

Cisco Comments on Recent WLAN Security Paper from University of Maryland



Recently, University of Maryland published a paper, "Your 802.11 Wireless Network has No Clothes," which highlighted some of the security problems in wireless LANs. While the paper from the University of Berkeley (January 2001) focused on overall vulnerabilities with 802.11 wired equivalent privacy (WEP) encryption, the University of Maryland paper focused on vulnerabilities in 802.11 wireless LAN authentication methods and protocols for access control. The paper also outlined how poor authentication implementations in the industry can cause even more damage than standard WEP. The paper also provides recommendations to address several of these classes of attacks.

Details from the paper can be found at <http://www.cs.umd.edu/~waa/wireless.pdf>

Summary

The paper highlights several deficiencies in 802.11 security implementations from the standpoint of authentication methods and protocols for access control. The authors also provide recommendations on how to mitigate eavesdropping and man-in-the-middle attacks using strong authentication and well protected shared keys. The Cisco Aironet® solution incorporates strong key management and authentication framework and is immune to the classes of attacks identified in this paper, unlike

some of our competitors. The major components of our overall security framework that address these deficiencies include:

- Strong mutual authentication
- Dynamic, per user, per session key
- Random starting value of initialization vector
- Independent WEP key derivation at both the client and the ACS Remote Access Dial-In User Service (RADIUS) server
- Policies for re-authentication on the ACS RADIUS server

Obtain additional details from the Cisco response to the paper from University of Berkeley at: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm

Excerpts from the paper and Cisco comments:

"This paper describes the flaws in the two access control mechanisms that exist in access points built using Orinoco/Lucent 802.11 Wavelan PCMCIA cards, and a simple eavesdropping attack against the 802.11 specified shared key authentication mechanism."

- Cisco agrees with the authors, that open authentication in 802.11 networks is not security at all. The authentication management frames are sent in the clear, even when WEP is enabled.



- Cisco also agrees that shared key authentication can be easily exploited through a passive attack by eavesdropping. The paper supports the virtues of mutual authentication as long as the “shared secret” is well protected and is not compromised. Cisco fully agrees with this and implemented its mutual authentication scheme EAP—Cisco Wireless (LEAP) in the Cisco Aironet security solution. Therefore, the Cisco solution is immune to eavesdropping and man-in-the-middle attacks.
- Shared key authentication uses standard challenge and response approach for authentication between the 802.11 client and the access point. Other companies, however, use the SSID, the WLAN network name, as the shared secret. The authors then write, “The end result, however, is that an attacker can easily sniff the network name—determining the shared secret and gaining access to the ‘protected’ network.”

“The use of a separate key for each user mitigates the cryptographic attacks found by others, but enforcing a reasonable key period remains a problem as the keys can only be changed manually.”

- Cisco agrees with the authors on the need for user-based encryption key. Cisco also believes it should be bound to the session and should be periodically rotated. Cisco fully agrees with this and implemented its mutual authentication scheme EAP—Cisco Wireless (LEAP) in the Cisco Aironet security solution.
- However, Cisco disagrees with the authors that the keys can only be changed manually, which is true if static WEP keys are used. With the Cisco solution, not only can we achieve per session key, but also force re-authentication via a global policy on the back-end ACS RADIUS server.

“Worse, in some cases, the details that are available indicate that the vendors ‘solution’ worsens the problem by using protocols with well-known vulnerabilities, e.g. un-authenticated Diffie-Hellman key agreement.”

The authors allude to the poor, unauthenticated Diffie-Hellman key agreement with another vendor’s implementation. Such a scheme is vulnerable to man-in-the-middle attack.

The Cisco Aironet solution is immune to man-in-the-middle attack as Cisco conducts a mutual authentication and verifies the legitimacy of the client as well as the ACS RADIUS server. The overall Cisco scheme, based on 802.1x standards, also ensures that the access point is legitimate and not a rogue device, because a secure channel for key exchange is established between the RADIUS server and the access point.

Ethernet MAC Address Access Control Lists

“First, MAC addresses are easily sniffed by an attacker since they MUST appear in the clear even when WEP is enabled, and second most all of the wireless cards permit the changing of their MAC address via software.”

- Cisco fully agrees with the authors that MAC addresses can easily be spoofed, and hence, not appropriate as a security handle.
- The Cisco Aironet solution is based on user-based authentication and not MAC address-based authentication.

Robust Key Management System for WEP
The authors acknowledge that robust key management would strengthen WEP-based security schemes and that higher-level security mechanisms such as IPSec would enhance security schemes. Customers can also use the network logon, access control lists in switches and routers, and policies on their firewalls to achieve robust end-to-end network security. Virtual private network (VPN) security can also be deployed in intranets where very high security is essential.

“Fortunately, the 802.11 standards body is currently working on significant improvements to the standard.”

- Cisco’s Dave Halasz chairs the 802.11 Task Group I on security. Cisco is committed to standards-based security solutions that address the limitations of WEP and promote interoperability between vendors. The Cisco security solution is closely aligned with the baseline security framework from the 802.11 standards bodies.



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.

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, 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 brands, names, or 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. (0101R) 08/01 BW7544