Technical Comparison between WAPI and IEEE 802.11i

Chinese National Body

Date: 2005.08.29

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.

Goal and Motivation

- The exact goal of two proposals (WAPI and 11i) is to resolve the security problem of WEP in WLAN.

  To provide:

  1 Secure access control

  2 Data confidentiality and integrality

Components

Item	WAPI	IEEE802.11i
Authentication protocol	WAI : 1 Digital certificate 2 Preshared key	IEEE 802.1x: Multiple identity
Key management protocol	Unicast key negotiation Multicast key notification	4-way handshake Group key handshake
Data encryption	WPI	WEP TKIP CCMP

Detailed technical item comparison

	Items	WAPI	802.11i	Evaluation
Security	Security	Rely on WAPI security	Rely on the security of IEEE802.1x.	802.11i uses IEEE802.1x protocol. The defects of 1x protocol will effect the security of 802.11i.
	Solving all WEP issues	✓	✓ ✗	WEP problems can still happen in 802.11i, which downgrades the security of 802.11i.
	Crypto Unit	MPDU	MPDU	Protect data payloads and MAC functions.

Detailed technical item comparison (cont'd)

	Items	WAPI	802.11i	Evaluation
Security	AE Entity's identity	Digital certificate	None	Entity identity assures that STA (AP) can identify the peer, AP (STA). Or, the forgery attack is possible.
	Mutual authentication	Directly.	Indirectly.	Mutual authentication between STA and AP should be completed directly. In fact, the mutual authentication is achieve only between AS and STA in 802.11i.

Detailed technical item comparison (cont’d)

	Items	WAPI	802.11i	Evaluation
Security	BK negotiation	Between ASUE and AE	Between ASUE and AS	BK negotiation between ASUE and AE is more efficient.
	BK security	✓	✗	BK from AS to AP has risk of being intercepted

Detailed technical item comparison (cont’d)

	Items	WAPI	802.11i	Evaluation
Interoperability	Authentication protocol	WAI	EAP + optional (unspecified)	Unspecified authentication protocol can lead to the problem of interoperation.
	Cipher algorithms	Optional (according laws and regulations of each country)	WEP, TKIP: RC4; CCMP: AES. (Specific)	In an international standard, the cipher algorithm should not be restricted.
	Interoperate with WEP devices	No	Yes	**NOTE**: WEP has serious security problems and can downgrade the system security.

Detailed technical item comparison (cont’d)

	Items	WAPI	802.11i	Evaluation
Compatibility	Backward compatible with WEP	No	Yes	WAPI devices cannot cooperate with WEP devices; 802.11i devices can. (**NOTE**: WEP has serious security problems.)

Detailed technical item comparison (cont'd)

	Items	WAPI	802.11i	Evaluation
Extension	Protocol extension	Easy	Easy	Information element makes extension possible.
	Protocol complexity	Simple	Complex	IEEE802.11i needs other protocols defined elsewhere.
	Network extension	Easy	Complex	When IEEE802.11i network is deployed, AS and AP must pre-configure a secure channel (IPSec or others).