Document : ISO/IEC WAPI N 28-2

Date : 2005-08-18

TITLE : Chinese response to the questions from IEEE (WAPI N 28-1) - CNB contribution for the Beijing meeting, 8-12 August

SOURCE : CNB

REQUESTED ACTION : For information

DISTRIBUTION :

Response to questions from IEEE "Some questions on WAPI N16 and 27"

Chinese National Body

Aug. 10th, 2005

1. The addition of a discovery and negotiation mechanism to WAPI is an interesting step. 802.11i has a seemingly almost identical one. What are the crucial differences between the WAPI and 802.11i mechanisms?

   Answer:

   The objective of Beijing meeting is to produce a joint proposal. For this objective, WAPI has been modified to add this element to allow it to coexist with 11i in the joint proposal for interoperability.

   The discovery and negotiation mechanism is basically similar with 11i's, but in procedure, they are different in some details such as in IBSS.

2. What process was used to select element ID 68?

   Answer:

   There are many reserved IDs in the current international standard ISO/IEC 8802.11. The selected element ID (68) in WAPI was chosen from the reserved IDs. It is not conflict with any currently used ID.

   If it is necessary to register the element ID, WAPI can apply for the element ID through standard procedure.

3. It appears from the contribution N16 that the WAI asymmetric key algorithms are taken from ANSI Std X9.62. Are there asymmetric key algorithms which are not taken from ANSI Std X9.62?

   Answer:

   WAPI uses ECDSA and ECDH. ECDSA is defined in X9.62. ECDH is defined in ISO/IEC 15946.

4. On slide 41, SNonce appears in the first two messages, but Snonce is not defined in any of the message format slides or in the N_16 submissions. What is Snonce?

   Answer:

   SNonce denotes the Authentication Identifier field in the Access Authentication Request packet and the Access Authentication Response packet.

5. Slide 10 shows frames going from the physical layer through the uncontrolled port to the WAI function in the SME. How are the WAI packets encapsulated at

the 8802-11 MAC layer, and how are those frames differentiated by the WAI SME from other frames passed up through the uncontrolled port?

Answer:

The WAI packets are sent as 8802-11 data frames.

WAI SME uses an EtherType to differentiate WAI packets from other frames passed up through the uncontrolled port.

The EtherType used is 0x88B4.

6. Can you identify the curves that are not specified in ANSI Std X9.62?

   Answer:

   WAPI does not specify the curves. The curve adopted in WAPI can be any secure curve.

7. Slide 16 asserts some advantages of WAI over 802.1X. Could you detail your view of these advantages? Could you describe the differences between the WAPI and 802.1X notions of controlled and uncontrolled ports?

   Answer:

   1) WAPI has some advantages over 802.1x as follows:

   Firstly, there is not a controlled port in Supplicant in 802.1x. But in WLAN, the Supplicant may be attacked. WAPI defines the controlled port in ASUE.

   Secondly, the Authenticator Entity in 802.1x is only a proxy of AS. Without the AS, the Authenticator Entity can not authenticate with the Supplicant. WAPI gives an independent identity to Authenticator Entity, so AE can complete authentication with ASUE directly.

   Finally, the SUCCESS message from AS to Authenticator in 802.1x is in risk. WAPI avoids the security threat.

   2) The main difference between 802.1x and WAPI is focused on the 802.1x Supplicant and WAPI ASUE. The 802.1x Supplicant does not have the concepts of controlled port and uncontrolled port. WAPI notices that the concept is unsuitable for WLAN. So WAPI ASUE has controlled port and uncontrolled port.

   In 802.1x, authentication is executed between Supplicant and AS. While in WAPI, authentication is executed between the ASUE and AE. So Authenticator in 802.1x controls the controlled port by the SUCCESS message from AS. AE in WAPI controls the controlled port directly.

8. What is the function of the ASUE signature in the Access Authentication Request (Slide 37)? Is it a security goal, a performance goal, both, or something else?

What key is used for the signature? It appears it is the same as the ASUE's ECDH key. What is the justification for using this key for two different functions?

Answer:

The ASUE signature in the Access Authentication Request is used to verify whether this ASUE possess the private key corresponding to the ASUE certificate.

The signature uses the private key corresponding to the certificate.

The private key corresponding to the certificate is not the same as the ASUE's ECDH key. The ASUE's ECDH key is randomly generated in local device.

9. Does IBSS negotiation (Slides 22-24) establish a unique, session-specific pairwise key for each invocation of the protocol? Can you describe the messages used for this function? In particular, does the exchange on Slide 57 occur in all deployments, including IBSS?

   Answer:

   A unique, session-specific pairwise key will be established for each invocation of the protocol.

   The messages used for this function depend on the security policy. If certificate authentication method is adopted, the certificate authentication procedure, unicast key negotiation procedure and multicast key announcement procedure will be performed orderly. If pre-shared key authentication methods is adopted, only unicast key negotiation procedure and multicast key announcement procedure are performed.

   The exchange on Slide 57 occurs in all deployments, including IBSS.

10. Could you detail the design tradeoffs that led to the use of SHA256 rather than some other hash function?

    Answer:

    Commonly used hash functions are MD5, SHA1 and SHA256, etc. MD5 has been cracked, and SHA1 has also been in risk; SHA256 can meet the requirements of the security at present and in the future years.

    In WAPI, asymmetric algorithm adopts ECDSA192, and the length of the hash value matching ECDSA192 had better no less than 192.

    SHA256 is selected according to the above principles.

11. Slide 76: Is the same packet sequence space ("KNonce") used in both directions, or are there different packet sequence spaces used for the multicast key request and response messages?

    Answer:

KNonce in the Multicast Key Response is the same as KNonce in the Multicast Request;

KNonce is the identifier of the freshness of message in this multicast key announcement process.

12. Slide 85: What does it mean that "WAI addresses known WEP problems?" Which WEP problems are being addressed, and in what way does it address them?

    Answer:

    There is only unidirectional authentication for WEP authentication;

    Because WEP encryption has many problems, the authentication message using WEP encryption could be forged easily.

13. The change from protection of MSDUs to MPDUs is one of the more significant architectural changes to WAPI introduced in N16. What was the rationale behind it?

    Answer:

    If fragment is enabled, protection of MPDUs is more efficient than of MSDUs, especially when AP is forwarding data traffic between two STAs.

    Protection of MPDUs facilitates the implementation of the dual mode products of WAPI and 11i.

    So the joint proposal adopts the protection of MPDUs.

14. Could you discuss the rationale behind the selection of OFB and CBC-MAC modes? Can the block cipher definition be made available to all parties?

    Answer:

    OFB and CBC-MAC modes are mature and widely used.

    Cryptographic algorithms to be applied in information security mechanism may be subject to national and regional regulations. An appropriate algorithm shall be adopted here, and which type of algorithm to be adopted is optional. It shall conform to national laws and regulations, and can be chosen according to specific requirements in different countries and regions.

    The algorithm SMS4 is chosen to be adopted in China. SMS4 is owned by Beijing Data Security Technology Co. Ltd.(BDST). (E-Mail: chinabdst@126.com)

15. Why 128 bits for the MIC block size?

    Answer:

    The block size of the cipher used in WPI MIC is 128 bits.

128-bit MIC can satisfy the security requirements of present and future networks.

16. We have a great deal of admiration for the core WAI design. How broadly applicable is WAI? What assumptions and dependencies does the WAI certificate authentication mechanism have with respect to the 8802-11 MAC layer? Is there any reason that WAI could not be used on 8802-3 or other LAN technologies? Are there some special characteristics that limit its applicability to other remote access functions, e.g., 802.16, PPP, VPN?

    Answer:

    Thanks for the compliments on WAI design.

    WAI is developed specially for WLAN to solve the defects of WEP. Now WAI is applicable only in WLAN.

    WAI and MAC layer protocol of ISO/IEC 8802-11 form an integral part for the purpose of implementing the authentication and privacy. Many status controls in WAI cooperate with MAC protocol.

    Through extensions, WAI may be applied to other networks such as 802.16. This is a subject being under consideration.

17. What translation must be done by the AP when bridging WAI packets between the 802.11 and AP/AS transport layers?

    Answer:

    WAI packets do not need to be bridged between 802.11 and AP/AS transport layer. For WAI protocol, the packet from STA is processed in AP. AP then generates a new packet and sends it to AS through the AP/AS transport layers.

18. When the system is using certificate authentication, the BK key derivation indicates that the Next Challenge to be used for BK updates is computed as part of the BK computation process. What are the security advantages of computing the Challenge seed and next challenge as part of the BK derivation?

    Answer:

    The next challenge must be identical for the pair of STAs and be unknown to others. It has the similar property to session key.

    The challenge from the BK derivation can meet the requirements.

19. The PNs used to prevent replay of data frames are 16 octets. What are the design requirements that drove the selection of this PN size? Please describe the rationale behind the selection for the initial PN values.

    Answer:

Since the PN is also used for IV of the block cipher with 128-bit (16 octets) block, the PN size is 16 octets.

The initial PN value in WAPI is selected according to the balance between the numbers "0" and "1".

20. When two stations are using STAKeys to protect data sent between them, are there any changes to how the data frames are encapsulated versus how they are encapsulated when using regular unicast keys ?

    Answer:

    They use the same encapsulation.