

### Critical Functions Needed in Secure Networks

#### Authentication

- Certificates and shared secrets securely identify the wireless devices and Network Nodes
- Mutual Authentication - of both the wireless device & Network Node - prevents access to the network before the parties are properly identified and authenticated
- Access/One Network 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 uses Virtual LANs to limit LAN access to authenticated wireless users, and to limit access to its management and control functions

#### Encryption

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

#### Other Features

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

### Wireless LAN Security Issues

Wireless LANs are meant to be easy to find; they announce themselves so that mobile devices can link to the network. Unfortunately, the information needed to link is also the information needed to gain unauthorized access to messages or to the network.

While security experts talk to specific attacks - traffic analysis, passive & active eavesdropping, man-in-the-middle, poisoned caches, session high-jacking, and replay - the real issue is protecting the information needed 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.

Legacy WLAN security systems have been compromised by attackers with moderate knowledge and commercially available tools. The Wi-Fi Alliance has a set of protocols (WPA and WPA2) in addition to the IEEE 802.11i specification. Any new WLAN system should employ the latest security tools - not patches to the old ones - to secure the network.

---

#### Access/One Network's Security Solution

Securing a network means *authenticating* potential users, *authorizing* them to access only specific files or information, and *encrypting* the information to prevent outsiders from eavesdropping on the airwaves and collecting the information needed to mount an attack.

Access/One Network users shared secrets to authenticate the enterprise security server with Network Nodes. Wireless devices send their certificates to the server via authenticated Network Nodes. Only authentication messages are permitted at first. Once the device is successfully authenticated, the Network Node enables full access between the device and the wireless network.

Once the device is authenticated, dynamic keys are used to keep the session private - protecting the data transmitted, as well as source & destination addresses, packet size, and number of packets - all information needed 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 Access/One offers more...

Access/One Network encrypts all of its network management and control data, making it impossible for attackers to intercept this information and hijack the network. VLANs assure that only fully authenticated users can gain access to the wired LAN, and that only certain people may access the management functions. And, Access/One Network detects rogue access points, preventing even benign users from unauthorized access via personal - and unsecured - access points. Finally, once a user is authenticated, the user security is maintained while the other user roams about the network.

See how you can not only close the door on attackers, but lock it and bolt it down.

## Close the Door

Fewer than half the installed WLANs even 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 & Access Control Lists

Turning off ID broadcasts or maintaining authorized device control lists does little to secure the network. WLANs always send identifiers (SSID) and device (MAC) addresses in the clear, along with 802.11 management and control frames.

### Enable Wired Equivalency 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 performance.

Access/One Network can do all these things, too, but we recommend installing locks on the door.

## Lock the Door

Access/One Network limits access to the wireless network via the IEEE 802.1x standard.

Certificates may be assigned to wireless devices by any enterprise certification server and linked to the network's directory. In the case of a Microsoft network, Certificate Server and Active Directory are used. Shared secrets are established in the security server, such as Microsoft IAS, and assigned to Network Nodes.

The Extensible Authentication Protocol with Transport Layer Security is used, as it is both 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 - and then the device is allowed to access the wireless LAN.

## Bolt the Door

Access/One Network encrypts all the time, using the AES standard.

Static AES protects the authentication message exchange, not only MAC address information is in the clear - not the 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 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 effectively hides and protects all security message transactions and all address data that might be used to mount an attack on the network.

## Quick Guide to 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, but officially called "EAP Cisco Wireless;" if you use EAP, why stop at "lightweight"?
- MAC** Medium Access Control, as in "MAC Address," 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.

## About Strix Systems

Strix Systems makes Networks Without Wires.™ Strix Systems' flagship product, the Access/One™ Network, increases mobile worker productivity by providing continuous and secure connection to company networks.

Our mission is to create a wireless local area network, drawing on the parallels of the successful wired network and providing all of the expected management and security that network managers expect.

Our vision includes multiple radio frequency technologies, built into a simple, secure, scalable, and self-tuning system, with the ability to easily add new applications and services.

Strix Systems  
26610 Agoura Road, Suite 110  
Calabasas, CA 91302

Phone: 818.251.1000  
Fax: 818.251.1099  
Email: [sales@strixsystems.com](mailto:sales@strixsystems.com)  
Web: [www.strixsystems.com](http://www.strixsystems.com)