Response of Chinese National Body to doc SC6WG1-SPV022

Chinese National Body

Date: 2005.08.31

Notice: This document is prepared for presentation at the ISO/IEC JTC1/SC6 plenary meeting August 28-September 2, 2005. It is the basis for discussion. The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.

SC6WG1-SPV020 key points

- ***China NB's WAPI explicitly ignores important market realities and engineering tradeoffs***

Comments:

- What's the market realities?

-- many ISO/IEC 8802.11-compliant equipments are faced with many security risks, and there is no international standard providing more secure mechanism until now.

-- The market urgently needs one or more better security technologies than WEP.

- What's tradeoff?

-- Using an security mechanism with defects is more dangerous than not using any security mechanism.

-- Legacy IT technologies can be used in order to provide backward compatibility, just not as well as the latest technologies;

But legacy security mechanisms with security defects should not be used.

-- Trade security for business interests is not acceptable.

-- International community needs for a reliable and uncompromised security mechanism.

Detailed positions has been expressed. Refer to **SC6WG1-SPV016, Status View on WAPI Proposal.**

SC6WG1-SPV020 key points (cont'd)

- ***China NB's proposal dictates a single authentication policy***

Comments:

- WAPI specify a single authentication mechanism (WAI), and it can meet the requirement of authentication
- 11i supports many authentication mechanism, and this makes the implementation of products more complex.
- Refer to **SC6WG1-SPV017, detailed comments on IEEE 802.11i, Part 3.**

SC6WG1-SPV020 key points (cont'd)

- ***International standards require a single default crypto suite to achieve universal interoperability***
- ***The 802.11i security claims have been independently verified by the international cryptographic community, while China's NB has refused to disclose the minimum amount of detail to allow independent verification of a single WAPI security claim***

Comments:

- WAPI defines the interface of cipher algorithm according to the ISO/IEC's

  common regulation of cipher algorithm
- Crypto suite to be applied in information security mechanism may be subject to national and regional regulations.

  It shall conform to national laws and regulations.
- Refer to **ISO/IEC WAPI N33, WAPI and Cipher Issue**.

SC6WG1-SPV020 key points (cont'd)

- ***IEEE is comfortable that 802.11i meets the requirements for an international standard and that WAPI, as currently formulated, does not***

Comments:

- WAPI fully complies with ISO/IEC requirements for international standardization
- We are certain that IEEE 802.11i does not meet all the requirements for international standard
- For details, Refer to **SC6WG1-SPV016, Status View on WAPI Proposal.**

SC6WG1-SPV020 Point 2: Mutual Authentication

- ***Authentication is explicitly outside the scope of IEEE 802, and JTC1/SC6 WG1***

Comments:

- WAI is designed for WLAN authentication function and it resolved the problem of WEP.
- The state machine of WAPI is controlled by the MAC protocol, and WAPI and MAC protocols have become an integrated part.
- The packets used in both proposals(WAPI and 11i) are in the same layer
- For details, refer to **SC6WG1-SPV016, Status View on WAPI Proposal.**

SC6WG1-SPV020 Point 2: Mutual Authentication(cont'd)

- ***802.11i clearly documents that it assumes mutual authentication***

Comments:

- IEEE 802.11i only assumes mutual authentication between STA and AS, not STA and AP
- For details, refer to **SC6WG1-SPV017, Detailed Comments on IEEE 802.11i.**

SC6WG1-SPV020 Point 2: Mutual Authentication(cont'd)

- ***It is straightforward to fit WAI into 802.11i***

Comments:

- Essential authentication frameworks of WAI and IEEE 802.11i are radically different

  E.g. WAPI adopts the peer port control model; 11i adopts the port model of 802.1x with the additional controlled port in Supplicant

- It is very difficult to fit WAI into IEEE 802.11i

SC6WG1-SPV020 Point 3: Comments on IEEE's response to security comparison

➢ About IEEE 802.1x

- We do not oppose the reusing of existed technology, but the existing technology must be suitable to the specified requirement.
- As we pointed in SC6WG1-SPV017, the 802.11i uses 802.1x which does not meet the requirement.

➢ About WEP

- One important goal of IEEE 802.11i is to solve the WEP problems.
- WEP has serious security flaws and is easy to crack. Allowing the technology, although its usage is discouraged, in WLAN systems would continue to put the WLAN users and networks under security risks.

SC6WG1-SPV020 Point 4

- ***IEEE is not opposed to WAPI***
- ***IEEE is opposed to***
  - ***Adopting standards without an open discussion and wide consensus***
  - ***Allowing China to fail by not standardizing WAPI in a manner that meets international requirements***

Comments:

- WAPI fully complies with ISO/IEC requirements for international standardization
- WAPI proposal has passed extensive review and has been modified to adopt comments and suggestions.
- for Details, refer to **SC6WG1-SPV016, Status View on WAPI Proposal.**