IEEE P802.11
Wireless LANs

|  |
| --- |
| CR for CID 1921 in LB240 |
| Date: 2019-11-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Feng Jiang | Intel | 3600 Juliette Ln, Santa Clara, CA 95054 |  | feng1.jiang@intel.com |
| Qinghua Li | Intel |  |  | qinghua.li@intel.com |

Abstract

This submission addresses the following LB240 CIDs: 1921

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CID | Page | Clause  | Comment | Proposed Change | Resolution |
| 1921 |  | 11.22.6.3.4 | It is not clear what attack models secure ranging is attempting or succeeding to guard against, or what the receiver needs to do in order to achieve the security. All there seems to be is a statement in 11.22.6.3.4 Secure LTF Measurement Setup that "With the preceding construction, an attacker not knowing Secure-LTF-Key-Seed, would not be able to predict the SAC that would be used for given measurement." It would be helpful to have something similar to 12.7.6.8 4-way Handshake Analysis to guide implementers and users. | As it says in the comment. Need informative text analysing the security mechanisms, the threat models that they address, and limitations on their effectiveness (e.g. not preventing the range being spoofed as further than it actually is). | RejectedThe comment suggests to add descriptive text for the attacke model and the detection behavior of receiver. However, these are fully described in the SFD document where different threat models were specified and the standard was develop according to. Also, the standard itself is limited to describing normative behavior of the interoperable part and the threat model is not part of which.   |