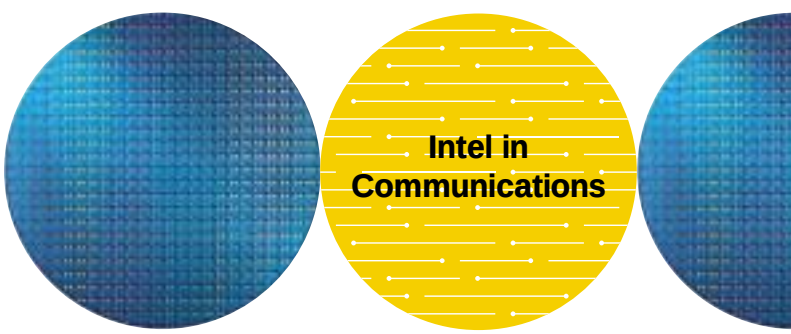
White Paper

Intel® Building Blocks for Wireless LAN Security

February 2003



Contents

Introduction 1

Wireless LAN Security Issues 1

Known 802.11 Security Vulnerabilities 1

Virtual Private Network (VPN) over WEP-based Wireless LAN 2

Due in 2003: Wi-Fi Protected Access (WPA) 3

Intel® Wireless LAN Security Building Blocks for Notebooks 3

In 2004: Hardware Support for 802.11i 4

Conclusion: Wireless LANs Can Address Security Today 4

Introduction

In a business environment where the only real constant is change, the flexibility and mobility enabled by enterprise wireless LAN technology can deliver significant competitive advantages. The potential cost savings and productivity gains help explain why the number of wireless LAN installations are expected to reach an estimated 50 percent of all enterprises in 2003[1]. The common goal of these deployments is a wireless network that provides all the features and benefits of traditional wired LANs, including continuous and trusted connectivity between a client and the corporate network.

The key word here is *trusted*. Like any network, wireless LANs must be secured to ensure protection of privacy and data integrity. The first step is for enterprise decision-makers to understand the nature and extent of wireless LAN security risks, as well as the solutions that currently exist to address areas of vulnerability. For example, employees can install "rogue" wireless LAN access points that can expose corporate networks to security breaches, and there are known security vulnerabilities inherent in the 802.11 standard itself. These security concerns have motivated some corporate enterprise managers to reduce the scope of their wireless LAN deployments or even to postpone them altogether. Fortunately, currently available solutions enable enterprises to move forward with full-scale wireless LAN deployments that address these security issues. This overview covers the native security issues inherent in 802.11 and standards-based wireless LAN building blocks available today from Intel.

Wireless LAN Security Issues

Note: Please also refer to the recent paper by the Wi-Fi** Alliance entitled *Enterprise Solutions for Wireless LAN Security.* Please refer to this paper for a more detailed discussion of wireless LAN security issues.

Known 802.11 Security Vulnerabilities

The 802.11 wireless LAN standard incorporates three mechanisms to provide secure client access to wireless LAN access points, including the Service Set Identifier (SSID), Media Access Control (MAC) address filtering and Wired Equivalent Privacy (WEP).

The SSID segments the wireless LAN into multiple networks, each of which has its own identifier. For example, each department of a company might have its own network. To access one of the multiple networks within the wireless LAN, the client and access point devices need to be configured with the appropriate SSID. The SSID identifiers can be compromised by an attacker, so additional security measures are needed.

MAC address filtering increases security by requiring each wireless access point to be configured with the MAC addresses of authorized client devices. Only client devices with listed MAC addresses can connect through that access point. The weakness of this approach is that an attacker can intercept the MAC address by "sniffing," or eavesdropping to intercept packets on the network, then configure the attacker's wireless card on a client device with that MAC address to gain access to the network. Encrypting the data sent between the wireless client and access point can help protect against sniffing, but effective protection requires strong encryption algorithms.

Wired Equivalent Privacy (WEP) was originally designed to provide encryption and authentication as part of the 802.11 standard. It employs an encryption algorithm which utilizes a key, or sequence of numbers entered by the user. With WEP, wireless clients and access points are manually configured with the same key, which can be 40 or 128 bits in length. In 2001, research teams at UC Berkeley and the University of Maryland published separate papers that disclosed security

flaws in 802.11 WEP, including both its encryption algorithm and authentication protocols. Moreover, publicly available tools are available that are designed to enable the recovery of encryption keys. It is possible for an attacker to sniff network transmissions and then use these tools to determine WEP encryption keys.

Despite the security vulnerabilities of 802.11 with WEP, proven enterprise solutions are available now that permit the secure deployment of enterprise wireless LANs. These solutions include deploying a proven Virtual Private Network (VPN) solution over the wireless LAN. Another solution is the IEEE 802.1X standard, which is supported by wireless solutions from Intel and other vendors.

Virtual Private Network (VPN) over WEP-based Wireless LAN

A Virtual Private Network (VPN) enables users on a public or un-trusted network, such as the public Internet or a WEP-based 802.11 wireless LAN, to establish a secure connection to a private network. The VPN protects the wireless LAN by creating a tunnel that shields data from unauthorized access. VPNs are widely used to permit secure remote access to corporate intranets. VPNs enable a high level of trust through the use of proven industry-standard security mechanisms, including IPSec (Internet Protocol Security). IPSec employs strong algorithms such as Data Encryption Standard (DES) and Triple DES (3DES) to encrypt data, with other algorithms for authenticating data packets. IPSec also employs digital certificates to validate public keys. When used over a wireless LAN, the VPN gateway handles authentication, encapsulation and encryption.

The combination of an IPSec-based VPN and 802.11 with WEP provides a practical and scalable solution for the protection of mission-critical data transmitted over a wireless LAN. This solution can be implemented today to address the inherent limitations of WEP encryption. A VPN is a proven enterprise solution for remote access that offers protection against targeted attacks and snooping. Combining a firewall with a VPN effectively isolates the wireless LAN to protect data and access to enterprise networks. For maximum protection of mission-critical data, Intel recommends that business users continue to use VPNs and firewalls in enterprise wireless networks until all devices can be protected with *WiFi Protected Access* (WPA), which is described below.

IEEE 802.1X: Multiple wireless LAN vendors have adopted the IEEE 802.1X standard, a framework designed to provide controlled port access between wireless client devices, access points and servers. IEEE 802.1X uses the physical characteristics of the wireless LAN infrastructure itself to authenticate devices that are attached to a port, and to deny access to the port when authentication fails. It employs dynamic keys, rather than the static keys used in WEP authentication, and it requires an authentication protocol for mutual authentication. This standard is supported in many access point and client products currently available on the market, including Intel® PRO/Wireless PC Cards and Access Points. Microsoft has implemented support for 802.1X in Windows* XP, but some devices require driver and firmware updates.

RADIUS: For authentication to work, the user's transmission must go through a wireless LAN access point to reach the back-end server performing the authentication. RADIUS (Remote Authentication Dial-in User Service) is a widely-used authentication utility. The wireless client contacts the access point, which in turn communicates with the RADIUS server on the enterprise LAN. The RADIUS server then verifies the client's credentials to determine whether the device is authorized to connect to the LAN. If the RADIUS server accepts the client device, the server sends

data, including security keys, to the access point to enable a secure connection with the client.

EAP: The wireless access point and the RADIUS server communicate using Extensible Authorization Protocol (EAP), a point-to-point protocol that supports multiple authentication methods. The support for EAP types depends on the OS supported. Check with the manufacturer to be clear about EAP type support. The Cisco variant of EAP, known as "lightweight EAP" (LEAP) derives encryption keys for each user and for each session.

Due in 2003: Wi-Fi Protected Access (WPA)

The IEEE is at work on a number of security enhancements to the 802.11 standard, collectively known as 802.11i. To accelerate the implementation of robust wireless LAN security solutions by multiple vendors, the completed components of the 802.11i standard are being made available for release during the first half of 2003. This subset of the 802.11i draft standard is called *Wi-Fi Protected Access* (WPA) and is designed as a software upgrade to existing Wi-Fi certified hardware, while maintaining forward compatibility with the future 802.11i standard. WPA is expected to be implemented in wireless LAN products shipped in the latter half of 2003. It provides wireless LAN users with data protection while helping to ensure that only authorized users gain access to the network. WPA is designed to address all known WEP vulnerabilities, and can provide effective protection against both non-targeted and targeted attacks. Implementation of WPA will make it possible for enterprises to protect their campus wireless LANs with scalability, without deploying VPN/firewall technology.

WPA combines the functionality of 802.1X with Temporal Key Integrity Protocol (TKIP). Designed for deployment as a software upgrade to existing WEP-based 802.11 devices, TKIP addresses the vulnerabilities of the static keys used in WEP. TKIP implements rapid re-keying by generating a new encryption key every 10,000 packets and uses a mixing function to cryptographically hash the initialization vectors of data packets with the shared key. TKIP also incorporates message integrity checking to identify altered packets. TKIP is based on the same RC4 algorithm with 40-bit key used in WEP. The combination of 802.1X authentication, authentication protocols, dynamic keys and TKIP enhancements is a transitional step that enables enterprises to implement wireless LANs increased data privacy and integrity protection.

During transition period, network managers will be able to mix WPA-enabled devices with legacy non-upgraded 802.11 devices. Access points are expected to include a software-based "switch" that will allow mixed WEP or WPA-only stations. The danger of this approach is that devices which have not been upgraded will remain vulnerable to attacks. Since vulnerability of the network is defined by the weakest link, such non-upgraded devices (network interface cards and access points) should be upgraded to WPA as soon as possible. The real security value of WPA will only be realized when all stations have been migrated to WPA.

Intel® Wireless LAN Security Building Blocks for Notebooks

With Intel® Centrino™ mobile technology, three components work together to deliver a breakthrough in freedom and capability—so consumers can work, learn and play on the go***. These components include:

- Intel® Pentium® M Processor
- Intel® 855 chipset family
- Intel® PRO/Wireless network connection

Intel Centrino mobile technology architecture ensures that consumers are using innovative and reliable technologies that supports leading wireless security protocols. Intel Centrino mobile technology is being validated with leading VPN infrastructure products, and is available with Intel® PROSet software that supports VPN-capable profiles to enhance protection and ease of use. Intel Centrino mobile technology supports 802.11b wireless LAN ratified standards and enables wireless connectivity from wireless LAN networks—including thousands of hotspots worldwide. Intel is working with hardware and software developers and wireless services providers, to deliver a reliable and integrated wireless mobile computing experience.

Intel Centrino mobile technology will support WEP and 802.1X security protocols at launch. After WPA, 802.11i and other security standards are ratified, Intel intends to offer building block products that implement the standards.

In 2004: Hardware Support for 802.11i

By the end of 2003 the IEEE TGi workgroup is due to complete the 802.11i standard. New hardware is expected to be available in the first half of 2004 with support for full 802.11i capabilities, including Advanced Encryption Standard (AES) encryption. The 802.11i standard will enhance wireless LAN security in the following ways:

- Use of the 802.1X authentication standards for both new and existing 802.11 devices.
- A TKIP security update for existing 802.11 hardware, providing a robust software and firmware "wrapper" for WEP.
- A security plan for new access point hardware with enhanced encryption capabilities, based on AES.

New access point hardware will be needed with the processing headroom to handle AES while maintaining high levels of network performance. AES encryption is expected to be available as a software upgrade on notebook PCs and other handheld platforms with adequate processing capacity. Current roadmaps for Intel® network processors and mobile processors address the requirements of AES.

Conclusion: Wireless LANs Can Address Security Today

The greatest threat to the security of an enterprise wireless LAN probably results from the failure to implement the effective security solutions that are currently available. While 802.11 wireless LANs that only WEP utilize, have significant security vulnerabilities, current industry wireless security standards and leading wireless security protocols are supported by Intel® wireless LAN products and are available in solutions from multiple vendors. Virtual Private Network technology provides additional protection for mission-critical data, and it can be scaled to meet the needs of large networks. The IEEE 802.1X standard is a port-based authentication framework with dynamic distribution of session keys for WEP encryption.

The availability of these solutions makes it possible for enterprises to deploy wireless LANs now with security. The emergence of WPA-enabled devices in 2003 provides enterprises with a clear migration path from 802.11 with WEP to 802.1X to Wi-Fi Protected Access with TKIP, and ultimately to 802.11i security solutions with the robust encryption of AES.

Intel Access

Developer Web Site	developer.intel.com
Networking Components Home Page	http://developer.intel.com/design/network
Other Intel Support: Intel Literature Center	developer.intel.com/design/litcentr 800 548-4725 7am - 7pm CST (USA and Canada)
General Information Hotline	800 628-8686 or 916 356-3104 5am - 5pm PST

For more information, visit the Intel web site at: **developer.intel.com**

UNITED STATES AND CANADA
Intel Corporation
Robert Noyce Bldg.
2200 Mission College Blvd.
P.O. Box 58119
Santa Clara, CA 95052-8119
USA

EUROPE
Intel Corporation (UK) Ltd.
Pipers Way
Swindon
Wiltshire SN3 1RJ
UK

ASIA-PACIFIC
Intel Semiconductor Ltd.
32/F Two Pacific Place
88 Queensway, Central
Hong Kong, SAR

JAPAN
Intel Japan (Tsukuba HQ)
5-6
Tokodai Tsukuba-shi
300-2635 Ibaraki-ken
Japan

SOUTH AMERICA
Intel Semiconductores do Brasil
LTDA
Av. Dr. Chucri Zaidan, 940-10º andar
04583-904 São Paulo, SP
Brazil

Intel may make changes to specifications and product descriptions at any time, without notice.

[1]Gartner—*Technology Adoption and Value: Survey Results*—December 2002

*Other names and brands may be claimed as the property of others.

**Wi-Fi Alliance—*Enterprise Solutions for Wireless LAN Security*—January 2003

***Wireless connectivity and some features may require additional software, services or external hardware that may need to be purchased separately. Availability of public wireless access points is limited. System performance, battery life wireless performance and functionality will vary depending on your specific hardware and software configuration. See http://www.intel.com/products/centrino/more.info for more information.

Intel, Pentium and Centrino are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

For more information, visit the Intel Web site at: developer.intel.com

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life-saving, or life-sustaining applications.

Copyright © 2003 Intel Corporation. All rights reserved. USA/0203/NP/ASI/PDF Please Recycle 252554-001