Safe travels

Wireless security in this modern world

L. Victor Marks (lvmarks@mac.com)
Freelance writer
June 2002

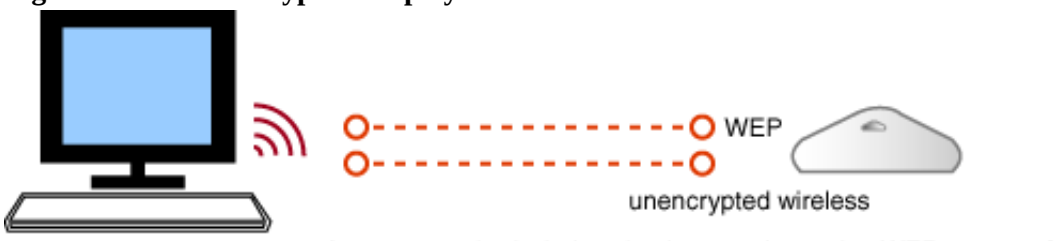
When many people think about wireless security, they think about Internet Protocol security and Virtual Protocol Networks -- what many fail to realize is that wireless security is also a social problem.

Certainly, in manager-speak, everything must be the ultimate in secure, but this, as most of us realize, is unattainable. There is no such thing as completely secure -- only more and less secure. Wireless is only as vulnerable as a wire that can be tapped. Therefore, when we talk about wireless security, we're talking about raising the bar higher so that only the desperate will attempt an attack.

Most everyone put up a huge fuss about WEP (the wireless equivelency protocol) and its inability to lock down connections to an impossibly Fort Knox-like level. This article discusses the technological advances since WEP, the brief steps you can take in either wireless *or* wired (because WEP was never meant to be more secure than a plain, unencrypted wire), and, finally, why security is such a big deal.

Wireless transmission and receival requires being within some close physical range; or, if further away, having a larger antennae or equipment. If you're that big a target, are there things you can do to lessen your attractiveness as one? Can you improve physical security, either through traditional means, or by making your building a Faraday cage that will block radio signals? 99.999% of the world is, on the whole, honest, and if you can figure out what may make you an appealing target, you can minimize your attractiveness as such. I do not recommend running without some security measure, but do understand that security is not a perfect end. Security is a goal that we strive for, and along those lines, it's worth examining some reasonable measures to take, and which measures are unnecessary.

Figure 1. WEP in its typical employ



A pretty standard wireless implementation, using WEP on top of 802.11b

A technological and social problem

First, you have no business putting someone else's security at risk. Whether in a home or an office

environment, if your own lack of security jeopardizes someone else's, this is unacceptable. Although absolute security doesn't exist, learn what you can do to weigh security in your favor. For instance:

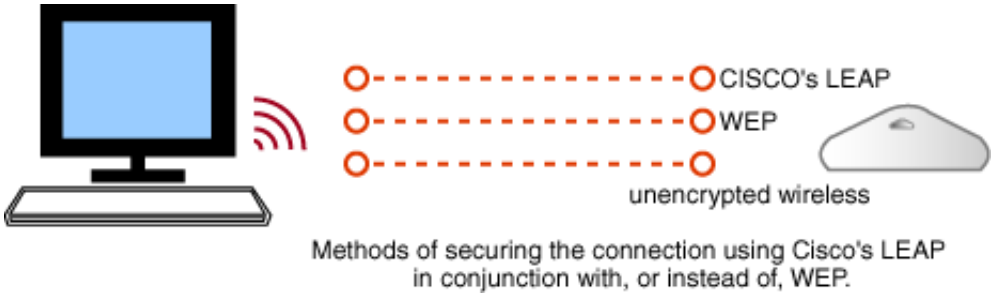
- Is there anything you can do to minimize your appeal as a target?
- Is your physical security in place, so that you would know if someone were lurking close by?
- Do you encrypt your packets? This costs a bit of bandwidth, but is well worthwhile.

WEP and other choices

Secure the connection between the wireless device and its base station.

Extensible Authentication Protocol (EAP), Lightweight EAP (LEAP), and a proper VPN, are all methods of weighing in on the side of greater security. On a small home wireless network, even configuring your access point to only allow connections from the MAC addresses of your wireless cards can help prevent intruders, who would have to spoof your MAC address to leech off of your network. Leeching your bandwidth (browsing, looking into your file shares) is different than listening, but is far more common.

Figure 2. Empoying LEAP instead of WEP.

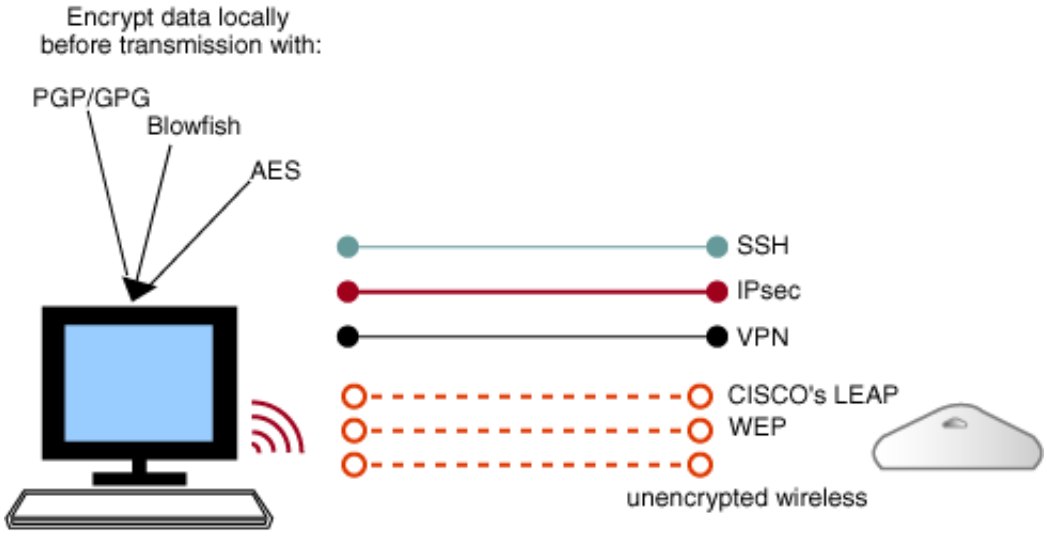


Methods of securing the connection using Cisco's LEAP in conjunction with, or instead of, WEP.

If your current wired network is well-secured, and your wireless network requires some form of encryption and authentication, youre doing pretty well.

Encrypt the data from its point of origin to its destination. Methods like SSH, Public Key Crypotgraphy (PGP and GPG), AES, and Blowfish all allow you to encrypt the data until it has reached a recipient with the proper privileges to decrypt it. When encrypting in this manner, you won't prevent outsiders from leeching connectivity from your wireless base stations, but you will curb them from understanding your data.

Figure 3. Encryption before transmission



Before even transmitting data, encrypt it locally, and then transmit it over wireless.

By keeping in mind that security is a journey, not a destination, you can weigh the costs of higher security and make reasonable decisions about how much you're willing to do to keep others out. For instance, where would you use wireless -- in your home? And if so, what information do you have on your computer that you'd want to protect? To answer this question, I briefly polled an IRC channel of random users about their data, and what sort of effort they had put towards security. What's important to protect,

only users answer. But I did find that few had put any thought into encrypting data before transmitting it, either because it hadn't occurred to them, or because they assumed it would take too much time.

Securing a wireless connection for a home user has to be something that's nearly effortless, or requires effort only once. Requiring a home user to create a PGP passphrase and encrypt their data with PGP, which requires a home user to create an encrypted connection via SSH, may be too big a burden. In a corporate environment, employees are obligated to keep data secure and many of the same considerations can be made: What's reasonable, and what becomes a burden? At what point have you stopped your employees from accomplishing work because they're too busy encrytping and decrypting data?

We need to implement solutions that don't require Herculean effort from the end-user, whether corporate employee or home user.

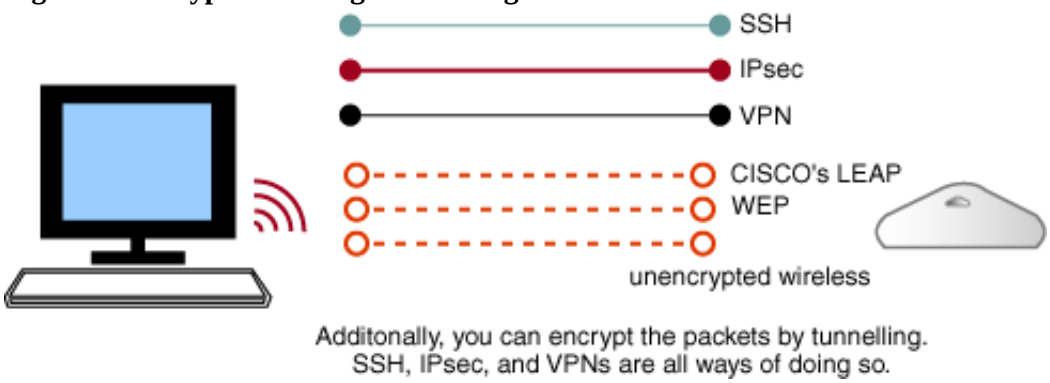
Tin-foil hats

If you're in the center of a metal frame building where you have difficulty getting cell phone service, you're more secure just by virtue of location and shielding. This certainly raises the bar for what a desperate person will have to do to get at your data. If you build your house as a Faraday cage, you'll also increase your security. Of course, you'll also have your builders, neighbors, guests, and family pondering if a rubber room and a nice jacket with buckles wasn't a more appropriate choice for you.

Once you start sending private data over the radio waves, such as your FTP user name and password, you are increasing the likelihood that some unauthorized snoop can "listen in" and grab your data.

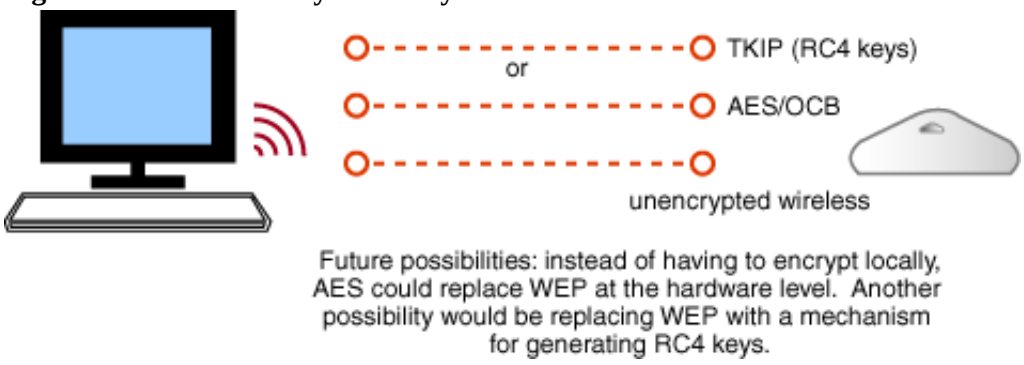
In most home 802.11b situations, I still believe that the combination of common sense and the use of WEP, and possibly SSH (Secure Shell), provides you with a reasonable level of security for broadcasting to your hobby Web site.

Figure 4. Encryption through tunnelling



But what if you want to use a Webcam in public and send images to a business site? Send this kind of data via a secure connection, either through use of IPsec, SSH, or another trusted method of securing a connection or encrypting the data.

Figure 5. Possibilities beyond today's discussion.



Taking a chance on compromising security in a business situation is likely to compromise your standing as an employee.

Resources

- Participate in the discussion forum on this article by clicking **Discuss** at the top or bottom of the

article.

- Check out the book *Secrets and Lies: Digital Security in a Networked World* , by Bruce Schneier.
- Kim Getgen's recent column points out last year's shortcomings when it came to secure wireless data transmission. (*developerWorks*, January 2002)
- Larry Loeb's *developerWorks* article "Going up the wireless stack" touches on some of the risks discussed here. (*developerWorks*, December 2001)
- Larry also covered WEP and how serious its flaws are. (*developerWorks*, April 2001)

About the author

L. Victor Marks is a voracious follower of all things wireless and is a regular contributor to the *developerWorks* Wireless zone. He's also a musician, and a fan of classic automobiles and products that meet their design goals without getting in the way of the user. You can contact Victor at lvmarks@mac.com .