



WIRELESS STANDARDS UPDATE Issue 10/2002

When transmitting data over the airwaves, the implementation of appropriate security measures are. The article below learns us that still a large amount of wireless networks are operational without any measure of security... The second article informs that the Wi-Fi alliance has started their interoperability tests for 802.11a products, enabling unification for these products.

CONTENT

<u>Page</u>	<u>Title</u>
1	Mapping the Lack of securit8
3	Wi-Fi start 802.11a product certification

✓ *Mapping the Lack of Security*

Anyone having a wireless network in place, or thinking about implementing one should consider some basic security criteria to protect their corporate and private data from malicious attacks. Knowing that a wireless network is yet another gateway into your network where the boundaries are not physically limited, these types of networks should be treated such as your existing wired networks in regard to the implementation of security measures and more...

It's a sobering statistic: 70% of the access points out there are running with out using any encryption. Worse, 27% are doing so while using the default SSID that came with the hardware, leaving it wide open to use by anyone in range with a Wi-Fi client.

These results were shared after a loosely organised "war-drive" session was held in August and September earlier this year. These people drive around with a wireless enabled laptop in their car and some basic software, scanning for un-encrypted "open" networks.

During that week, around 200 Wi-Fi-using enthusiasts and security professionals took to the roads of major cities in the United States and Europe to statistically log and map as many access points as possible. The goal: to make sure the public and the IT pros know that they need to start securing their wireless local area network (WLAN) connections.



The second is held starting from October 26 and goes through November 2. Currently, the war drivers are planning to drive around looking for open access in major North American cities as well as some smaller communities. In other continents, drivers will check in Barcelona, Spain; Seoul, South Korea; Johannesburg, South Africa; Sao Paulo, Brazil; and Wellington, New Zealand.

WWWD (World Wide War Drive) participants are also admonished not to use their accumulated wardriving data for their own gains. The goal is to provide general information about vulnerabilities in WLANs without getting specific. If the drivers have one message to share, it's probably 'don't use the factory settings.' The WWWD home page specifically lists basic ways to prevent anyone from outside your network getting unauthorised access: use a unique SSID, disable SSID broadcasting, turn on WEP encryption, and filter Internet access by MAC address of clients on the network.

Hopefully the results of this "war-drive" session will show that network managers have taken the necessary measures by implementing the correct level of security. By activating the security functionalities that are embedded in the wireless equipment, the large majority of malicious attacks can be stopped without any additional cost at all.

For your own benefit, don't be part of that 70% that leaves their network open to the public, enable security today!

✓ Wi-Fi Alliance Begins Wi-Fi Certification of 5 GHz IEEE 802.11a products

Availability of Multiple IEEE 802.11a Chipsets Allows Interoperability Testing to Begin

The Wi-Fi Alliance announced that Wi-Fi interoperability certification testing will begin on November 29th for 5 GHz IEEE (Institute of Electrical and Electronics Engineers) 802.11a based products. (Products based on 802.11a standard available in the United States today)

Testing will be conducted at the organisation's San Jose, California interoperability testing laboratory. The laboratory will begin accepting products into the testing queue on October 18, 2002.

The Wi-Fi Alliance began interoperability testing of IEEE 802.11b based products in March of 2000. There are currently over 450 Wi-Fi CERTIFIED products in a broad range of platforms and applications on the market today.



The 802.11a interoperability testing has been initiated because a basic requirement of the Wi-Fi Alliance has been met – the availability of multiple products based on a second IEEE 802.11a chipset. The announcement of a second chipset was made in mid-April of this year and products were available for testing two months later. The availability of products allowed the Wi-Fi Alliance to develop the interoperability “benchmark” test bed, which is the reference that all products are tested against. There are currently four access points and five station cards from seven different manufacturers based on three different chipsets in the “benchmark” test bed. Products that pass the certification will be granted the Wi-Fi CERTIFIED seal of interoperability.

“This is an important step in the development of a broad range of future products, and provides the foundation for the dual band (IEEE 802.11a and 802.11b) product interoperability testing”

These interoperability tests on 802.11a-products available in the United States will prove great value to when these products become widespread available over Europe. Dual-mode 802.11 a/b radiocards will become available which allow you to seamlessly integrate 802.11a and 802.11b wireless equipment.