1 Common Criteria

Common Criteria is the best known and most widely used methodology to evaluate and measure the security value of an IT product. The methodology aims to be independent, as an independent laboratory conducts the evaluation, which a certification body will certify afterward. Security Functional Requirements (SFR) are summarized in so-called Protection Profiles (PP). If the definition of a Security Target (ST) and the Evaluation Assurance Levels (EAL) are comparable, this allows the comparison of security functions of different products. (The definition of a Security Target typically references the PP—if one exists that fits the purpose of the product).

1.1 Introduction

A clear definition of security in IT products is challenging. Security should be considered a process that never ends, not a static condition that can be met or not. A Common Criteria certificate (below EAL7) does not make a clear statement about error-proneness of the system, but it adds an important value to the product that cannot be described with the presence of technology alone: That someone has independently inspected the design of the system in such way that it corresponds to the claims that are made, and that explicit care has been taken in producing and maintaining the product.

The certificate states a degree of maturity of both the product with its security functions and the processes of the company that has designed, built and engineered the product, and that will maintain the product across its lifecycle. As such, Common Criteria aims to be fairly holistic with its approach to take everything into account that is relevant for the security of an IT product.

1.2 Evaluation Assurance Level (EAL)

The Evaluation Assurance Level denotes the degree of confidence that the product fulfills the described claims. The levels are from 1 through 7:

- EAL1: Functionally tested
- EAL2: Structurally tested

- EAL3: Methodically tested and checked
- EAL4: Methodically designed, tested and reviewed
- EAL5: Semi-formally designed and tested
- EAL6: Semi-formally verified design and tested
- EAL7: Formally verified design and tested

While EAL1 only provides basic assurance for products to meet security requirements, EAL2 to 4 are medium assurance levels. EAL5-EAL7 describe medium-to-high and high assurance. EAL4 is expected to be the highest level of assurance that a product can have if it has not been designed from the start to achieve a higher level of assurance.

1.3 Generic Guiding Principles

Much of the advice in this guide is based on the following guidelines. Consider them when defining your own security processes or deciding about configurations that are not explicitly covered here.

Use Data Encryption Whenever Possible

Refer to the *About This Guide* section of this guide. In *Section 1, "Assumptions and Scope"*, the limitations of cryptography are briefly outlined.

Be aware that cryptography is certainly useful, but only for the specific purposes that it is good for. Using cryptography is not a generic recipe for better security in a system, its use may even impose additional risk on the system. Make informed decisions about the use of cryptography, and feel obliged to have a reason for your decisions. A false sense of security can be more harmful than the weakness itself.

SUSE Linux Enterprise Server supports encryption for:

- Network connections (the **`openssl`** command, **`stunnel`**), for remote login (**`openssh`**, **`man ssh(1)`**)
- Files (**`gpg`**)
- Entire file systems at block layer (`dm-crypt`, **`cryptsetup`**)
- VPN (**`ipsec`**, **`openvpn`**)

Minimal Package Installation

It is useful to restrict the installed packages in your system to a minimum. Binaries not installed cannot be executed.

During installation of the system, you can limit the set of packages that is installed. For example, you can deselect all packages and select only those that you want to use. For example, the selection of the `apache2-mod_perl` package in YaST would automatically cause all packages to be selected for installation that are needed for the Apache package to operate. Dependencies have often been artificially cut down to handle the system's dependency tree more flexibly. You can chose the minimal system, and build the dependency tree from there with your (leaf) package selection.

Service Isolation—Run Different Services on Separate Systems

Whenever possible, a server should be dedicated to serving exactly one service or application. This limits the number of other services that could be compromised if an attacker can successfully exploit a software flaw in one service (assuming that flaw allows access to others).

The use of AppArmor for services that are provided on a system is an effective means of containment. For more information, see *Book "*Security Guide*"* and the man page of **apparmor**.

The use of virtualization technology is supported with SUSE Linux Enterprise Server. While virtualization is generally designed for server consolidation purposes, it is also usefulness for service isolation. However, virtualization technology *cannot* match or substitute the separation strength that is given by running services on different physical machines! Be aware that the capability of the hypervisor to separate virtual machines is not higher or stronger than the Linux kernel's capability to separate processes and their address spaces.

System Fingerprinting and Backups

Doing regular backups and having a fingerprint of your system is vital, especially in the case of a successful attack against your system. Make it an integral part of your security routine to verify that your backups work.

A fast and directly accessible backup adds confidence about the integrity of your system. However, it is important that the backup mechanism/solution has adequate versioning support so that you can trace changes in the system. As an example: The installation times of packages (`rpm -q --queryformat='%{INSTALLTIME} %{NAME}\n' PACKAGE NAME`) must correspond to the changed files in the backup log files.

Several tools exist on SUSE Linux Enterprise Server 15 SP2 which can be used for the detection of unknown, yet successful attacks. It does not take much effort to configure them.

In particular, we recommend using the file and directory integrity checker `AIDE` (Advanced Intrusion Detection Environment). When run for initialization, it creates a hash database of all files in the system that are listed in its configuration file. This allows verifying the integrity of all cataloged files at a later time.

Warning: Backdoors

If you use AIDE, copy the hash database to a place that is inaccessible for potential attackers. Otherwise, the attacker may modify the integrity database after planting a backdoor, thereby defeating the purpose of the integrity measurement.

An attacker may also have planted a backdoor in the kernel. Apart from being very hard to detect, the kernel-based backdoor can effectively remove all traces of the system compromise so system alterations become almost invisible. Consequently, an integrity check needs to be done from a rescue system (or any other independent system with the target system's file systems mounted manually).

Be aware that the application of security updates invalidates the integrity database. `rpm -qlv packagename` lists the files that are contained in a package. The RPM subsystem is very powerful with the data that it maintains. It is accessible with the `--queryformat` command line option. A differential update of integrity database with the changed files becomes more manageable with some fine-grained usage of RPM.

1.4 For More Information

The Common Criteria evaluations inspect a specific configuration of the product in an evaluated setup. How to install and configure the reference system that was used as baseline in the Common Criteria evaluation is documented in an “Administrator's Guide”, which is part of the Common Criteria evaluation documentation.

However, it would be incorrect to understand the evaluated configuration as a *hardened* configuration. The removal of setuid bits and the prescription of administrative procedures after installation help to reach a specific configuration that is sane. But this is not sufficient for a hardening claim.

- For more information about SUSE Linux Enterprise Server security certifications and features, see https://www.suse.com/support/security/certifications/.
- Find a list of SUSE security resources at https://www.suse.com/support/security/.
- Apart from the documentation that comes with the Common Criteria effort, see also the following manual pages:

  pam(8), pam(5)
  apparmor(7) and referred man pages
  rsyslogd(8), syslog(8), syslogd(8)
  fstab(5), mount(8), losetup(8), cryptsetup(8)
  haveged(8), random(4)
  ssh(1), sshd(8), ssh_config(5), sshd_config(5), ssh-agent(1), ssh-add(1), ssh-keygen(1)
  cron(1), crontab(5), at(1), atd(8)
  systemctl(1), daemon(7), systemd.unit(5), systemd.special(5), kernel-command-line(7), bootup(7), systemd.directives