

Defining Best Practices for Designing and Implementing 802.11 Wireless Security

Revision 1.5, 12 June 2002

L. Taylor Banks, CISSP
Vigilar, Inc.

Wireless network technologies are quickly becoming a viable means of extending existing IT infrastructures in ways that were not previously possible due to engineering and financial constraints. With rapid adoption, however, have come security problems not present in wired environments. As a result, wireless network engineers and architects must find new ways to mitigate the risks associated with wireless deployments.

This white paper defines industry accepted best practices for the design and implementation of 802.11 (b, a, or otherwise) wireless networks using methodologies, techniques, and technologies that eliminate the risks associated with wireless deployment.

Defining Best Practices for Designing and Implementing 802.11 Wireless Security	1
<i>Problems</i>	3
Access Problems	3
Policy Abuse Problems	3
Performance Problems	3
Authentication Problems	4
Confidentiality Problems	4
<i>Considerations for Designing a Secure Wireless Network</i>	5
Policy Review and Architecture	5
Vendor Interoperability	6
Size and Growth	6
Traffic Categorization and Data Classification	6
<i>Additional Challenges</i>	8
<i>Wireless Security Models</i>	8
Minimal	8
Intermediate + Authentication (I+A)	9
Intermediate + Encryption (I+E)	10
Intermediate + Authentication + Encryption (I+AE)	11
Advanced	13
<i>Conclusions</i>	15
<i>Credits</i>	16
<i>References</i>	16

Problems

As the problems with 802.11 networks have been covered in great detail elsewhere, they will be mentioned in brief detail here to provide a basis for further discussion of the means by which to eliminate or overcome them. Additional references are also provided at the end of this document.

The problems with wireless can be broken down into categories, many of which are specific to the 802.11 protocol. The problems will be addressed as follows:

- Access Problems
- Policy Abuse Problems
- Performance Problems
- Authentication Problems
- Confidentiality Problems

Access Problems

The problems with wireless networks extend beyond technology, and encompass a number of issues that are introduced merely because of the use of radio waves in public airspace. Because of this, and with the rapid adoption of 802.11 in major metropolitan areas, wireless networks are easy for non-associated individuals to locate. Because the beacons sent by wireless access points employ no means of encryption (the beacons associate wireless clients with a given network), anyone with a laptop and a wireless card can easily determine their presence. In fact, modern ‘war-drivers’ might find tens if not hundreds of wireless networks within a given 10-mile radius using high-gain vehicle-mounted antennas.

Policy Abuse Problems

To exacerbate the problem, wireless networks are becoming easier to deploy. Wide availability and low cost of wireless components, combined with the ease of device configuration and lack of secure default settings for operation promote rogue implementations. It is not uncommon to find unauthorized access points in an organization, setup by a department manager with no understanding of proper security practices and little regard for corporate policies and procedures.

Unfortunately, little can be done to mitigate these risks, short of RF shielding, frequent monitoring for rogue devices, and strict enforcement of security policies.

Performance Problems

In addition to the overhead imposed by the 802.11 protocol implementation (which can equate to as much as 50 percent of available throughput), all wireless users associated with a single access point share the same effective bandwidth (up to 11Mb for 802.11b, 54Mb for 802.11a). Because the medium access is based on contention, the user with the

greatest signal strength (which might or might not be the closest user to the access point) will consume a significant portion of available bandwidth, causing significant performance problems for the remaining users. Additionally, while the number of users *supported* per access point may vary (most vendors' 802.11b products support up to 32 users, 802.11a products up to 64), typical enterprise network traffic requirements cap the number of users per 802.11b access point at 20 or under.

Authentication Problems

Authentication problems are one of the most prevalent concerns in any network, wired or wireless. In fact, wireless networks have many of the same problems found in typical Ethernet networks. Specifically, 802.11 does not require a means by which to authenticate frames. Open Systems Authentication is the default authentication mechanism in 802.11, and authenticates anyone who requests authentication. Despite the ability to also perform Shared Key Authentication, vulnerabilities exist that allow an attacker to easily authenticate without knowing the shared secret. Because of this, it is entirely possible to inject frames into a wireless network through spoofing of the source MAC address. Because the source address of an authorized user can be easily obtained (see Confidentiality Problems below), it is a trivial task for a skilled attacker to redirect wireless traffic, hijack a trusted connection, and imitate an access point in order to capture authentication credentials. While this problem has been partially addressed through the use of switched media in Ethernet networks, such options are not available when the medium is open air. Recently, vendors have implemented rudimentary access control systems that restrict access by MAC address and several vendors are beginning to support the 802.1x authentication protocol in anticipation of upcoming 802.11i standards.

Confidentiality Problems

Unfortunately, because packets between 802.11 devices must contain source and destination MAC addresses in the clear, it follows that elementary packet capture in a wireless network will reveal the MAC address of the access point, as well as users who are allowed access by MAC address. Despite the fact that 802.11 utilizes the WEP (Wired Equivalent Privacy) protocol for encryption, it has been publicized that WEP is only marginally successful at protecting data in transit. Many of the problems with WEP are due to reuse of the short 24-bit initialization vector (IV), which allows for keystream determination through statistical analysis and known-plaintext attacks. Because of this, WEP is subject to active packet injection attacks. It was also determined by Scott Fluhrer, Itsik Mantin, and Adi Shamir that a weakness in the Key Scheduling Algorithm in RC4 (the stream cipher that serves as the basis for WEP) would allow for decryption of WEP-encrypted packets in as little as 15 minutes!

Considerations for Designing a Secure Wireless Network

In addition to the aforementioned issues, there are considerations for deciding on appropriate security policies regarding wireless network implementation and usage. These factors will have a significant effect on the resultant security and performance of the wireless networks, and should therefore be *carefully* considered before finalizing the network design.

Policy Review and Architecture

A full security policy review is necessary in order to properly understand and implement a wireless security policy that meets existing security goals. It is vitally important that wireless networks be considered at high-risk for compromise. Logical network design should always place wireless segments in packet-filtered or firewalled networks, with policy-based separation from private or protected internal networks (Figure 1).

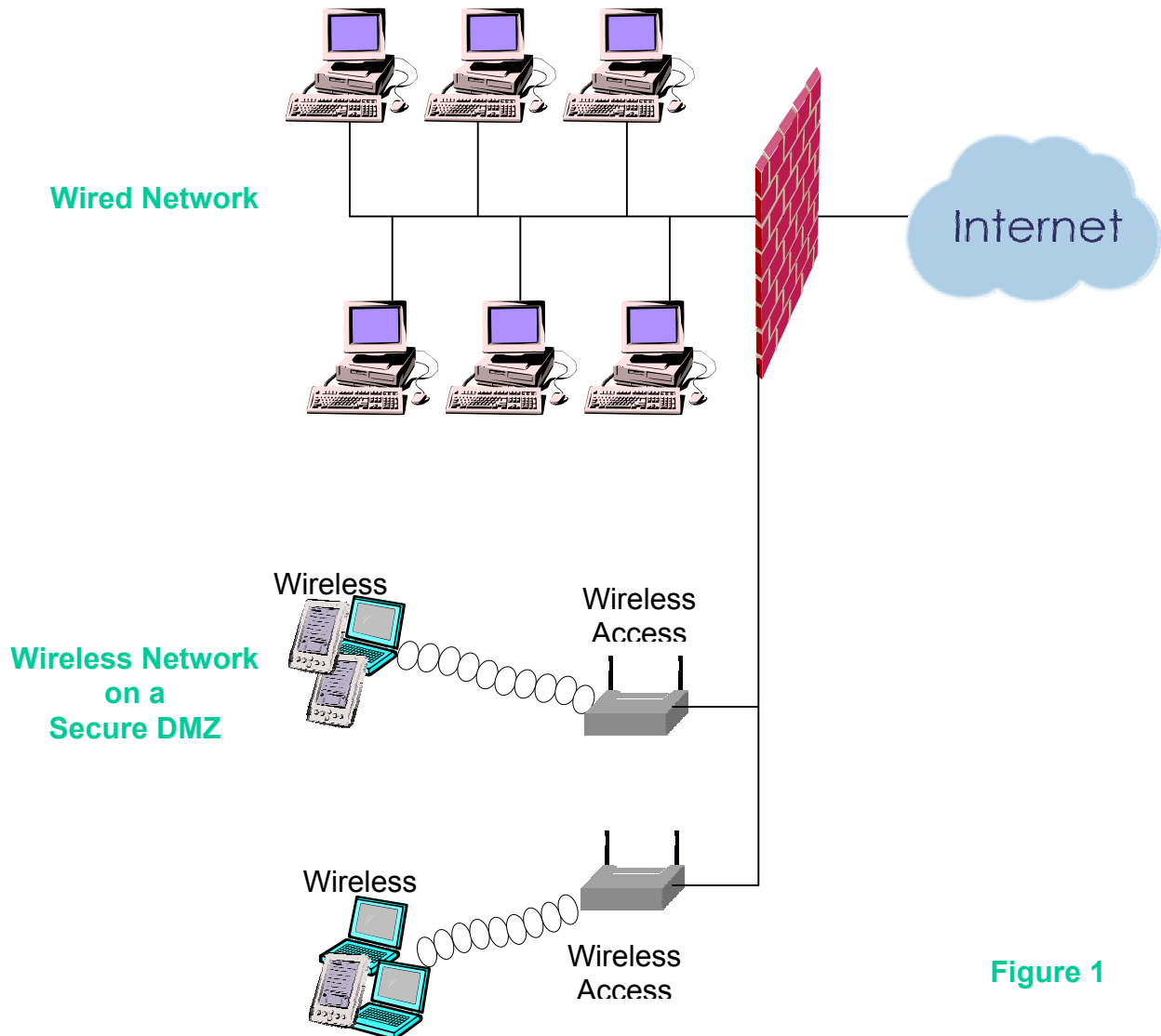


Figure 1

Vendor Interoperability

It is expected that vendor preferences may affect an organization's purchases. It should be noted that some vendors are implementing features that may be proprietary and will not interoperate well with other 802.11 products. As such, precautions should be taken when evaluating hardware.

Size and Growth

The most important factor when designing a security strategy for wireless networks is the expected network size (i.e. number of nodes). Although certain methodologies may be acceptable in a network with fewer than 25 wireless users, such mechanisms might be administratively prohibitive in networks with 500 wireless users. For this reason, consider three size categories of wireless networks:

- ‘Small’ wireless networks with fewer than 25 nodes.
- ‘Typical’ wireless networks with 25 – 100 nodes.
- ‘Enterprise’ wireless networks with >100 nodes.

Beyond several hundred nodes additional considerations are necessary, however from a design perspective, it will be more effective to further segment the infrastructure such that individual groups of 100 – 200 nodes can be more effectively managed.

The size of a network has many implications, not the least of which is the resultant range of wireless devices. In considering the physical area coverage of access points, consider also their proximity to other wireless networks and public places. If the network can be made to cover the desired area—even if the outer limits are at a significant distance from the access points (and can only achieve lower-bandwidth connections)—without allowing signals to bleed into peer networks or publicly accessible areas, the network is further secured from malicious attackers and casual observers. Testing should be done throughout all phases of implementation that will identify wireless coverage areas, and points of possible access. Also, when conducting tests, using a high-gain antenna will help identify otherwise weak signal areas that a well-prepared attacker will be able to find.

Having established the target size of an implementation, it is important to consider scalability in relation to the expected growth of the wireless infrastructure. Although initial design considerations may designate a network as Small, plans to expand beyond Enterprise classification within 6 months should be considered during initial design.

Traffic Categorization and Data Classification

The types of traffic and classifications of data traversing our wireless networks have significant bearing on the measures that must be taken to protect them. The classification of data will guide the efforts that will be employed to obscure it, whereas the types of

traffic on the wire will be more pertinent when considering the performance implications of a chosen security measure.

Traffic can be categorized in a variety of ways. For the sake of security and performance, it is most effective to determine not only the layer 4 protocols in use (TCP, UDP), but also those used at layer 7 (DNS, HTTP, HTTPS, etc). In doing so, traffic that can be adversely affected by encryption could be identified.

Data classification relates not to the type of traffic (HTTP, SMTP), but instead to the traffic's sensitivity. Whereas HTTP data might not be of a sensitive nature, SMTP and POP3 traffic tends to contain confidential information, and as such it is necessary to take further measures to ensure it is not intercepted in transit. In other cases, it may be the HTTP data that contains sensitive information, and therefore it is important to distinguish between traffic categorization and data classification.

Additional Challenges

There are numerous challenges encountered when designing and implementing wireless networks, many of which pertain to concepts already discussed above. However, additional issues exist that will not always relate to the *security* of the resultant wireless infrastructure, and are beyond the scope of this document. Such considerations might include: physical landscape, transmit power, antenna gain, antenna alignment, free space attenuation, possible interference, power consumption, sustained available bandwidth, etc.

Wireless Security Models

Minimal

The Minimal Security Model represents the lowest level of security that should be implemented in any deployed wireless network. It is recognized that this level of security does not effectively mitigate all wireless network risks, and should only be used when further measures are not required or are infeasible.

Small/Minimal

- Private Network (non-broadcast SSIDs – supported by most vendors)
- WEP encryption enabled (40/56/64 or 128 bit)
- MAC-based access control (supported by most vendors)

Typical/Minimal

- Private Network (non-broadcast SSIDs – supported by most vendors)
- WEP encryption enabled (40/56/64 or 128 bit)
- MAC-based access control (supported by most vendors)

Enterprise/Minimal

- Private Network (non-broadcast SSIDs – supported by most vendors)
- WEP encryption enabled (40/56/64 bit due to bandwidth considerations)

In the Minimal Security Model, requirements for Small and Typical networks do not differ since each of the specified mechanisms is considered administratively feasible for networks in these classes, and helps to mitigate the risks of compromise.

As it is generally considered administratively prohibitive to attempt MAC-based access control when the wireless user-base exceeds 50-100 nodes, it has been excluded from the Enterprise classification above.

Intermediate + Authentication (I+A)

The Intermediate + Authentication Security Model includes all of the relevant measures implemented in the Minimal Security Model, and specifies an additional form of required authentication, preferably performed OOB (out of band, i.e. using an isolated authentication server on a private wired segment adjacent to the wireless access point). Using this Model ensures that access to wired and/or other wireless networks is granted only to authorized users.

Small/I+A

- Private Network (non-broadcast SSIDs – supported by most vendors)
- WEP encryption enabled (40/56/64 or 128 bit)
- MAC-based access control (supported by most vendors)
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)

Typical/I+A

- Private Network (non-broadcast SSIDs – supported by most vendors)
- WEP encryption enabled (40/56/64 or 128 bit)
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)

Enterprise/I+A

- Private Network (non-broadcast SSIDs – supported by most vendors)
- WEP encryption enabled (40/56/64 or 128 bit)
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)

In contrast to the Minimal Security Model above, the Typical and Enterprise classifications in the I+A Security Model do not differ, as the tradeoff associated with not implementing MAC-based access control in mid-sized networks is diminished by the additional security provided by less-fallible authentication.

The same logic could be applied to the Small classification, however maintaining both authentication mechanisms in networks of this size is worth the additional layer of security provided by two-factor authentication.

Intermediate + Encryption (I+E)

The Intermediate + Encryption Security Model includes all of the relevant measures implemented in the Minimal Security Model, and specifies an additional form of required encryption using a secure algorithm with long keys. Generally, this encryption would be performed between the access point and any attached networks using a device devoted to the purpose. The criteria for selection of the I+A Security Model and the I+E Security Model are based upon the classification of data traversing the wireless network. Whereas the I+A Security Model places a greater focus on restricting access to attached networks, the I+E Security Model depends on lesser authentication mechanisms, but places a greater emphasis on encrypting the data in transit to prevent even unauthorized users from capturing data.

Small/I+E

- Private Network (non-broadcast SSIDs – supported by most vendors)
- MAC-based access control (supported by most vendors)
- Third-party encryption (IPSec, SSL, TLS)

Typical/I+E

- Private Network (non-broadcast SSIDs – supported by most vendors)
- MAC-based access control (supported by most vendors)
- Third-party encryption (IPSec, SSL, TLS)

Enterprise/I+E

- Private Network (non-broadcast SSIDs – supported by most vendors)
- Third-party encryption (IPSec, SSL, TLS)

Here, the Enterprise classification in the I+E Security Model differs from both Small and Typical classifications, in that it only uses authentication provided by the 802.11 protocol (see Authentication Problems) and the specific implementation of encryption (which may be none). Because this may be less secure, alternatives for Enterprise networks would be either the I+A or I+AE Security Model.

Intermediate + Authentication + Encryption (I+AE)

The Intermediate + Authentication + Encryption Security Model includes all of the relevant measures implemented in the Minimal Security Model, and specifies both an additional form of required authentication and an additional form of required encryption. Although still considered to be an Intermediate Security Model, this Model better addresses the problems identified in most 802.11 implementations, at the cost of reduced performance and greater administrative burden.

Small/I+AE

- Private Network (non-broadcast SSIDs – supported by most vendors)
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)
- Third-party encryption, using OOB authentication (IPSec, SSL, TLS)
- Wireless Gateway used in conjunction with authentication and encryption

Typical/I+AE

- Private Network (non-broadcast SSIDs – supported by most vendors)
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)
- Third-party encryption, using OOB authentication (IPSec, SSL, TLS)
- Wireless Gateway used in conjunction with authentication and encryption

Enterprise/I+AE

- Private Network (non-broadcast SSIDs – supported by most vendors)
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)
- Third-party encryption, using OOB authentication (IPSec, SSL, TLS)
- Wireless Gateway used in conjunction with authentication and encryption

In this model, all network classifications specify the same set of requirements. Because all three network classifications are using OOB authentication mechanisms, the need for MAC-based access control is lessened, and with the added administrative burdens of third-party encryption, it becomes impractical.

Taking authentication and encryption a step further, a third party device can be put on the wireless side of the network in between the wireless access point and the firewall itself for the purpose of acting as an IPSEC termination point *and* as an authentication gateway (Figure 2).

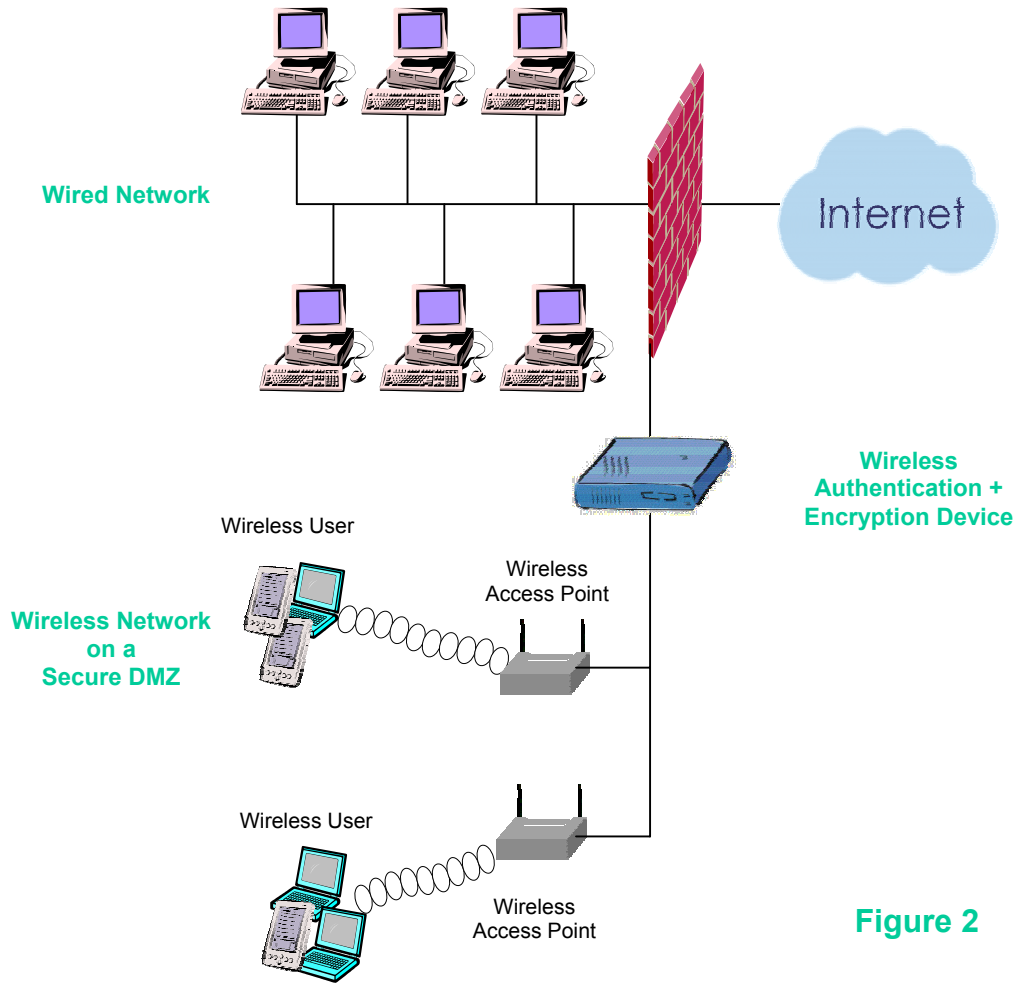


Figure 2

The authentication device should be capable of talking to an LDAP or RADIUS server for the purpose of transparent authentication and dynamic MAC address filtering.

If encryption is employed, the encryption should terminate at the wireless gateway for the purpose of encrypting all traffic as it leaves the wireless LAN.

Advanced

The Advanced Security Model includes all of the relevant measures implemented in the I+AE Security Model, re-introduces short-key WEP and MAC-based access control, and places additional focus on restricting access to the wireless medium itself (in the previous Security Models, most of the mechanisms and methodologies used protect the traffic and prevent access to attached networks). It is likely that an additional device (and possibly access point) would be required in order to provide such protection and to provide additional access information to authenticated and authorized users. Automation of these tasks would be necessary to make this model administratively feasible.

Small/Adv

- Private Network (non-broadcast SSIDs – supported by most vendors)
- Automated MAC-based access control
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)
- WEP encryption enabled (40/56/64 bit due to bandwidth considerations)
- Third-party encryption, using OOB authentication (IPSec, SSL, TLS)

Typical/Adv

- Private Network (non-broadcast SSIDs – supported by most vendors)
- Automated MAC-based access control
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)
- WEP encryption enabled (40/56/64 bit due to bandwidth considerations)
- Third-party encryption, using OOB authentication (IPSec, SSL, TLS)

Enterprise/Adv

- Private Network (non-broadcast SSIDs – supported by most vendors)
- Automated MAC-based access control
- OOB user authentication (LDAP, Active Directory, RADIUS, SecureID, etc.)
- WEP encryption enabled (40/56/64 bit due to bandwidth considerations)
- Third-party encryption, using OOB authentication (IPSec, SSL, TLS)

In the case of the Advanced Security Model, elementary encryption is being provided by WEP to help ensure that details of the wireless network's configuration are not easily determined. Additional third-party encryption ensures the integrity of data in transit in ways that the WEP protocol cannot. Authentication is done using MAC-based access control and an OOB authentication mechanism, ensuring that an attacker would have to spoof not only the client's physical address, but also capture authentication credentials.

Future concerns of wireless networks will be *not* in the wireless-to-wired network communications, but in the wireless-to-wireless, where wireless technologies will be ubiquitous.

While there is no Security Model that can unconditionally guarantee the security of a wireless network, techniques such as these successfully mitigate most of the associated risks and decrease the probability of compromise significantly.

Security Mechanism

		Private	WEP/64	WEP/128	MAC Access Contol	OOB Auth	Strong Encryption
Small	Min	X	X	X	X		
	I+A	X	X	X	X	X	
	I+E	X			X		X
	I+AE	X				X	X
	Adv	X	X		X	X	X
Typical	Min	X	X	X	X		
	I+A	X	X	X		X	
	I+E	X					X
	I+AE	X				X	X
	Adv	X	X		X	X	X
Enterprise	Min	X	X	X			
	I+A	X	X	X		X	
	I+E	X					X
	I+AE	X				X	X
	Adv	X	X		X	X	X

Table 1

Conclusions

The security controls provided by the 802.11 protocol do not effectively eliminate the risks associated with deployment of wireless networks. In order to combat these risks, additional measures must be taken to ensure that our data and networks are not vulnerable to attack.

In order to effectively design wireless security policy, it is necessary to consider several factors that directly affect deployment risks:

- Existing security policy
- Interoperability of protocols and security measures
- Size and potential growth of a network
- Traffic categorization and data classification

Understanding the relationships amongst these elements allows us to identify the security requirements of a given environment and implement a Security Model to address them.

The Security Models defined in this document specify a means of combining the proven technologies that are currently used to protect wired networks with methodologies specific to wireless deployments that help to avoid vulnerability.

By leveraging the Security Models outlined in this white paper, we can effectively secure most wireless networks, and help ensure that our private information remains private.

Credits

Thanks to [Beth Milliken](#), [Renee Beckloff](#), and [Joseph Dell](#) for editorial assistance.

References

W. Arbaugh, N. Shankar, Y.C. Wan, [Your 802.11 Wireless Network has No Clothes](#), <http://www.cs.umd.edu/~waa/wireless.pdf>

N. Borisov, I. Goldberg, and D. Wagner, [Security of the WEP algorithm](#), <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

W. Arbaugh, [An Inductive Chosen Plaintext Attack against WEP/WEP2](#), <http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm>

A. Stubblefield, J. Ioannidis, A. Rubin, [Using the Fluhrer, Mantin, and Shamir Attack to Break WEP](#), AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, August 21, 2001, <http://www.cs.rice.edu/~astubble/wep/>

M. Gast, [Seven Security Problems of 802.11 Wireless](#), <http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html>

J. Kabara, P. Krishnamurthy, and D. Tipper, [Capacity Based Network Planning for Wireless Data Networks](#), <http://www.mobilesummit2001.org/>