REPLACES: SC 27 N 14293

ISO/IEC JTC 1/SC 27/WG 2

Cryptography and security mechanisms

Convenorship: JISC (Japan)

Document type: standing document

Title: **SC 27/WG 2 Standing Document 6 — Guidelines for effective communications on security mechanism issues**

Status: In accordance with Recommendation 1 and 22 (contained in SC 27/WG 2 N1043) of the 49th SC 27/WG 2 meeting at Mexico City, Mexico on 20th - 24th October, 2014, this document is posted on the SC 27 internal website. This document is being circulated to experts of National Bodies and liaison organizations for information.

Date of document: 2015-03-12

Source: Projects (David Grawrock, Art Manion, Damir Rajnovic and Grigory Marshalko)

Expected action: FYI

No. of pages: 1 + 13

Email of secretary: sc27wg2-secretary@ipa.go.jp

Committee URL: http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg2

ISO/IEC JTC 1/SC 27/WG 2 N1023

Date: 2015-03-12

Workgroup Standing Document

ISO/IEC JTC 1/SC 27/WG 2

Secretariat: DIN

Guidelines for Effective Communications on Security Mechanism Issues (SD 6)

Standing Document

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC JTC 1/SC 27/WG 2 Standing Document 6 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*, Working Group WG 2, *Cryptography and Security Mechanisms*.

0 Background

ISO/IEC standards can include cryptographic algorithms along with modes and protocols to use those algorithms. The assumed security of the standardized mechanism correlates to the amount of corresponding cryptographic research. Prior to inclusion in a standard, there is a consensus, evidenced by National Body voting, that the cryptographic mechanism provides an appropriate level of security.

After publication, security research on the algorithm, modes, and protocols continues. Cryptanalysis on the standardized mechanism or other cryptographic algorithm may reveal that the assumed security properties are not present. The state of cryptanalysis typically moves slowly and hence the lowering of the assumed security level also slowly lowers. Users, both developers and customers, of the standard will need information to make risk decisions regarding the security level provided by the cryptographic algorithm. Users of the standard are buying the cryptographic expertise of the ISO/IEC JTC 1/SC 27 workgroup and typically do not have the expertise to quantify the effect new cryptanalysis results have on their operational applications that rely on the ISO standard. The users rightly will look to the experts to make a statement relative to the standard.

The issue is timing. Users, who are dealing with operational applications, have days, maybe weeks, to respond to press, or customers. SC27 timeframes are in biannual meetings meaning official responses could take 18 to 24 months.

The purpose of this standing document is to establish the mechanism whereby the workgroup can establish an inquiry in relation to some cryptanalysis or attack, how to draft a statement, and overall workgroup activity towards reviewing cryptanalysis progress.

1 Possible Security Issues

1.1 Issue source

Security issues can arise from a variety of sources. New theoretical cryptanalytic results and the publication of successful attacks both indicate that the assumed security level may not be correct. From the security level viewpoint, there is no difference between any sources of an issue. From a user viewpoint there is a difference. With new theoretical results, the issue is still under discussion by the cryptographic experts and knowledge of papers and other research directions flows at a fairly slow but persistent direction. Publication of an attack indicates that the threat is far from theoretical and users must respond immediately to the new threat.

1.2 Issue type

Security issues are not all the same, and for this standing document, have two classifications:

a) Critical issues

   1) Issue source provides sufficient evidence of a significant decrease of the security level described in the standard

2) Assumption is that most fielded attacks result in critical issues

b) Potential issues

1) Issue source does not provide sufficient evidence of a significant decrease in the security level, or the decrease is not significant

2) Assumption is that many theoretical results will result in potential issues

There are only two types as cryptanalysis only gets better with time and what was, at the start, only a very slight decrease can, over time, turn into a complete break. Therefore, potential issues can, and some will, change over time to critical issues.

2 Inquiry Process and Timeline

2.1 Inquiry

The response to the identification of an issue, critical or potential, is to establish an inquiry. The inquiry does not start at the next SC 27 meeting but immediately through use of the Expert mailing list (Annex A). The inquiry will determine whether the issue is a critical issue or a potential issue. An inquiry statement will be created to explain the nature of the issue and the impact of the issue to SC 27. This statement may also include possible suggestions for industry.

2.2 Inquiry establishment

Anyone – an organization, individual, user, vendor, WG2 member or not – can start an inquiry. The process is to send an email with the relevant information regarding the issue to the Experts mailing list (Annex A).

The individual sending the first email to initiate the inquiry can also fill the role of rapporteur, but there is no requirement that they do so. For example, one individual may discover a research paper regarding an algorithm and another member of the list could be part of the team that developed the algorithm. In that case, it makes much more sense that the team member fulfills the rapporteur role as opposed to the person initiating the inquiry. If an inquiry is initiated by a non-WG2 member, then it would be necessary for a WG2 member to act as rapporteur. The expectation is that WG2 would ratify the rapporteur assignment at the next SC 27 meeting.

2.3 Inquiry discussion

Those members of the mailing list that have an interest in the issue discuss the ramifications of the issue. The goal for this discussion is to create a consensus statement. In normal circumstances, all communication should be over email or rarely phone conferences. The need and use for face-to-face meetings should only occur in extremely rare circumstances. It is also entirely possible that those with interest in the issue may participate in conferences and discussions regarding the issue. Those participating in these discussions should communicate the results with the mailing list.

2.4 Inquiry opinion

The goal of the mailing list discussion is for the participating experts to form an opinion regarding the issue. This is purely an expert opinion where the experts understand the ramifications of the issue and how it applies to ISO standards. Their opinion is not an official ISO statement nor does their opinion bind any actions on current or future ISO standards. For the issue at hand, ISO merely plays the role of assembling some experts and allowing them to form an expert opinion.

Critical issues require fast communication. Obtaining 100% agreement regarding the expert opinion is not helpful to those needing to respond to press and customers. The consensus definition uses the standard ISO definition: Statement approval requires 2/3 of the experts in favor, and no more than 1/4 against. It is highly probable that given the quick nature of the inquiry a significant minority position may arise. In this case, the statement should contain the caveats that form the basis of the minority position.

Given the nature of cryptographic analysis, it is also highly likely that the expert consensus will change over time. As the consensus changes, the experts should also consider the need to publish additional statements regarding the issue.

2.5 Inquiry statement

The statement should contain, at a minimum, the following:

a) Issue description

b) Issue type, potential or critical

    1) Experts may also indicate likelihood that potential issue could be come critical

c) Effect on ISO standards

d) Potential industry responses

e) Opinion status

    1) Consensus

    2) Minority report if present

3 Statement Publication

3.1 Potential issue

As potential issues do not significantly affect ISO standards, there is no reason to make immediate statements. Publication of potential issue statements should occur at the next SC 27 meeting where the workgroup can vote on the statement.

3.2 Critical issue

Information about a critical issue needs to be distributed to industry without waiting for the next SC 27 meeting, which could be up to six months away. With approval from the Experts mailing list (Annex A), the rapporteur will send the statement to the Liaison list (Annex B). There is no concurrent inclusion of the statement on the ISO web site. The statement will be posted after it has been drafted and approved through official SC 27 procedures. This difference in publication schedules is one rationale for the wish list. As few issues will suddenly appear that are critical, most will slowly move from potential with the ever-increasing improvements in the cryptanalysis. A potential issue that becomes a critical issue will hopefully have a long history of statements regarding the issue and numerous mitigations or responses already agreed to by the Experts group.

3.3 Publication mechanism

After gaining consensus, the rapporteur sends the statement to the ISO secretariat for inclusion on the ISO web site and/or sends the statement to the Liaison members of Annex B. At the same time, if the issue is confirmed, a WG2 SD12 part concerning defects in international standards should be updated according to the developed statement.

4 Wish list

4.1 Rationale

To avoid issues "sneaking" up and suddenly becoming critical issues, the workgroup will establish a wish list of topics to review and establish consensus. The purpose is to draw the attention of the cryptographic community to topics that require research. The idea is that over a period, as an algorithm undergoes additional cryptanalysis, the workgroup will monitor the changes to the assumed level of security. When, and if, an issue moves to critical, then the issue team will have lots of advice to provide to industry. In fact, with the early notification of the potential issue, the workgroup will already be working on changing the standard.

4.2 Topics

WG2 will maintain Annex C to provide guidance to researchers and analysts as to the set of topics that warrant review and effort. The wish list is not the WG2 roadmap; rather it is a list of research topics on existing standards or potential future areas.

Candidate topics should include:

a) Cryptanalysis of specific mechanisms

    1) Mechanisms includes algorithms, modes, and protocols

b) Fundamental issues of cryptography

    1) Factoring, one-way properties, etc.

c) New attacks

   1) Models and assumptions relative to mechanisms included in ISO standards

4.3 List maintenance

The WG updates Annex C twice a year at the ISO meetings according to National Body contributions.

4.4 List distribution

Distribution of the wish list to the cryptographic community goes through the SC27 website, National Bodies, and WG2 experts.

4.5 Impact on SD4 and SD12

The results of research on wish list topics, if confirmed, should be included in SD4 if they deal with a specific standardised primitive, or SD12 if they deal with general problems, concerning security assessment of cryptographic mechanisms.

Annex A
(Informative)
Experts mailing list

A.1 The initial list will be the WG2 mailing list: <sc27wg2@ipa.go.jp>.

Annex B
(Informative)
Liaison mailing list

B.1 Forum of Incident Response and Security Teams (FIRST)

FIRST will be used to disseminate inquiries to the wider vendor and user communities. This dissemination will be done on the best effort basis and no guarantees are given that the every potentially affected vendor will be reached.

FIRST will also disseminate inquiries to vulnerability coordinators as needed. Coordinators are likely to be FIRST members such as Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) and the CERT Coordination Center (CERT/CC).

FIRST will maintain a mailing list and publicly accessible web page.

FIRST will act as a conduit to, if necessary, connect interested parties directly with the designated contact in WG2.

Annex C
(Informative)
Topic wish list

C.1 Research concerning the development, parameter choice, and evaluation of statistical tests for physical RNG testing (Added 2014-10-20)

C.2 RNG Te RNG testing (Added 2014-10-20)

