Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14142
Date:	2009-12-02
Replaces:	
Document Type:	Liaison organization contribution
Document Title:	Liaison Statement from IEEE SA 802 LAN/MAN Standards Committee to ISO/IEC JTC 1/SC 6 on the 6N14123
Document Source:	IEEE SA 802 LAN/MAN Standards Committee
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	3

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

20 November 2009

Ms. Jooran Lee
Secretary of ISO/IEC JTC1/SC6

Dear Ms. Jooran Lee

The IEEE 802.11 Working Group has been developing the IEEE 802.11 standard series since 1990 and continues to do so. Indeed, the Working Group recently completed 802.11n (to provide throughput of up to 600 Mb/s), 802.11r (to provide fast, secure roaming) and 802.11w (to provide improved security for management frames). Work is almost complete on a variety of additional amendments (802.11u, 802.11v and 802.11z) and work on the next generation of amendments is continuing. Further details are available on the IEEE 802.11 Working Group web site (www.ieee802.org/11).

On 29 October 2009, the ISO/IEC JTC1/SC6 Secretariat notified IEEE 802 that the China National Body had submitted a "proposal for a new work item" (ISO/IEC JTC 1/SC6 N 14123) to "provide an alternative security mechanism for use with ISO/IEC 8802-11". This alternative security mechanism is commonly known as WAPI (WLAN Authentication and Privacy Infrastructure). IEEE 802 appreciates the opportunity to review the new work item proposal and provide comments to SC6 and its National Body members.

IEEE 802 would like to make two points regarding the New Project proposal:

1) The evidence provided in ISO/IEC JTC 1/SC6 N 14123 does not support the assertion that there are serious security loopholes in current WLAN standards. There are no known attacks on the mandatory security components included in ISO/IEC 8802-11 and its amendments.

   The "Purpose and justification" section of ISO/IEC JTC 1/SC6 N 14123 specifies three issues related to ISO/IEC 8802-11 and its amendments. None of the issues raised provides any evidence that the security provided by ISO/IEC 8802-11 and its amendments is in any way flawed when the mandatory security components are enabled:

   - Issue 1 refers to a paper called *WiFi Epidemiology: Can Your Neighbors' Router Make Yours Sick?* by Hao Hu, Steven Myers, Vittoria Colizza and Alessandro Vespignani published in early 2008. A copy is available at http://arxiv.org/pdf/0706.3146.

     The "Purpose and justification" section in ISO/IEC JTC 1/SC6 N 14123 implies that this paper documents a flaw in existing WLAN standards. In fact, the paper actually focuses on Access Points that either have no security or use WEP, a protocol that was deprecated with the ratification of IEEE 802.11i in 2004 (ISO/IEC 8802-11:2005 Amd6). Indeed, the authors of the paper explicitly "*assume that WPA is not vulnerable to attack*".

     The cited paper does not call into question the security provided by ISO/IEC 8802-11 and its amendments.

   - Issue 2 refers to an article in a trade magazine, *Network World*, in January 2008 that simply reports on a version of the paper referred to in Issue 1.

     The cited article does not call into question the security provided by ISO/IEC 8802-11 and its amendments

   - Issue 3 cites two papers published in late 2008 and early 2009 that describe similar mechanisms to attack WPA. The papers are available at:
     - http://dl.aircrack-ng.org/breakingwepandwpa.pdf
     - http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf

The existence of these attacks is not surprising. TKIP was designed in 2003 with a 5 year horizon to allow devices that implemented WEP to transition to a higher level of security without a hardware upgrade. The industry is in the process of deprecating TKIP, and it is notable that TKIP is prohibited in IEEE 802.11n.

The cited papers do not call into question the security provided by ISO/IEC 8802-11 and its amendments when the mandatory security components are enabled..

2) The best way to integrate WAPI technology into the international standard for WLAN is to bring the work into the IEEE 802 process.

The standardisation of WAPI independently from the IEEE 802.11 Working Group process will duplicate existing functionality and will isolate WAPI devices from most amendments to the IEEE 802.11 series since 2003, including 802.11e (QoS), 802.11j (Japan), 802.11k (Wireless Network Management), 802.11n (High Throughput), 8021r (Fast roaming) and 802.11w (Management Frame Protection).

The IEEE 802.11 Working Group believes that the ongoing development of the 802.11 series should continue to occur in the Working Group, as it has since 1990. The success of this approach is proven by the current operation of over a billion devices worldwide. The development of the standard by the IEEE 802.11 Working Group will avoid duplication of effort and enable interoperable access to all 802.11 technologies by consumers around the world. We continue to encourage the ISO/IEC JTC1 and SC6 National Bodies to provide their vital review during the IEEE Sponsor Ballot process and when the IEEE 802.11 standards are proposed as ISO/IEC standards.

Any individual from any company or country is encouraged to propose improvements to the IEEE 802.11 standards by proposing amendments to the IEEE 802.11 Working Group. The IEEE 802.11 Working Group is an open and consensus based international forum, with active participation of recognized 802.11 experts from more than 30 countries. IEEE 802 renews its offer, made on numerous occasions during the last five years, to consider the WAPI technology in the IEEE 802.11 Working Group.

In summary, the justification in ISO/IEC JTC 1/SC6 N 14123, based on the assertion that there are security loopholes or flaws in ISO/IEC 8802-11 and its amendments, is not supported by the cited evidence. In addition, we believe the best way for the international community to gain the benefits of WAPI technology is to bring the work into the IEEE 802 standardization process. IEEE 802 again invites the contribution of WAPI technology for consideration.

Yours sincerely,

Paul Nikolich
Chairman of IEEE 802 Executive Committee
p.nikolich@ieee.org