ISO/IEC JTC 1/SC 22/OWGV N 0075

Response of ISO/IEC JTC 1/SC 22/OWGV to: ISO/IEC JTC 1/SC 27 N5494, "JTC 1/SC 27/WG 4 Liaison Statement to JTC 1/SC 22 on Collaborative work on Application Security"; and to ISO/IEC JTC 1/SC 27 N5482, "Report of the Application Security meeting, held in Glenburn Lodge (South Africa), Nov. 17th 2006"

Date	10 May 2007
Contributed by	OWGV Secretary
Original file name	
Notes	Prepared as directed by Action Item #04-28 for transmission to SC 27 and SC 22.

Response of ISO/IEC JTC 1/SC 22/OWGV to: ISO/IEC JTC 1/SC 27 N5494, "JTC 1/SC 27/WG 4 Liaison Statement to JTC 1/SC 22 on Collaborative work on Application Security"; and to ISO/IEC JTC 1/SC 27 N5482, "Report of the Application Security meeting, held in Glenburn Lodge (South Africa), Nov. 17th 2006"

Prepared by Jim Moore, Secretary of OWGV, 10 May 2007

I realize that this response will not reach SC 27 in time for formal tabling at the May 2007 meetings. Because of unfavourable scheduling of meetings, SC 22/OWGV was not able to consider these documents until its meeting of 30 April to 2 May 2007. SC 22 will not be able to consider the SC 27 documents until its meeting in September 2007. Therefore, this response is to be considered as representing only SC 22/OWGV and may not fully represent the concerns of SC 22.

SC 27 N5494 notes the establishment of a new WG 4 on Security Controls and Services standards which is initiating a study period on the topic of Application security, focusing on the objectives and scope as defined in SC 27 N5482. It requests inputs from SC 22 and welcomes exchange of information and collaborative work.

SC 22/OWGV is responsible for ISO/IEC work item 22.24772, a technical report providing "Guidance for Avoiding Vulnerabilities through Language Selection and Use." Relevant excerpts from the approved work item are provided below:

Scope: The guidance could be applicable to any software development project applying the programming languages considered in the TR. The advisability of applying the guidance would vary depending upon the criticality of properties such as safety, security or privacy. In addition to producing a Technical Report, it is possible that the working group might create recommendations for working groups that maintain the standards or specifications for the programming languages considered in the TR.
Purpose and justification - Any programming language contains constructs that are vague or difficult to use. Many language definitions include "implementation dependencies" that can affect their semantics in different execution environments. There is a set of "common mode" failures that occur across a variety of languages. Finally, there are weaknesses in language constructs that can be exploited by attackers, for example, the now-famous "buffer overrun" attacks. As a result, software programs sometimes execute differently than was intended by their developers. These problems can have serious consequences for systems that are intended to implement integrity properties such as safety, security or privacy. Although the consequences may be less severe, there is also the cost of dealing with electronic vandalism enabled by vulnerabilities in programs that are not themselves intended to have high integrity properties.

Successful treatment of these problems would result in the production of software codes that exhibit more predictable behaviour in execution. Although an ideal result is currently impractical, "predictable execution" is an ideal toward which we can strive. One criteria for selecting guidance for the report would be whether the guidance improves the predictability of execution.

The purpose of this project is to prepare comparative guidance spanning a large number of programming languages, so that application developers will be better informed regarding the vulnerabilities inherent to candidate languages and the costs of avoiding such vulnerabilities. An additional benefit is that developers will be better prepared to select tooling to assist in the evaluation and avoidance of vulnerabilities.

In developing the guidance, the project will prefer linguistic means of avoiding vulnerabilities but, when necessary may describe extra-linguistic means (e.g. static analysis or targeted testing). In developing the guidance, the project will prefer the avoidance of identified risks but, when necessary, may describe means to mitigate the risk of vulnerabilities that cannot be economically avoided. Finally, in cases where identified problems can be neither avoided nor mitigated, the report may assist users in understanding the nature of risk that must be accepted.

The admission that some problems must be treated via analysis or testing introduces a secondary consideration in recommending linguistic means for avoiding vulnerabilities; in some situations, one construct might be preferred over another on the grounds that it is easier to test or easier to analyze. This relationship between construction and subsequent verification activities makes it clear that the report will be useful both for those emphasizing "correctness by construction" and those who desire to improve the predictability of execution through testing and analysis.

Although a strict reliance on empirical evidence of effectiveness and quantified analysis of cost/benefit is not feasible, the project will be guided by both of those notions in its selection of guidance to be included in the report. Because of the dearth of quantifiable evidence, a cautious approach to incorporating guidance may be appropriate. ...

The project is intended to product a Type 3 Technical Report within 36 months, that is, by January 2009. Currently, we anticipate that the body of the document will describe code vulnerabilities in generic terms and that the document will also contain language-specific annexes that re-describe those generic vulnerabilities in terms of a selected programming language. The language-specific annexes will be prepared in cooperation with SC 22 working groups or other organizations who maintain the standards for each of the programming languages.

Additional information regarding OWGV can be found at its web site:
http://www.aitcnet.org/isai/

In reviewing SC 27 N5482, we see that the potential scope of work includes "security design patterns" and "secure coding". We believe that there is a substantial possibility of overlap between the SC 22 and the SC 27 projects in the area of "secure coding"; we believe that there are also possible overlaps in the area of "security design patterns".

For this reason, it is important that the two groups maintain effective communication so that the respective documents are appropriately related. For example, an SC 27 document might provide treatments for the set of vulnerabilities described in the OWGV document.

Toward this end, SC 22/OWGV is interested in arranged a colocated meeting with SC 27/WG 4. Our respective groups could schedule the meeting so that, perhaps, one day is used for a joint meeting. OWGV is actively investigating the possibility of hosting such a colocated meeting in July 2008 or December 2008 and will offer an invitation to SC 27/WG 4 when details are known.

SC 22/OWGV maintains a mailer in addition to its web site. We would be delighted to include liaison representatives of SC 27/WG 4 in the mailing list. Please provide the OWGV secretary, James Moore, James.W.Moore@ieee.org, with the email addresses of those to be enrolled.

If SC 27/WG 4 has a web site and/or a mailer, please enroll the OWGV Secretary, James Moore, so that he has access to that material. In this case, please use his native email address, moorej@mitre.org.

OWGV notes that SC 27 N5482 references several documents of JTC 1/SC 7. OWGV also plans to reference SC 7 documents, so its comments upon the references in N5482 may be relevant. Those comments are:

- ISO/IEC 15504 concerns process assessment but is not the CMMI. The description is N5482 is inaccurate in this regard.
- For descriptions of life cycle processes, OWGV will rely upon the most recent editions of two SC 7 documents, ISO/IEC 12207, Software life cycle processes, and ISO/IEC 15288, System life cycle processes. Practices, e.g. verification and validation methods, will be localized with respect to those processes.
- For descriptions of risk management, OWGV will rely upon an SC 7 document, ISO/IEC 16085, System and software risk management process.
- For descriptions of measurement, OWGV will rely upon an SC 7 document, ISO/IEC 15939, System and software measurement.
- For descriptions of project management, OWGV will rely upon an SC 7 document, ISO/IEC 16326, System and software project management.