

ISO & 802 Security

Bruce Kraemer

April 21, 2011

History -1

- Some time around 2005 China introduced to the ISO/JTC1/SC6 WG1 a proposal to replace the 802.11 security system with WAPI.
- An ad hoc designated JTC1 was established within 802.11 to organize responses and engage within SC6 meetings. The current chair is Andrew Myles (Cisco).
- Debate ensued about the flaws of 802.11, the superiority of WAPI, the concept of replacement vs addition and national versus international standards and copyrights. The situation in ISO is not yet resolved.
- A recent missive:
- <https://mentor.ieee.org/802.11/dcn/10/11-10-1358-02-0jtc-proposed-liaison-letter-to-sc6-in-relation-to-n14436.doc>

History -2

During August of 2010 China introduced to the ISO/JTC1/SC6 WG1 an additional pair of documents that claim the security systems embodied in 802.16 and 802.1x/AE are seriously flawed. They proposed to open up study groups to explore replacement options. Due to late document submission the proposals were not eligible for NB voting during the September 2010 meeting.

- In November, Paul Nikolich expanded the roll of the JTC1 to help organize 802 wide responses and engage within SC6 meetings.
- China has resubmitted these latest two security replacement proposals for consideration during the June 2011 ISO/JTC1/SC6 WG1 meeting to be held in San Diego during the week of June 20.

IEEE Position

- There are a number of political, legal, interpersonal and technical topics at play here.
- The intent is to focus the attention of 802.1 on only the technical arguments and counterpoints – leaving the other topics to National bodies of IEEE SA.
- IEEE has a well established reputation as a group of technical experts and the intention, in this matter, is to emphasize and maintain that stature.

Recent events

- 802.1 has previously prepared an analysis of the China NB assertions.
- During the March 802 plenary, the 802.1 commentary was encapsulated into a letter that was conveyed to SC6 under Paul Nikolich's signature.
- <https://mentor.ieee.org/802.11/dcn/11/11-11-0442-01-0jtc-liaison-to-sc6-related-to-802-1x-ae.docx>
- Additionally, during March, Bruce Kraemer was designated as the 802 head of delegation to identify and organize the delegates who would help prepare any additional pre-meeting material and be in attendance at the June 2011 SC6 meeting.

802.1 Security

- **Abstract of 11-11-0442**
- This document contains a proposed liaison from the IEEE 802.11 Working Group to ISO/IEC JTC1 SC6 and its National Body members.
- The liaison is based on:
- ISO/IEC document ISO/IEC JTC1/SC6 N14399, which is a proposal for a NP for a standard that could replace IEEE 802.1X
- ISO/IEC document ISO/IEC JTC1/SC6 N14402, which is a proposal for a NP for a standard that could replace IEEE 802.1AE



14402



14399

Excerpt from 11-11-0442

- We have reviewed N13399 and N14402 and believe they contain significant misconceptions, misunderstandings and errors related to IEEE 802.1X and IEEE 802.1AE. Appendix A of this liaison contains a brief review of some of the claims about IEEE 802.1X and IEEE 802.1AE contained in N14402. We have not provided a separate review of N14399. We note as a caveat that neither contribution contains sufficient detail for us to provide a complete review. Appendix B of this liaison contains a limited review of the TLSec proposal in N14402. We have not yet undertaken a detailed review of TePA-AC. IEEE 802 is interested in hearing more details about TePA-AC and TLSec to help improve our understanding of these proposals.
- We recommend that the members of ISO/IEC JTC1/SC6 engage with world recognized experts on IEEE 802.1X and IEEE 802.1AE and members of the IEEE 802.1 Working Group before approving the New Projects proposed by N13399 and N14402. The goal of any engagement would be ensure that SC6 has a proper and thorough understanding of IEEE 802.1X and IEEE 802.1AE before starting any project that might unnecessarily duplicate their functionality. We note that unnecessary duplication of standards is contrary to the explicit goals of IEEE, ISO/IEC and the WTO.

What's needed?

- During April, May, June Some amount of assistance from the 802.1 community to review and prepare written responses to SC6 proposals or comments.
- A member who can be available for delegation preparations via teleconference and also be prepared to both present and interactively defend/embellish the 802 security position during the SC6 meetings in San Diego during the week of June 20.