



WIRELESS SECURITY

Technology and Talent, What a Combination

Wireless Local Area Networks (WLAN) are transforming enterprise networks with high speed connections across the airwaves that cost effectively extend the boundaries of the conventional wired network and enhance productivity.

WLAN – Risk vs. Reward

The airborne nature of the 802.11 WLAN opens it to intruders and attacks that can come from any direction. Often times an intruder's physical presence within the confines of your facility is not necessary, when the parking lot next door will do. WLANs are vulnerable to intruders and hackers who:

- Listen to the airwaves and eavesdrop on unencrypted messages or crack the encryption
- Steal an authorized user's identity and gain access to the entire network
- Launch Denial of Service (DoS) attacks that cripple the WLAN by jamming or flooding the airwaves

The landscape of today's wireless environment is confusing and complicated. The alphabet soup of IEEE Standards and Authentication methods make security decisions and strategies difficult to achieve. Only in best case, homogeneous situations, can manufacturer's security offerings work to meet the concerns and demands of today's business environment.

Candidates For Immediate Impact:

Education

Elementary Schools
Secondary Schools
College and Universities

Healthcare

Hospitals
Clinics
Medical Schools

Enterprise

Research Laboratories
Manufacturing Facilities
Law Firms

Government

Military
State Government
Public Safety

What does Wireless Security look like?

Companies are deploying firewalls and VPN gateways to secure the WLAN traffic once it reaches the wired network. While this is a good start, the real danger lies in the airwaves. Encryption and authentication of WLAN traffic is essential, but WLANs also require monitoring and defenses to identify and respond to new threats unique to WLANs.

Integrated Systems' primary goal is to deliver turnkey wireless solutions based on secure, reliable, and best in class hardware and services available. Utilizing our fundamental knowledge of wireless technology, Integrated delivers a security solution that protects your wireless network by monitoring and analyzing WLAN traffic to discover network vulnerabilities, protect against intruders and attacks, enforce network policies, and manage the network to maximize performance.

Integrated Systems embraces a philosophy based on supporting the individual needs of various 802.11 networks with WLAN security solution that can begin by serving small WLAN deployments and scale to support enterprise WLAN's with hundreds of access points and thousands of clients.

Let's Get Specific...

Our evaluation and process of a reliable security solution begins and ends with the customer's best interests in mind. The criterion that we insure is the following:

- Authentication Methods
- Wireless Encryption
- Multiple Gateways
- Policy Management
- Wireless Network Management
- Ease of Use
- Scalability
- Public Access
- IP Address Assignment

Where Does One Start?

To fully realize the benefits of the investment in a wireless infrastructure, they must be secure, flexible and easy to manage. At Integrated Systems we strive to provide Wireless Security Solutions that are agnostic to standards, work in your existing environment and ensure compatibility with the technologies of the future.

Our process begins with a Security Audit and Performance Assessment by Certified Specialist. This is a procedure that evaluates your current or planned wireless architecture for optimum performance, shapes signals to cover only the areas intended and flush out unauthorized users or Rogue Access Points. A comprehensive deliverable is then created to provide the customer with complete plan of action to address the found concerns.

Hardware alone does not simply solve security problems, careful attention to proper installation, integration and management are all integral parts of a successful ongoing security strategy. ISI's commitment to the customer is to advise in the selection of the "Best in Class" hardware, install this equipment as a component of a comprehensive strategy, and create the cultural understanding of ongoing practices.