Moving Forward on Programming Language Vulnerability Work
Jim Moore, The MITRE Corporation, James.W.Moore@ieee.org, +1.703.983.7396
6 October 2005

To: Members of the SC 22 High Integrity Study Group

As you know, our study group has cooperated for several months via an email distributor and a web page to initiate standards work to provide guidance on avoiding vulnerabilities in programming languages. We succeeded through several steps:

- In September 2004, we persuaded ISO/IEC JTC 1/SC 22 (Programming Languages and Environments) to create a study group on "Future Directions" and a sub-study group on High Integrity Software (us!) to specifically investigate the "demands that the development of high integrity systems places on programming languages."
- In March 2005, we persuaded the study group on Future Directions to endorse our work. They directed us to prepare a New Work Item Proposal (NP) on programming language vulnerabilities. If approved, the NP would initiate a standardization project.
- In June 2005, we submitted an NP. During the succeeding three month period, it was balloted by the national bodies (countries) who participate in JTC 1/SC 22.
- At last weekend's plenary meeting of JTC 1/SC 22, the balloting results were reviewed and SC 22 took steps to create a project.

The purpose of this note is to describe the terms of the project and the ways in which you may continue to participate. Some of you may not be interested in a long account; you should page forward to the section, "What this Means to our Study Group".

I first have to state that the results of the balloting were not originally clear-cut. JTC 1 has a complicated balloting system for initiating new work. Several criteria must be achieved before a project can be approved. Approval is complicated when there is poor "turnout" for the vote and when National Bodies fill out the complicated balloting form incorrectly. Both of these factors affected our situation, making it unclear until after the meeting (and after two NBs had modified/clarified their positions) whether a formal standards project had actually been approved.

I also have to state that SC 22 has a long—mostly discouraging—history with "cross-language" projects. Some participants feel that working groups for cross-language projects attempt to inappropriately dictate requirements to language standardization working groups while others feel that language standardization working groups pay insufficient attention to cross-language working groups. These diametrically opposed beliefs combine to guarantee both ineffective results and unpleasant interaction. It's fair to say that much of SC 22's time and attention over the past few years has been devoted to dealing with the problems of cross-language working groups rather than dealing with constructive work.

The factors described in the two preceding paragraphs affected the consideration of our proposal, both during the National Body balloting and during the consideration of the balloting results. Because the participants in the plenary meeting of SC 22 were convinced that the work is important, they wanted to insure that study would continue regardless of the outcome of the ballot, but they also wanted to ensure that the work would proceed in a manner that is responsive to the needs of SC 22 and connected to the work of the language working groups.

I apologize for the tedious introduction, but the background is necessary in making sense of the results. I will quote the relevant resolution and then do my best to explain their implications. (By the way, the text of these resolutions comes from a pre-approval draft; the text I quote is substantively correct but still subject to editorial correction.) Each of these resolutions was approved unanimously by the eight National Bodies represented at the meeting: Canada, Germany, Japan, Korea, Netherlands, Switzerland, United Kingdom, and United States.

Resolution 05-54: Appreciation: Study Group on Vulnerability

JTC 1/SC 22 expresses its gratitude to the participants of the Study Group on Vulnerability for their contributions on the work.

Resolution 05-55: Appreciation: Convener Study Group on Vulnerability

JTC 1/SC 22 expresses its gratitude to the Convener of the Study Group on Vulnerability, James W. Moore for his leadership of the group.

The plenary meeting voted its appreciation of the study group (you) and its convener (me).

The next resolution is the important one. Because it is large, I will deal with it in pieces.

Resolution 05-14: JTC 1/SC 22 N 3913, NP Ballot on Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use

JTC 1/SC 22 notes that the “No” votes of the UK on Questions 1 and 2 are changed to "Yes" due to resolution of the concern noted in their ballot; and that final disposition of the NP is not yet possible pending clarification of the vote of one National Body.

The first paragraph notes that the UK held a favorable vote hostage to the resolution of a concern in its ballot—agreement from at least two of the programming language working groups that they would participate in the new work. Both WG 9 (Ada) and WG 14 (C) were willing to commit on the spot. When they did, the UK changed its vote to approval. The resolution records this result. The final clause of the first sentence refers to an NB whose apparent actions were not consistent with their balloting position, raising the question of whether they had made a mistake in filling out the balloting form. This question could not be answered until after the adjournment of the meeting. Ultimately, their vote was clarified in a manner supportive of the proposed work.

To deal with any necessary work, JTC 1/SC 22 creates an Other Working Group on Vulnerability (OWG: Vulnerabilities), in accordance with sub-clause 2.6.2 of the JTC 1 Directives, with the following terms of reference:

This is an unusual result. Because it was not clear if the NP had been approved, SC 22 had to formulate a manner in which some work could proceed regardless of the balloting result. Furthermore, SC 22 wanted a mechanism that would ensure accountability to SC 22 as a whole. The solution was to form an "Other Working Group" (OWG). Unlike a normal project Working Group, an OWG does not have an indefinitely long life, but instead exists until the next meeting of the parent body to carry out some specific task of the parent. This mechanism would have allowed the OWG to perform continued study if the NP were to have been judged to have failed, and it also would permit initial work on a standards document in case the NP succeeds. Perhaps most importantly, though, it ensures accountability to SC 22 because at each of its annual plenary meetings, SC 22 will have to make an explicit decision to "continue" the OWG.

Following a newly adopted convention of SC 22, the name of the OWG is "OWG: Vulnerabilities".

- Definition of the task: Using the statement of scope previously provided in JTC 1/SC 22 N 3913, create an initial draft document and, if necessary, a revised New Work Item Proposal.

The ambivalent definition of the task was intended to permit the OWG to proceed, regardless of whether the project was approved. Because it was approved, the OWG can focus on creating an initial draft document.

- Time frame: Submit the materials by the next plenary meeting of JTC 1/SC 22.

There was some concern that the scope of work, as stated in the NP, was too large. It was agreed that an effective way to treat this concern is to prepare a draft within a year. The draft would serve to explicitly define the scope of the work. By the way, the next plenary meeting of SC 22 begins 18 September 2006 in London.

- Membership: Open to all JTC 1/SC 22 P and O members, liaison organizations, and subgroup representatives.

As is typical, the participants of the OWG are to be representatives of the National Bodies ("P and O members) and representatives of liaison organizations. Untypically, other subgroups of SC 22 – notably the language Working Groups – are invited to name representatives. Of course, this is intended to create communications with the language groups.

- Convener: James W. Moore (US).
- Administrative Support: The MITRE Corporation.

The official mechanism for naming a convener begins with NBs nominating conveners in their ballots. None did this, so SC 22 named me to the job. My employer will continue to support the work.

- Meetings: Continued operation by email and website collaboration pending invitations by working groups to co-locate meetings.

The OWG is authorized to perform work by email and website collaboration. However, the participants in SC 22 strongly encourage us to collocate meetings of our OWG with meetings of language working groups.

JTC 1/SC 22 instructs working groups to work with OWG: Vulnerabilities to co-locate meetings on this topic as appropriate.

Finally, SC 22 instructed the language working groups to invite the OWG to collocate.

Given all of the ambiguities of this result, it would be understandable to question the level of importance accorded to the OWG's work by SC 22. I can respond that every participant at the meeting told me that the work was important – even those who voted against the NP as it was balloted. Tangible evidence of importance is provided by the following resolution. It cites our work as an example of SC 22's ability to make a contribution in meeting the threat of global terrorism.

Resolution 05-28: ISO Advisory Group on Security

JTC 1/SC 22 requests its Chair to inform JTC 1 of JTC /SC 22’s concerns with regard to the Final Report of the ISO Advisory Group on Security (JTC 1/SC 22 N 3942). Specifically:

- The final report does not seem to address the full breadth of JTC1's involvement in security
- JTC 1 should directly involve itself in the preparation of the proposed security guide.
- JTC 1/SC 22 is already involved in Security and Vulnerability issues. For example the projects on Programming Language Vulnerabilities initiated by James W. Moore and discussed by JTC 1/SC 22 at its September 2005 plenary.
- Because JTC 1/SC 27's scope specifically excludes mechanisms, it overlooks the role that JTC 1/SC 22 can provide through language and environment support.

JTC1's report on security should note JTC 1/SC 22's actions in this area.

The title of this paper is "Moving Forward", but the text so far has looked back. The next section describes what we must do.

What this Means to Our Study Group

The bottom line is that SC 22 has approved a new project to create ISO/IEC TR 24772, *Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use*, a Technical Report of Type 3, in accordance with the scope outlined in the New Work Item Proposal. They have put the work on a "short leash" by assigning it to an OWG, a group that must be recreated on an annual basis. They have appointed me as the convener of the OWG and have invited national bodies, liaison organizations, and other working groups to appoint members of the

OWG. They permit continued work electronically, but they want the OWG to collocate meetings with those of language working groups. They require that we produce an initial draft document by their next meeting, 18 September 2006.

The most obvious unanswered question is the status of the study group, now that the OWG has been created. As things currently stand, most of you do not qualify for membership in the OWG that will actually do the work. I have two responses to this situation:

a) As convener of the OWG, I will continue to operate the study group as an adjunct of the OWG, using it as a mechanism for identifying resources, gaining expert advice, broadening consensus, and publicizing results.
b) Nevertheless, it will be the membership of the OWG that makes the decisions. So many of you may wish to join the OWG. The next part of this note will give you advice on how to accomplish that.

There are three ways to qualify to participate in the OWG as defined by the SC22 resolution:

1. The first way is to represent a P or O member (country) of SC 22. These members are listed in the annual report of the SC 22 Secretariat, available at: http://www.open-std.org/jtc1/sc22/docs/report
   Those of you from the US or the UK would pursue this possibility by contacting the head of delegation from your national body: Rex Jaeschke (rex@RexJaeschke.com) or Jon Diamond (jon.diamond@btinternet.com), respectively. If you are from another country, write me a private note and I will try to hook you up. Be aware that participation in this manner may require you or your employer to pay fees to your national body.
2. The second way is to represent a liaison organization. Two liaisons to SC 22 are listed in the Secretariat's report: ECMA International (R. Jaeschke) and Free Standards Group (N. Staughton). These don't look promising, but there is still hope. It is relatively easy to create a Category C liaison to a project such as ours. If you are a member of a group that *should* be interested in this work, write me a private note and I will respond with information on how to seek a liaison relationship. We will probably create several liaisons as a mechanism to work with languages that are not under the umbrella of SC 22, e.g. Java and C#.
3. The third way is to represent another subgroup of SC 22, particularly the existing project working groups. If you are a member of such a group, then contact its convener to ask if you can be appointed as the group's representative.

If none of this seems attractive, then please remain as a participant in our study group. I will attempt to use the mailer and the web site to keep you involved. If, at any time, you think I'm falling short in this regard, please send me a note.

In closing, I take this opportunity to thank you for your contributions. We have succeeded in describing an important problem and initiating action to resolve it. I look forward to your continued participation in whatever form is appropriate for your circumstances.

Annex 1: New Work Item Proposal, SC 22 N 3913

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: 2005-06-23	Proposer: ISO/IEC JTC 1/SC 22
Secretariat: ANSI (United States)	ISO/IEC JTC 1 N **3913**

A **proposal for a new work item** shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal - to be completed by the proposer Guidelines for proposing and justifying a new work item are given in ISO Guide 26.

Title Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use
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 behavior 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. A consequence of this observation is noted in the box labeled, "Preparatory work offered with target date(s)".

Finally, the technical report may prove useful as a "registry" of vulnerabilities. For example, if the report provides unique names for identified vulnerabilities, then tool vendors could describe the range of effectiveness of their tools in terms of the names used by the report. Although this is not the primary intended purpose of the report, the project will consider catering to this usage.

Programme of work

If the proposed new work item is approved , which of the following document(s) is (are) expected to be developed?
____ a single International Standard more than one International Standard (expected number: ....)
____ a multi-part International Standard consisting of .... parts
____ an amendment or amendments to the following International Standard(s) ....
__X__ a technical report , type ....3.......

Relevant documents to be considered

- The programming language standards of ISO/IEC JTC 1/SC 22.
- For market reasons, the specifications of popular languages that are not the subject of ISO standards.
- The software engineering standards of ISO/IEC JTC 1/SC 7, as a source of extra-linguistic mitigation methods.
- Existing documents providing usage guidance for individual languages, e.g. ISO/IEC TR 15942, MISRA C, NUREG/CR-6463.
- Standards dealing with functional safety, notably, IEC 61508.
- Existing work on safe programming approaches, e.g. the SPARK language, ISO/IEC draft TR 24731 (Specification for Secure C Library Functions)

So far, the study group has assembled a list of 82 resources to be considered.

Cooperation and liaison

The proposal recognizes that a normally constituted working group will not suffice to perform the necessary work. In addition, to the usual National Body participants, it is proposed to use experts appointed by each existing working group in JTC 1/SC 22, liaison experts appointed by other organizations maintaining programming language specifications, and liaison experts appointed by other standards committees maintaining related documents.

Preparatory work offered with target date(s)

A web site provides a summary of progress to date: http://www.aitcnet.org/isai/. It is proposed to perform the work on the "normal" (36 month) schedule. However, it is recognized that the work may be performed in increments that subdivide the schedule or with refinements that would produce subsequent amendments or revisions.

Signature:

Will the service of a maintenance agency or registration authority be required? ......NO................
- If yes, have you identified a potential candidate? ....
- If yes, indicate name ....

Are there any known requirements for coding? ......NO..............

-If yes, please specify on a separate page

Are there any known requirements for cultural and linguistic adaptability? .....None beyond those already implicit in the programming languages being treated.......
- If yes, please specify on a separate page

Does the proposed standard concern known patented items? ....NO..........
- If yes, please provide full information in an annex

Comments and recommendations of the JTC 1 Secretariat - attach a separate page as an annex, if necessary

Comments with respect to the proposal in general, and recommendations thereon: It is proposed to assign this new item to JTC 1/SC 22

Voting on the proposal - Each P-member of the ISO/IEC joint technical committee has an obligation to vote within the time limits laid down (normally three months after the date of circulation).

Date of circulation:	**Closing date for voting:**	**Signature of JTC 1 Secretary:**
YYYY-MM-DD	YYY-MM-DD	Lisa A. Rajchel

NEW WORK ITEM PROPOSAL - PROJECT ACCEPTANCE CRITERIA		
Criterion	**Validity**	**Explanation**
A Business Requirement		
A.1 Market Requirement	Essential _X__ Desirable ___ Supportive ___	Exploitation of software vulnerabilities is becoming an increasingly expensive problem.
A.2 Regulatory Context	Essential ___ Desirable ___ Supportive __X_ Not Relevant ___	Application of the guidance might be cited in warranties of fitness for particular purposes.
B. Related Work		

B.1 Completion/Maintence of current standards	Yes _X__ No___	See explanation of "relevant documents".
B.2 Commitment to other organization	Yes _X__ No___	See explanation of "relevant documents" and "cooperation and liaison".
B.3 Other Source of standards	Yes _X__ No___	See explanation of "relevant documents" and "cooperation and liaison".
C. Technical Status		
C.1 Mature Technology	Yes _X__ No___	Guidance has already been prepared for several individual languages. This proposal would provide a uniform approach supporting comparison among languages.
C.2 Prospective Technology	Yes ___ No_X__	
C.3 Models/Tools	Yes _X__ No___	Tooling can be used for analysis of vulnerabilities or mitigation of their risks. Both roles are relevant to this work.
D. Conformity Assessment and Interoperability		
D.1 Conformity Assessment	Yes ___ No__X_	
D.2 Interoperability	Yes ___ No__X_	
E. Other Justification		

Annex 2: Ballot Summary, SC 22 N3990

ISO/IEC JTC 1/SC22
Programming languages, their environments and system software interfaces
Secretariat: U.S.A. (ANSI)

ISO/IEC JTC 1/SC22 N3990

TITLE:
Summary of Voting for SC 22 N 3913, New Work Item Proposal for Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use

DATE ASSIGNED:
2005-10-05

SOURCE:
SC 22 Secretariat

BACKWARD POINTER:

DOCUMENT TYPE:
Summary of Voting

PROJECT NUMBER:

STATUS:
Per the results of this ballot, and as no comments were received during the JTC 1 review period, the NWIP has been approved and this project has been added to the SC 22 Programme of Work. Please note that this project has been assigned the ISO/IEC designation "24772". The OWG: Vulnerabilities is instructed to begin work on this project and prepare a disposition of comments for those National Body comments received on the SC 22 ballot. The NP summary of voting is located at:
http://www.open-std.org/jtc1/sc22/def/n3990.pdf

ACTION IDENTIFIER:
FYI

DUE DATE:

DISTRIBUTION:
PDF

CROSS REFERENCE:

DISTRIBUTION FORM:
Open

Address reply to:
Sally Seitz, ANSI, 25 West 43rd Street, New York, NY 10036
Telephone:(212)642-4918, Fax: (212)840-2298, Email: sseitz@ansi.org

Committee: ISO/IEC JTC 1/SC 22
Ballot Number: SC 22 N 3990
Ballot Title: New Work Item Proposal for Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use
Source: JTC 1/SC 22 Secretary

National Body	Q. 1	Q. 2	Q. 3	Q. 4	Q. 5	Q. 6	Comments
Austria							
Belgium							
Canada	Y	Y	Y	N	N	N	
China	Y	Y					See below
Czech Republic	Y	Y	N	N	N	N	
Denmark	Y	Y					
Egypt							
France							Abstain, lack of resources
Germany	Y	Y	Y	N	N	N	
Italy							Abstain
Ireland							
Japan	Y	Y	Y	N	N	N	
DPR of Korea							
Korea, Rep. of	Y	Y	N	N	N	N	
Netherlands	N	N	N	N	N	N	See below
Romania	Y	Y	N	N	N	N	
Russian Federation	Y	Y	N	N	N	N	
Slovenia							
Switzerland							Abstain
Ukraine							

United Kingdom	**N**	**N**	**Y**	**N**	**Y**		**See below**
United States	**Y**	**Y**	**Y**	**N**	**N**	**N**	**See below**

National Body Comments

China

CN	SCOP	Paragraph 2	Te	working group	Special group for short term	Wu yan

Netherlands

- the scope is too wide and too vague; as described, and seeing the list of documents to be considered, it is not difficult to fill a 1000+ page TR. We prefer a smaller, less ambitious project plan with a first edition of the TR within 2-3 years. Based on such a document, further editions covering other areas could be considered.

- the relationship with the proposed work as described in SC22 N3886 (Report of 2005-03-31 Sc22 Ad Hoc on Future Directions) under point 1 is unclear. The Netherlands opposes to develop more than one TR in this area.

If the above points are taken into account in a revised NWI proposal, the Netherlands is willing to consider changing its vote.

United Kingdom

Q1. UK notes that 'it is proposed to use experts appointed by each existing working groups'. If such experts do not actively participate in the project, then the resulting technical report will be yet another worthy effort destined to lie ignored and unread. UK will change its vote to 'YES' when at least two SC22 working groups have agreed to actively participate in the project.

Q2. See above

Q3. Comments: UK will participate while at least two SC22 working groups actively participate in the project.

Q6. Comments: www.knosof.co.uk/cbook/cbook1_0b.pdf is a very relevant commentary on C.

United States
The US is prepared to make contributions as requested.