IEEE P802.11
Wireless LANs

|  |
| --- |
| Security Inputs to IEEE 802.11 TGai |
| Date: January 19, 2012 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | 723 Carlaw Avenue Toronto ON Canada M4K 3K8 | USA: +1 (415) 690-7363Toronto: +1 (647) 867-5658Skype: rstruik | rstruik.ext@gmail.com  |

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. Y/N/A = 20/0/3.

**Strawpoll #2:** Scenario #2 should be included, where devices are STA and AP respectively and where AS may provide authorization service. Y/N/A = 7/2/14.

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. Y/N/A = 2/1/20.

**Strawpoll #4:** This should include all properties (mutually), including #6. Y/N/A = 4/3/20.

Security properties may include:

1. Identity protection

**Strawpoll #5:** Optional support for #1 should be included. Y/N/A = 5/3/19.

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 internationally accepted cryptographic standards (NIST/FIPS series, IETF)

**Strawpoll #6:** Schemes should satisfy #1, where the onus is on proposals/proposers to provide solid evidence. Y/N/A = 8/1/9.

**Strawpoll #7:** Schemes should satisfy #2, where the onus is on proposals/proposers to provide solid evidence. Y/N/A = 6/1/14.

**Strawpoll #8:** Schemes should satisfy #3, where the onus is on proposals/proposers to provide solid evidence. Y/N/A = 10/1/9.

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. Y/N/A = 9/0/7.

**Strawpoll #10:** Scenario #2 should be supported. Y/N/A = 2/4/14.