



# Wireless LAN Security

Peter J. Welcher and Marty Adkins

## Introduction

This article continues the series started last month, with an article introducing Wireless LAN Technology. The previous article can be found at <http://www.netcraftsmen.net/welcher/papers/wireless01.html>.

We'll start with an instant update: some timely links. Then we give an assessment and overview of the current State of Wireless LAN security. Given our space constraints, we can't provide you with all the details of all the protocols and ideas that are floating around. So we include a set of links you can follow if you desire more in-depth information.

## Recent Links

When one writes about new technology, things change. Fast. So we'll start with some update items that might be of interest.

The term "Wi-Fi" is apparently now going to be applied to both 802.11b and 802.11a, instead of calling the latter "Wi-Fi5". This strikes Pete as a bad choice, leading to possibly incompatible Wi-Fi-compatible devices. See the article at [http://www.80211-planet.com/news/article/0,,1481\\_1428541,00.html](http://www.80211-planet.com/news/article/0,,1481_1428541,00.html).

We also have delays in 802.11g until next May, and another quasi-standard (chip technology from Texas Instruments) called 802.11b+. See [http://www.extremetech.com/print\\_article/0,3998,a=29831,00.asp](http://www.extremetech.com/print_article/0,3998,a=29831,00.asp). Cisco's current positioning on 802.11g appears to be that it is a speed upgrade to 802.1b. Dual radios are here to stay?

Fluke is offering a free Wireless LAN Poster. See <http://www.flukenetworks.com/wireless>.

Qualcomm is apparently implementing 802.11 features into future CDMA chips for cell phones. See [http://www.80211-planet.com/columns/article/0,4000,1781\\_1438661,00.html](http://www.80211-planet.com/columns/article/0,4000,1781_1438661,00.html).

## What's Up with Wireless LAN Security

"Wireless is like having an RJ45 jack in the parking lot."

In other words, WLAN provides physical access to your corporate network from outside the building, and along with that comes ability to snoop on others' traffic. To secure this, we need to deny access to intruders, and we also need to securely negotiate a good encryption key and then encrypt packets so intruders can't snoop on our messages.

So you can see there are two main aspects to securing WLAN:

- Device and/or user authentication (preferably two-way)
- Good encryption technology (key management and rotation, solid encryption mechanism)

We'll briefly look at each of these. I'll stay in "executive summary mode". I think you can pick up enough information about unfamiliar terms from the context. If not, the links are good detailed references (and much longer than this article can be). If the acronyms start getting to you, just go to the next main section, where we provide a summary of the state of WLAN security.

## Authentication Techniques

- Open System Authentication (i.e. "none")
- SSID as Authentication
- Shared Key Authentication
- MAC Address Authentication (access list)
- 802.1x and Extensible Authentication Protocol (EAP)

Brief comments:

- Open authentication is a common default, and really does equal no security.
- The WAP's SSID is broadcast in clear text form by WAP and client, hence can be obtained by snooping on traffic. This is true even if you turn off SSID beaconing by the WAP.
- MAC addresses are sent in the clear, hence can be obtained by snooping. The attacker may then change their wireless NIC MAC address to match.
- Do you really want to manage hundreds of MAC addresses anyway?
- Shared keys are feeble to begin with (employee leaves, laptop stolen, etc.).
- The 802.11 protocol does not adequately secure transmission of the shared key. Attackers can determine both the shared authentication key and the key used in the authentication process. That authentication process key is re-used as the WEP key, which means not only the authentication but subsequent encryption are compromised.
- At any scale, you really want centralized authentication administration.
- Authentication should authenticate client to network but also authenticate the network device to the client. Methods that do not do so are vulnerable to a "man-in-the-middle" attack, where a hacker's computer masquerades as the WAP.

The 802.1x standard is the newest approach. It uses a RADIUS server for authentication, with some form of credentials transferred using the Extensible Authentication Protocol (EAP). The credentials are either username/password or a security certificate. There are currently four EAP methods in use, and one new proposed version:

- EAP-MD5
- EAP-Cisco Wireless (or LEAP)
- EAP-TLS (Transport Layer Security)
- EAP-TTLS
- PEAP

Comments:

- EAP-MD5 does no key management or dynamic key generation, and hackers can learn the WEP key as before. There is also no WAP authentication, so attackers can use a rogue WAP to fool clients. One-way authentication is just not secure enough. "Just say no!"
- LEAP dynamically generates session keys. You can also have dynamic change of key every few minutes. And LEAP does two-way authentication. All this is good.
- LEAP uses MS-CHAPv1 authentication, which can be compromised with work (potential weakness). And other vendors have not added LEAP to their client software (yet), some may have work in progress to sell into all-Cisco-WAP environments using LEAP.
- EAP-TLS comes from Microsoft, cf. RFC 2716. It uses certificates instead of username and password. EAP-TLS does two way authentication and dynamic key generation. Drawbacks: EAP-TLS requires Public Key Infrastructure for certificates (PKI). And the easiest way to deploy EAP-TLS is MS clients using and logging into Active Directory.
- EAP-TTLS has authentication via username and password, with the WAP using a certificate to authenticate to the client.
- PEAP: Microsoft and Cisco combined to draft this coming standard, which apparently revises Funk's EAP-TTLS.

In short, right now you end up picking and choosing which \*EAP\* protocol to use based on which vendors' gear is in your network, and also on what each vendor supports. All of this takes research and time.

The University of Maryland Mishra-Arbaugh paper mentions some Denial of Service attacks that can take place with vanilla 802.1x, see [below](#). You really need keys securing management and control protocols. Cisco's [response](#) to the University of Maryland paper notes this.

See also the [ArsTechnica article](#) mentioned below, it was very concisely informative and readable!

## Encryption Technologies

- Key Management (how is the key communicated or agreement checked)
- Key Rotation (changing the user's key periodically)
- Broadcast Key Rotation (periodically changing the key used with broadcast packets)
- WEP Encryption
- 128 bit WEP (Lucent WEP Plus)
- IPsec Encryption
- TKIP Encryption (Temporal Key Integrity Protocol)

TKIP is an enhancement to WEP proposed by Cisco. TKIP relies on per-packet keying and Message Integrity Check (MIC). These mitigate the ability of a WEP hacker to crack the key (it keeps changing) or to perform man-in-the-middle replay of packets (due to message integrity check detection of tampering, plus sequence numbers).

Comments on these techniques...

- WEP key management can be painful. You may have to touch each wireless device. Changing keys can be a good practice. Managing keys across hundreds of users really requires a power tool. Whatever the encryption scheme, you'll want key management tool(s).
- If the IT group's PC setup process leads to a single WEP key across many users, then you have a process problem: lose a laptop or have one person leave the WEP key lying around, and you're compromised.
- Changing the encryption scheme "frequently enough" is a well-known technique for defeating hackers. The objective is to change the key before a hacker can accumulate enough data to compromise the key.
- The RC4 stream cipher used in WEP is insecure (weak). The key can be found by analyzing sufficient data (using a tool such as AirSnort). Some of the WEP initialization vectors (IVs) that pad key length are weak and can also be found by capturing enough packets, leading to key compromise.
- 128 bit WEP extends WEP keys from 40 bits to 104 bits. This increases the time for brute force cracking of keys -- but the above attacks against WEP don't use brute force!
- Various vendors automatically rotate the broadcast key (used to encrypt broadcast frames). Doing so every 10 minutes can deny attackers time to crack the key. This does help secure broadcasts but not ordinary traffic.
- You always have to consider attackers bypassing the WAP and transmitting directly to an IPsec user's PC. Some form of personal firewall is needed. Unless your IPsec client allows you to force all traffic to and from the client to be via the IPsec concentrator.
- Unless your WAP forces IPsec use, two hackers may still be able to use the WAP to communicate or deny service by using up the bandwidth.
- Correctly implemented IPsec VPN's can really help secure WLANs, despite the above, but this does increase the administrative hassle.
- IPsec can be a performance drain. Buying IPsec concentrators for all wireless users to connect through could add considerable cost. On the other hand, once you've done that you're ready to fully support mobile users connecting in whatever way is available.

The consensus is that Wireless Equivalent Privacy (WEP) does a weak job of authenticating devices, and that it typically selects poor unchanging keys and does not constitute good encryption technology.

The 802.11i standards effort is attempting to rectify the WEP security situation.

A good thought from the [University of Maryland document below](#) is that we're used to firewalls securing the outside of our networks. We may consequently have done less to secure the hosts in the network, feeling that the firewall was enough. Now with WLAN we are providing direct internal access to the network. This means we really should re-examine our security strategy. It might indeed be time to harden the hosts and servers. And regularly check patch levels in an automated way.

## The State of Wireless LAN Security

Wireless LAN security has received plenty of press during the past year. Everyone agrees that Wireless Equivalent Privacy (WEP) really isn't equivalent at all, regardless of whether the key is 40 bits in length, as required by 802.11b, or 128 bits in length, as most vendors now support. The first flaws were documented and reported by Jesse Walker in October 2000. Yet 19 months later, there still is not a single comprehensive solution implemented by most vendors.

A rather lucid treatment of WLAN security is in the Cisco white paper titled *Wireless LAN Security in Depth*, at [http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl\\_wp.htm](http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm). A good treatment from three researchers at University of Maryland is in *Your 802.11 Wireless Network Has No Clothes*, <http://www.cs.umd.edu/~waa/wireless.pdf>. Both of these explain the basic folly of simplistic 802.11 remedies such as not broadcasting the SSID, MAC address access control, and shared key AP association. More detailed information is also available in the Cisco white papers listed below ([cisco1](#), [cisco2](#)).

It appears that most vendors have implemented some form of key rotation while waiting for 802.11i, but these are proprietary. This means client and WAP must both be from the same vendor. The other approach is to use an overlay security package from a vendor such as [Wavelink](#).

Most wireless vendors have now rallied behind the forthcoming IEEE 802.11i security enhancements. Draft 2 of 802.11i completed ballot in May 2002, so vendors should be working on compliance. In the interim, vendors have modified their WEP implementations on both clients and APs to address the known vulnerabilities. Techniques include broadcast key rotation, Temporal Key Integrity Protocol (TKIP) to prevent interception a la Aircsnort, and Message Integrity Check (MIC) to prevent man-in-the-middle and rogue AP attacks.

Still, WEP involves a shared password, which is definitely not appropriate for an enterprise. Say 5000 users have it, and one leaves or loses a card. What do you do then? Realizing that enterprises require per-user authentication, vendors have also implemented wireless extensions to 802.1x, a standard for port-based access control in switches. But there are four variants plus proprietary extensions! The Cisco links below go into some detail on the variants.

Since Microsoft already provides support for 802.1x in WindowsXP, it has jumped on this bandwagon as well. Accepting that few enterprises would upgrade to WindowsXP just to gain 802.1x authentication, Microsoft has committed to offer the EAP-TLS variant for all supported Windows O/S (not Windows 95) during 2Q2002. For more information on this, see <http://www.microsoft.com/windowsxp/pro/techinfo/administration/wirelesssecurity/default.asp>. See also <http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/secwireless.asp> about EAP-TLS support. Microsoft may have committed to support platforms other than XP but there has been no visible progress on any other than Pocket PC.

One of the most popular vendor extensions is Cisco's Lightweight Extended Authentication Protocol (LEAP), which can utilize a RADIUS authentication server. While it appears to be a solid interim workaround, it requires Cisco software running on every client. Moreover, Microsoft has stated its intention to create yet another protocol/approach called Protected EAP (PEAP) which relies on their MSCHAPv2 and has this under discussion in an IETP working group. Lucent/Agere has their workaround, Proxim planned theirs for July 2002, and so on. Each of these methods requires special client software and/or an O/S patch. And none support one-time passwords (token cards). Ugh!

But won't this just settle out and we'll all be happy with a common 802.11i solution? No time soon, it appears. Plus Cisco and other vendors have announced their intention of migrating from DES to the new AES encryption standard sometime in 2003. Only the newest products will be upgradeable (in Cisco's case, the Aironet 1200). And finally in February 2002, Mishra and Arbaugh of the University of Maryland pointed out two security flaws in the 802.1x standard!

So what to do? All of these seem to have forgotten the poor user and support staff. Yet ignoring WLAN security is not an option! The easiest alternative in many organizations may be to use the existing IPsec VPN solution for all WLAN clients. Advantages:

- Per-user authentication utilizing existing platforms and administration. It's treated identically to other VPN-type access.
- Same method, same client configuration, and same user procedure regardless of physical location or remote access method - DSL, cable modem, hotel, airport, or internal WLAN. (Is "internal WLAN" an oxymoron?)
- Not tied to a particular WLAN client (vendor-neutral).
- Users sharing the same AP are totally isolated from one another - WLAN sniffing is ineffective.

The disadvantages and issues to be resolved are:

- Roaming - when the client reassociates to an AP assigned to a different IP subnet, the IPsec tunnel has to be torn down and re-established (user must authenticate again). This is largely a design issue of how WLANs are connected and addressed in the enterprise network. Ideally, all WLANs within a building (switch block pair) will be one IP subnet. There are scaling and other tradeoffs to be worked out.
- Performance impact of VPN software on the client (WEP is performed in hardware).
- IP multicast does not map well to many VPN tunnels running over the campus.
- How to prevent WLAN access prior to VPN authentication. A combination of protocol filters on a Cisco WAP could be configured to pass only DHCP, DNS, and VPN traffic. Also, enabling a Cisco feature called Publicly Secure Packet Forwarding (PSPF) prevents WLAN clients on the same AP from communicating with each other.
- QoS. Unless the IPsec client sets ESP tunnel header ToS bits from IP header bits, the WLAN driver probably cannot see the information it needs to prioritize delay-sensitive traffic, e.g. VoIP. (Important if/when your CDMA cell phone does 802.11 inside the building.)

## Further Reading

**Wireless LAN Security****Link**

NIST DRAFT  
SP800-48  
wireless

<http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>

NASA White  
Paper on the  
Wireless Firewall  
Gateway

<http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/index.html>

University of  
Maryland *Your  
802.11 Wireless  
Network Has No  
Clothes*

<http://www.cs.umd.edu/~waa/wireless.pdf>

University of  
Maryland *An  
Initial Security  
Analysis of the  
IEEE 802.1x  
Standard*

<http://www.cs.umd.edu/~waa/1x.pdf>

Ars Technica  
*Wireless Security  
Blackpaper*

<http://www.arstechnica.com/paedia/w/wireless/security-5.html>  
Parts 1-4 are also interesting.

WLANA Security  
links

<http://www.wlana.org/learn/security.htm>

*Cisco Aironet  
Wireless LAN  
Security  
Overview*

[http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w\\_ov.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm)

Cisco A  
*Comprehensive  
Review of 802.11  
Wireless LAN  
Security and the  
Cisco Wireless  
Security Suite*

[http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.htm)

Cisco *SAFE:  
Wireless LAN  
Security in Depth*

[http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl\\_wp.htm](http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm)

Cisco *Security for  
Next Generation  
Wireless LANs*

<http://www.cisco.com/warp/customer/102/wlan/nextgen.html>

Cisco  
*Authentication  
with 802.1x and  
EAP Across  
Congested WAN  
Links*

[http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp\\_an.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp_an.htm)

Cisco Aironet  
*Response to  
University of  
Maryland's Paper*

[http://www.cisco.com/warp/partner/synchronicd/cc/pd/witc/ao350ap/prodlit/1680\\_pp.htm](http://www.cisco.com/warp/partner/synchronicd/cc/pd/witc/ao350ap/prodlit/1680_pp.htm)

Microsoft WLAN  
Security White  
Paper, *Making  
IEEE 802.11  
Networks  
Enterprise-Ready*

<http://www.microsoft.com/windows2000/docs/wirelessec.doc>

Microsoft  
Windows 2000  
Marketing  
Bulletin, *Wireless  
802.11 Security  
with Windows XP*

<http://www.microsoft.com/windowsxp/pro/techinfo/administration/wirelesssecurity/default.asp>

Microsoft,  
*Microsoft Leads  
in Securing  
Wireless  
Networks*

<http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/secwireless.asp>

CMP  
Publications,  
*Wireless  
Security: Why  
Worry?*  
(TechWeb.com:  
August 5, 2002)

[http://www.techweb.com/tech/mobile/20020212\\_mobile](http://www.techweb.com/tech/mobile/20020212_mobile)

Proxim Security  
White Paper

[http://www.proxim.com/learn/library/whitepapers/pdf/harmony\\_security.pdf](http://www.proxim.com/learn/library/whitepapers/pdf/harmony_security.pdf)

## The Operational Side of WLAN

There are two scary things about Wireless LAN technology (WLAN). The first is that it is very inexpensive, so anybody can go to the local Best Buy and pick up a cheap generic box and install it. The second boils down to the quotation above. By the way, a well-known retail chain made the WLAN news when someone in the parking lot of one of their stores was capturing credit card transactions in the clear from store 802.11b mobile cash registers! (Oops!) Your organization probably does **not** wish to appear in the news headlines for such a security breach, either.

The first item reminds me of the wild days of pulling cable, and then finding out who'd been a little too enthusiastic about the **PULL** part of that. I don't think any networking organization wants to have to go diagnose WLAN dead zones. My current candidate for the most fun to find: conflicts between WAP's that two groups installed with overlapping coverage -- on different floors, yet.

The second item speaks for itself. Unless the organization puts in place an coherent policy with teeth on wireless security, you will have none. All it takes is one uncontrolled WAP and your network is in principle physically compromised.

Both items imply to me that one wants the IT organization out in front leading on this one as much as possible, before you have Do It Yourself (DIY) entrenched. I'd also help the person responsible for security run a memo up the chain of management ASAP, to get policy put in place. If management will not support a strong security policy on this, you need to get that in writing to CYA for the inevitable security incident. Or else start preparing your resume (list your last position as "fall guy").

If you need help in figuring out the technical side of things, or presenting the business case to upper management, the Cisco Networkers 2002 slides are a good resource. Contact your Cisco AM or SE for PDF versions, or ask your buddies for the URL. (The PDF's are publicly accessible but we're reluctant to give the URL since Cisco's web site doesn't show a visible link to this area.) Cisco makes a good argument for manageable WAPs for the Enterprise, and Cisco also seems to have a good handle on the security issues.

Since this is a key issue for major enterprises, you can also expect vendors to provide tools to help detect and cut off rogue

WAPs.

## WLAN Network Management and Security Management

CiscoWorks Wireless LAN Solution Engine Software Version 1.0 was recently announced. It is software that runs on the Cisco 1105 hardware (1 RU high). The management interface is web-based. CiscoWorks WLSE apparently allows template-based configuration of large numbers of access points and bridges from a central location. It provides security alerts for misconfigured access points and bridges. WLSE also monitors the WLAN infrastructure (WAPs and connected switches), and also the LEAP authentication server. It reports on WAP utilization and also on client associations. WLSE can provide syslog or SNMP trap notifications to the central Network Management Station (NMS). It can also notify the administrator of problems via email. Links:

- [http://newsroom.cisco.com/dlls/prod\\_061702.html](http://newsroom.cisco.com/dlls/prod_061702.html)
- <http://www.cisco.com/univercd/cc/td/doc/pcat/cwwlanse.html>
- <http://www.cisco.com/warp/customer/cc/pd/cxsr/1105/ps3915/>

From Networkers 2002 slides I see that Cisco is partnered with *wavelink*, which has software to detect rogue access points and to rotate WEP keys automatically (on both WAP and mobile devices). See also <http://www.wavelink.com>. Network World had a brief article about Wavelink, see <http://www.nwfusion.com/newsletters/wireless/2002/01209376.html>. The key point is that multiple vendors support Wavelink because it complements their solution. Cisco's position: LEAP doesn't run on all WLAN clients, and there is a large costly installed base of legacy clients. Wavelink provides key rotation for such clients.

A company named AirDefense has some interesting web pages. They sell appliances and server and application software that detect rogue WAPs and ad hoc wireless networks, among other things. Their software also seems to have some IDS functionality to it. They claim support for gear from Cisco, Symbol, 3Com, Linksys, Lucent, and Apple. You can check them out for yourself at <http://www.airdefense.net/>. Other vendors are also starting to push the idea of detecting rogue WAPs.

Web search also turned up *airwave*, at <http://www.airwave.com/>. The web pages claim the software works with devices from all vendors.

There is currently a plethora of WLAN network management products, many more than will eventually survive, and certainly more than we've listed above. If you know of any other **good** ones, please email me (Pete).

I'm puzzled why a couple of the above vendors want me to register to get their white paper advertising their product. Is this a trend? They want me to read this white paper and buy their product, don't they? So why do they put in place something that discourages me from obtaining the white paper? I know they'd like a sales lead, but I generally do not want sales people calling me.

## Conclusion

We finish with a couple of odds and ends.

(Pete) At this point, I have no idea what next month's article will be about. Please do send email and let me know what you'd be interested in. And thanks to those who did so and haven't seen anything in print yet: there have been several good suggestions that I intend to get to Some Day Soon.

## 802.11 Standards

In case you're suffering 802.11 overload (which 802.11<letter> means what), we offer the following table:

802.11 Standard	Purpose
A	5 GHz, 54 Mbps
B	2.4 GHz, 11 Mbps
D	Multiple regulatory domains (more countries)
E	QoS
F	Inter-Access Point Protocol (IAPP)

G	2.4 GHz, 54 Mbps
H	Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) (European requirements)
I	Security

## A Good Book

(Pete) If you're looking for a good read, you might consider getting the book, *Troubleshooting Campus Networks: Practical Analysis of Cisco and LAN Protocols*, by Priscilla Oppenheimer, Joseph Bardwell. Published by Wiley, 608 pages, list price \$55, ISBN 0471210137. See also <http://www.amazon.com/exec/obidos/ASIN/0471210137/> . I've been reading bits and pieces and enjoying the wealth of accurate technical information in the book. The book contains a chapter on troubleshooting WLAN, and was published just in time for these articles!

---

Dr. Peter J. Welcher (CCIE #1773, CCSI #94014) is a Senior Consultant with Chesapeake NetCraftsmen. NetCraftsmen is a high-end consulting firm and Cisco Premier Partner dedicated to quality consulting and knowledge transfer. NetCraftsmen has nine CCIE's, with expertise including large network high-availability routing/switching and design, VoIP, QoS, MPLS, network management, security, IP multicast, and other areas. See <http://www.netcraftsmen.net> for more information about NetCraftsmen. Pete's links start at <http://www.netcraftsmen.net/welcher> . New articles will be posted under the Articles link. Questions, suggestions for articles, etc. can be sent to [pjw@netcraftsmen.net](mailto:pjw@netcraftsmen.net) .

Marty Adkins (CCIE #1289, CCSI #93021) is also a Senior Consultant with Chesapeake NetCraftsmen. Marty specializes in network design and strategic advice, as well as troubleshooting. Marty's expertise includes routing, switching, ATM and wireless. Marty has taught the Cisco Internetwork Troubleshooting (CIT) course for years, using the "salvo" approach with many problems to fix. His teaching and advice has helped many down the path to their CCIE. He also used to run "instructor boot camp" and produced many fine Cisco certified instructors.

---

9/4/2002

Copyright (C) 2002, Peter J. Welcher