SystemEXPERTS
LEADERSHIP IN SECURITY

A Perspective On Practical Security 2002

Wireless 802.11 LAN Security: Understanding the Key Issues

SystemExperts Corporation

Brad C. Johnson

Introduction

The rapid deployment of wireless LANs is testimony to the inherent benefits of this technology. Unfortunately, most wireless deployments are, at this time, fundamentally insecure. This is not an exaggeration. Based on our work with a wide range of organizations, it is an accurate assessment of the reality of the current state of the security of wireless 802.11-based environments.

This situation is caused by two overarching problems. First, the technology itself is new and immature. Second, the technology is deceptively simple. Deploying a wireless environment is fundamentally easy. Deploying a wireless environment that meets the requirements of your existing security policies, while minimizing business risk, is not. It can be done, but requires substantial planning and a commitment to address a number of significant architectural, implementation, and operational issues.

Wireless LAN deployment has clearly not yet reached its potential. But, the pundits are wrong on one essential point. They look at the deficiencies of the technology and think that organizations *shouldn't* be deploying it yet. The pundits miss the plain fact that organizations *are* deploying it anyway. Further, wireless LANs are a *stealth technology*. Most IT departments in large organizations are significantly underestimating how much wireless has already been installed by enterprising departments as well as individuals.

While there is no substitute for practical experience with a new technology, this brief white paper is intended to help you understand the breadth of issues that need to be dealt with and to offer advice on how to avoid some of the most common mistakes. Let's take a look at some of the security issues.

The Current State of WLAN Security

The current state of insecurity is caused by a combination of factors:

- The default configurations of the wireless "servers" (Access Points) are insecure. They are set to be "open" to make them easy to deploy and use out of the box.
- The physical transport is invisible and therefore it is difficult to understand and control its boundaries.
- There are interoperability issues among Access Points. That is, because the security and configuration features vary by vendor, if you have more than one type of Access Point (even if it's different types of Access Points from the same vendor) you're going to have to understand (in detail) what the compatibility issues are among them.

- Many wireless setups are installed by end-users and not by IT or security professionals.
- The standard data encryption protocol (WEP) that is used on almost every Access Point in the market has been proven to be insecure.

Deploying a wireless network does not require special expertise. If a department is eager to expand its network and it can't or doesn't want to wait for the normal IT process, it can expand the network itself cheaply (about $200 or less for an Access Point and $100-200 per client) and easily. Plug an Access Point into your Ethernet jack, plug a wireless card into your laptop, and in most cases, you're done.

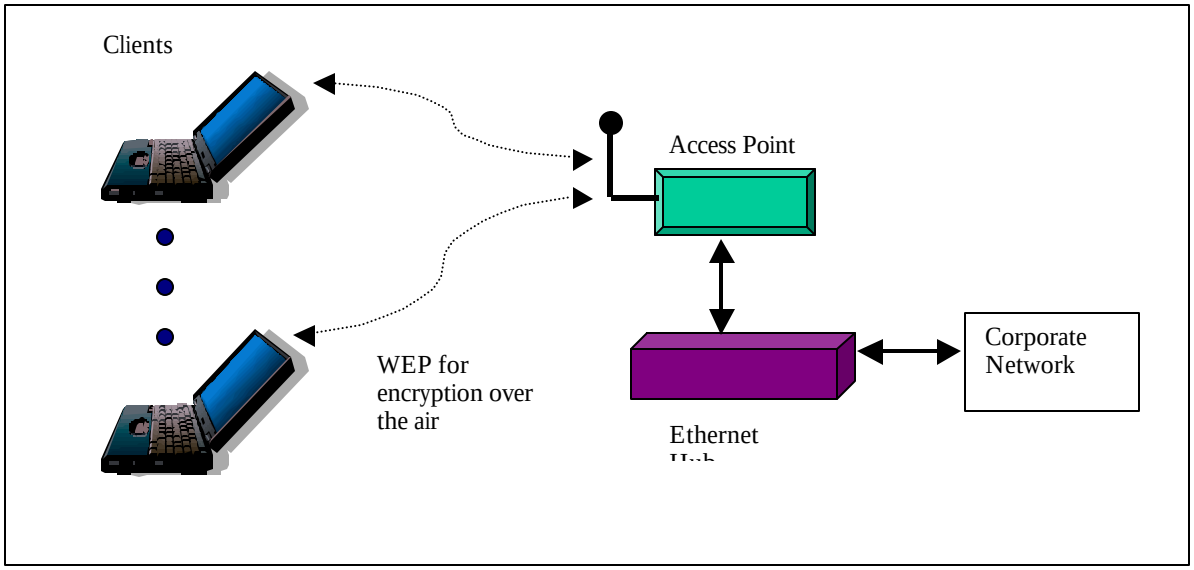

Figure 1: Basic Wireless LAN Environment

Figure 1 shows the basic components of a wireless LAN. Clients with wireless network cards communicate over the air to an Access Point. The Access Point is connected to a wired environment, typically an Ethernet network. When it receives packets of data from the client (as long as MAC filtering hasn't been set to block the transfer) it will place the packets on the wired network. If WEP was used to encrypt the data while the packets were transmitted in the air, the Access Point will decrypt them before putting the data on the wire.

There are several variations on this design:

- Roaming: where a client will eventually communicate with two or more Access Points while in motion.
- Extension Points: where there are multiple Access Points in between the client and the one connected to the wired environment (used to increase the distance from the client to the wired network).
- Peer-to-peer or Ad-Hoc: where clients talk directly with each other without the use of an Access Point – this is also called the Independent Basic Service Set (IBSS).

The Wireless Network Boundary is Dynamic

Let's look a little deeper into the problem of managing the boundaries of the wireless environment. Compared to the wired environment where you can literally follow the path from one component to the next, the wireless boundaries are amorphous and constantly changing. They expand and contract for all sorts of reasons. Some of these reasons are:

- Barriers (e.g., walls, people, and weather) can reduce the distance that an Access Point and a client can be from each other.
- Antennas can increase the distance.
- Interference from other wireless devices or radio signals can reduce the distance.
- Antenna adjustments (e.g., turning it around or making it horizontal instead of vertical) and alternative antenna types (directional vs. omni-directional) can change the shape and size of the coverage area.

These and other factors can make it very difficult to answer the simple question, "Where does our network go?" One of the most important issues in deploying a secure wireless environment is ensuring that the coverage area of your Access Point is appropriate. Let's take a look at Figure 2 to see an example of this. Here you can see that on the left, the antenna being used, as desired, radiates the signal throughout only the first floor of the building. In the other building, it has been placed too close to one of the exterior walls and sends the signal too far in several directions – including outside of the building.

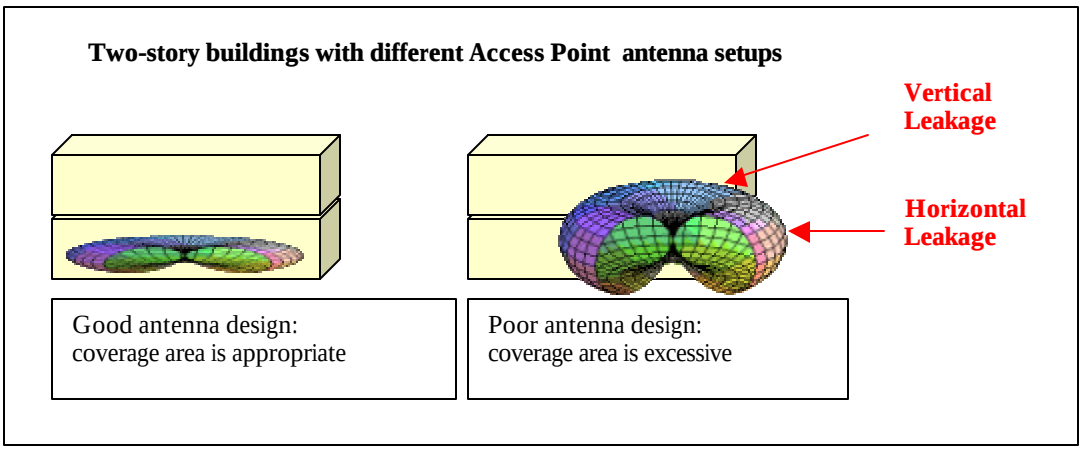

Figure 2: Antenna Design Considerations

Existing Problems with the WLAN Components

A wireless environment is like any other portion of your network. It is comprised of a number of different components. Some of the major components include the protocols that the wireless devices use, the way in which wireless cards and Access Points are configured, the management interfaces and mechanisms that control how the devices work, as well as some of the physical properties of the antennas that are used to send and receive the signals.

Let's take a look at some of these components and the corresponding problems in products that are currently available.

- Authentication: The default authentication mode for most Access Points is *open* which allows any client to connect (associate) with it.
- Authorization: The authorization control on most Access Points is MAC (Medium Access Control) level address filtering (i.e., these filters allow or disallow the forwarding of packets). Unfortunately, you can change the MAC address of most clients to be anything you want it to be.
- Access Point Management: Most Access Points use well-known SNMP community strings (passwords) for management and those that provide an HTTP interface are accessible by anybody who happens to know the IP address of the device.
- Access Point Configuration: All major Access Point products are set up to be in their most insecure configuration out of the box.
- The IEEE Protocol: The wireless network traffic is largely controlled through management and control packets. Management packets are sent in the clear, even if WEP (encryption) is enabled.
- Encryption: The standard WEP protocol has been proven to be insecure in several fundamental ways. It requires only a modicum of CPU capability and network traffic to determine the supposedly "secret" WEP encryption keys.
- Client WEP Key Storage: Leading vendors either store the WEP keys directly on the client wireless card (so stealing it gives you the capabilities associated with the card) or on the local disk in a way that is obvious and easy for anybody to copy and use.
- Wireless Networking Boundaries: Most Access Points and client wireless cards come with omni-directional antennas that are hard to control and often quite complex to determine their actual range and capabilities.

Given these limitations, the only practical approach for any organization to take is to assume that end-to-end security should be provided outside the bounds of the wireless infrastructure. You should not count on the wireless environment for any protection of sensitive business data.

A number of industry-wide efforts are underway to address these fundamental problems. These include the IEEE Security Subgroup (Enhanced Security Network and a replacement for WEP) and the IETF's Extensible Authentication Protocol (EAP). In addition, vendors are tackling these problems as well. One good example of a vendor initiative is Cisco's Lightweight EAP extension. As these initiatives produce results, the measures available to secure wireless environments will become more effective.

With so many documented issues and concerns, one has to wonder, "Are people taking wireless security seriously enough?" The overall problem is that most businesses don't have the discipline, controls, or policies in place to handle the dynamic nature of the wireless components. Most security guidelines are geared towards the more slowly changing wired environment that, in many cases, forces the end-user to get help or permission to change his computing environment.

Some Real Examples

Often, concrete examples of problems catalyze necessary changes. One of the most enlightening exercises you can do in the wireless environment is to survey your network. You should be able to answer straightforward questions like: Do we know how far our network goes? Can unauthorized users use our wireless network? Is our confidential information accessible to anyone outside of our premises?

Here are a few short examples that illustrate that in many cases, the network goes further than you would like, and that all too often, unauthorized users can use your network and access your confidential information.

- I was asked to come to New York to film a cable TV program on wireless issues. I took a taxicab ride from Grand Central Station to Wall Street. During the ten-minute ride, I decided to "sniff" for wireless traffic. I collected over 50,000 wireless packets and noted over 100 separate Access Points.
- Another company in New York was concerned that employees were using the internal network from a local coffee shop in a nearby, but separate, building. While sitting in the coffee shop, I not only could see several Access Points for this company, I could see Access Points for a number of other companies as well.
- Another company in the Boston area was worried that sensitive data was traversing the airwaves in the clear (it was assumed to be unintentional but nonetheless a serious concern). They should have been worried about just a little more than that. I pulled into the parking lot and was surprised to see (without getting out of my car) that I could not only reach their Access Point, I could both associate and authenticate to it (they were broadcasting their SSID and not using WEP). I was able to get a valid IP address and DNS server through their DHCP server, sniff the unencrypted traffic to notice a local file share that was being offered, and mount that file share (which just happened to be the company white pages with personal information on every employee).

Ok, enough bad news. What can we do about all these problems? The next few sections provide advice and recommendations to make your wireless deployments more secure.

Practical Recommendations to Make Things Better

The issues of securely deploying a wireless LAN are not fundamentally different than deploying any LAN. You will need to deal with authentication of users (proving who users are), granting and managing authorization privileges (controlling what users can do), auditing actions, determining and managing how addresses are issued, watching for anomalous behavior, designing the network with reasonable segmentation (to restrict access to sensitive portions of the net), ensuring that confidential information is properly encrypted in transit, and configuring systems to offer only the minimum set of services. Most organizations are not yet effectively dealing with these issues.

There are proven tactics companies can take to improve the situation. These include:

- Baseline Assessment: Most organizations don't know how much wireless technology they already have deployed and they don't know how it is configured. Use a third party to conduct a survey to find and characterize each Access Point. Only an accurate survey will enable you to understand your wireless security exposures.
- Wireless Policies: Update your security policies to specifically address wireless. Your goal should be to make the wireless policies as consistent as possible with their wired counterparts.
- Best Practices: Properly securing a wireless environment is not easy but it isn't a mystery either. Prepare a brief (2 to 4 pages) document describing required configuration changes that must be made before an Access Point can be attached to the Corporate Network.

Despite the known security risks, wireless environments are being deployed in large numbers. Given this reality, there are a number of practical measures that organizations should take to make the environment as secure as possible.

Immediate Actions For (almost) Everybody

- Use WEP to encrypt the data while it is in transit. Even though there are significant problems with the current version of WEP (and, in fact, there are publicly available programs that can determine the WEP key), using WEP will help thwart casual snoopers from seeing your data in the clear.
- Change the default SNMP community strings (passwords). The common management protocol used to manage *all* Access Points is SNMP. SNMP stores its management information in a special database called a MIB. Access to the MIB is controlled with a password (officially called a community string). Every manufacturer configures its products with a default community string. Because these defaults are public (well known), if you don't change your community string, then anyone who is within reach of your Access Point can connect to it and change its configuration.
- Change the default Access Point Service Set ID (SSID, a.k.a. Network Name). To start a connection (i.e., to both authenticate and then associate) with an Access Point, the client needs to know its SSID. It can know the SSID in one of five ways: 1) you have been told what it is by your administrator and you "type it in" 2) the Access Point is broadcasting it out and your client wireless card "hears" it and uses it 3) the Access Point has been set to a NULL SSID and will accept connections from anybody, 4) the Access Point hasn't been changed since it was taken out of the box and it still has the default, or 5) the client sends out a "probe-response" packet asking for it, and the Access Point responds with the answer (more on this issue in the next section). Unless you are trying to encourage anonymous or unknown users from using your Access Point, you should change the default SSID.
- Disable the broadcast SSID feature on your Access Point. As mentioned above, one of the ways that clients can figure out the SSID is for the Access Point to broadcast it for all to see. These are actually called *beacon packets*. They include other information in addition to the SSID. Unless you need this feature (e.g., to facilitate roaming) you should disable it.
- Change the default password for administrative access to your Access Point. Another important configuration parameter is the password for the administrator account. All manufacturers have defaults (which again are essentially public information) for this account. It should be changed (and should have strong password quality characteristics) as soon as possible to prevent unauthorized users from connecting to your Access Point and making unauthorized configuration changes.

Configuration and Management Actions to Consider

- Consider the use of MAC level (Ethernet) address filtering to limit which clients your Access Point will "pay attention" to. Every piece of network interface hardware has a unique 12 character address assigned to it. This is called the MAC address. Most manufacturers offer the ability to restrict traffic via this address.
- While using MAC filtering is a good practice to consider, let's remember a couple of important facts about this type of filtering. Firstly, the MAC address that is broadcast by a client can be changed to be different than the actual MAC address that was assigned to the network interface card. Secondly, this does not restrict the client's ability to send 802.11 traffic over the air. It is used by the Access Point to determine whether or not to allow traffic from that address to pass onto the wired (Ethernet) network.
- Consider placing the Access Point in your DMZ (as opposed to being attached directly to your internal networks) and in front of a firewall. Having a firewall between your internal network and the Access Point is always a good practice because it gives you management flexibility and control. If you must connect your Access Point directly to your internal LAN, then recognize that you will need to consider and act on most, if not all, of the recommendations listed in this paper.
- Consider configuring the Access Point so that it won't respond to "probe-response" requests. This means that clients will have to explicitly "know" your Access Point connection information a priori. As described earlier, one way for the client to figure out the SSID is to send out a request (called "probe-response") asking for it. If the Access Point has not been configured to disable responding to these requests, it will send out a packet giving, among other information, the SSID. The publicly available "war driving" tools use this technique; they constantly send out "probe-response" packets on all channels and record all Access Points (and other configuration information that is sent out) that respond.
- Consider whether or not your Access Point should offer DHCP for new clients. While most Access Point manufacturers provide the capability for the device to offer dynamic IP addresses via the DHCP protocol, enabling

this feature means that *any client*, including ones that you don't want, will also be offered the same capability to connect to your network infrastructure.

Antenna Specific Actions

- Survey your site to understand how far your Access Points are actually broadcasting their signals. If you are in a multi-floor building, remember to map the vertical coverage too.
- To restrict the signal, you may need to change the placement of the Access Points or to consider the use of more specialized (directional) antennas.
- To restrict the strength of the signal, if the manufacturer of your Access Point allows it, you may want to reduce the power of your antenna. This will reduce the overall coverage area (e.g., to keep it within your physical boundaries and not radiate past your walls).

Development and Integration Actions to Consider

- If sensitive data is going to be transmitted to or from the clients, you need to look into some type of end-to-end security solution to protect it (e.g., some type of Virtual Private Network (VPN) technology or other third-party authentication, authorization, and encryption mechanisms).
- The wireless environment is going to *require* integration of Intrusion Detection mechanisms. Given the ease of deploying wireless network extensions and the current state of wireless insecurity, it is vital that you monitor for unauthorized or inappropriate traffic.

Is it safe to use public 802.11 environments?

Having already covered many issues that you'll be faced with, let's take a look at what may be the most common wireless situation, public environments. More people are going to be exposed to a wireless environment out in the "public" then they are in their work environment. That is, at an airport, in a cafe, on some campus, in a networked neighborhood, in a hotel, at a conference, or some other public location. Most users have no idea how risky it is to use this type of public 802.11 wireless environment. The problem is that they either don't understand the subtle exposures that they may be creating for themselves or they don't appreciate how truly open the wireless environment really is. It is not an accident that these types of environments are potentially risky. For organizations that create public wireless networks, their main objective is to provide a convenient, hassle-free connection point to the Internet. The more standard, open, and generic the setup is, the easier it will be for consumers to use it. Here are a few specific examples.

In most public wireless networks, you will be required to set your SSID to null (i.e., blank or no value) such that the public Access Point can "connect" (associate) with you and vice versa. Using a blank client SSID means that you are willing to associate with any Access Point that is offering an open network. Most people achieve this by first booting up their laptop, then using their client software to change the SSID to be blank, and then trying to associate with the public Access Point. Unfortunately, your client remembers what your last SSID was. In many cases, this is the SSID from your corporate network. When your laptop is turned on, it will try to find an Access Point as soon as possible. In fact, as soon as it has power, it will start sending out requests to try to (re)connect. Anyone sniffing the wireless traffic will have seen your corporate SSID (in between the time you booted it up and you changed it) and can potentially take advantage of that by using that SSID when they are close to *your* company's Access Points.

Another vulnerability that many people don't appreciate is that the wireless card in their laptop is capable of receiving and sending data on any of the wireless channels and that it is capable of seeing the same data that the Access Point is seeing. In other words, just like in the Ethernet world, all packets are broadcast for everybody to see. There are a number of programs that are available for free that allow anyone to set up his client to capture and view this traffic. In addition, there is no way to tell if someone else is sniffing your data. So, while most people intuitively understand that a public wireless network is not a secure environment, they don't understand how easy it is to accidentally or unknowingly expose private information to others within this environment.

Conclusion

Today, most organizations deploying wireless LANs simply haven't put enough effort into its security – it isn't right, but it is true. Just like in the wired world, organizations only began to take Internet security seriously after there had been a series of highly visible and financially damaging hacker attacks. Only a similar series of public wireless disasters will catalyze the change needed for organizations to take wireless security more seriously.

While there are a number of inherent security problems with the 802.11 technology, there are also many straightforward measures that can be taken to mitigate them. As with many new technologies, the best way to get started is to recognize the problems and make a commitment to address the ones that can reasonably be solved in your environment.

Figure 3 contains a consolidated list of the recommendations found throughout this paper. You need to decide which recommendations are appropriate for your environment.

Context	Recommendations
Immediate Changes	Use WEP to encrypt the data Change the default SNMP community strings Change the default AP Service Set ID (SSID) Disable the broadcast SSID feature Change the default password for the administrative account
Configuration Changes	Use MAC level filtering Put the AP in your DMZ Don't allow the AP to answer "probe-response" requests Disable DHCP
Antenna Actions	Survey your site Change the placement of your AP to control coverage areas Use directional antennas Reduce the signal strength
Development Actions	Use external end-to-end security mechanisms Integrate Intrusion Detection

Figure 3: Consolidated Wireless 802.11 LAN Recommendations

SystemEXPERTS
LEADERSHIP IN SECURITY

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Networld-Interop, CSI, and InternetWorld are among the most popular and highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients.

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

Security Blanket & Emergency Response

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked and web sites or critical business resources are compromised, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment.

Intrusion Detection and Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

Security Policy & Best Practices

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice.

Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

Boston Los Angeles New York San Francisco Tampa Washington DC Sacramento

www.SystemExperts.com **info@SystemExperts.com**