IEEE 802 JTC1 Standing Committee

|  |
| --- |
| Proposed liaison statement to JTC1/SC6 relating to proposal for an SC6 Security Ad Hoc  |
| Date: 20170315 |
| Editor(s): |
| Name | Affiliation | Email |
| Andrew Myles | Cisco | amyles@cisco.com |
|  |  |  |
|  |  |  |
|  |  |  |

Abstract

This document contains a proposal for a liaison statement from IEEE 802 to ISO/IEC JTC1/SC6 in relation to the proposed SC6 Security ad hoc

## Proposed liaison letter to SC6/WG1

TO:

Mr. Yun-Jae Won, Chair of ISO/IEC JTC1/SC/WG1, yjwon@keti.re.kr

Dr Hyun Kook Kahng, Chair of SC6 ISO/IEC JTC1/SC6, kahng@korea.ac.kr

CC:

Jooran Lee, Secretary of ISO/IEC JTC1/SC6, jooran@ksa.or.kr

SUBJECT: Proposed SC6 Security Ad Hoc

DATE: 17 March 2017

Dear Dr Hyun Kook Kahng & Mr Yun-Jae Won,

IEEE 802 is writing to express its concerns relating to the proposed formation of a Security Ad Hoc within ISO/IEC JTC 1/SC 6. While IEEE 802 broadly supports the goal of improving security for SC 6-developed or approved standards, we believe that the Security Ad Hoc may not be the right vehicle to accomplish that task in regards to IEEE 802 standards that are submitted to SC 6 for possible ratification under the PSDO agreement.

The presentation requesting the formation of the Security Ad Hoc noted that the China NB had presented detailed technical objections to the security mechanisms found in ISO/IEC/IEEE 8802-1X. IEEE 802 understands those objections are summarized in 6N15613. The Switzerland NB representative at the time had some related concerns. IEEE 802 initially responded to those objections in 6N15658, showing that the alleged security flaws were not applicable to IEEE 802's use of the underlying security techniques and mechanisms.

IEEE 802 has requested, but not received, clarification on how our response in 6N15658, and later responses, do not adequately address the alleged security flaws detailed in 6N15613 and have now been making similar requests for information for more than three years. Neither the China NB nor the Switzerland NB have provided additional evidence of the alleged security flaws in ISO/IEC/IEEE 8802-1X or have demonstrated any security flaws. Having failed to elicit such information, IEEE 802's response to each 60-day or FDIS ballot comment in the PSDO process that cites the alleged security flaws in ISO/IEC/IEEE 8802-1X has been to politely decline to alter the proposed ISO/IEC/IEEE 8802 standard in question. This does not stem from any unwillingness on IEEE 802's part to modify the standards in response to properly justified comments originating from the PSDO process, but rather the impossibility for IEEE 802 to address alleged security flaws for which there is no available evidence.

IEEE 802 would warmly welcome a more substantive dialogue with SC6's security experts on these matters and have issued several invitations for any concerned SC6 NBs to participate in such discussions at IEEE 802 meetings (including one held in Beijing and, most recently, our just concluded meeting in Vancouver). With the exception of the Switzerland NB, who participated in a very productive discussion at the IEEE 802 meeting in Geneva in 2014, no other NBs have accepted our invitations. In contrast, IEEE 802 representatives have participated in such discussions at multiple SC6 meetings.

Given that only the China NB has been submitting any comments recently relating to alleged security flaws in ISO/IEC/IEEE 8802‑1X, it would be more effective for one or more representatives from the China NB to attend an IEEE 802 meeting, and thus have full access to the full range of IEEE 802 security experts, so that a resolution to this long lasting impasse can be reached. It is not reasonable to expect a large number of IEEE 802 security experts to attend an SC 6 meeting to deal with the unsubstantiated concerns of a single NB.

To recap, while IEEE 802 supports the goals of SC 6’s propose Security Ad Hoc Group, we believe it would be far more productive for a China NB representative to present an updated explanation of the alleged security problems with ISO/IEC/IEEE 8802-1X to IEEE 802 security experts at an IEEE 802 meeting. IEEE 802 reiterates its invitation for the China NB to attend an IEEE 802 plenary meeting, noting that IEEE 802’s July 2017 plenary meeting will be held in Berlin, Germany. We also extend this invitation to any other NBs that would like to participate in or observe the discussion. It is our sincerest hope that direct dialogue will lead to resolution and we look forward to a more productive working relationship under the PSDO agreement.

Regards,

/s/ Paul Nikolich

Paul Nikolich, Chairman, IEEE 802