War driving by the Bay

Wireless network hacking turns cyber attack into street crime.
By Kevin Poulsen, http://www.securityfocus.com/news/192
April 12, 2001 4:57 PM PT

SAN FRANCISCO--In a parking garage across from Moscone Center, the site of this year's RSA Conference, Peter Shipley reaches up though the sunroof of his car and slaps a dorsal-shaped Lucent antenna to the roof-- where it's held firm by a heavy magnet epoxied to the base.

"The important part of getting this to work is having the external antenna. It makes all the difference" says Shipley, snaking a cable into the car and plugging it into the wireless network card slotted into his laptop. The computer is already connected to a GPS receiver -- with its own mag-mount roof antenna -- and the whole apparatus is drawing juice through an octopus of cigarette-lighter adapters. He starts some custom software on the laptop, starts the car and rolls out.

Shipley, a computer security researcher and consultant, is demonstrating what many at the security super-conference are quietly describing as the next big thing in hacking. It doesn't take long to produce results. The moment he pulls out of the parking garage, the laptop displays the name of a wireless network operating within one of the anonymous downtown office buildings: "SOMA AirNet." Shipley's custom software passively logs the latitude and longitude, the signal strength, the network name and other vital stats. Seconds later another network appears, then another: "addwater," "wilson," "tangentfund."

After fifteen minutes, Shipley's black Saturn has crawled through twelve blocks of rush hour traffic, and his jury-rigged wireless hacking setup has discovered seventeen networks beaconing their location to the world. After an hour, the number is close to eighty.

"These companies probably spend thousands of dollars on firewalls," says Shipley. "And they're wide open."

"Absolutely huge"
Dramatic drops in hardware prices over the last year have made it enormously attractive and convenient for corporations and home user to go wireless, in particular with equipment built on the 802.11 standard - which was popularized with Apple's AirPort, and is now widely used on PCs. But computer security experts say that in the rush towards liberation from the tethers of computer cable, individuals and

companies are opening the doors to a whole new type of computer intrusion.

"It's absolutely huge," says Chris Wysopal, also known as ""Weld Pond," director of research and development at Boston-based @Stake. The company added wireless auditing to their consulting menu approximately two months ago, after months of laboratory research convinced them that it was a grave problem. "802.11 is inherently less secure than other wireless technology, Wysopal says, "and the way it's being deployed makes it worse."

The 802.11 cards and access points on the market implement a wireless encryption standard, called the Wired Equivalent Protocol (WEP), that in theory makes it difficult to jump onto someone's wireless network without authorization, or to passively eavesdrop on communications. But in January, researchers at the University of California at Berkeley published a paper revealing a number of severe weaknesses in WEP that allow attackers to crack the crypto with sophisticated software, and ordinary off-the-shelf equipment.

"Hardware to listen to 802.11 transmissions is readily available to attackers in the form of consumer 802.11 products," reads the paper. "The products possess all the necessary monitoring capabilities, and all that remains for attackers is to convince it to work for them."

But the consensus at the RSA Conference is that attackers hardly need resort to cryptanalysis. Most networks in the wild aren't using WEP at all, or are using it with the encryption key set to one of several well-known default values.

According to Wysopal, many corporate and home users erroneously believe that their network name, or 'SSID', serves as a secret password. Other implementers simply don't consider that their wireless network's electronic "cloud" extends beyond the walls of the building. If they've set up their wireless access points behind their firewall, they're opening their internal network to anyone with a laptop. Even if they put their access points outside a firewall, intruders may be able to use them to get out to the Internet, whether to stage attacks, or just for free bandwidth.

"I think almost every large hi-tech corporation has wireless exposure now," says Wysopal. "Sometimes you can just drive into their parking lot... turn on your laptop and be on their network. We've seen it in a lot of brand name companies that you would recognize."

Al Potter, Manager of Network Security Labs at ICSA, has one word for the exposure he's seen: "Terror."

War Driving

Many here believe that hackers are already cruising around metropolitan areas in cars and on bicycles, with their laptops listening for the beacons of wireless networks. Using such a network doesn't even require special software or hardware, an ordinary $150.00 consumer wireless card will latch on to the beacons and put you on the net.

Grand computer capers will be pulled off, not from bedrooms and college dorms, but from windowless vans in company parking lots, and from park benches and empty stairwells. "It's fun, it's the new thing," says Wysopal. "It's kind of like war dialing: you never know what you're going to get."

War dialing is the timeworn technique in which a hacker programs his or her system to call hundreds of phone numbers in search of poorly protected computer dial-ups. The name comes from the movie WarGames, which features Matthew Broderick performing the technique.

In the late nineties, as a research project, Peter Shipley war dialed every phone number in the San Francisco Bay Area-finding dial-ups leading to banks, hotels, and scores of unprotected personal computers. The survey took three years to complete. The goal, Shipley said, was to raise awareness of the threat posed by unprotected modems, and the project won attention from the print media and online news.

Now, in the same spirit, and with the help of some hobbyist friends, Shipley plans to "war drive" the streets of San Francisco, Oakland, and portions of Silicon Valley to the south. When he's done, he'll have a database that maps the geographic location of, in all likelihood, thousands of open 802.11 networks. He doesn't plan on publishing the raw data -- he doesn't want to help attackers spot choice targets -- but he says the numbers will speak for themselves. "I can give you the density of open networks an area, organized by zip code," says Shipley. "People don't believe there's a security problem if you don't prove it to them."

Shipley says he doesn't plan on actually using anyone's network. But to make the experiment real, and, perhaps, to avoid unwanted attention, he's already plotting ways to hide the hacked antenna magnetically held to the roof of his car. "I'm thinking of putting a pizza sign on it."

tips@securityfocus.com