# PACKET

CISCO SYSTEMS USERS MAGAZINE

THIRD QUARTER 2001

## Next-Generation Routing

**Break Through to the Service-Enabled Internet**

**Content Delivery**

**Storage-Area Networks**

**Wireless LANs**

**IP+Optical**

**Voice**

Cisco Systems

cisco.com/go/packet

Reprinted with permission from *Packet*™ magazine Volume 13, No. 3, copyright © 2001 by Cisco Systems, Inc. All rights reserved.

# SECURING THE Wireless LAN

Cisco plugs holes in the 802.11 standard.

BY GAIL MEREDITH

Is your wireless lan (wlan) secure?

WLANs are gaining popularity because they are easy to deploy and provide ubiquitous access to enterprise resources from anywhere in the campus. But a surprising number of enterprises don't bother to activate wireless security features. *The Wall Street Journal* (April 27, 2001) described two hackers with a laptop and a boom antenna driving around Silicon Valley listening to network after network. The best "pickups" were outside Fortune 500 enterprises that, according to the hackers, should know better.

"Enterprises must become fully aware of the security and management implications of adding wireless technologies to their network," says David Halasz, manager of software development in the Wireless Networking Business Unit at Cisco and chair of the IEEE 802.11 security task group. "You can be outside a building or be near an employee's house and still be part of the network. Robust wireless security implementations with hassle-free management are mandatory for successful integration of wireless into an enterprise framework."

But even if an enterprise does activate WLAN security based on the 802.11 standard, that doesn't mean airwaves are secure, according to a study by researchers at the University of California, Berkeley. The report exposes the vulnerabilities of the static Wired Equivalent Privacy (WEP) standard, raising questions as to why it was adopted at all, saying, "If WEP had been examined by the cryptographic community before it was enacted into an international standard, many of the flaws would have been almost surely eliminated."

In fact, the widespread perception in the networking community is that the only way to secure a WLAN is to use virtual private network (VPN) technologies at additional expense and management. The UC Berkeley report states that "no commercial system we are aware of has mechanisms to support such techniques" that effectively defend against attacks via wireless connections.

Cisco acknowledges the weaknesses of the static 802.11 WEP standard cited in the Berkeley study. Unfortunately, the Berkeley researchers were apparently unaware of the Cisco Aironet® wireless networking solution. Using security based on IEEE 802.1x draft standard for the 802.11 framework, Cisco Aironet WLAN security provides dynamic, per-user, per-session WEP that mitigates many of the concerns identified by the study and increases the overall robustness of 802.11 WEP encryption.

Security features include mutual authentication, secure key derivation, dynamic WEP keys, reauthentication policies, and Initialization Vector (IV) changes. All enterprises need do is turn them on.

## Mutual Authentication

Many currently available products use simple, one-way authentication. This approach invites man-in-the-middle attacks, where hackers can intercept transmissions using rogue devices—such as access points—and gather confidential information from the client station, copy or modify packets, and reinsert them into the network as valid packets. "In a wireless network, you cannot make any assumptions on trust boundaries," says Halasz. "You have to ensure the legitimacy of both the client and the infrastructure providing network access. Mutual authentication is the only way to go [to prevent man-in-the-middle attacks]."

For its Aironet solution, Cisco created an authentication scheme based on the Extensible Authentication Protocol (EAP) called EAP-Cisco Wireless or LEAP. Using the 802.1x draft standard for port-based security as a foundation, but with the necessary modifications for WLANs, LEAP provides mutual authentication between Cisco Aironet client cards and the backend



Reprinted with permission from *Packet*™ magazine (Volume 13, No. 3), copyright © 2001 by Cisco Systems,Inc. All rights reserved.

Remote Authentication Dial-In User Service (RADIUS) server (see figure).

### Authentication and Secure Key Derivation

First-generation 802.11 products use static WEP keys for authentication as well as encryption, making WLANs vulnerable to password-replay attacks. The Cisco Aironet solution decouples authentication from encryption. The end-point's knowledge of the shared secret is used to construct individual responses to challenges during the mutual authentication phase. The responses to the challenges are encrypted with one-way hashes of the original shared secret. The password itself is never sent out, and the challenges are random. These, together with good password selection and change policies, ensure that brute-force attacks can be mitigated, says Kittur Nagesh, product line manager in the Wireless Networking Business Unit at Cisco.

The unicast session key is derived using a Message Digest 5 (MD5) one-way hash of the hashed shared secret and the mutual challenge-response messages. This method prevents a would-be hacker from deriving the session key by intercepting the challenge responses. "You cannot decrypt a one-way hash," says Nagesh. "Just like you cannot get the egg back from scrambled egg." The binding of random challenge-responses to the key derivation ensures that the session key changes on every reauthentication after timeouts or due to roaming.

### Dynamic WEP Key

The 802.11 standard left the implementation of WEP key management schemes to the vendors. Most first-generation 802.11 products use a single, shared key for all users in a network, which presents several problems—the most obvious is risk of compromise via a stolen or lost device that contains the key.

The second problem is WEP key management. Shared keys used with static WEP must be manually entered into every access point and end-user device, which can be time-consuming, especially if a network administrator has to rekey an entire network every time an end-user laptop is missing. "That's just not feasible when you have thousands of users," says Bill Rossi, vice president and general manager of Cisco's Wireless Networking Business Unit. "We have a dynamic security scheme. Once you login and are authenticated, the encryption key is set up automatically for the duration of your session."

### Reauthentication Policies

WLANs practically invite traffic-injection attacks, where hackers exploit predictable patterns to insert their own packets onto a

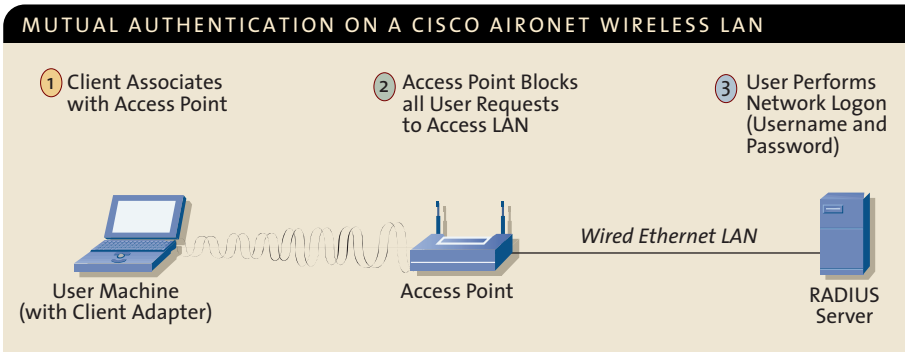
*Continued on page 77*

GIAMPIERO BENVENUTI



Reprinted with permission from *Packet*™ magazine (Volume 13, No. 3), copyright © 2001 by Cisco Systems,Inc. All rights reserved.

*Wireless LAN, Continued from page 75*




**MUTUALLY SECURE:** The client authenticates the network via a RADIUS server; likewise, the RADIUS server authenticates the client. The two sides of the authentication scheme are decoupled on separate secure channels, with the access point in the middle.

corporate LAN. While standard 802.11 WEP includes defenses against both traffic injection and statistical attacks, static WEP implements those defenses incorrectly.

A stream cipher expands a short key into an infinite, pseudo-random key stream. The sender performs an XOR to the key stream with plaintext to produce ciphertext. The receiver uses the same key to generate an identical key stream. Attackers can exploit this weakness by intercepting traffic, flipping bits, and injecting modified packets into the network. If an attacker intercepts two ciphertexts encrypted with the same key stream and initialization vector, plaintexts could then be recovered in a statistical attack.

The Cisco Aironet solution allows network administrators to establish and centrally administer reauthentication policies in mid-session, say every 30 minutes—well within the rollover duration of a 24-bit initialization vector. This flow disrupts a hacker's ability to intercept, break, and use session keys to gain entry to a network and greatly minimizes active attack windows.

## Initialization Vector Changes

The 802.11 WEP standard provides for an integrity check with an IV number in each packet header. However, the IV field is only 24 bits long, which for a single session would require reuse of IV numbers after approximately five hours. When multiple sessions communicate via a single access point, IV values can overlap, which increases the likelihood of intercepting two ciphertexts encrypted with the same key and provides the basis for table-based attacks. Attackers can build a decryption table after learning plaintext for some packets, then computing the RC4 key stream generated by the IV in use, and decode other packets in the stream. Over time, an attacker can build a table of IVs and key streams.

The Cisco Aironet 802.1x solution counteracts vulnerability by changing the IV value on a per-packet basis, so hackers can find no predetermined sequence. It also starts sessions with random IV numbers rather than the same value for each session. In conjunction with reauthentication, changing IV numbers makes it difficult for hackers to create table-based attacks.

## CRC-32 Checksum

The integrity check function of the 802.11 standard is vulnerable because it uses a linear CRC-32 checksum, making it possible to compute the differences between two CRCs by flipping bits in a message. Neither the 802.1x nor the existing 802.11 standard address this issue.

According to Nagesh, "A hacker can modify a packet and do bit flipping to make a CRC—hence the packet—appear legitimate, and simulate known protocol behavior to these modified packets. The only way to protect against this vulnerability is with a per-packet message integrity check. We're looking into this for future products, as well as following evolving standards," Nagesh adds.

## Standards Promote Interoperable Security

Cisco is working with several companies to develop an interoperable security framework for wireless LANs. Cisco, Microsoft, and other companies have jointly proposed a baseline security framework based on IEEE 802.1x to the IEEE 802.11 standards bodies. Based on standards such as EAP and RADIUS, 802.1x for 802.11 provides a scalable framework that supports a variety of authentication schemes, including biometrics, certificates, and one-time passwords.

However, to sufficiently address unique requirements of wireless in areas such as mutual authentication and replay protection among others, these authentication schemes will need to evolve from their traditional deployment in wired and dialup networks.

## No Single Security Solution Fits All

Securing the WLAN is just one component of the overall enterprise security framework. Security experts recommend that enterprises deploy several layers of defense across the network to mitigate threats. Additional security components might include firewalls, intrusion detection systems, and segmenting networks.

Cisco's implementation of 802.1x wireless security does much to mitigate the threats posed by use of the static WEP standard. The Cisco Aironet solution can protect organizations from most attacks, and Cisco and its partners are working through the standards bodies to counteract the remaining vulnerabilities. The timing is critical, because people are discovering the freedom of wireless IP connections via PC laptops and personal digital assistants (PDAs).

Predicts Rossi, "A year from now, you won't be able to buy a laptop or PDA without a wireless connection already embedded onto its motherboard. Once 802.11 networking is standard on notebooks, people will be able to go anywhere and stay connected. And that's the goal of wireless networking." ▲▲

**FURTHER READING**

**For more information, go to *Packet Online* at cisco.com/go/packet/wlan.**



Reprinted with permission from *Packet*™ magazine (Volume 13, No. 3), copyright © 2001 by Cisco Systems,Inc. All rights reserved.