Advanced search Search
IBM home | Products & services | Support & downloads | My account

IBM developerWorks : Wireless : Wireless articles

Out of the sky -- Wireless waves: Through a scanner, darkly

e-mail it!

Thom Stark (thom@starkrealities.com)
Professional curmudgeon
October 2001

Call it "LAN mapping" or "LAN cruising," it means the same thing: roaming the streets, searching for unsecured Wi-Fi APs. But, is it really a hostile act? Internet security consultant Peter Shipley doesn't think so -- and he invented it.

Contents:

Helen wheels
Power to the people
Indigo blues
Miles away
Bring it on home
Resources
About the author
Rate this article

Related content:

WEP2, credibility zero
More dW Wireless resources

In many ways, Peter Shipley is a typical Goth. He looks the part, with long, dark hair, a graveyard pallor, and a penchant for black leather. On his personal Web page, he admits that he spends most of his free time dancing to Goth and Industrial music. He's gone so far as to admit to having written an official Club Edict for a certain unnamed off-color nightclub "event" that takes place in San Francisco's bohemian SOHO district.

But Shipley is not your ordinary Goth. He makes his living as a network security consultant. His black Nissan's license plates read "LIV2HAK". He has a reputation as a researcher whose methods are, to put it mildly, somewhat out of the ordinary. Since early Fall of 2000, he has been studying vulnerabilities in wireless LAN systems.

On July 31 of this year, we spent over an hour talking about what he's discovered in that effort. What follows is what you might call "condensed cream of Shipley," taken directly from that interview.

Helen wheels

After getting his permission to tape our conversation, I asked Shipley what prompted him to begin playing with wireless networking.

"I've always been analyzing networks that are insecure," he replied, "and I think some of my peers were talking about what the next big problem is in security and what to look out for, and wireless came up quite a few times."

I inquired about his hardware and software setup.

"The first one I used was based on the Lucent card," he said, "set up in 'ANY' mode. The whole thing runs on FreeBSD. I effectively have a script that resets the card, associates with an AP, and then pulls the GPS of my current location and logs it to a file."

"Quite literally, when you finish the night you'll have ten thousand data points," he added, "which will distill down to three to four hundred APs. So the first pass of the script generates a list only of the highest signal strength. That does not do any triangulation. And after that, we have a Perlgram that using Mapquest or the Tiger census mecca, we generate a map of the Bay Area with these points on it."

I asked him what his goal was and he responded, "What I want eventually to get out of this process is a good demographic sampling. And that's going to be a couple of months in the process."

When I asked what trends his data had revealed, Shipley said, "A majority of people are running their APs in effectively open mode -- basically wide open, no encryption. A majority are also running in default SSID and IP ranges, which strongly implies that they've used little or no configuration when they set up their wireless LAN."

I asked him what advice he'd give WLAN administrators and he replied, "The only true solution I find at this point -- and probably in the future -- is to set up IPsec. You wish to place your WAPs or APs -- your wireless access points -- on a DMZ zone. This DMZ zone should be restricted from the Internet and from your internal network. And the only thing you should allow out of this DMZ zone are connections or computers that have authenticated themselves with IPsec."

He explained, "The general scenario is: you bring up the laptop, the laptop associates with the local wireless LAN. And then you set up an IP tunnel -- there are several free versions available -- and you just use that as an IPsec tunnel into your firewall."

I noted that, in his war-driving presentation at Defcon 6, he'd estimated that as many as 85% of all WLANs don't even have WEP encryption-enabled.

"Enabling encryption is not going to protect you," he responded. "It simply stops the drive-by surveyors at a certain level. Your network will still be detected, but at least it will stop people who will pull over and end up using your system. We've seen very little control on wireless systems. You can quite literally walk around San Francisco and without difficulty have free wireless access."

Power to the people

I felt I had to bring up the issue of the legality and morality of war-driving.

"While I'm not an attorney," he replied, "I can say that they openly transmit the beacon and they're willingly transmitting a beacon designed to advertise the presence of their AP."

"Now, actually listening to the data that's being transmitted is a different story," he added. "But the FBI and other agencies are pushing a concept through, based on the Carnivore, saying that 'Well, we're not looking at the data, we only look at headers.' And they're stating that it's O.K. to only look at headers, as long as you don't look at data, and they're, like, bending the law a little bit in their own favor."

"This interpretation of the law can be bent in our favor, also," he noted. "That way I could analyze those IP headers, as long as I don't look at the data."

Shipley went on to explain, "I found that a majority of large companies, including several firewall companies in Sunnyvale, not only have wireless access, but I was seeing BGP and IGRP broadcast -- relayed wireless. Which indicates that the AP they're using is not on a DMZ, and not only is it on one of their networks, but on one of their primary, backbone networks. Now, if I want to be mean, if I get onto one of their routers -- very trivially -- I can insert fictitious routing information and they'll never figure out what happened."

"If you can do man-in-the-middle between two large routing broadcasts," he continued, "you can basically shut down connections. And the way BGP typically works is: If it sees you lose your TCP connections, assume that most routers have gone down and drop all the routes. Just transmitting bogus default routes up until I drop out can keep a whole company offline for the better part of a day. Because once I stop transmitting these routes, it can take the better part of a day for the corrected routes to correctly proliferate through the corporate network."

"The thing is," Shipley told me, "I came forward and went public with this effort because I wanted companies to know this is out there. Since then, there are literally hundreds and hundreds of people -- copycats -- out there who have copied my hardware and are doing this."

"There are inevitably going to be people who will say, 'You shouldn't be doing that,' I observed.

"I've been hearing that for over a decade," he replied. "There's a huge debate that's been going on for a long time about whether security information should be shared or not. I'm a strong believer that it should be. After a decade or so of a very close-mouthed policy, things didn't get better. Now that we have an open policy -- with Bugtraq and other groups -- things are actually getting better. Microsoft is actually pretending to care about security."

I couldn't help but laugh.

Indigo blues

I asked whether he was interested in other aspects of wireless technology, such as Bluetooth, and Shipley responded, "...There's some interesting areas to look into. For example, now that I have 2.4 GHz amplifiers, parabolic dishes, and such, a lot of interesting data can be accomplished, if you get on top of [San Francisco's] Market Street or a large business district and beam down at people."

"The majority of Bluetooth security so far has been that it's a small network," he observed.

"A 'piconet'," I agreed.

"Well, it's not a 'pico' net, if I have a decent amplifier," he demurred. "I can literally be 10 stories up on a business building. This is very feasible. Let's just say that one out of every 30 people, or one out of every 50 people walking by has a Bluetooth-compatible device in five years. Given the number of people walking by, I can still walk away with thousands of people's data in an afternoon."

Jumping from interception to interference, Shipley said, "Bluetooth is bursty, but for somebody who's doing a continuous transmission over a certain frequency, [interference] could be a problem."

"Every person I know who's into Bluetooth, and I've brought this up, they go, 'Oh, Bluetooth handles that problem by making sure its data gets through by retransmitting.'"

Portraying both sides of the conversation, he went on, "'But, you understand, they interfere with one another. They go, 'But Bluetooth will be resistant to their interference.'"

"And what does that do for your telephone?" I asked.

"Exactly," he replied.

**Editorial note: Bluetooth operates on the globally unlicensed 2.4 GHz spectrum, which many are using. Although Bluetooth includes a fast frequency hopping rate, small data packets, and adaptive transmission power, the IEEE, working with the Bluetooth SIG, has recently issued a "recommended practice," which specifies some relatively simple things that can be done to significantly mitigate even the performance issue.*

Miles away
I asked if there was anything about 802.11 LANs he thought developerWorks readers should know.

"Well, there's a few things, I guess. One of which was my ability to quite literally log on to a network from over twenty miles away."

He explained, "I went up to the Lawrence Hall of Science (in the hills above the U.C. Berkeley campus) with my parabolic dish and I logged on to a site which is near the Exploratorium (an award-winning science museum in western San Francisco). That's fifteen miles, not counting the height difference."

"What I did was, I scanned for the farthest networks I could reach. So I didn't know exactly where I was receiving, I just logged MAC addresses of the APs, which is part of the beacon. And when I compared my database -- and my database, of course, had the longitude and latitude of these sites, based on my driving -- and I was able to produce X,Y distance. I was able to associate with various other corporate networks without any difficulty and quite literally, over the horizon."

His tone became derisive. "I've actually heard various people make these statements of, 'Well, we just have strong security and, if any kids park in our parking lot, we'll find them.' They're not going to find them. I can do these things, quite literally, from the next city."

"So, if you're counting on distance to keep you safe, you're living in a fool's paradise," I summarized.

"Distance," said Peter Shipley, "is not a solution."

Bring it on home
Just about then, our connection was abruptly broken, bringing our conversation to a sudden conclusion. Our hour-long talk had already given me plenty of food for thought, though -- as it should you.

Shipley's work is creating what I think is a badly-needed store of hard data about WLAN security practices in the real world -- and the picture it paints is a grim one for anyone who understands what it implies.

Users are not deploying even the pitiful security of WEP. Too many of them are not bothering to customize the configuration of their WLANs, even to the extent of substituting meaningful SSIDs and shared passwords for the out-of-the-box defaults.

I found Shipley's observations about the trivial protection of distance even more disturbing, because that vulnerability will continue to exist even if the problem of persuading users to deploy basic security precautions can be solved.

It's not just the pitiful, clueless users' problem, you see, because it's not just their data that's at risk. It's yours and mine and that of our parents, our children, our friends, and co-workers.

Peter Shipley is the canary in our wireless coal mine. We would all be well-advised to heed his warning.

Resources

- Check out Peter Shipley's dis.org Web page.
- View slides of Shipley's presentation on war-driving from Defcon 6.
- Read the complete transcript of the interview with Peter Shipley.
- Read the white paper Using IPSec to construct secure Virtual Private Networks.
- Check out IBM's Virtual Private Network solutions.

About the author

Thom Stark is a professional writer and an amateur horseman. He lives in Mariposa, California, home of Yosemite National Park. He owns several acres of oak trees and gopher holes, and has a wife, a dog, and a decrepit Mercedes convertible, all of which he loves. He makes his living by advocating common sense and a focus on delivering value to end users. His hobbies include reading comics and science fiction, playing the guitar and singing -- occasionally on key. His passions include the life of Alexander the Great, and leaving the world a better place than he found it. He also writes a monthly column and occasional feature articles for Boardwatch Magazine. He maintains a non-commercial Web site where much of his work is archived.

e-mail it!

What do you think of this article?

○ Killer! (5) ○ Good stuff (4) ○ So-so; not bad (3) ○ Needs work (2) ○ Lame! (1)

Comments?

Submit feedback