

# Cisco Shares Findings From Recent WLAN Security Research



In a recent research paper entitled “Weaknesses in the Key Scheduling Algorithm of RC4,” co-authors Scott Fluhrer from Cisco Systems and Itsik Mantin and Adi Shamir from The Weizmann Institute describe a serious attack on WEP that is practical to implement. The paper identifies several weaknesses in the key scheduling algorithm of RC4, a widely used stream cipher in software applications, that can provide unauthorized users with a small number of key bits they can use to construct the “WEP key” necessary to gaining network access.

Cisco is aware of the WEP limitations identified in the paper and regularly conducts internal and external projects in several areas related to wireless local area network (WLAN) security. Cisco has shared its finding through the Wireless Ethernet Compatibility Alliance (WECA) and IEEE 802.11 standards to deliver interoperable security solutions to its customers and the industry.

Cisco is also pleased that the Cisco Aironet® Series of Wi-Fi™ (IEEE 802.11b)-compliant WLAN products provides a security solution to address several of the limitations identified in the paper. This security solution includes Dynamic WEP Key Management, which allows network administrators to set time increments in which WEP keys are exchanged per user, per session. Increasing the frequency in which keys are exchanged helps systems mitigate this type of attack. Cisco maintains time recommendation guidelines for customers based on their security needs and deployments.

This solution, unique to the Cisco Aironet Series, is a result of joint efforts by Cisco, Microsoft, and other industry leaders to define the IEEE 802.1x enterprise-class security architecture for wireless 802.11 networks. Recognizing that no single security scheme works for all customers, in addition to Aironet wireless security solution, Cisco also offers VPN, firewall, and Cisco IOS® Software services to enhance the end-to-end security of networks.

For additional information contact Linda Horiuchi, Public Relations Manager, 408 853-5464 or refer to these documents on security:

<p>Cisco Aironet 350 Series Wireless LAN Security</p>	<p><a href="http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html">http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a00801f7d0b.html</a></p>
<p>Response to University of Maryland WLAN Security Paper</p>	<p><a href="http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a008009246e.html">http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a008009246e.html</a></p>
<p>Cisco Aironet Response to Press— Flaws in 802.11 Security</p>	<p><a href="http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a0080088832.html">http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a0080088832.html</a></p>



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9

France  
www.cisco.com  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA

www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems Australia, Pty., Ltd  
Level 9, 80 Pacific Highway  
P.O. Box 469  
North Sydney

NSW 2060 Australia  
www.cisco.com  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco.com Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic  
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel  
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal  
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden

All contents are Copyright © 1992–2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement. Aironet, Catalyst, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0105R)

08/01 BW7510