

Wireless Local Area Network Security: A Framework for Repairing the Broken WEP Protocol

Russ Housley
Vigil Security, LLC
housley@vigilsec.com

Jesse Walker
Intel Corporation
jesse.walker@intel.com

Nancy Cam-Winget
Cisco Systems
ncamwing@cisco.com

The IEEE 802.11 standard published in 1999 includes the Wired Equivalent Privacy (WEP) algorithm to protect communication from eavesdropping and to prevent unauthorized wireless network access; however, WEP has critical security flaws. A task group within the IEEE 802.11 working group, TGi, has developed standards for improved wireless local area network security. This paper exposes the security flaws in WEP and shows how IEEE 802.11i corrects them.