
The ISO PPST Guide – Tool or Irrelevance?

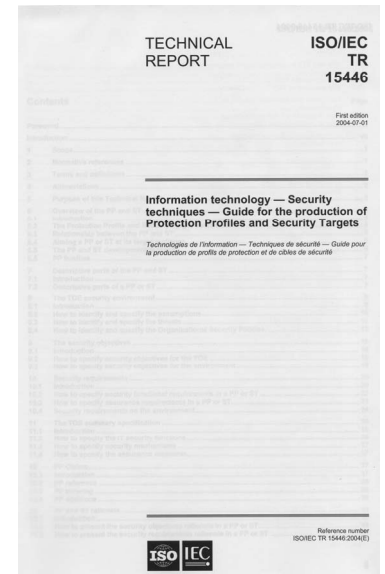
Dr. Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk

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 V2.1*



History

- Need for supporting document to CC/15408 identified:
 - *First Draft 1996*
 - *Approved for Publication 2000*
 - *Published 2004*
 - *Available for Free Download 2005*

- Not an example of prompt and efficient standardisation!

- Why?

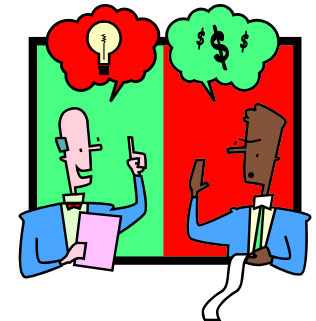
Personnel

- Large document, therefore key role for editor
- Editor assigned other work responsibilities by employer
- Eventually resigned editorship and left WG3
- Hiatus before this speaker took over



Consensus

- Standards Working Groups work by consensus
- Guidance is subjective and best practice continually develops
- Difficult to avoid revisiting past decisions



Availability

- Standards Bodies make lots of money from selling standards
 - *BSI: TR 15446 GBP 160*
 - *ANSI: TR 15446 USD 165*
 - *JSA: TR 15446 JPY 20,034*
- Reluctant to permit free downloading
- And to advertise it when it exists!



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

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

What Does It Contain?

- Section by Section guidance for PP and ST Contents

- Appendices:
 - *Guidance Checklist*
 - *Generic examples of threats, policies etc.*
 - *Section on cryptographic functionality*
 - *Three worked examples:*
 - *Firewall PP, Database PP, Trusted Third Party PP*

Origin

- 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*
 - *Nothing on composition, evaluation reuse etc.*

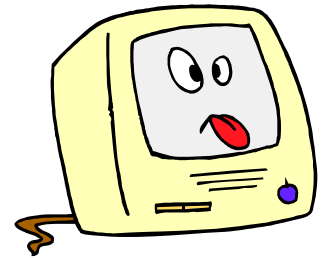
Consequences

- Mainly about “What”, not “How” or “Why”
- Applicable to and influenced CC V2, much less relevant to CC V3



How Useful Is It?

- Varies from section to section
- Often helpful, but not in depth
- Worked Examples now obsolete
 - *Produced originally against CC V1*
 - *Better models (real PPs) exist*
 - *No proper examples of STs*



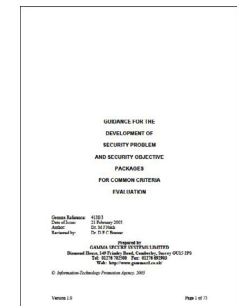
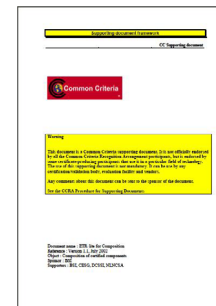
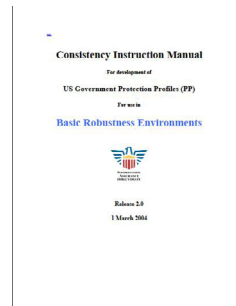
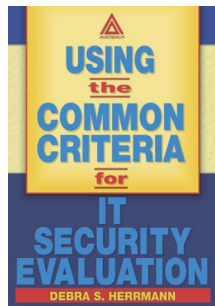
The Future

- Is it worth updating?
- Does it need to be no-cost downloadable?
- Is its scope right?



Is It Worth Updating?

- Other sources of information now exist
 - *Books explaining CC*
 - *Consistency Instruction Manuals*
 - *“Supporting Documents”*



- Are best methods proprietary?

“No Cost” Availability

- Very hard to get no-cost availability for current document
- The rules have been changed to stop it happening again!
- Really needs CCDB endorsement and joint publication to remain Free of Charge



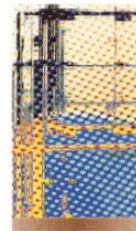
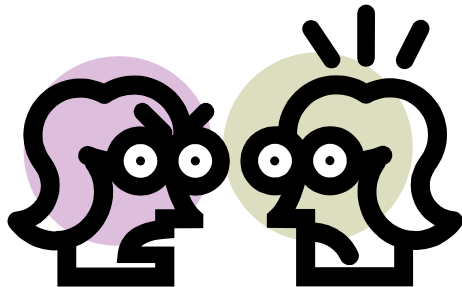
Best Practice

- Proprietary Knowledge and Techniques
- Will experts in writing PPs and STs be allowed to contribute?
- Can published PPs/STs be recommended as examples?
- Can experts be bothered to contribute?



What Should the Scope be?

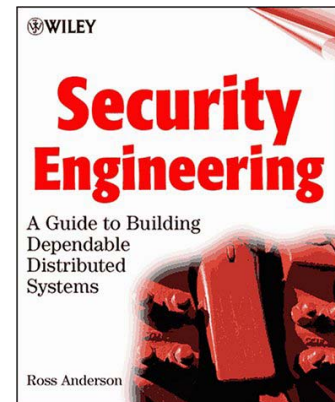
- Should it include examples?
- How should it deal with contentious areas?
- Should it cover threat and policy identification?



The ISO/IEC Common Criteria for Information Technology Security Evaluation could benefit from focusing on development, rather than evaluation, to provide assurance.

What About “Why” and “How”

- More subjective, often contentious
- Are reasons and techniques important or not?



What Does the Audience Think?

Over to you

The ISO PPST Guide – Tool or Irrelevance?

Dr. Mike Nash

Gamma Secure Systems Limited

www.gammassl.co.uk