- Discretionary Access Control
- Authoritative Access Control
- Virtual Machine Environments
- Security Management

3.1 Auditing

The Lightweight Audit Framework (LAF) is designed to be an audit system making Linux compliant with the requirements from Common Criteria. LAF is able to intercept all system calls as well as retrieving audit log entries from privileged user space applications. The subsystem allows configuring the events to be actually audited from the set of all events that are possible to be audited.

3.2 Cryptographic Support

The TOE provides cryptographically secured communication to allow remote entities to log into the TOE. For interactive usage, the SSHv2 protocol is provided. The TOE provides the server side as well as the client side applications. Using OpenSSH, password-based and public-key-based authentication are allowed.

In addition, the TOE provides confidentiality protected data storage using the device mapper target dm_crypt. Using this device mapper target, the Linux operating system offers administrators and users cryptographically protected block device storage space. With the help of a Password-Based Key-Derivation Function version 2 (PBKDF2) implemented with the LUKS mechanism, a user-provided passphrase protects the volume key which is the symmetric key for encrypting and decrypting data stored on disk. Any data stored on the block devices protected by dm_crypt is encrypted and cannot be decrypted unless the volume key for the block device is decrypted with the passphrase processed by PBKDF2. With the device mapper mechanism, the TOE allows for transparent encryption and decryption

of data stored on block devices, such as hard disks.

3.3 Packet Filter

The TOE provides a stateless and stateful packet filter for regular IP-based communication. OSI Layer 3 (IP) and OSI layer 4 (TCP, UDP, ICMP) network protocols can be controlled using this packet filter. To allow virtual machines to communicate with the environment, the TOE provides a bridging functionality. Ethernet frames routed through bridges are controlled by a separate packet filter which implements a stateless packet filter for the TCP/IP protocol family.

The packet filtering functionality offered by the TOE is hooked into the TCP/IP stack of the kernel at different locations. Based on these locations, different filtering capabilities are applicable. The lower level protocols are covered by the EBTables filter mechanism which includes the filtering of Ethernet frames including the ARP layer. The higher level protocols of TCP/IP are covered with the IPTables mechanism which allows filtering of IP and TCP, UDP, ICMP packets. In addition, IPTables offers a stateful packet filter for the mentioned higher level protocols.

3.4 Identification and Authentication

User identification and authentication in the TOE includes all forms of interactive log-in (e.g. using the SSH protocol or log in at the local console) as well as identity changes through the su or sudo command. These all rely on explicit authentication information provided interactively by a user.

The authentication security function allows password-based authentication. For SSH access, public-key-based authentication is also supported.

Password quality enforcement mechanisms are offered by the TOE which are enforced at the time when the password is changed.

3.5 Discretionary Access Control

DAC allows owners of named objects to control the access permissions to these objects. These owners can permit or deny access for other users based on the configured permission settings. The DAC mechanism is also used to ensure that untrusted users cannot tamper with the TOE mechanisms.

In addition to the standard Unix-type permission bits for file system objects as well as IPC objects, the TOE implements POSIX access control lists. These ACLs allow the specification of the access to individual file system objects down to the granularity of a single user.

3.6 Authoritative Access Control

The TOE supports authoritative or mandatory access control based on the following concept:

To separate virtual machines and their resources at runtime AppArmor rules defined by AppArmor policies are used. The virtual machine resources are labeled to belong to one particular virtual machine by that policy. In addition a virtual machine is awarded a unique label by that policy. The TOE ensures that virtual machines can only access resources bearing the same label.

3.7 Virtual Machine Environments

The TOE implements the host system for virtual machines. It acts as a hypervisor which provides an environment to allow other operating systems execute concurrently.

3.8 Security Management

The security management facilities provided by the TOE are usable by authorized users and/or authorized administrators to modify the configuration of the TSF.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The Security Target [ST] makes ten assumptions on the usage and the operative environment of the TOE.

A.PHYSICAL

It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.MANAGE

The TOE security functionality is managed by one or more competent individuals. The system administrative personnel are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.

A.AUTHUSER

Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

A.TRAINEDUSER

Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.

A.DETECT

Any modification or corruption of security-enforcing or security-relevant files of the TOE, user or the underlying platform caused either intentionally or accidentally will be detected by an administrative user.

A.PEER.MGT

All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to be under the same management control and operate under security policy constraints compatible with those of the TOE.

A.PEER.FUNC

All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality.

A.IT.FUNC

The trusted IT systems executing the TOE are assumed to correctly implement the functionality required by the TSF to enforce the security functions.

A.KEYS

It is assumed that digital certificates, certificate revocation lists (CRLs) used for certificate validation, private and public keys, as well as passwords used for:

- SSH client authentication,
- SSH server authentication,
- Password protecting the disk encryption schema

generated externally or by the TOE, meeting the corresponding standards and providing sufficient security strength through the use of appropriate key lengths and message digest algorithms. It is also assumed that Administrators verify the integrity and authenticity of digital certificates and key material before importing them into the TOE, and verifying that certificates are signed using strong hash algorithms.

A.CONNECT

All connections to and from remote trusted IT systems and between physically-separate parts of the TSF not protected by the TSF itself are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

4.2 Organizational Security Policies

The Security Target [ST] contains four Organizational Security Policies which have been considered during the evaluation of the TOE.

P.ACCOUNTABILITY

The users of the TOE shall be held accountable for their security-relevant actions within the TOE.

P.USER

Authority shall only be given to users who are trusted to perform the actions correctly.

P.PROTECT_SSH_KEY

When using SSH with public-key-based authentication, organizational procedures must exist that ensure users protect their private SSH key component against its use by any other user.

Note: The protection of the key can be established by access permissions to the file holding the key (when using the OpenSSH client, the key file permissions are automatically verified and the key is rejected if the permissions are not restrictive), or by encrypting the key with a passphrase. Making the SSH private key available to any other user is akin to telling that user the password for password-based authentication.

P.CP.ANCHOR

Users shall control the confidentiality protection anchor for their confidentiality-protected user data, and reset/replace/modify it if desired.

4.3 Clarification of Scope

The Security Target contains eleven threats, which have been considered during the evaluation.

T.ACCESS.TSFDATA

A threat agent might read or modify TSF data without the necessary authorization when the data is stored or transmitted.

T.ACCESS.USERDATA

A threat agent might gain access to user data stored, processed or transmitted by the TOE without being appropriately authorized according to the TOE security policy.

T.ACCESS.TSFFUNC

A threat agent might use or modify functionality of the TSF without the necessary privilege to grant itself or others unauthorized access to TSF data or user data.

T.ACCESS.COMM

A threat agent might access a communication channel that establishes a trust relationship between the TOE and another remote trusted IT system or masquerade as another remote trusted IT system.

T.RESTRICT.NETTRAFFIC

A threat agent might get access to information or transmit information to other recipients via network communication channels without authorization for this communication attempt by the information flow control policy.

T.IA.MASQUERADE

A threat agent might masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to user data, TSF data, or TOE resources.

T.IA.USER

A threat agent might gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated.

T.ACCESS.COMPENV

A threat agent might utilize or modify the runtime environment of other compartments in an unauthorized manner.

T.INFOFLOW.COMP

A threat agent might get access to information without authorization by the information flow control policy.

T.COMM.COMP

A threat agent might access the data communicated between compartments or between a compartment and an external entity to read or modify the transferred data.

T.ACCESS.CP.USERDATA

A threat agent might gain access to user data at rest which is confidentiality protected without possessing the authorization of the owner, either at runtime of the TOE or when the TSF are inactive.

5 Architectural Information

Ubuntu is a highly-configurable Linux-based operating system which has been developed to provide a good level of security as required in commercial environments.

Ubuntu provides virtualization environment based on the Linux KVM technology. Ubuntu implements the host system for the virtual machine environment and manages the virtual machines. In addition, Ubuntu provides management interfaces to administer the virtual machine environment as well as full auditing of user and administrator operations.

The KVM technology separates the runtime environment of virtual machines from each other. The Linux kernel operates as the hypervisor to the virtual machines but provides a normal computing environment to administrators of the virtual machines. Therefore, the Linux kernel supports the concurrent execution of virtual machines and regular applications. Ubuntu uses the processor virtualization support to ensure that the virtual machines execute close to the native speed of the hardware.

In addition to the separation of the runtime environment, Ubuntu also provides system-inherent separation mechanisms to the resources of virtual machines. This separation ensures that the large software components used for virtualizing and simulating devices executing for each virtual machine cannot interfere with each other. The AppArmor policy also restricts virtual machines to a set of defined resources assigned to the respective virtual machine. Any other resource, including general operating system resources or resources from other users are inaccessible based on the AppArmor restrictions. Using the AppArmor policy, the virtualization and simulation software instances are isolated. The virtual machine management framework uses AppArmor transparently to the administrator. The virtual machine management framework assigns each virtual machine a unique AppArmor label. In addition, each resource dedicated to this virtual machine is assigned the same AppArmor label. The AppArmor policy enforces based on these labels that a virtual machine can only access its own resources. Resources from other virtual machines, the hosting operating system as well as other users are inaccessible.

6 Documentation

The Evaluated Configuration Guide [ECG] explains how to set up the TOE in accordance with the evaluated configuration.

General guidance for the functionality of the TOE is provided through the man pages, which are part of the TOE.

7 IT Product Testing

7.1 Developer Testing

The developer performed extensive automated testing on two hardware platforms:

IBM s390x (z architecture mainframe) with IBM z14 processors

Supermicro SYS-5018R-WR server with Xeon processor.

The developer testing has a good coverage of almost all TSFI functionality on both external and internal interfaces.

All tests were successful, and the results were as expected.

7.2 Evaluator Testing

The evaluator repeated all the automated developer tests, along with the evaluator's independent tests, on both hardware platforms:

IBM s390x (z architecture mainframe) with IBM z14 processors

Supermicro SYS-5018R-WR server with Xeon processor.

A number of extra tests were also run on the Supermicro platform.

All tests were successful, and the results were as expected.

7.3 Penetration Testing

The evaluator performed "DBus fuzzing" and "syscall thrashing" on the

Supermicro SYS-5018R-WR server with Xeon processor.

No problems were found during the penetration testing.

However, the vulnerability database search revealed some residual vulnerabilities. Residual vulnerabilities are vulnerabilities that are out of scope because they require a higher attack potential than the actual EAL is designed to protect from.

The residual vulnerabilities are: CVE-2018-20623, CVE-2019-1549, CVE-2020-8648, CVE-2020-10942, and CVE-2020-24977.

8 Evaluated Configuration

The TOE has been tested on the following hardware platforms:
IBM s390x (z architecture mainframe) with IBM z14 processors
Supermicro SYS-5018R-WR server with Xeon processor.

The instruction in the Evaluated Configuration Guide [ECG] must be followed during installation.

The TOE supports the use of IPv4 and IPv6, both are also supported in the evaluated configuration. IPv6 conforms to the following RFCs:

- RFC 2460 specifying the basic IPv6 protocol
- IPv6 source address selection as documented in RFC 3484
- Linux implements several new socket options (IPV6_RECVPKTINFO, IPV6_PKTINFO, IPV6_RECVHOPOPTS, IPV6_HOPOPTS, IPV6_RECVDSTOPTS, IPV6_DSTOPTS, IPV6_RTHDRDSTOPTS, IPV6_RECVRTHDR, IPV6_RTHDR, IPV6_RECVHOPOPTS, IPV6_HOPOPTS, IPV6_{RECV,}TCLASS) and ancillary data in order to support advanced IPv6 applications including ping, traceroute, routing daemons and others.
- Transition from IPv4 to IPv6: dual stack, and configured tunnelling according to RFC 4213.

The default configuration for identification and authentication are the defined password-based PAM modules as well as public-key based authentication for OpenSSH. Support for other authentication options, e.g. smart card authentication, is not included in the evaluation configuration.

If the system console is used, it must be subject to the same physical protection as the TOE.

Deviations from the configurations and settings specified with the Evaluated Configuration Guide are not permitted.

The TOE comprises a single system (and optional peripherals) running the TOE software listed. Cluster configurations are not permitted in the evaluated configuration.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Systematic Flaw Remediation	ALC_FLR.3	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Certifier Comments and Recommendations

As the threat landscape is shifting at a high pace, the current security level can swiftly change, as new potential vulnerabilities that could affect the TOE or its underlying platform are regularly discovered. The certifier notes that for many scenarios a reasonable policy would be to keep products up to date with the latest version of the firmware/software. However, the benefit of installing firmware/software updates must be balanced with the potential risks that such changes might have unexpected effect on the behavior of the evaluated security functionality. Ubuntu LTS is intended to be updated over time as indicated by the augmentataion by ALC_FLR.3. The developer intends to maintain and update the TOE in order to keep it relevant over time.

12 Glossary

AppArmor	Application Armor, Linux kernel Security Module
CPU	Central Processing Unit
CRL	Certificate Revocation List
DAC	Discretionary Access Control
DBUS	Desktop Bus (a software bus)
ECG	Evaluated Configuration Guidance
GID	Group Identifier
GPG	GNU Privacy Guard
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IOCTL	Input/Output Control
LAF	Lightweight Audit Framework
LTS	Long-term Support
OpenSSH	Open Secure Shell
OSI	The Open Systems Interconnection model
PAM	Password-based Modules
PoC	Proof of Concept
RFC	Request for Comments
SHA	Secure Hashing Algorithm
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
UDP	User Datagram Protocol
UID	User Identifier

13 Bibliography

ST	Security Target for Ubuntu 18.04 LTS, Canonical Group Limited, 2020-12-02, document version 1.0
ECG	Evaluated Configuration Guide, Canonical Group Limited, 2020-04-08, document version 0.3
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003
CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004
SP-002	SP-002 Evaluation and Certification, CSEC, 2019-11-30, document version 32.0
SP-188	SP-188 Scheme Crypto Policy, CSEC, 2020-11-03, document version 10.0

Appendix A Scheme Versions

A.1 Quality Management System

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was entered into the registry 2020-01-08:

QMS 1.23 valid from 2019-10-14

QMS 1.23.1 valid from 2020-03-06

QMS 1.23.2 valid from 2020-05-11

QMS 1.24 valid from 2020-11-19

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.24".

The certifier concluded that, from QMS 1.23 to the current QMS 1.24, there are no changes with impact on the result of the certification

A.2 Scheme Notes

The following Scheme Notes has been considered during the evaluation:

Scheme Note 15 Demonstration of test coverage v4.0

Clarifications on testing.

Scheme Note 18 Highlighted requirements on the Security Target v3.0

Clarifications concerning requirements on the Security Target.

Scheme Note 22 Vulnerability assessment v3.0

Clarifications regarding the vulnerability assessment.

Mandatory update of the vulnerability database search, if older than 30 days, at the end of the evaluation.