IEEE P802.11
Wireless LANs

|  |
| --- |
| Addressing Comments by Chinese NB during FDIS Ballot of ISO/IEC/IEEE 8802-11 |
| Date: 2018-04-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  3333 Scott Boulevard, Santa Clara, California,  United States of America |  |  |
|  |  |  |  |  |

Abstract

IEEE Std 802.11-2016 was submitted to ISO/IEC/JTC1/SC6 for ratification under the PSDO process. During FDIS balloting, thirteen comments were received from the China National Body (see ISO/IEC JTC1/SC6 document N16794). This submission proposes resolutions to those comments for liaison back to ISO/IEC/JTC1/SC6 as part of the PSDO process.

***Comments dealing with deprecated algorithms***

**CN1**

Comment:

*In general, ISO/IEC/IEEE FDIS 8802-11 (ED 2) is supposed to enhance the function of the current ISO/IEC 8802-11:2012 and its amendments. But WEP and TKIP, which should not be used in WLAN because of their weak and well-known security defects, are reserved; also, the current well-known KRACK attack which causes session key reinstallation have not been resolved in this proposal. All of these conflicts with the design goal of ISO/IEC/IEEE FDIS 8802-11 (ED 2). In fact, security methods specified by ISO/IEC/IEEE FDIS 8802-11 (ED 2) have many technical weaknesses to be addressed and security defects that cause serious concern. So, ISO/IEC/IEEE FDIS 8802-11 (ED 2) should not be ratified as an international standard because of the technical reasons mentioned above.*

Proposed Change:

*Please revise the FDIS text.*

**CN5**

Comment:

***WEP mechanism downgrades the security levels, so the proposal does not resolve or improve security problems actually*** [emphasis in original]. *Since WEP security mechanism is reserved, all known WEP security defects still exist. Products conformed to ISO/IEC/IEEE FDIS 8802-11 (ED 2) may use WEP mechanism which will result in the loss of security. In addition, the security of the system applying higher security mechanism will be actually downgraded in the mixed environment which allows the multiple security mechanisms to coexist. So TKIP and AES-CCMP cannot protect the traffic as expected in this case. The security level of the whole system will be downgraded. The sole design goal and necessity of ISO/IEC/IEEE FDIS 8802-11 (ED 2) as a replacement of ISO/IEC 8802-11:2012 is to resolve the obvious problems such as WEP and enhance the usability of ISO/IEC 8802-11:2012. But the reservation of these obvious problems such as WEP in ISO/IEC/IEEE FDIS 8802-11 (ED 2) makes all these impossible.*

Proposed Change:

*WEP is vulnerable to be broken in practice and shall be removed from this proposal.*

**CN6**

Comment:

*TKIP, the security mechanism reserved in ISO/IEC/IEEE FDIS 8802-11 (ED 2), introduces denial of service attack. TKIP uses Message Integrity Code (MIC) called Michael to detect forgery attempts. Only 220 security can be provided by the MIC. So the countermeasure, which means that if two invalid messages are detected within one minute (i.e. evidence of active attack) then the network will be shut down for one minute, is adopted to fill up the security loophole. Thus, if the attacker continually transmits two invalid messages every minute, the whole network is not available and DoS attack is easily launched.*

Proposed Change:

*TKIP is vulnerable to be broken in practice and shall be removed from this proposal.*

**CN11**

Comment:

*An ISO/IEC/IEEE FDIS 8802-11 (ED 2) transition security network (TSN) allows the creation of pre-robust security network associations (pre-RSNAs) as well as RSNAs. Beacon frames have to specify WEP as the group cipher suite in RSNE, so that pre-RSNA STAs can coexist with RSNA STAs in a BSS. Similarly, pre-RSNA STAs ignore RSNE in beacon frames, thus RSNA STAs have to use TKIP as the pairwise cipher suite and WEP for authentication in an IBSS. Due to the weakness of the WEP technology, even the CCMP,GCMP security technologies will be attacked successfully and easily.*

Proposed Change:

*The* *TSN mechanism will bring the new security issues, which should be removed in this proposal.*

**Proposed resolution to CN1, CN5, CN6, CN11**

Reject.

It is acknowledged and agreed that both WEP and TKIP are vulnerable to attack and that using either one of them, or the TSN mechanism, would result in a compromise of network security. However, WEP and TKIP, and therefore the TSN mechanism, are all deprecated by the standard, meaning they have been superceded (by CCMP and GCMP) and are no longer considered safe to implement. As stated in section 5.1.2 of IEEE 802.11-2016, both WEP and TKIP are “unsuitable for the purposes of this standard.” IEEE 802.11 includes deprecated protocols for historical reasons.

Michael, the MIC capability of TKIP, was designed to offer security against attacks on O(220). Shutting down the BSS was deemed to be a suitable countermeasure at that time given the perceived strength of Michael. A thorough discussion on the strength of Michael, and better countermeasure, is described in:

 https://mentor.ieee.org/802.11/dcn/03/11-03-0211-00-000i-michael-attacks-and-countermeasures.ppt

Regardless, MIC capability of TKIP is also deprecated and marked as unsuitable.

***Comments dealing with KRACK***

**CN1**

See above

**CN12**

Comment:

***The well-known KRACK attack which causes session key reinstallation has not be resolved in this proposal*** *[emphasis in original]****.*** *Investigators have proved the weakness of IEEE 802.11, that 4-way handshake, group key handshake, STAKey handshake, FT handshake and so on, are vulnerable to a key reinstallation attack, which will happen regardless of whether there is an active attacker or not. Finally, it resulted in data to be replayed, decrypted and forged. Please refer to* [*https://papers.mathyvanhoef.com/ccs2017.pdf*](https://papers.mathyvanhoef.com/ccs2017.pdf)*. It is indicated by thorough research and analysis that the nonce and replay counter are easily reset to their initial value which will result in reinstallation of session key. Indeed, the experiments of the attack on different system demonstrated that the key could be reinstalled and the IV was initialized maliciously.*

Proposed Change:

*To meet the nonce uniqueness requirements, the nonce values need to be carefully detected and set to instruct implementers to prevent nonce resetting during key installation events.*

**Proposed resolutions to CN1 & CN12**

Reject.

The KRACK attack is against implementations of ISO/IEC/IEEE FDIS 8802-11, not against the standard itself.

Indeed, nonce uniqueness is already clearly described in IEEE 802.11-2016. For instance, section 12.5.3.1 states: “CCM requires a fresh temporal key for every session. CCM also requires a unique nonce value for each frame protected by a given temporal key, and CCMP uses a 48-bit packet number (PN) for this purpose. **Reuse of a PN with the same temporal key voids all security guarantees** [emphasis added].” There is similar text in the standard for GCMP.

Nonetheless, an additional reminder was added to Draft P802.11REVmd in the MLME primitive that performs key installation. This change will be seen in a forthcoming PSDO submission when the current maintanence cycle is completed in the IEEE 802.11 WG.

***Comments dealing with PMK and its transport***

**CN4**

Comment:

*Pairwise Master Key (PMK) in ISO/IEC/IEEE FDIS 8802-11 (ED 2) is an important security element, but it has to be transported from the authentication server to the access point, which will result in security risk of PMK.*

Proposed change:

*The PMK is suggested to be created at AP and STA to avoid security problem in transmission.*

**CN8**

Comment:

*Though PMK can be delivered through an additional secure channel, the details of the secure channel are not specified in this proposal. This does not guarantee security of secure channels. Besides, every AP should establish a secure channel with the authentication server before supplying services to clients. This complicates the configuration of network and limits the expansibility and flexibility of users, especially for large-scale networks.*

Proposed change:

*The secure channel is an important factor in the authentication procedure in ISO/IEC/IEEE FDIS 8802-11 (ED 2). How to establish the secure channel shall be clearly specified in this proposal.*

**CN3**

Comment:

***Devoid of real mutual authentication*** *[emphasis in original]****.*** *Though ISO/IEC/IEEE FDIS 8802-11 (ED 2) assumes a mutual authentication between a authentication server and a station, the authenticated identities of the access point and the station are not known by each other. For example, in the EAP-TLS protocol, authentication by certificate happens between the client and server. So extra secure channels are needed to be negotiated between AP and server to notify AP the result of authentication and the secure parameter PMK. Also, the AAA protocol, which is necessary to ISO/IEC/IEEE FDIS 8802-11 (ED 2), cannot guarantee the security of key delivery from the authentication server to the access point. So, the forgery attack against the access point or the station is possible.*

Proposed change:

*The AP shall have an independent identity. Both a non-AP STA and AP shall authenticate each other*

**Proposed resolution to CN4, CN8 and CN3**

Reject.

There is no requirement in ISO/IEC/IEEE FDIS 8802-11 to transmit a PMK from an authentication server to the Authenticator. An external AS is an optional enhancement for authentication credentials that are more suited to central management, for instance using username/password credentials.

Techniques in the standard to derive a PMK on both the STA and AP/Authenticator include:

1. The SAE protocol (section 12.4) which describes a way to derive a PMK between STA and AP using a zero knowledge proof authenticated with a simple password.
2. The Fast Initial Link Setup (FILS) protocol, which amends ISO/IEC/IEEE 8802-2016 and has been approved by ISO/IEC/JTC1/SC6 using the PSDO process, includes the ability to establish a PMK as the result of a Diffie-Hellman key exchange between STA and AP authenticated using either X.509 certificates or raw public keys.
3. Terminating the EAP exchange directly on the AP/Authenticator and deriving a PMK there. To use the example from comment CN3, EAP-TLS using certificates could easily be terminated on the Authenticator without requiring an external Authentication Server.

Since ISO/IEC/IEEE FDIS 8802-11 is restricted to to the PHY and MAC layers of the OSI model, description of communication between the Authenticator and a centrally-managed authentication server is out of the scope of the standard.

While such a protocol is out of scope, section 4.10.6 of ISO/IEC/IEEE FDIS 8802-11 clearly describes the requirements placed on the Authenticator-to-AS protocol if a deployment requires one.

* The first two are “*[m]utual authentication between the Authenticator and the AS*” and “*[a] channel for the Supplicant/AS authentication.*” Suitable protocols to satisfy these requirements are listed in 4.10.6 as RFC 2865 (RADIUS) and RFC 3588 (Diameter) with further discussion in section 12.7.1.3.
* The final requirement is “*[t]he ability to pass the generated key from the AS to the Authenticator in a manner that provides authentication of the key source, preserves integrity of the key transfer, and preserves data confidentiality of the key from all other parties.*” A suitable technique to ensure the confidentiality and integrity of the key as well as an authenticated key transfer is using either one of the aforementioned protocols with RFC 6218 attributes and ISO 20038-2017 Key Wrapping using AES.

***Comment dealing with ciphersuite negotiation***

**CN13**

Comment:

*In ISO/IEC/IEEE FDIS 8802-11 (ED 2), CCMP/GCMP/BIP are mandatorily based on AES encryption algorithm without other options.*

*Actually, a cryptographic algorithm is one module of a security protocol, and it is usually used in the security protocol. The security protocol and cryptographic algorithm is relatively independent, and the security protocol is applicable to multiple different cryptographic algorithms. Cryptographic algorithms are only adoptable modules, and which algorithm to be applied is subject to the user’s requirement and national/regional laws and regulations.*

*But in this proposal, only AES is specified. That’s to say, the compliance to the proposal is being bound by using AES. It causes the neglect of other nations’ interests and makes the proposal not applicable in different nations.*

Proposed change:

*Cryptographic algorithms to be applied to information security mechanism may be subject to national and regional regulations. In this specification, cryptographic algorithms are instantiated, which should conform to national laws and regulations, and can be chosen according to specific requirements in different countries and regions.*

**Proposed resolution to CN13**

Reject.

All standards need to have mandatory-to-implement options to ensure interoperability, which is a primary purpose of international standardisation. ISO/IEC/IEEE FDIS 8802-11 has chosen a well-vetted and internationally designed and recognized cipher (AES) for that purpose.

There is no requirement for ISO/IEC/IEEE FDIS 8802-11 to comply with the laws of every country around the world. Indeed, any attempt to do so is likely to fail because of the diversity of laws and because they can change over time. However, ISO/IEC/IEEE FDIS 8802-11 provides the ability to negotiate different ciphers through cipher suites in the RSNE that may allow local laws and regulations to be better satisfied in some countries.

There are two options for using other ciphers with ISO/IEC/IEEE FDIS 8802-11:

1. Produce a published and readily-available definition of the cipher, a proof of security by reputable cryptographers, a set of test vectors, and a public submission of how to modify 802.11 so the cipher can protect 802.11 frames (including the 802.11 header) that meets the requirements of 802.11 ciphers—namely, confidentiality, data source authentication, data integrity, and anti-replay protection. Bring these documents and any additional supporting documentation to a future IEEE 802.11 Working Group meeting and advocate for the inclusion of the cipher in table 9-131 and allocation of a Suite number by ANA; or,
2. Purchase a CID from the IEEE RAC, use it to create a registry of non-public ciphers, and use the Vendor Specific cipher suite from table 9-131 with a Suite number from that registry.

Choosing option 1 or 2 depends on whether or not, respectively, the China NB wishes for there to be substantial implementation and use of their national cipher outside of the jurisdiction of the local laws and regulations it states are necessary to abide by.

***Comment dealing with EAP method negotiation***

**CN7**

Comment CN 7003:

*The authentication protocol is not specified in ISO/IEC/IEEE FDIS 8802-11 (ED 2). It just provides an authentication framework 802.1X EAP, but no method details. There are many different EAP-based protocols for WLAN specified by IETF drafts, such as EAP-TLS, EAP-MD5 EAP-TTLS, EAP-PEAP, and so on. The security of each 802.1X-EAP protocol is another problem which shall be noted. Furthermore, there are many methods for breaking up 802.1X-EAP protocols in the internet like MITM attack. They have to be implemented for interoperability and then make conformance difficult and management complex.*

Proposed change:

*The authentication protocol shall be re-designed in order to resolve the issue.*

Proposed resolution to CN7

Reject.

ISO/IEC/IEEE FDIS 8802-11 places security requirements on implementations, it does not require that any particular EAP method be supported, especially not EAP methods that are susceptible to attack.

The standard clearly states that if IEEE 802.1X-2010 is used, the EAP method shall support mutual authentication. Any EAP method that was susceptible to “breaking up” in the form of a MITM attack would not satisfy that requirement. There is no requirement to implement all EAP methods, much less EAP methods susceptible to attack.

In fact, the freedom afforded deployments by this minimal requirement has resulted in plain unitary EAP methods, tunnelled EAP methods, and chained EAP methods that address unique and complex requirements seen in the real world dealing with machine authentication in addition to user authentication using every credential possible—certificates, smart cards, SIM cards, token cards, username/password, etc. The wide deployment of 802.11 with 802.1X/EAP authentication indicates a great success in this approach, not the problem alleged in the comment.

***Comment on redesigning the 4-way Handshake***

**CN9**

Comment:

*The 4-way handshake protocol described in JTC1/SC6/IEEE FDIS 8802-11 is incomplete. When Supplicant receives message 3 and sends message 4, its controlled port is open, but the controlled port of Authenticator is still closed. If message 4 isn’t received by Authenticator, then the port statuses of both sides are not the same. The loss of msg.4 will result in the loss of synchrony of peers and the failure of 4-way handshake protocol, even though it doesn’t include security issues. Because the retransmit of msg.3 in plaintext is not accepted by the station which has unblocked the control port and expected the ciphertext.*

Proposed change:

*The mechanism shall be re-designed in order to resolve the issue.*

**Proposed resolution to CN9**

Reject.

The Supplicant state machine accepts an unencrypted, and retransmitted, message 3 in the event of a loss of message 4. The state machines for the 4-way Handshake are very robust and will synchronize in the presence of packet loss. They been proven using formal methods.

In fact, it was this case— a lost message 4 and retransmitted message 3—where the MLME-SETKEYS primitive gets called a second time which resulted in certain faulty implementations resetting the nonce to zero in the KRACK attack. In other words, the KRACK attack against certain implementations was possible because the 4-way Handshake state machine permits an unencrypted and retransmitted message 3 to be processed.

There is no issue to resolve, the mechanism has been proven in theory and in practice to operate effectively and as intended.

***Comment on not using URN but use OUIs instead***

**CN2**

Comment:

*URN used in this proposal is not recommended for using in ISO standards.*

Proposed change:

*Suggest using OID to manage the resources those involved in the proposal.*

**Proposed resolution to CN2**

Reject.

Many of the mentioned identifiers are specific to ISO/IEC/IEEE FDIS 8802-11 and managed by the IEEE 802.11 ANA. When extensibility is desired, OUIs are already used. For example, the specification of cipher suites, authentication and key management suites, and key data encapsulations allow for external organizations to use an assigned OUI to manage resources.

***Comment about too many messages in EAP***

**CN10**

Comment:

*According to the Figure 4-31—IEEE 802.1X EAP authentication operates the authentication procedure depending on over 20 messages exchange. It is much too complex and time-consuming.*

Proposed change:

*The authentication protocol shall be re-designed in order to resolve the issue.*

**Proposed resolution to CN10**

Reject.

It is not clear where “over 20 messages” came from. The total number of messages could be 14 if RFC 5931 is used. This EAP method defined in RFC 5931 satisfies the requirements ISO/IEC/IEEE FDIS 8802-11 places on EAP methods and uses 6 messages.

In addition, the Fast Initial Link Setup (FILS) protocol, which amends ISO/IEC/IEEE 8802-2016 and has been approved by ISO/IEC/JTC1/SC6 using the PSDO process, performs a Diffie-Hellman key exchange, authenticated with digital signatures, and generates traffic encryption keys all in just 4 messages total, including the 802.11 Authentication and 802.11 Association frames.

Any potential issue has already been resolved.

**References:**