

# IWS

## TECHNICAL NOTE

### Critical Functions for a Secure Network

#### Authentication

- ▶ Certificates and shared secrets securely identify the wireless devices and network nodes.
- ▶ Mutual Authentication—of both the wireless device and network node—prevents access to the network until parties are properly identified and authenticated.
- ▶ Access/One Network IWS uses common enterprise servers (such as Microsoft IAS, Funk Odyssey, Cisco ACS).

#### Authorization

- ▶ Enterprise systems already in use can authorize user access to information on the wired network.
- ▶ Access/One Network IWS uses virtual LANs to limit LAN access to authenticated wireless users, and to limit access to its management and control function.

#### Encryption

- ▶ Static encryption keys hide initial exchanges to protect identities.
- ▶ Dynamic keys take over to protect authenticated users.

#### Other Features

- ▶ Access/One Network IWS encrypts all of its network management and control information, keeping it out of unauthorized hands.
- ▶ Access/One Network IWS detects rogue access points.
- ▶ User security is maintained as individual users roam the network.

[www.strixsystems.com](http://www.strixsystems.com)

## WIRELESS LAN SECURITY

### Don't just close the door on attackers—lock it and bolt it down

#### Securing the Wireless LAN

Wireless LANs are designed to be easy to find—they announce themselves so that mobile devices can link to the network. Unfortunately, the information needed to link them can be used to gain unauthorized access to messages or to the network as a whole.

While security experts talk to specific attacks—traffic analysis, passive and active eavesdropping, man-in-the-middle, poisoned caches, session hijacking, and replay—the solution lies in protecting the information used to launch these attacks.

The payoff is assured confidentiality, elimination of unauthorized access to corporate secrets, and protection against liability lawsuits for unlawful network use by outsiders.

The Wi-Fi Alliance has a set of protocols (WPA and WPA2), in addition to the IEEE 802.11i specification. Any new WLAN system must employ the latest security tools (not patches to the old tools) to ensure their network security.

#### The Access One Network IWS Security Solution

Securing a network involves AUTHENTICATING potential users, AUTHORIZING access to only specific information, and ENCRYPTING data to prevent eavesdropping.

With Access/One® Network IWS (Indoor Wireless System), wireless devices send their certificates to the server via authenticated network nodes, which enable full access between the device and the wireless network **only** when authentication is completed. Dynamic keys then keep the session private by protecting the data, as well as source and destination addresses, the packet size, and number of packets—all of which can be used to mount a damaging attack. By using the strongest available authentication and encryption standards, Strix Systems assures compatibility with a wide range of client devices and commonly deployed security servers. But Strix doesn't stop here.

Access/One Network IWS encrypts all of its network management and control data. VLANs assure that only fully authenticated users have access to the wired LAN and that management functions are restricted to approved users. In addition, rogue access points are detected, preventing even benign users from unauthorized access. Finally, user security is maintained as individual users roam the network.

Strix Systems, Inc.  
26610 Agoura Road,  
Calabasas, CA 91302  
USA

1-877-STRIXSYS (787-4979) Toll Free



# Security Terms & Acronyms

## AES

### *Advanced Encryption Standard*

Chosen by IEEE 802.11i security task group and endorsed for secure government use; there is no known technique to break this code.

## EAP

### *Extensible Authentication Protocol*

A point-to-point protocol extension used by 802.1x; enhanced by TLS (Transport Layer Security), which provides mutual authentication and dynamic keying. Combined with AES, EAP-TLS is the holy grail of wireless LAN security.

## LEAP

### *Lightweight EAP*

Known as "EAP Cisco Wireless," but if you use EAP, why stop at lightweight?

## MAC

### *Media Access Control*

A MAC address is a unique identifier for a piece of hardware, such as a wireless device.

## SSID

### *Service Set Identifier*

Used by access points to announce themselves to wireless devices.

## WEP

### *Wired Equivalent Privacy*

Defined in the 802.11 spec as an optional security mechanism; proven to be flawed in a now-famous UC Berkeley paper.

## WPA

### *Wi-Fi Protected Access*

An interim fix until IEEE 802.11i standards are approved. Includes Temporal Key Integrity Protocol (TKIP) to replace static WEP keys and a Message Integrity Checksum (MIC) to protect TKIP keys.

## Close the Door

Fewer than half the installed WLANs have security properly configured and running. So the first step is to close the door. Here are some common steps used to secure legacy wireless LANs:

- ▶ **CLOSED SSID SETS AND ACCESS CONTROL LISTS:** Turning off ID broadcasts or maintaining authorized device control lists does little to secure the network. WLANs always send identifiers (SSIDs) and device (MAC) addresses in the clear, along with 802.11 management and control frames.
- ▶ **ENABLE WIRED EQUIVALENCE PROTOCOL (WEP):** The WEP security protocol has a limited number of possible keys, and is relatively insecure.
- ▶ **INSTALL WI-FI PROTECTED ACCESS (WPA):** This Wi-Fi Alliance solution rotates keys and uses a message integrity check (MIC) to plug breaches in the WEP protocol. The MIC requires significant processing and may adversely affect the network's performance.

Strix does all this too, but we recommend installing locks on the door.

## Lock the Door

Access/One Network IWS limits access to the wireless network via the IEEE 802.1x standard. Certificates can be assigned to wireless devices by any Enterprise certification server and linked to the network's directory. A Microsoft network uses Certificate Server and Active Directory. Shared secrets are established in the security server, such as Microsoft IAS, and assigned to network nodes.

The Extensible Authentication Protocol (EAP) with Transport Layer Security (TLS) is used because it is secure and widely available. With mutual authentication, both the network node and the wireless device must be authenticated using their secrets and certificates, respectively. The network node blocks all traffic except authentication messages until the server signals a success, after which the device is allowed to access the wireless LAN.

## Bolt the Door

Access/One Network IWS always encrypts—all the time—using the AES standard. Static AES protects the authentication message exchange, so only MAC address information is in the clear, not certificates or dynamic encryption seeds. Once a user is authenticated, dynamic AES takes over, with keys changing rapidly enough to defeat code breakers.

All Access/One Network IWS wireless links are secured with AES, including device connections and all wireless network connections between network nodes. A separate encrypted tunnel is used to protect management and control information.

Access/One Network IWS effectively hides and protects all security message transactions and all address data that could be used to mount an attack on the network.