Study Period on IT Security Testing, Evaluation and Assurance Standards and Techniques leading to an update of the WG3 roadmap

Motivation

During the lifetime of SC27 WG3 (25 years) many of the technologies involved[1], and the expectations of those using IT security standards have changed. Some of the standards relating to IT product security have also changed (and new standards have been/are being developed). An important set of standards in the area of IT product security evaluation: ISO/IEC15408 and ISO/IEC18045, are due for review (in collaboration with the CCDB). To perform this review, in the most effective manner, the working group has launched a study period which, while having ISO/IEC15408 and ISO/IEC18045 as a focus, covers all relevant standards in order to provide a sound basis for updating the WG3 roadmap.

In discussion amongst WG3 experts at the Jaipur meeting the following observations were made:-

- No significant update to ISO/IEC 15408 and ISO/IEC 18045 in the last 10 years.
- Development practices have changed since the standards were produced
- Tools and techniques for assisting evaluation have also changed
- There are pressures to make evaluation more efficient and effective
- There are increasing calls from regulation/policy bodies for clear and consistent certification of IT product security to satisfy their needs (for example for critical infrastructures).
- The standards are also used outside of government focused recognition arrangements (e.g. finance industry, transport, etc.) and need to take account of those needs
- The standards are being used in very different ways e.g.
    - Conformance vs highly skilled, loosely guided, expert evaluator.
    - Search for vulnerabilities in a single product vs overall product development process improvement
    - Using transparent vendor assertion vs evaluator judgement
    - In widely different markets (government procurement vs financial etc.)
- Vulnerabilities always remain. Some of the bodies involved do not consider the search for vulnerabilities to be the primary aim of the evaluation, whereas other bodies consider the vulnerability evaluation as an essential part.
- Evaluations may improve developer process but not by applying ISO/IEC15408 process requirements
- Some aspects (such as composition) are not fully addressed by ISO/IEC 15408 and ISO/IEC 18045
- There is also a need to provide better information for system integrators
- These wide differences can lead to non comparability/lack of trust of results and tensions in recognition.
- Ensuring comparability (where it is needed)
- The absence of performance metrics hinders the development (and use) of the standards (it is not possible to convincingly argue what works and what doesn't).
- The recent update to the CCRA, with its support for collaborative Protection Profiles developed by industry, highlights a need to support relatively fast moving updates to some of the documents associated with evaluation while still ensuring appropriate levels of consistency/comparability between evaluations.
- There is a need for a robust and clear mapping between all relevant assurance standards (e.g. ISO/IEC 27034, 19790, 17825, and 20543)

[1] and their development approaches

Scope

The scope of this study encompasses all aspects of IT product security assurance. Whilst it has a primary focus upon ISO/IEC 15408 and ISO/IEC 18045, it is most important that the result of the study period(s) also provides a good foundation for update of the WG3 roadmap and clearly identifies areas where other standards have relevance to IT product security assurance (for example ISO/IEC 27034 for product development lifecycle aspects).

Expected timeframe

The working group seeks initial inputs (based around, but not limited to, the questions posed below). Responses received by 29 February 2016 will be reviewed by the working group at the Tampa meeting (11-15 April 2016). The WG3 roadmap will then be updated, appropriate new work items identified, and relevant results of the study period used to facilitate review of ISO/IEC 15408 and ISO/IEC 18045 and any subsequent update (in collaboration with CCDB).

Contributions are requested on the following topics, clearly indicating the responder viewpoint (e.g. developer, end user, certification body, security consultant, etc.), and backed, where possible with clear argument/evidence:

1. What areas of IT product security assurance do you feel are not well covered by existing standards?
2. Where do the current standards work well and where should they be improved?
3. Is there sufficient flexibility in the current standards to be able to cover differing needs (markets/architectures/product technologies)?
4. Where are IT vendors' current security best practices being used to demonstrate to their customers the security assurance in their products and services? Please indicate which ISO standards such specific individually adopted best practices are mappable to.
5. In which areas would you use self-declaration of security from vendors, customer performed assessment, or trusted third party evaluation and certification?
6. Is there a limit to the depth and rigour of testing and analysis that you would be comfortable with?
7. How could/should robust metrics be incorporated into the IT product assurance process?
8. How should the development process and the evaluation be integrated to provide the appropriate level of assurance in an efficient and effective way?
9. How are the potentially conflicting needs for transparency of development approach/artefacts and developer intellectual property best resolved? – Is there a limit to the transparency and maturity of the development model that you would be able to accept?

Terms of Reference

The rapporteurs will examine contributions provided during the study period and present the results to interested WG 3 experts during the next WG 3 meeting which will be held in Tampa, Florida, according to the SC 27 calendar.