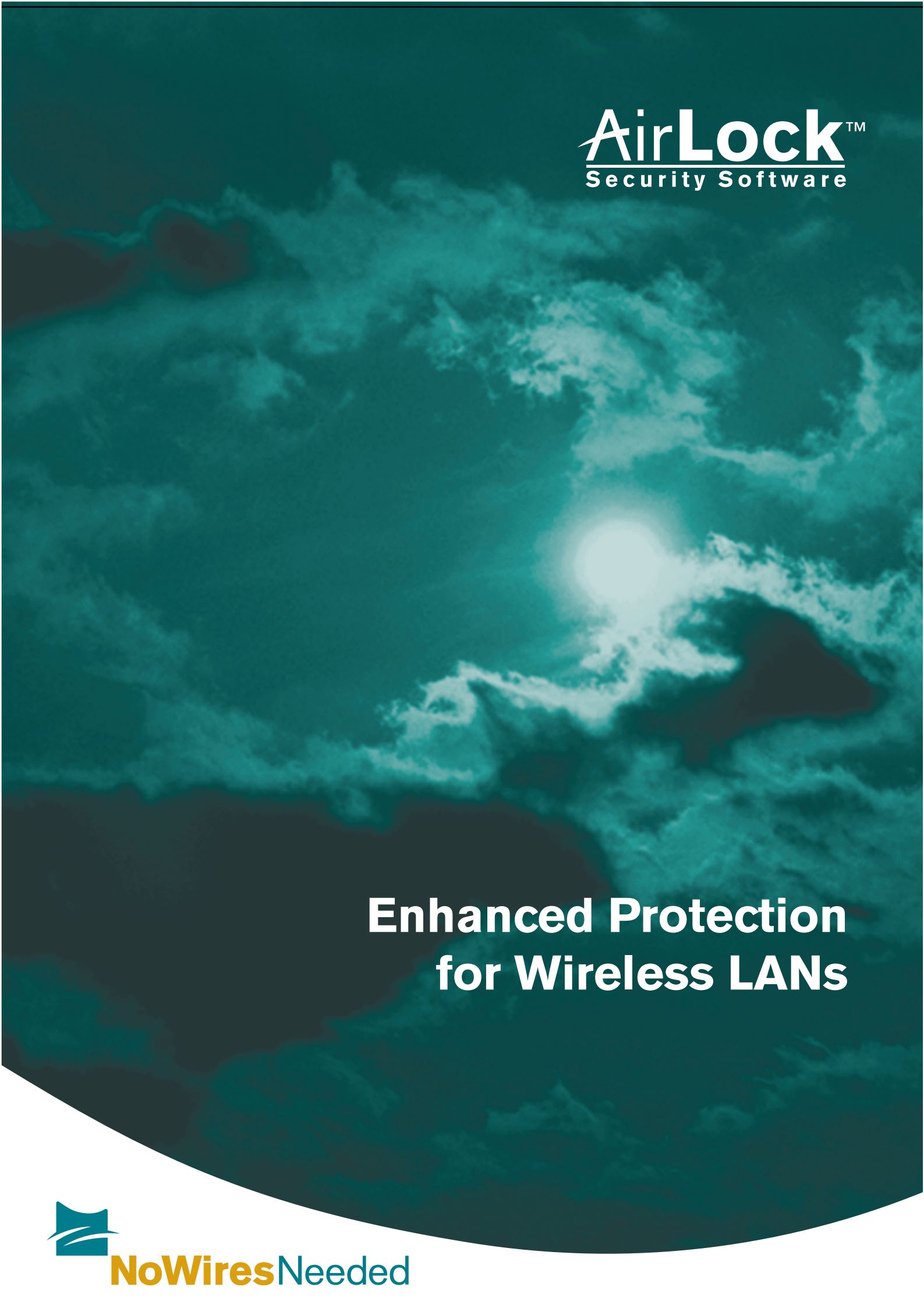

AirLock™
Security Software
Enhanced Protection
for Wireless LANs
NoWiresNeeded

AirLock™ Security Software

Enhanced Protection for Wireless LANs

Wireless LANs are rapidly emerging as a compelling means to improve business productivity. Mobile workers in conference rooms can have access to the same information they have at their desk. Small business owners can take their network with them as they expand in a new location. The recent adoption and interoperable implementation of the IEEE 802.11 high-rate wireless standard means that these users can now expect levels of performance and availability comparable to those of traditional wired Ethernet -- without wires.

The many benefits of sending information through the air comes at a potential cost of data security. This paper describes the security issues surrounding wireless LANs. It includes an explanation of the IEEE 802.11 standards-based security approach and describes how AirLock™ Security Software builds on this standard to provide a solution that is even more secure and easier to use.

The many benefits of sending information through the air comes at a potential cost of data security. This paper describes the security issues surrounding wireless LANs. It includes an explanation of the IEEE 802.11 standards-based security approach and describes how AirLock™ Security Software builds on this standard to provide a solution that is even more secure and easier to use.

WLAN Security Challenges

A wireless LAN (WLAN) communicates through the air, making it vulnerable to eavesdroppers, masqueraders, and disrupters. Whereas the wires of a traditional business network, typically enclosed in a building with access limited to employees and escorted visitors, minimize the threat that physical access to the network may be gained by unauthorized persons, a WLAN has no such physical mechanism to prevent access to the network. WLAN signals penetrate walls and extend for some distance beyond the secured facility of the corporation. This means that a carefully placed antenna could be a significant distance away and still listen to the information on the WLAN, or a neighbor with an 802.11 adapter could intentionally or unintentionally do the same. Also, a malicious intruder might connect to the WLAN and access sensitive information on networked computers. Finally, an intruder may try to disrupt the WLAN simply by using the WLAN excessively. To address these problems, the 802.11 specification provides two security tools; privacy and authentication.

Figure 1, Threats to Wireless LAN Security

WLAN Security Background

There are many different tools used to provide "security" in a network. A network manager may create a list of users that may use the network. Users may need to enter a username/password pair to be allowed access to certain resources on the network. These tools work at the level of user authentication, to allow or to prevent access by users. Certain applications and protocols, such as Lotus Notes and IPSec, encrypt the information they exchange to protect it from prying eyes. The 802.11 standard uses similar tools to authorize, "authenticate" (in the language of the standard) a station and to keep the information exchanged over the WLAN private, through encryption technology.

Authentication involves proving an identity, usually by showing that a secret code is held. This can be done in several ways, by proving a shared secret code is known by only authorized stations or by proving a secret code is held that can only be known by a single station. Once identity is proven, the station is allowed to make use of the WLAN resources. There are many ways to prove an identity, some more reliable than others. These methods vary from simply asserting an identity, to sending a message encrypted with a shared secret key, to a full exchange of public key information.

Privacy is accomplished by modifying the information that is sent in such a way that only the intended recipients can recover the original information. The method most commonly used in WLANs is to encrypt the information. Encryption is usually accomplished by passing the information through a filtering function that will provide an output that appears to be a random sequence of bits and is difficult, if not impossible, to reverse. The function is fixed and well known, but uses a parameter that has a significant effect on the output. This parameter is known as the key. As long as both sender and recipient use the same key, the sender can encrypt information for the recipient and the recipient can decrypt it and recover the original information. For single key encryption systems, the security of the encryption is highly dependent on the size of the key The more bits in the key, the more time it will take, on average, to decrypt the key.

802.11 Security Features

The IEEE 802.11 standard for WLANs provides mechanisms to address the threats to WLAN security. To deal with unauthorized reception of the information carried by WLANs, the standard provides a mechanism, named wired equivalent privacy (WEP), which calls for encrypting the information transmitted on WLANs. Only receivers that

also have the correct encryption key can receive and correctly decrypt the information. This mechanism was designed to provide a level of security similar to that of a typical wired network, where access to the cabling of the network is restricted by physical security procedures, which allow only authorized employees into a corporate building. The WEP mechanism uses the RC4 encryption algorithm from RSA Data Security, Inc. and a 40-bit key.

Similarly, the IEEE 802.11 standard provides a mechanism, called shared key authentication, which prevents access to the WLAN by stations that do not know a shared secret code necessary to complete the authentication handshake. This mechanism was designed to provide a level of authentication similar to that of a typical corporate network with limited physical access, preventing the connection of unauthorized equipment to the LAN cable. Using this mechanism, a mobile station is challenged by an access point and must return the challenge, encrypted with a shared key. If the mobile station responds properly, it is then successfully authenticated.

Weaknesses of 802.11 Security

Both security mechanisms of the 802.11 standard suffer from significant weaknesses. A significant weakness of both the shared key authentication and WEP mechanisms is their reliance on encryption keys of only 40 bits. At the time the standard was written, U.S. export regulations severely limited the export of equipment that used keys longer than 40 bits. Unfortunately, 40-bit keys are too short to provide anything but temporary security in today's world, given the computing power of current personal computers and the ease with which hundreds or thousands of computers can be teamed up to solve a single problem.

A second weakness of the 802.11 security mechanism is the lack of any provision for the exchange, delivery or management of keys. Each of these tasks is necessary in any system that incorporates encryption and is necessary to support the 802.11 shared key authentication mechanism. If the method used to exchange keys between parties that wish to encrypt their conversation is not secure, the resulting encryption is worthless regardless of the strength of the encryption algorithms used or the length of the keys. It is also critical that the parties to an encrypted conversation use the same keys. Otherwise, the attempt to exchange information will be impossible. Thus, a method for managing the keys used by the stations in a WLAN is also necessary. Because 802.11 lacks any of these mechanisms, this places the burden on the system designer to design and implement protocols to accomplish these necessary security tasks.

A false sense of security

One attempted security method involves hiding information from the user. This "security through obscurity" is rarely effective and often provides a false sense of security.

Some WLAN equipment vendors do not allow a user to display the service set identifier (SSID) or network name of the WLAN. This is done on the theory that what a user doesn't know can't be used as a tool to enter a network without authorization or to set up an imposter network. Only authorized users will be provided with the SSID necessary to access the network. Unfortunately, only equipment from vendors hiding the SSID in this fashion provide this "security". Equipment from another vendor can easily be used to discover this information, since the SSID is broadcast in every beacon frame, usually several times a second, and in all probe response frames, used by mobile stations when seeking an access point. Thus, hiding the SSID from users in some vendors' 802.11 equipment provides no security at all. If a network relies on hiding the SSID as its sole means of security, an imposter AP could easily be set up that would attract mobile users and could record login sequences and other sensitive information.

AirLock™ Security Software

The AirLock™ security software builds on the basic security features of 802.11 by adding superior protection and ease of use. Essentially a security overlay, the software is completely interoperable with WEP-enabled products. Stations enabled with AirLock™ security software will communicate at the highest available level of IEEE 802.11 security when complementary devices are not Airlock™ security software enabled. In addition, the operation of AirLock™ security software is completely transparent to the user. There are no keys to manage or enter and no configurations to change when adding stations equipped with the software to a new or existing 802.11 WLAN. Adding stations and access points equipped with the AirLock™ security software makes the WLAN more secure.

How the AirLock™ Security Software Corrects the Weaknesses of 802.11 Security

The AirLock™ security software addresses all of the security weaknesses of the IEEE 802.11 standard. The software adds a public keybased mechanism to significantly strengthen authentication. Every station enabled with AirLock™ security software is manufactured with its own Diffie-Hellman public and private key pair. The AirLock™ security software adds key negotiation that allows WLAN stations to create robust encryption keys, without the need to use a secure key exchange protocol or to use any kind of key management. The software also includes an access control list that allows only known mobile stations to communicate with an access point. Finally, the AirLock™ security software adds virtually impenetrable 128-bit keys to protect the information on the WLAN.

Public Key Authentication

Public key encryption algorithms have a special property that links the public and private keys when they are created, but makes it nearly impossible to determine one of the keys from the other. Using one of the keys to encrypt information requires that the other key of the pair be used to decrypt that information. This property allows the public key to be freely distributed to other stations to allow them to encrypt information that can only be decrypted by the owner of one particular private key. Similarly, information can be encrypted with the private key. Encryption with the private key provides no security for the information, since the matching public key may be very widely distributed. However, a message that is properly decrypted with a public key could only have been encrypted using the matching private key. This can be used to guarantee the source of information.

Using the properties of public key algorithms, AirLock™ security software provides a much more secure authentication mechanism than the shared key algorithm of 802.11. The software provides this additional security without requiring additional key management, station configuration, or user intervention.

Key Agreement

AirLock™ security software provides a secure method for stations to exchange the keys to be used for encryption, without requiring any additional key management or a secure channel. A station enabled with AirLock™ security software will negotiate a shared key to be used with another station to encrypt their information exchanges using the industry standard Diffie-Hellman key agreement algorithm. This algorithm allows two stations to exchange information in such a way that each station will generate the same encryption key, while any other station that listens to the exchange will not have enough information to create that same key. This allows every software-enabled station to communicate securely with every other station enabled with the AirLock™ security software without requiring the user to enter keys and without requiring the use of additional key management. Every access and client device enabled with AirLock™ security software is manufactured with its own 1024-bit public and private key pair. Using this key pair and Diffie-Hellman public key encryption, the AirLock™ security software enhances the security of the 802.11 authentication protocol. In addition to the 802.11-based shared key authentication mechanism, the AirLock™ brand of software provides a much stronger public key authentication mechanism.

Diffie-Hellman Key Agreement

The Diffie-Hellman key agreement algorithm was the first published "public key" mechanism. This algorithm allows two conversants to create a shared secret code between them, without revealing enough information so that an eavesdropper could create the same secret code. The algorithm works using exponentiation and modular arithmetic. The security of this algorithm is based on the extreme difficulty of calculating discrete logarithms. The steps to creating the shared secret are the following.

1. The conversants (let's call them Alice and Bob) agree on a large prime number, n, and g, such that g is primitive mod n. (g is primitive mod n if g is less than n and for every i from 1 to n-1 there exists some a where $g^a = i \pmod{n}$.) This pair of numbers can be chosen in the open.

2. Alice chooses a random large integer x and sends Bob

$X = g^x \bmod n$

3. Bob chooses a random large integer y and sends Alice

$Y = g^y \bmod n$

4. Alice computes

$k = Y^x \bmod n$

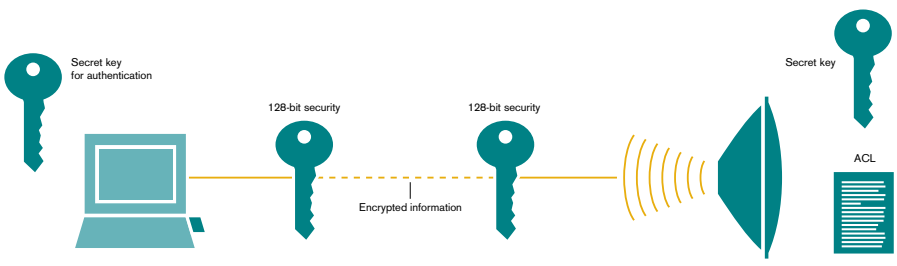
5. Bob computes

$k' = X^y \bmod n$

Both k and k' are equal to $g^{xy} \bmod n$. An eavesdropper can not compute k unless she knows x or y, or can compute the discrete logarithm to recover x or y. Alice and Bob can now select bits from k to use as a shared key for any encryption algorithm.

Access Control List

An access control list (ACL) is used to allow only those mobile stations that are known to the access point to use the WLAN. AirLock™ security software allows the ACL to be created either manually or automatically. When created manually, an administrator may enter the addresses of the mobile stations that are to be allowed access to the WLAN. To create the ACL automatically, the access point is placed in a promiscuous mode and learns the addresses of the mobile stations that are allowed to access the WLAN from those mobile stations themselves.



More Robust Encryption

AirLock™ security software uses the RC4 algorithm found in the IEEE 802.11 industry standard buts uses 128-bit keys. RC4 is an algorithm that has received significant peer review by the cryptography community and is generally considered to be strong and secure. By using 128-bit keys, AirLock™ security software addresses the most significant weakness of WEP, which uses a key that is short enough to be breakable by brute force mechanisms with today's computing power. 128-bit keys are considered by the cryptographic community to be secure today and for many years into the future.

Summary

There are security threats to a WLAN that are not present to the same degree in a wired LAN. The IEEE 802.11 standard for WLANs provides some basic mechanisms to address these threats. However, the strength of the mechanisms used by 802.11 is not sufficient for many customers. NoWiresNeeded™'s AirLock™ security software adds significantly stronger mechanisms to those provided by 802.11, providing a much more secure WLAN in a fashion fully interoperable with 802.11. This solution provides stronger privacy using 128-bit keys and stronger authentication using public key algorithms. The AirLock™ security software also simplifies security implementation requirements, by being much easier to manage and allowing stations to create keys using the Diffie-Hellman key agreement algorithm. Using the AirLock™ security software from No Wires Needed™ in an 802.11 wireless LAN provides much greater security for the information carried on the WLAN.

Table 1; Summary and Comparison of 802.11 and AirLock™ Security Features

Feature	802.11	Airlock™
Encryption	WEP, using RC4 with 40-bit keys	RC4 and 128-bit keys
Key agreement	None, must be accomplished manually or with a secure external protocol	Diffie-Hellman key agreement
Authentication	Shared key mechanism, using 40-bit keys	Public key mechanism, using 1024-bit keys
Extensibility	Not currently available in the standard	Fully extensible, algorithms and key length are negotiable between stations

NoWiresNeeded
The Netherlands

P.O. Box 343
3720 AH Bilthoven
The Netherlands
Voice +31.30.229.6060
Fax: +31.30.229.6061
E-mail: info@nwn.com
Website: www.nwn.com

Visitors address:
Rembrandtlaan 1a
3723 BG Bilthoven

No Wires Needed USA Inc.

P.O. Box 2164
Menlo Park
California 94026-2164
United States of America
Voice: +1.650.324.1105

P.O. Box 2368
Westfield
New Jersey 07091-2368
United States of America

No Wires Needed UK

P.O. Box 1782
Coventry
CV4 8ZF
United Kingdom
Voice: +44.870.205.1122