IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Title: Proposed Update to the D1.1 Draft, New WEP Section

Author:

Dave Bagby
AMD
Email: david.bagby@amd.com

Abstract: **This paper proposes changes to the D1.1 Draft to reflect the discussions held during the May 95 meeting.**

Action: **Adopt the changes in this paper to update the relevant portions of P802.11/D1.1**

This document (distributed at the meeting as D96.doc) contains a change for the new section on the Wired Equivalency Privacy (WEP). It is the actual text to implement the rc4 motion. This text was created from the D95s2.doc (95/095) file and so should be applied on top of the D95s2 file. i.e. the correct layer of mods is:

D1.1 chapter --> apply D95sx docs ---> apply D96.doc ---> result in D1.2 text.

1.

1.0.1. WEP Algorithm Specification

WEP uses the RC4 ~~The specific~~ PRNG algorithm from RSA Data Security, Inc..

Details of the RC4 algorithm are specified in <insert document reference here> available from RSA. Please contact RSA for algorithm details and the uniform RC4 liscense terms which RSA offers to anyone wishing to use RC4 for the purpose of implementing the 802.11 WEP option.

~~is unspecified at present. Reviewers of this draft are encouraged to comment on appropriate PRNG algorithms for adoption by 802.11.~~