ISO/IEC JTC 1/SC 22/WG 23 N0358

Software Code Signing

Jim Moore

7 September 2011

Revision 3

Proposed Work

- Append digital signatures to source code so that:
  - Receiver can identify the developer of the code
  - Receiver can be assured that the code has not been modified by a third party
  - Receiver can determine the responsible party for each set of changes to code
  - Receiver can “unwrap” changes (i.e. to get back to a previously signed version which is trusted or has been verified)
- All of these are real-world problems today.

Background

- NWIP was balloted last year – SC 22 N 4575.
- Balloting results:
  - "Sufficient definition"– 10 (yes), 1 (no), 7 (abstain)
  - "Support the addition"– 9 (yes), 1 (no), 8 (abstain)
  - "Commit to participate"– 4(yes), 6 (no), 8 (abstain)
  - "Offer project editor"– 1 (yes), 10 (no), 7 (abstain)
  - "Contribution ready"– 0 (yes), 11 (no), 7 (abstain)
  - "Contribution in 90 days"– 0 (yes), 11 (no), 7 (abstain)
  - "Development track"– 18 (default), 0 (acc.), 0 (ext.)

One comment on ballot

- From Japan:

  Since there is no working draft attached to the proposal, the proposal does not comply with the clause 2.3.4 of ISO/IEC Directives, Part 1, which says that the originator of the new work item proposal shall make every effort to provide a first working draft for discussion, or shall at least provide an outline of such a working draft. We cannot judge it gives the sufficient definition of the new work item. For example, the following questions should be answered. - What kind of technology is applied to the issue? - What is to be standardized? encryption method? protocol in software market? - Can the technology be applied to any programming language without changing the language per se? - Does the technology assume a general and conceptual infrastructure or a specific one available now?

Responses to Comment

- *What kind of technology is applied to the issue?*
  - Well-known digital signature technology
- *What is to be standardized? encryption method? protocol in software market?*
  - Application programming interfaces to add/check/use signatures
  - Format of signature
- *Can the technology be applied to any programming language without changing the language per se?*
  - The APIs are written in a language-independent manner.
- *Does the technology assume a general and conceptual infrastructure or a specific one available now?*
  - A method of operation is described in an informative part of the draft.

Participation

- Agreed to "participate" on original NWIP vote:
  - Canada (SCC)
  - China (SAC)
  - Italy (UNI)
  - USA (ANSI)
- Additional possible candidates:
  - Japan for expertise in a "modern" language (Ruby)
  - Netherlands for expertise in language-independent interfaces
  - UK for expertise in software security
  - Others?

Summary

- A preliminary working draft is now available.
- It will be circulated with a revised NWIP.
- We hope that additional nations will choose to "participate."
  - Participation means simply the willingness to review drafts and cast a ballot. Attendance at meetings is not required.
- We prefer to do the work in SC 22 due to experience in language-independent specification