doc: IEEE P802.11-95/096a

0..

May 1995

Title:

100

IEEE 802.11 . . . Wireless Access Method and Physical Layer Specifications

Presentation Material for the RC4 - WEP Discussion

Author: Dave Bagby AMD 4,9 Email:david.bagby@amd.com 165 100

1

This document (distributed at the meeting as D95a.ppt) contains the slides used to discuss a change to the Wired Equivalency Privacy (WEP). It a proposal to simplify the WEP, based on comments contained in document 95/112

1. 注意/11

 $\hat{g}_{1}^{(1)} = (\hat{r} - \hat{r} + \hat{q}_{1} + \hat{q}_{2} +$

the second state of the second state of the . and the margin of the state $\left\| (v_{1},v_{2},v_{3},v_{3}) - v_{3} \right\| = \left\| \partial U \right\|_{1}^{2} \left\| \partial u_{2} - v_{3} \right\|_{1}^{2} \left\| \partial \Omega E^{\frac{1}{2}} \left(- \sum_{i=1}^{2} \frac{1}{i} \left\| \nabla V \right\|_{1}^{2} + \sum_{i=1}^{i$

Sec. Street

and the second table of the second second

on a pride state in the 王 新闻 的复数

i ar

182

2 8

1 19 1⁴0

WE BELL COLLECTION OF ALLA

 \mathcal{X}

181

1 Hale

3 3 13

3. a. a. 14

21

doc: IEEE P802.11-95/096a

May 1995

WEP Privacy mechanism Completion

• Conditionally Adopt RC4 to Complete WEP.

- Best and Only technical solution proposed.
 - » Use of internet pseudo RC4 would likely result in legal action.
- Well known alg, has withstood cryptographic test of time.
- Takes advatnage of RC4 special export status
- Very reasonable implemention
 - » See previous papers
- Proposed adoption conditions detailed in RC4 motion slide.
- Proposed D1.2 text to support the motion contained in second page of doc 95/96.

IEEE 802.11 MAC document D95/96 - May 1995

David Bagby

1