

The logo graphic consists of several overlapping, light blue circular and elliptical shapes that create a sense of motion and connectivity. The word "Intermec" is written vertically in a bold, sans-serif font, with the 'I' at the top and the 'c' at the bottom, positioned to the right of the graphic.

Intermec

White
Paper

M o b i l e L A N TM s e c u r e
P O S I T I O N

Intermec

EXECUTIVE SUMMARY

Network security is gaining attention as more enterprises install wireless LANs. Buyers of information technology should understand wireless LAN security provisions, with their flaws and fixes, even as IEEE develops improved security standards. Interoperability, functionality and future migration are essential considerations as network administrators contemplate how to acquire, maintain and protect their wireless LAN investment.

SECURITY IN WIRELESS NETWORKS: INTERMEC'S POSITION

Concern over data security has become the reason not to implement wireless LANs. Fear of unauthorized access to sensitive information and eavesdropping on the network may, however, be unfounded. Are the security issues different between wired and wireless networks? Are today's wireless networks as secure as their wired counterparts? How serious is security in a wireless LAN, and what should an enterprise know before making a wireless product selection? These questions are the focus of this paper. The prevailing wireless security standards will be examined and the future of security solutions in wireless LANs will be addressed.

THE WIRELESS SECURITY PROBLEM

Users are learning how wireless differs from conventional wired networks. Wireless technology changes the network paradigm of the wired user going to where the data is, to the data going to the user. The mobile user can call the data up anywhere in range, any time. As such, wireless can support a variety of business critical applications that cannot be effectively met with conventional, wired connections. For day to day applications, wireless can provide convenient network access to improve worker productivity.

Wireless networks, by their nature, have the potential to provide access to any party in range of the system. That includes parties outside of the physical security perimeter of a network, whether in a parking lot, an adjacent floor or office, or the next building. Although the range of wireless LAN systems is limited, wireless signals can be received at distances of several hundred feet beyond the physical perimeter of a facility. In larger facilities that use multiple wireless LAN access points that interconnect wireless users with wired networks, each access point is a potential point of entry inside the firewall.

Recent published technical studies, highlighted within the networking and popular press, have pointed out security vulnerabilities in the increasingly popular IEEE 802.11b wireless LAN standard. Current users of 802.11 have seen the benefits of going wireless and want to know how to protect their proprietary data. These users, as well as those who hesitate to deploy 802.11 technology because of security concerns, will benefit from understanding the nature of these security issues and the short and long-term remedies.

802.11 WEP

The original 802.11 wireless LAN standard in 1997 for frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) systems included a privacy feature named Wired Equivalent Privacy (WEP). WEP has been carried forward to the popular 802.11b (Wi-Fi™) standard, and the high speed 802.11a standard that will begin deploying in the second half of 2001.

HISTORY

WEP encryption was added to the 802.11 standard midway through its seven-year development cycle as a means of addressing concerns about casual eavesdropping on wireless networks. Originally proposed by representatives of a few computer and chip manufacturers, the WEP mechanism was based upon technology current in 1994. Its goal was to establish a reasonable level of privacy and satisfy U.S. export restrictions at the time of adoption. The latter led to the use of a well-known commercial cipher from RSA Security known as RC4, plus a short encryption key. The resulting privacy feature is known as WEP 64. At the time the 802.11 committee was an open standards committee composed largely of individuals representing companies developing and commercializing core wireless networking technology who had very little security expertise. WEP 64 was never intended or assessed as a security capability.

The development of the 802.11b high rate DSSS standard made it possible to extend the range and application of wireless LANs in areas formerly served only by traditional, wired local area networks. The subsequent formation of the Wireless Ethernet Compatibility Alliance (WECA) led to formalized technical guidelines and interoperability testing for 802.11b products from multiple manufacturers. Due to relaxation of export restrictions, WECA standardized on a longer key length for WEP, known as WEP128. The availability of WECA-certified products that carry the Wi-Fi label signaled to the networking market that wireless is legitimate networking technology with strong industry backing.

IMPLEMENTATION OF WEP IN 802.11

At the time WEP was incorporated with IEEE 802.11, the standard was planning to support a maximum data rate of 2Mbps. The 802.11 community was concerned about the performance capability of a 2Mbps networking technology at a time when 100Mbps Ethernet was nearing its first commercial deployment. RC4 had been selected as the encryption algorithm for WEP because it was exportable, easy to encrypt and decrypt using uncomplicated hardware. All of this was crucial to good throughput performance of WEP enabled products. RC4 also prioritized throughput and ease of implementation over robust security. As standards continued to develop and performance became increasingly critical at the higher data rates supported in 802.11b, hardware encryption remained the same.

The largest shortcoming in the implementation of WEP has nothing to do with the execution of the encryption and decryption process, but rather, it is the lack of standardized authentication and key distribution capabilities within 802.11. Lack of these features makes it extremely difficult to change security settings routinely in all but very small wireless network installations.

ATTACKS ON WEP

The success and widespread deployment of 802.11b has caused it to come under scrutiny by individuals with expertise in network security analysis. Their analysis has exposed weaknesses in the specific implementation of WEP encryption in 802.11. Additionally, in some cases these analyses have exposed weaknesses in the basic RC4 algorithm.

Documented attacks on WEP make use of both the implementation flaws in WEP encryption and specific knowledge about the content of messages that have been encrypted. These attacks depend on monitoring wireless transmissions then capturing and processing large numbers of data packets to recover the security key. The encryption patterns generated from a WEP 128 key are very long, but by monitoring large numbers of transmissions, patterns in the encryption are exposed that can be used to break the encryption key. With each paper, the attacks on WEP have become more refined. The first attacks required the capture several hours of encrypted data. The most recent papers report that WEP can be broken with observation of a few million packets.

There are two types of documented attacks on encryption technologies such as WEP. An active attack involves sending known data from outside the network to a user known to use an encrypted, wireless connection. For example, email text sent over the Internet to a wireless networked user can be compared with the encrypted wireless data. Active attacks can be effective, but are easier to monitor, detect and potentially expose the attacker who must be within close physical proximity to the wireless network.

Recent papers describe passive attacks, which are normally undetectable, since they require only passive monitoring of wireless signals. These attacks use knowledge of format and contents of common networking protocols to provide the unencrypted source information used for comparing with encrypted data and breaking of the key.

These attacks on WEP have further sensitized the network security community to the 802.11 wireless security issue. Both the manufacturer and user community for wireless LANs should expect additional analyses of WEP leading to other potential attacks and further concerns.



BLUNTING ATTACKS ON 802.11 WIRELESS LANs

Press reports regarding 802.11 wireless security call attention to valid and significant concerns. However, they overlook the fact that many wireless network installations do not use the security mechanisms available within 802.11 today. Users and administrators of wireless LANs can and should turn on all of the security features in the wireless LANs they have now. Once the basics are in place there are further steps that will blunt the more sophisticated intruder.

Recognize that Wireless Security Is a System Problem.

Secure wireless communication requires the participation of access points and client devices. These devices must be able to identify one another and exchange encrypted data using shared security keys. Effective management of authorized users and security keys may require a security server function.

Start with the Basics.

Establish policies for the use of wireless LANs on your network and the importance of using the security settings in wireless access points and clients. Make sure that policies are applied to all access points including those installed by individuals or individual work groups. Verify that WEP is enabled in all access points and NIC cards. While not infallible, WEP remains an effective deterrent to most intruders. Change WEP key values from manufacturers' defaults and change keys as frequently as is practical for your installation. Make sure that all access points and clients are WEP128 capable.

Enable Access Control Lists.

If your access points contain access control list functions, use them. While not effective against passive monitoring, access control lists can deny unauthorized parties direct access to your network through your wireless LAN.

Consider Transport Level Security.

For some applications, Internet technologies, such as Virtual Private Networking (VPN) can be used within wireless clients to provide transport level security

Assess Your Wired Ethernet's Vulnerability.

An easily accessible Ethernet port in an unsecured area is a direct point of interconnection to your network. It constitutes an opportunity to install a rogue access point that can be used for illegitimate access.

Assess Your Vendors' Current Features and Plans for Improved WEP Security.

Because WEP is implemented in hardware in most access points and NICs, upgrading these products to use improved software security capabilities other than WEP may significantly impact system performance. Major WLAN equipment providers are actively pursuing system enhancements to secure WEP while maintaining or enhancing performance. These enhancements fall into two general categories: (a) changes to the WEP encryption algorithm to address some of the implementation weaknesses in the original 802.11 standard, and (b) key administration features to facilitate periodic WEP key changes to prevent intruders from capturing enough data to decrypt the WEP key.

In assessing security-enhanced equipment, consider the following:

- Is it standards based and likely to be available from multiple manufacturers?
- Does it promote the interoperability of 802.11 products?
- Is the approach published and open to scrutiny by independent network security experts?
- And is it going to keep pace with security changes within the 802.11 standard?

Track Progress in Ongoing Changes to the 802.11 Standard's Security Capabilities.

The IEEE standards development process continues in a task group dedicated to security. The development process is described in detail below.

SECURING WEP

Intermec's Approach

Intermec is basing short-term security improvements on portions of the 802.11i draft, and other published standards. Authentication, access control and key exchange, are based on 802.1x port based security, as incorporated within the 802.11i draft. Secure clients and security server interface are based upon Remote Authentication Dial-In User Service/ Transport Layer Security (RADIUS/TLS), Extensible Authentication Protocol/Transport Layer Security (EAP/TLS), and Remote Authentication Dial-In User Service/ Extensible Authentication Protocol (RADIUS EAP). EAP/TLS is the security mechanism included in the new Microsoft operating system release, Windows® XP. Many access point and NIC card manufacturers, including Intermec, are planning to support XP clients. EAP/TLS provides secure client authentication and facilities for periodically changing WEP keys, which are the fundamental improvements needed to secure 802.11 on an interim basis. Because the EAP/TLS is based upon open standards, it is easily extensible to other client operating systems including previous versions of Windows, Unix, Linux, as well as to Intermec thin client portable computers.

Competitive Approaches to the Problem

While many of Intermec's competitors support EAP/TLS for Windows XP, others commonly adopt proprietary technologies for key exchange or encryption for other client types and operating systems. These approaches weaken 802.11 as an open standard and increase the complexity of managing security in multi-vendor environments. Proprietary methods also make it difficult for independent network security experts to analyze and expose weaknesses in implementation so that they can be remedied.

Task Group 802.11i is assigned to focus on improving the security levels of 802.11 Wireless LANs. The 802.11i security standard will apply to both 802.11b and higher speed 802.11a systems. A revised standard is expected by mid to late 2002. Until then the working drafts are available to 802.11 participants. Users of wireless equipment have an opportunity to participate in the formation of the standard. Draft standards are subject to revision, because the 802.11i security initiative is a work in progress. The current draft includes a number of distinct security improvements contributed by the many companies committed to the standards process.

For the near term, the focus of 802.11i is on using 802.1x port-based security, administration and key distribution using EAP. Proposals are also being made to better secure WEP, or introduce a more robust mechanism for using current RC4 hardware. In future, 802.11i will use Advanced Encryption Standard (AES). When finalized, some of the 802.11i standard security features will be available from wireless product vendors through software upgrades. Some features, particularly AES, may require hardware upgrades and result in more costly upgrades. Intermec's modular access point designs make possible simple upgrades of wireless security to support both AES and improved security concurrently, for current generation wireless clients.

Intermec has been doing advanced development in parallel with the development of the current 802.11i draft standard. Some features and capabilities required by the current draft are complete in our product set while others are still under development. As the standard matures from draft to its final release, our product set will continue to evolve. All of the required 802.11i capabilities except AES are being implemented as field software upgrades to currently shipping 802.11 products including clients and access points. Future products with AES hardware support will also support WEP and WEP2 for compatibility with earlier installations. Intermec's **MobileLAN** access 2100 and 2101 access points shipping now have a modular design to allow them to embrace AES and let enterprises upgrade at minimal cost rather than replacing existing hardware.



SECURITY BASED ON A DRAFT STANDARD

The challenge to any wireless vendor is to decide how to design solutions in parallel with developing standards. Suppliers that finalize pre-standard implementations will very likely need to revise and refine their products when the 802.11i security standard is released. Inevitably, some companies will be slightly ahead in their offering of enhanced security features, but they will be based on a draft standard, not an authorized standard. Buyers should be cautious of vendors claiming to have 802.11i security features before the standard is released. Any vendor's claim based on a draft standard presents a perceived, short-term advantage, and might be non-compliant when the final standard is released. Because of obvious technical holes in the current draft, early implementations will include some proprietary functions that will not be interoperable with clients or access points from multiple vendors. The majority of manufacturers will offer these capabilities within in a few months of one another. This majority, like Intermec, will be able to enhance security capabilities for currently shipping products through field software upgrades. End users need to be aware which functionality is included within the standard, and which functionality represents proprietary content.

AFTER THE IEEE 802.11i SECURITY STANDARD IS RELEASED

The essential milestone for 802.11 security is not when the first manufacturer offers a subset of the standard, but when multiple manufacturers demonstrate reliable, interoperable security implementations that are consistent with the full intent of 802.11i. Intermec is a strong advocate of interoperability testing through the University of New Hampshire and the Wireless Ethernet Compatibility Alliance (WECA). As security issues stabilize, wireless LAN customers will be able to return to assessing alternative suppliers based on their individual products and core competencies. Further, with the capabilities defined by the 802.11i security standard, wireless LANs will be more secure than their wired counterparts. It's important to remember that absolute security is an abstract, theoretical concept and does not exist anywhere. All LANs, wired and wireless, are vulnerable to attack and eavesdropping. The best approach for the security-conscious is to take advantage of widely accepted, industry approved and rigorously tested security measures. Finally, it goes without saying that network security isn't a one-time fix. It requires ongoing consideration by network administrators. There will always be enhancements on the horizon. Obtaining an appropriate level of security for a network isn't impossible and shouldn't seem daunting to a network administrator.

Until the new 802.11i standard is released, be cautious of a vendor's opinion that differs from the industry standard. Proprietary measures intended to provide extended levels of security may do so at the cost of interoperability and roaming, which are critical features. Proprietary techniques to enhance security render a system hostage to a particular vendor. In some instances, independent evaluations have identified that system performance has been compromised by a vendor's proprietary security enhancements.

INTERMEC'S POSITION ON INTEROPERABILITY AND FUNCTIONALITY

As a mobile computing company, Intermec is focused on the dual mission of serving both information technology and operations groups within the enterprise. We focus equally on functionality of access points, companion products and clients across a broad range of devices. For the benefit of end users, we incorporate not only security implementations but also operational factors such as battery life and robust roaming performance. These functions allow operational efficiency and result in cost savings for real-world mobile computing applications. For the IT staff, we emphasize mission critical operation, and ease of management and administration.

Intermec's philosophy has always been to design technologies based on standards and interoperability. We maintain leadership positions in industry associations dedicated to wireless LAN standards. Key Intermec people are active on the 802.11i board. Maintaining interoperability is a key accomplishment of Intermec's interim security solution because we believe customers are best served by standards-based products that are Wi-Fi interoperable. This motivation drove us to develop our interim security solution around the Microsoft Windows XP security initiative. Because Microsoft is hardware vendor neutral, we consider their security initiative to be a good interim approach. Microsoft Windows XP allows Intermec to continue to offer the encryption of WEP while also adding a stable, easy-to-administer feature for key management which interfaces with existing security schemes like RADIUS servers.

Intermec's security offering, named **MobileLAN secure**, is incorporated into all **MobileLAN** products. These include access points, clients, NICs and servers. Additional features will be released on an ongoing basis. As the 802.11i draft further solidifies, Intermec will begin incorporating the standards capabilities into the **MobileLAN secure** offering in addition to supporting the Windows XP model.

The **MobileLAN** family of products is strategically focused on enabling the mobile worker in business critical environments. Intermec understands that a variety of mobile devices and operating systems will need to support the security standards being developed. Our commitment is demonstrated with the release of **MobileLAN secure**, which maintains the stability and efficiency of mobile devices, preserves the performance of wireless networks, supports interoperability while providing various levels of security, efficient network management, and seamless integration into existing security schemes.



North America

Corporate Headquarters
6001 36th Avenue West
Everett, Washington 98203
tel: 425.348.2600
fax: 425.355.9551

Systems & Solutions
550 2nd Street S.E.
Cedar Rapids, Iowa 52401
tel: 319.369.3100
fax: 319.369.3453

Media Supplies
9290 Le Saint Drive
Fairfield, Ohio 45014
tel: 513.874.5882
fax: 513.874.8487

**Europe/
Middle East & Africa**

Headquarters
Sovereign House
Vestern Road
Reading, Berkshire RG1 8BT
United Kingdom
tel: +44.118.987.9400
fax: +44.118.987.9401

Gothenburg
Idrottsvägen 10
P.O. Box 123
SE-431 22 Mölndal
Sweden
tel: +46.31.869500
fax: +46.31.869595

**Asia/
Latin America**

Hong Kong
26-12 Shell Tower
Times Square
1 Matheson Street
Causeway Bay
Hong Kong
tel: 852.2574.9777
fax: 852.2574.9725

Singapore
25-16 International Plaza
10 Anson Road, 079903
tel: 65.324.8391
fax: 65.324.8393

Australia
15 Stamford Road
Oakleigh, Victoria 3166
tel: 61.3.9563.0000
fax: 61.3.9563.4000

South America and Mexico
17921 B Skypark Circle
Irvine, California 92614
tel: 949.442.9393
fax: 949.757.1687

**Worldwide
Fax Document
Retrieval Service**
800.755.5505
(North America Only)
tel: 650.556.8447

Internet
www.intermec.com

Sales
800.347.2636
(toll free in N.A.)
tel: 425.348.2726

Service and Support
800.755.5505
(toll free in N.A.)
tel: 425.356.1799

Copyright © 2001 Intermec Technologies Corporation. All rights reserved. Intermec is a registered trademark of Intermec Technologies Corporation. All other trademarks are the property of their respective owners. Printed in the U.S.A. 611072-02B 10/01

In a continuing effort to improve our products, Intermec Technologies Corporation reserves the right to change specifications and features without prior notice.