

Cisco Aironet Security Solution Provides Dynamic WEP to Address Researchers' Concerns



Background

Recently, researchers at the University of California, at Berkeley, published a document identifying "security flaws in the 802.11 security protocol (WEP)," that "seriously undermine the security claims of the system" and use WEP insufficient for wireless LAN (WLAN) security. Articles about the researchers' findings have appeared in *The Wall Street Journal* and other publications. Cisco was aware of these limitations before the company defined its Aironet® security architecture. With the recent Aironet Software Release 11.0 and ACS 2.6, Cisco offers centrally managed, dynamic per user, per session WEP that addresses several of the concerns that the researchers refer to in their paper.

Cisco agrees with Berkeley researchers who cite inherent weaknesses in WEP as defined by IEEE 802.11b, the standard for WLANs, and that these weaknesses exist regardless of the length of the encryption key used. The weakness of most WLANs is their use of static WEP keys shared among users. "In practice, most installations use a single key that is shared between all mobile stations and access points," the Berkeley report states. "More sophisticated key management techniques can be used to help defend from the

attacks we describe; however, no commercial system we are aware of has mechanisms to support such techniques."

Cisco Aironet Wireless LAN Security Solution

In fact, Cisco Aironet wireless security solution offers the more sophisticated key management techniques desired by the researchers. The recently introduced Cisco Aironet WLAN security solution combines several innovations, such as dynamic, per-user, per-session WEP and integrated network logon, that address several of the limitations of WEP, while promoting hassle-free enterprise deployment. Cisco also believes that these features, along with best practices in network design and deployment, and standards efforts on open security framework, such as IEEE 802.1x, will help drive new interoperable solutions to better meet customer needs. By employing a dynamic, not static, WEP encryption key for every user and enabling that key to change frequently, the Cisco Aironet security solution greatly diminishes the applicability of certain attacks identified by the Berkeley researchers.

Using the Cisco Aironet Security solution as a reference, the next sections:

- Discuss inherent limitations of WEP



- Identify areas where the Cisco Aironet wireless security solution augments WEP as defined by IEEE 802.11b to achieve increased levels of robustness and to minimize the vulnerabilities to certain classes of attacks to which WEP and RC4-based security schemes are susceptible
- Identify other solutions that Cisco offers its customers to achieve integrated end-to-end security
- Outline the standards initiatives that Cisco has undertaken to promote inter-operable security standards for wireless networks

Inherent limitations of WEP

We agree with the authors that WEP has its inherent limitations. In general, the extent of vulnerability depends on whether static or dynamic WEP is used. Unfortunately, many WLAN deployments use static WEP keys that significantly compromise security, as many users in a given WLAN share the same key. The Cisco Aironet wireless security solution augments 802.11b WEP by creating a per-user, per-session, dynamic WEP key tied to the network logon, thereby addressing the limitations of static WEP keys while providing a deployment that is hassle-free for administrators.

Cisco enhancements to 802.11b WEP to increase security

By employing dynamic WEP keys, the Cisco Aironet security solution enhances WEP to decrease its predictability (to the hacker), significantly minimize any attack windows, tie it to the user session and, optionally, network logon. All of these properties working together have been designed with large-scale enterprise deployments in mind without compromising overall network security. Cisco has partnered with several vendors to achieve innovations from an end-to-end standpoint and develop an open, extensible framework for the future.

The following are the key enhancements to the Cisco security solution.

- **Mutual authentication**—The Cisco Aironet Wireless security solution offers customers a mutual authentication scheme instead of one-way authentication. Standards-based mutual authentication implementations that are easily deployable are still evolving. Therefore, Cisco created EAP—Cisco Wireless (LEAP) to ensure mutual authentication between a wireless client and a back end RADIUS server (Access Control Server 2000 V2.6). Communication between the access point and the RADIUS server is via a secure channel. This eliminates “man-in-the-middle attacks” by rogue access points and RADIUS servers. Even though the paper does not address this area of concern, Cisco recommends that customers factor this class of vulnerability into their wireless security requirements.
- **Secure key derivation**—The original shared secret secure key derivation is used to construct responses to the mutual challenges. It undergoes irreversible one-way hashes that make password-replay attacks impossible. The hash values sent over the wire are useful for one-time use only at the start of the authentication process, and therefore, never after.
- **Dynamic WEP keys**—In addition, by offering a hassle-free, dynamic per-user, per-session WEP key, Cisco has made it easy for administrators to move away from static WEP keys, thus increasing the security. Cisco believes that one of the biggest security exposures in WLANs is primarily due to static WEP and the tremendous administrative burden it imposes. With the Cisco Aironet solution, session keys are unique to the users and are not shared among them. Also, with LEAP authentication, the broadcast WEP key is encrypted using the session key before being delivered to the end client. By having a session key unique to the user, and by tying it to the network logon, the solution also eliminates vulnerabilities due to stolen or lost client cards or devices.

- Reauthentication policies—Customers can also set policies for reauthentication at the back-end RADIUS server ACS2000. This will force users to reauthenticate more often and get new session keys. Because the vulnerability window can be configured to be very small, we can minimize attacks where traffic is injected during the session.
- Initialization Vector changes—The Cisco Aironet wireless security solution also changes the initialization vector (IV) on a per-packet basis so that hackers can find no predetermined sequence to exploit. This capability, coupled with the reduction in possible attack windows, greatly mitigate exposure to hacker attacks due to frequent key rotation. In particular, this makes it difficult to create table-based attacks based on the knowledge of the IVs seen on the wireless network.

Other Cisco solutions for enhanced end-to-end network security

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. Customers can enable VPN clients on their laptops or access devices from public areas and establish secure tunnels to their enterprise networks. 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. End-to-end VPN security can also be deployed in intranets where very high levels of security is essential.

Standards efforts to promote inter-operable wireless security

Cisco is working with several companies to develop an interoperable security framework for WLANs. Cisco, Microsoft, and other companies have jointly proposed a baseline security framework based on IEEE 802.1x to the IEEE 802.11b standards bodies. 802.1x for 802.11, based on standards such as Extensible Authentication Protocol (EAP) and RADIUS, provides an extensible framework that supports a variety of authentication schemes including biometrics, certificates, and one-time passwords that can evolve to the unique needs of wireless in the future. In addition, it provides a framework on which client vendors and back-end RADIUS server vendors can independently develop value-added services and applications.

Summary

In summary, Cisco Aironet WLAN solutions offer industry-leading, prestandard security solutions that are ready for large-scale enterprise deployment. The Aironet solution has significantly enhanced the WEP-based security scheme for 802.11b to increase security levels while interoperating with other vendors at the base-level (standards-based WEP) functionality. The wireless security solution integrates with other Cisco products to offer an end-to-end network security solution to meet customer needs.



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