Common Criteria Demystified
Have you tried out our new XYZ OS?
Have you tried out our new XYZ OS?

No, why should I?
Have you tried out our new XYZ OS?

It’s so secure

No, why should I?
Have you tried out our new XYZ OS?

It’s so secure

No, why should I?

How secure?
Have you tried out our new XYZ OS?

It’s so secure

Very

No, why should I?

How secure?
Have you tried out our new XYZ OS?

It’s so secure

Very

No, why should I?

How secure?

Prove it!
What would it take to prove it?
What would it take to prove it?

Independent 3rd party review that includes:
• Code review
What would it take to prove it?

Independent 3rd party review that includes:
• Code review
• Testing
What would it take to prove it?

Independent 3rd party review that includes:
- Code review
- Testing
- Review of the Development Process
What would it take to prove it?

Independent 3rd party review that includes:
• Code review
• Testing
• Review of the Development Process
• A list of Security Features and the Threats they counter
What would it take to prove it?

Independent 3rd party review that includes:

- Code review
- Testing
- Review of the Development Process
- A list of Security Features and the Threats they counter
- Security Guidance so I can lock it down
What would it take to prove it?

Independent 3\textsuperscript{rd} party review that includes:
- Code review
- Testing
- Review of the Development Process
- A list of Security Features and the Threats they counter
- Security Guidance so I can lock it down
- A vulnerability assessment so that I know you’ve patched everything
Is that all?
Is that all?

Maybe some penetration testing because bad guys do that, too
Is that all?

Maybe some penetration testing because bad guys do that, too

Sounds like a lot of work
Is that all?
  Maybe some penetration testing because bad guys do that, too
Sounds like a lot of work
  Maybe so, but serious claims demand serious proof
Common Criteria is an internationally agreed upon set of requirements that:

- Facilitates comparability of independent security evaluations
- Provides a common set of requirements for security functionality
- Requires assurance measures applied during product development and evaluation

Common Criteria addresses protection of assets from unauthorized disclosure, modification, or loss of use
Acronyms and Terms Used in Common Criteria

TOE - Target of Evaluation
PP - Protection Profile
ST - Security Target
TSF - TOE Security Functionality
SFR - Security Function Requirements
Acronyms and Terms Used in Common Criteria

Developer - Company that makes a Product
Scheme - Government agency that sets security rules
Assurance - Confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted
A threat consists of an adverse action performed by a threat agent on an asset. Adverse actions influence one or more properties of an asset from which that asset derives its value. Examples of threat agents are: hackers, users, computer processes, and accidents.

Example from OSPP:

T.LOCAL_ATTACK
An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.
Assumptions

● The accepted beliefs around the operational environment that Security Functions will not address
● If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide its security functionality

Example from OSPP:

A.PROPER_ADMIN
The administrator of the OS is not careless, willfully negligent, or hostile, and administers the OS within compliance of the applied enterprise security policy.
A security objective is a concise and abstract statement of the intended solution to the Threat under stated assumptions

- May be levied on TOE or the Operational Environment

Example from OSPP:

O.PROTECTED_COMMS
To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant OSes provide mechanisms to create trusted channels for CSP and sensitive data. Both CSP and sensitive data should not be exposed outside of the platform.
Security Function Requirements (SFR)

- SFR’s are a translation of the Security Objective into a detailed and complete level of abstraction but independent of any specific technical solution.

Example from CC Part2:

When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions].
Security Function Components

- Protection of TSF
- Audit
- User Data Protection
- Identification & Authentication
- Cryptographic Support
- Resource Utilization
- Trusted Path
- Communication
- Privacy
- Security Management
- TOE Access
A PP is intended to describe a type of Product
- Contains Threats, Objectives, Assumptions, Operational Environment, SFRs, and Assurance Activities that this kind of Product may encounter

Many Products may evaluate to the same PP

Typically written by:
- A user community seeking to come to a consensus on the requirements for a given Product type
- A government specifying its requirements as part of its acquisition process
Categories of PP’s

Examples of Product types with a PP:
● Application Software
● Operating System ← OSPP
● Full Disk Encryption
● Network Device
● Firewall
● VPN Gateway
● Multifunction Printer
● Mobile Device
● USB Flash drive
● Smart Card
● VOIP
The Security Target is a further detailing of the PP that explains how the TOE meets the Security Objectives for the listed Threats:
- Contains a TOE summary specification, showing how the SFRs are implemented in the TOE
- Talks about exact technologies like SELinux, pam, or the kernel
- Provides a structured description of the activities to determine correctness of the TOE in the form of Security Assurance Requirements

Serves as a basis for agreement between the developer and the evaluator on the exact security properties of the TOE and the exact scope of the evaluation.
Electives

- A PP transcribes SFR’s from the Common Criteria Catalog with some solutions imposed.
- Many SFR’s contain options describing different ways to counter a threat.
- ST writer removes possible solutions leaving the actual implementation.

Example (before and after)

When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: list of actions].

When the defined number of unsuccessful authentication attempts has been met, the TSF shall disable the user logon account until it is re-enabled by the authorized administrator.
Assurance Requirements

- Assurance requirements are a description of what the evaluator will do to confirm that the SFR is fully met by an implementation.
- Results are recorded as evidence to be used in an Assurance Argument by the Lab to a scheme that approves the certification.

Example from OSPP:
- Test 3: The evaluator will attempt to modify all shared libraries that are used throughout the system.
- Test 4: The evaluator will attempt to modify all system executables.
- Test 5: The evaluator will attempt to modify all system configuration files.
The Evaluation (tying it all together)

● A Developer picks a PP
● That PP is supported by specific schemes (nations)
● The scheme has accredited a number of labs that it tests periodically to verify their capabilities
● The developer contracts a lab to conduct an evaluation of the ST following the Assurance Activities to prove the TOE counters Threats.
● The Lab conducts testing and submits paperwork to the scheme
● The scheme reviews documentation to determine if test results, methodologies, facility, developer documentation, user guidance meets are requirements
● If so, a Certificate is Issued stating the product meets all requirements
● Otherwise, more testing or documentation may be required
● All signatory countries to the Mutual Recognition Treaty accept the evaluation
How can I help?

- For your product type, find the PP (if one exists) and read it
- Look at the SFR’s to see if they are met
- If the SFR has electives, try to provide as broad a coverage as possible so the ST writer can claim as much as possible
Yes, But Why Should I Care?

- Because your customers care
  - Common Criteria recognized worldwide by dozens of countries
- Because it’s mandatory
  - Most federal customers require Common Criteria evaluated products be purchased over those without evaluation
- Because others are doing it
  - Other OS vendors, container runtimes, virtualization, etc
- Because you want to ensure your hard work reaches the hands of people who want to use it!
The RHEL Common Criteria Status Today

- Generally, only once or twice per major RHEL Release
  - Test development & evaluation took years to complete
  - Evaluation only applies to the OS itself, not the layered products
- RHEL 7.1 has been evaluated twice:
  - General Purpose Operating System Protection Profile (GP OSPP)
  - versions 2.0 and 3.9 of this Profile*
  - Intel x86_64 and IBM Power architectures
- RHEL 7.6 is next!
  - New GP OSPP version 4.2
  - Test-driven evaluation process - much faster to complete
    - Evaluation must be completed within 180 days once entered
  - Some profile limitations in what can be claimed

* [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org) for more info
What’s Possible Moving Forward

- RHEL 8.0 is designed for Common Criteria evaluation
  - The planned target for evaluation will be the first minor release of RHEL 8
  - Targeting OSPP 4.2 or 4.3 (adds TLS 1.3 support)
- Shorter evaluation times will lead to more frequent evaluations!
- Seeking additional enhancements to GP OSPP:
  - Mandatory Access Control (MAC) / SELinux requires extensions to the PP
  - Need a way to support Secure Boot requirement on non x86_64
What’s Next For YOU?

- Learn more about Common Criteria
- Support a layered product? Find out if there is a Protection Profile that works
- Ask questions!
  - Especially if you are working on components of the OS that are part of the Target of Evaluation (ToE)
Questions?

sgrubb@redhat.com
mthacker@redhat.com
Owners → Confidence → Countermeasures → Sufficient → Risk → Assets
Owners require Confidence that Countermeasures are Correct, which are sufficient and therefore minimise Risk to Assets.
Sufficiency

- A high level justification in the ST that the Security Objectives are able to counter each threat.
- Provides a tracing of which objectives remove, diminish or mitigate a threat.
- Only found in the Security Target and summarizes how a threat was countered

The threat of accessing TSF data without proper authorization (T.ACCESS.TSFDATA) is mitigated by:

- O.DISCRETIONARY.ACCESS requiring that data, including TSF data stored with the TOE, have discretionary access control protection,
- O.SUBJECT.COM requiring the TSF to mediate communication between subjects.