IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Inputs to IEEE 802.11 TGai | | | | |
| Date: March 14, 2012 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | Toronto ON, Canada | USA: +1 (415) 690-7363  Toronto: +1 (647) 867-5658  Skype: rstruik | rstruik.ext@gmail.com |

**All motions are relative to Section 4 of the sfd document (12/151r5).**

Device joining may include an authentication scheme, where two devices A and B derive a shared key (key agreement) and show that these have computed correctly (key confirmation) in each of the following scenarios:

1. Both devices do not share a secret key, but each shares a key with a mutually trusted third party.
2. Both devices do have (access to) a certificate of their public key, issued by a trusted third (certificate authority).
3. Both devices do share a weak secret key.
4. Both devices do share a secret key.

**Strawpoll #1:**

Scenario #1 should be included, where devices are STA and AP respectively and third party is AS.

**MOTION #1:**

**The draft should include an authentication scheme, where STA and AP derive a shared key (key agreement) and show that these have computed correctly (key confirmation), where both devices do not share a secret key, but each shares a key with a mutually trusted third party AS.**

**Moved:**

**Seconded:**

**Y/N/A:**

**Strawpoll #2:** Scenario #2 should be included, where devices are STA and AP respectively and where AS may provide authorization service.

**MOTION #2:**

**The draft should include an authentication scheme, where STA and AP derive a shared key (key agreement) and show that these have computed correctly (key confirmation), where both devices do have (access to) a certificate of their public key, issued by a trusted third party (certificate authority), and where AS may provide authorization service.**

**Moved:**

**Seconded:**

**Y/N/A:**

Authenticated key agreement schemes generally include the following security properties:

1. Key establishment
2. Key Agreement
3. Implicit key authentication
4. Explicit key authentication
5. No unilateral key control
6. Forward secrecy
7. Entity authentication
8. Unknown Key Share Resilience

**Strawpoll #3:** This should include all properties (mutually), except #6.

**MOTION #3:**

**The authentication scheme(s) in the draft shall provide the following security properties:**

1. **Key establishment**
2. **Key Agreement**
3. **Implicit key authentication**
4. **Explicit key authentication**
5. **No unilateral key control**
6. **Entity authentication**
7. **Unknown Key Share Resilience**

**Here, properties are provided mutually.**

**Moved:**

**Seconded:**

**Y/N/A:**

**Strawpoll #4:** This should include all properties (mutually), including #6.

**MOTION #4:**

**The authentication scheme(s) in the draft should provide forward secrecy.**

**Moved:**

**Seconded:**

**Y/N/A:**

Security properties may include:

1. Identity protection

**Strawpoll #5:** Optional support for #1 should be included.

**MOTION #5:**

**The authentication scheme(s) in the draft should optionally provide for identity protection.**

**Moved:**

**Seconded:**

**Y/N/A:**

Further considerations:

1. Schemes shall be demonstrably free of known security weaknesses (burden on proposers)
2. Schemes shall be well-studied by the cryptographic community
3. Schemes should be standardized via int ernationally accepted cryptographic standards (NIST/FIPS series, IETF)

**Strawpoll #6:** Schemes should satisfy #1, where the onus is on proposals/proposers to provide solid evidence.

**MOTION #6:**

**The authentication scheme(s) in the draft shall be demonstrably free of *known* security weaknesses.**

**Moved:**

**Seconded:**

**Y/N/A:**

**Strawpoll #7:** Schemes should satisfy #2, where the onus is on proposals/proposers to provide solid evidence.

**MOTION #7:**

**The authentication scheme(s) in the draft shall be well-studied by the cryptographic community.**

**Moved:**

**Seconded:**

**Y/N/A:**

**Strawpoll #8:** Schemes should satisfy #3, where the onus is on proposals/proposers to provide solid evidence.

**MOTION #8:**

**The authentication scheme(s) in the draft Schemes should be standardized via internationally accepted cryptographic standards (such as NIST/FIPS series, IETF, etc.).**

**Moved:**

**Seconded:**

**Y/N/A:**

Joining protocols would involve authorization, where:

1. Authorization of the STA may be provided by the third party AS;
2. The third party providing authorization may be different from the third party potentially providing authentication support.

**Strawpoll #9:** Scenario #1 should be supported.

**MOTION #9:**

**With the authentication scheme(s) in the draft, authorization of the STA may be provided by the third party AS.**

**Moved:**

**Seconded:**

**Y/N/A:**

**Strawpoll #10:** Scenario #2 should be supported.

**MOTION #10:** (NOT RIGHT NOW)

*Considerations on cryptographic strength (\*new\*)*

Crypto schemes should generally be designed conservatively and take into account:

* Protection lifetime;
* Progress in cryptanalytic attacks;
* Progress in computational speed.

NIST, NESSIE, IETF generally recommend a so-called cryptographic bit strength of 112 bits, which is higher than 80-bit (and not longer recommended by NIST). NSA’s Suite B and most IETF drafts go for 128 bit cryptographic bit strength.

NOTE: AES-128 and, e.g., the GCMP mode of operation have 128-bit cryptographic *design* strength.

**MOTION #11:**

**The authentication scheme(s) in the draft SHALL have cryptographic strength of at least 80 bits and SHOULD have cryptographic strength of 128 bits.**

**Moved:**

**Seconded:**

**Y/N/A:**

*Considerations on carrying additional data fields (\*new\*)*

Cryptographic authentication schemes often include the option to include additional data fields in the protocol flows (so-called “piggy-backing”). This can be used to convey additional information between communicating entities with authenticity assurances and logical tie-up with the protocol execution in play.

Examples include provision of DHCP IP address information and authorization information along the authenticated key agreement protocol.

NOTE: Most international standards include this provision, so this does not necessarily require changes to existing specification in practice.

**MOTION #12:**

**The authentication scheme(s) shall provide for the optional inclusion of additional information in their protocol flows, so as to assist in conveying this information in parallel and logically tied to the protocol.**

**Moved:**

**Seconded:**

**Y/N/A:**