

Wireless Attacks and Penetration Testing (part 3 of 3)

Jonathan Hassell 2004-07-26

In the previous two installments ([part one](#), [part two](#)) of this series, I've discussed the types of attacks your wireless network is subject to see and some techniques you can use to pen-test your WLAN. In this final part, I'll look at ways to mitigate the risks I've outlined in the previous parts of the article and spend a bit of time looking at some proposed solutions currently in front of the IETF.

Basic Steps to Fix WEP Problems

There are a few different procedures you can perform to temporarily fix problems with WEP. Think of these as "do these immediately" items, meant to be implemented as soon as practical.

- Use longer WEP encryption keys, which makes the data analysis task more difficult. If your WLAN equipment supports 128-bit WEP keys, use it and don't accept anything less.
- Change your WEP keys frequently. There are devices that support "dynamic WEP" which is off the standard but allows different WEP keys to be assigned to each user. Increasing the number of WEP keys in use increases the difficulty a hacker will encounter in cracking it. Since dynamic WEP is non-standard, implementations from different vendors are usually inoperable; stick with one manufacturer.
- Place APs only on their own firewalled interface. Locate all access points outside your internal LAN, on a separate firewall interface on the firewall server/device.
- Use a VPN for any protocol, including WEP, that may include sensitive information.
- Implement a different technique for encrypting traffic, such as IPSec over wireless. To do this, you will probably need to install IPsec software on each wireless client, install an IPsec server in your wired network, and use a VLAN to the access points to the IPsec server. (Obviously, this is not an inexpensive proposition.) Using this method, WLAN users establish an IPsec tunnel to the IPsec server, thereby encrypting all wireless traffic through this tunnel. IPsec clients and servers are available from a number of vendors; there's even an open source implementation.

There's also the option of upgrading firmware on your network devices, which deserves some extended discussion. One reader, in response to [part two](#) of this series, wrote, "I run pen tests all the time and the weak IV exploit is virtually non-existent. The manufacturers have eliminated that issue, at least as far as I have been able to tell. I have only been able to crack

it once in the past several years and that was because an old wireless adaptor with outdated firmware was on the system." Indeed this can be the case. The developers of AirSnort indicate that some NICs and access points no longer generate the initialization vectors (described in part two of this series) that result in the WEP key being easy to crack. The lesson here is to update the firmware on all of your NICs and access points, and if you're using wireless adapters that are two years of age or older, consider investing in new ones.

However, don't only look at the symptoms going away: look at the problem. Since WEP uses RC-4, and RC-4 demands that you only use a key once and then never reuse it, WEP *is* inherently flawed. The only mechanism built into the protocol that changes the key is the 16-bit IV value. It's built into the protocol that every 65,536 packets, the IV changes. No matter how firmware is upgraded, once that value is looped again, that's the weakness and that's an easy way in. Firmware upgrades shouldn't be ignored, but they also shouldn't be considered anything more than a stopgap measure while you evaluate a WPA implementation that suits your needs.

WPA-PSK and WPA-Enterprise

Now that you've implemented stop-gap measures, let's take a look at some possible permanent fixes to mitigate WLAN security risks. Up to this point, you might be thinking that the easiest way to rid yourself of the insecurities of WEP is to rid yourself of WEP period. And that's not a bad idea. The wireless community has responded to the problems and issues with WEP by introducing a new sort of security scheme, known as WPA, or Wi-Fi Protected Access.

A foundation of WPA is the Temporal Key Integrity Protocol, or TKIP. In short, TKIP does what WEP doesn't: the TKIP algorithm is stronger than the WEP encryption mechanism but can be done on existing wireless hardware. TKIP verifies the security configuration after encryption keys are determined and synchronizes by changing the unicast encryption key for each frame-- this means no more static keys to break.

To be completely honest, that's actually not exactly true. Consider one variation of WPA, called WPA Pre-Shared Key (WPA-PSK). WPA-PSK is a simplified but still powerful form of WPA most suitable for small business and home office networking. To use WPA-PSK, a person does set a static key initially, like with WEP, but WPA uses TKIP and automatically changes the keys at a preset time interval, making it much more difficult for hackers to find and exploit them. So while there is still a static key, it's much more difficult to break and find.

Another variation of WPA is known as WPA-Enterprise, which requires the TKIP encryption as described above plus a back-end authentication server or device of some sort, and the use of EAP, or the Extensible Authentication Protocol. In EAP, RADIUS packets are wrapped in EAP messages and sent to a RADIUS server on the back end. The RADIUS server then decrypts that message and looks at the RADIUS packet contained therein; it finally communicates with other devices to determine if that access should be granted, wraps the result into another EAP message, and then communicates with its client. This type of communication is known as EAP-over-RADIUS.

All of this isn't to say that WPA and its associated mechanisms don't have problems. Robert Moskowitz of ICSA Labs has found that WPA passphrases containing dictionary words less than 20 characters long could possibly be cracked. This is made possible partly because a cracker can make an access point regenerate the key exchange with the client in less than 60 seconds. Even though the key exchange is indeed secured, it can be extracted and cracked offline. Choose your passphrases carefully.

Another concern is the fact that EAP itself transmits information in clear text; it doesn't do any sort of encryption, and because of the sensitive nature of the data it transmits, this is a genuine issue. Transport Layer Security, or TLS, was initially used to encrypt EAP sessions, but this requires the placement of certificates on all possible clients. TTLS was then seen as a fix to this problem, but Microsoft and Cisco also released Protected EAP, or PEAP, which addresses the same problem in a different way. Most experts familiar with the battle between the proposed standards say PEAP is a given winner.

If you have a Windows infrastructure, you can enable WPA by moving to Windows XP (either edition) with Service Pack 1. You will also need to download the WPA support patch, which can be found at <http://support.microsoft.com>. Windows XP Service Pack 2 will include support for WPA out of the box, with no need for an additional patch.

Of course, of the two solutions, WPA-Enterprise is the safest and most secure, but what if you don't want to invest in an expensive RADIUS server backend? Linksys senses this need and has "Wireless Guard," which works like an outsourced RADIUS environment, integrated into the latest models of their Wireless-G access point products. Here's how it works, in a nutshell: when a user connects to the wireless network, he is prompted for a username and password as usual. The access point takes these credentials and establishes a secure link over the Internet to Linksys' RADIUS servers in their datacenter and attempts to match the given credentials to a

list of authorized users, configured by your organization's administrator. Access is granted if the credentials are valid; if not, access is denied, and the administrator is sent a note about the attempted intrusion. Meanwhile, all data and traffic on the wireless network is completely encrypted as described above. The Wireless Guard technology is an easy way to implement WPA-Enterprise in smaller organizations. The pricing is reasonable for the functionality provided; visit <http://www.linksys.com/wirelessguard> for more information.

Looking to the Future

While WPA is a very good current solution, the best is yet to come: 802.11i, which is really the panacea for which we're all searching. 802.11i also includes TKIP, which results in a keyspace that would take 100 years of continuous transmission to fully deplete. The new specification also includes a more efficient and direct mechanism to detect packet tampering.

But most importantly, 802.11i adds the Advanced Encryption Standard (AES), which supports a longer and more secure stream of data than TKIP alone. AES is currently in wide use over the globe and has been adopted by the US government, and it's effectively impenetrable. While the AES keys will be the same length as TKIP keys--128 bits--the underlying algorithm is many times stronger. The downside of using AES is that the cryptography is very calculation-intensive and it may be difficult to find a current device that can support these extensive operations and provide reliable, acceptable performance to the end user at the same time.

802.11i will also support 802.1x and the Extensible Authentication Protocol (EAP). Using 802.1x authentications, clients have several defined roles, and the roles applied to them dictate the network access allowed to the client until his identity is approved by some back-end authentication server, like RADIUS as described earlier. EAP is used to funnel messages back and forth. This mechanism can also be used to either provide new keys to everyone on a regular basis (which isn't required) and to provide unique master keys to each individual client, further reducing the risk of key interception and ensuring someone gaining access to one key can't access traffic encrypted using other keys from other clients.

Wrapping it Up

In this series, we've examined wireless security in detail and looked at very common techniques crackers use to gain unauthorized access to your wireless network. We've also discussed ways to mitigate the risks that the WEP protocol introduces and looked to the future at 802.11i, the

real solution for security over the airwaves. While one can imagine that wireless networks will likely never be as totally secure as wired connections simply because of their nature, there are many good things to come to ensure WLAN integrity is protected as much as our current technology allows.

About the author

[Jonathan Hassell](#) is an author and consultant specializing in Windows administration and security. He is the author of *Managing Windows Server 2003* and *RADIUS*, both published by O'Reilly & Associates, and *Hardening Windows*, published by Apress. He also holds periodic public seminars; see www.hardeningwin.com for details. He has written for *Windows & .NET Magazine* and *WindowsITSecurity.COM* and is a contributor to *PC Pro*, a leading computer magazine in the United Kingdom.

View [more articles](#) by Jonathan Hassell on SecurityFocus.

Comments or reprint requests can be sent to the [editor](#).

[Privacy Statement](#)

Copyright 2006, SecurityFocus