How to write PPs and STs – ISO/IEC TR 15446 The PPST Guide

Dr. Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk

Common Criteria

What is ISO/IEC TR 15446?

- Guide for the production of Protection Profiles and Security Targets
- A Technical Report
  - *Not Quite A Standard*
  - *In this case, an advisory guide*
- ISO Document, not endorsed by CCDB
  - *Refers exclusively to ISO/IEC 15408*
  - *But actually equally applicable to CC*


TECHNICAL REPORT

ISO/IEC TR 15446

Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets

Brief history

- Need for supporting document to explain CC/15408 criteria identified:
  - *First Draft 1996*
  - *Approved for Publication 2000*
  - *Published 2004*
  - *Available for Free Download 2005*
- Publication delayed due to resourcing issues
- Lost influence and impact as a result

Availability

- Can be purchased as paper or pdf from ISO in Geneva
  - *ISO Online Store CHF 216 (approx €130)*
- Can be purchased from National Standards Bodies
- But can also be downloaded for free from ISO in Geneva!

A Reminder:
ISO/IEC TR 15446:2004 is available for free download from:

http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/ITTF.htm

(select “freely available standards” and page through list)

TR 15446:2004

- Matched CC Version 2.1 (ISO/IEC 15408:1999)
- Contents:
  - *Explanation of CC rules and requirements*
  - *Generic examples (threats, policies, assumptions, objectives)*
  - *Mapping threats to objectives*
  - *SFRs corresponding to common requirements*
  - *Expressing crypto functionality in CC*
  - *Three worked examples of PPs:*
    - Firewall, Database, Trusted Third Party

Common Criteria

Problems

- Produced by people trying to understand new criteria, not people passing on real-world experience
- Mainly produced by evaluators, not product and system developers
  - *Very little on identifying threats, policies, assumptions*
  - *Very little practical advice on writing PPs/STs*

Consequences

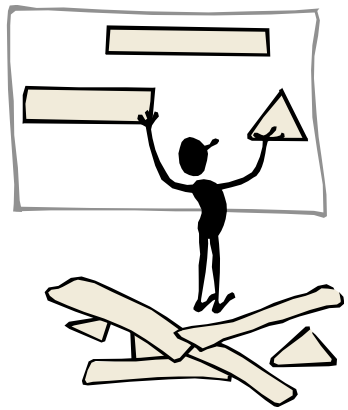
- Mainly about “What”, not “How” or “Why”
- Applicable to and influenced CC V2, much less relevant to CC V3
- Never adopted as an official Supporting Document by CCDB

Early Revision

- Normal ISO practice is to start revision five years after publication
- Revision normally takes at least three years
- Revision of TR 15446 approved in November 2005
  - *Four years early*
- Why?

Why early revision?

- See presentation at 6th ICCC
- Major weaknesses identified
- Needed to be updated to CCV3.1
- Some content no longer appropriate
- Not enough practical help

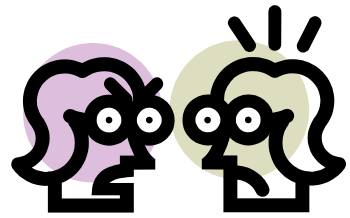


Revision Process

- Mike Nash (Gamma, UK) and Helmut Kurth (Atsec, US) appointed as joint Project Editors
- Started revision work February 2006
  - *Document completely restructured*
  - *Topics removed, new topics added*
  - *Document almost entirely rewritten*
- Final ballot closes September 26th 2008
  - *Could be published November 2008!*

ISO consensus

- Often a problem to get consensus within a standards development group
- However authors had very extensive practical experience and got it right first time (mostly)
- Most review comments were constructive, incisive and practical
  - *A few cases of "we do it differently so your way must be wrong"*



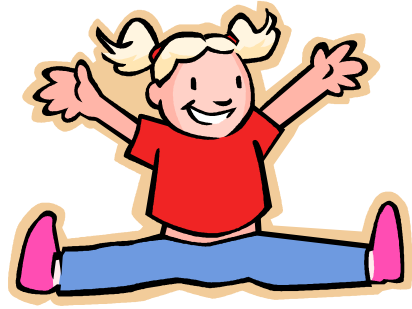
Common Criteria

Structural Changes

- Now no description of what to put in a PP or ST
  - *Found in CC V3.1 Part 1 Annexes A/B*
- Now no lists of generic examples
  - *Widely misunderstood as prescriptive*
- Now no worked examples of PPs or STs
  - *Examples for real products readily available*

Instead, just...

- Uses of PPs and STs
- Reading and understanding PPs and STs
- Specifying PPs and STs
- How to deal with special cases



Specifying a PP or ST

- CC V3.1/15408 now define the required contents
- The new PPST Guide has a section for each stage of the specification process:
  - *Introduction, SPD, objectives, requirements, Summary Specification*
- Each stage broken down into tasks to be performed by the PP/ST author
  - *Possible methodology and practical hints supplied for each task*

Common Criteria

Methodologies

- All used in practice and in public domain
- Mostly published at ICCC or by national schemes
  - *Example: "Reading a PP/ST" based on BSI Guide (as presented at ICCC8)*
- Surprising degree of modularity

Common Criteria

Philosophy

- There are many ways to prepare a PP or ST
- Every single one of them is right!
- For each step of the production process, the PPST Guide describes one possible way
  - *You can follow it or not*
  - *The rest of the Guide remains valid and relevant*

Practical Advice

Lots of checklists

One common approach, and the one recommended by this methodology, is to use a fixed list of five types of threat agent:

Lots of detail

There are only two instances in the list of SARs in ISO/IEC 15408-3 where assignments are allowed: ADV_INT.1.1D and ADV_SPM.1.1D. In the first case the PP/ST author needs to define with the assignment the subset of the TSF for which the element applies, in the second case the PP/ST author needs to define with the assignment the set of security policies that are formally modelled.

Lots of hints and examples

One test of whether you have pitched your security objectives at the correct level of detail will come when you construct the rationales for the security objectives and the security requirements. If one rationale is trivial whilst the other is large, complex and difficult to understand, it is likely that your security objectives are either too detailed or too abstract, depending on which step is too complex.

A warning

- ISO rules on public availability have changed
- Published PPST Guide 2008 will **not** be available for ISO no cost download
- Final draft version and a list of later changes **will** be available on the web if you know where to look

How to write PPs and STs – ISO/IEC TR 15446 The PPST Guide

Dr. Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk

Common Criteria