



ISO/IEC JTC 1/SC 27 **N 6653**

ISO/IEC JTC 1/SC 27/WG 3 **N 948**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: other

TITLE: Final Report on WG3 Study Period on Secure System Design

SOURCE: 36th SC 27/WG 3 meeting

DATE: 2008-04-17

PROJECT: -

STATUS: This document was available at the above-mentioned meeting. It is being circulated for information.

ACTION: FYI

DUE DATE:

DISTRIBUTION: P-, O-, and L- Members
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair
E. Humphreys, K. Naemura, M. Ohlin, M.C. Kang, K. Rannenber, WG-Conveners

MEDIUM: Server

NO. OF PAGES: 1 + 1

FINAL REPORT ON STUDY PERIOD FOR SECURE SYSTEM DESIGN

The second half of the study period for secure-system design did not see any further technical contributions. The rapporteur notes two documents of relevance that have been:

N6494 In which the Australian National Body comment in response to SC 27 N6336 -- Second call for contributions to WG 3 Study Period on Secure System Design that a project on Secure System Design in WG 3 should take account of, and avoid overlap with, the WG project 27034 - Application Security - being developed in WG 4.

N6448 In which the ISSEA liaison statement thanks ISO/IEC SC 27/WG 3 for the Liaison statement and the Interim Report on Secure Systems Design Study Period.

They note that ISSEA has studied the report with interest and would like to actively participate in any project that might arise as a result of the Study period.

ISSEA did not have a separate contribution to submit to the Study Period, but contributed the following observations:

ISSEA did not find any mention of the “Systems Security Boundaries” in the Interim Report, nor “Security Span of Control”. It is ISSEA's belief that both of these topics are very important and ought to be included, either separately or combined, in the Study Period and any subsequent projects. ISSEA would submit that clear and definitive understanding of both of these aspects are essential to an effective Secure Systems Design;

ISSEA found no mention of environment, infrastructure, physical and personnel security in the Interim Report. It is likely that they are implicitly included, and this of course, is just the start of this activity. Much can be achieved in all of these areas and in some cases only achieved by security in these areas and thus would commend them as important topics for inclusion in the overall approach;

ISSEA would like to suggest that WG 3 take an “operational” view with regard to any work arising from the Study Period. The reason for this suggestion is that most materials that ISSEA is aware of and has reviewed, seem to take a “system in isolation” or “system as a product” view, rather than a “system in operation” view. While ISSEA recognizes that taking such a view might make any resulting document more complex, it is considered that it will make any document more valuable to the community, regardless of which subset is the actual audience, more usable, and thus, hopefully, more popular.

The rapporteur thanks the Australian National Body and ISSEA for their observations. They state important aspects to be considered for any new work item that may be started by WG 3 on the topic of Secure System Design.

Conclusion

The Interim report identified that there are some new work items which could usefully be considered by WG3. Since no additional technical contributions have been received in the second half of the study period, the rapporteur refers to the Interim report for the analysis of the topic.

The rapporteur recommends that WG3 consider a series of new work items in this area specifically

- Guidance on a secure-systems design process
- Secure-System design principles
- Common terminology and definitions