

O'Brien: On the hunt for naked Wi-Fi hotspots with a wireless detective

By [Chris O'Brien](#)

[Mercury News Columnist](#)

Posted: 04/03/2010 02:00:00 PM PDT

http://www.mercurynews.com/breaking-news/ci_14802784



To my untrained eyes, it was a bright and clear Silicon Valley day as we sat in the parking lot of a North San Jose high-tech company. But Dr. Amit Sinha, Motorola engineer and Wi-Fi detective, knew we were surrounded by invisible danger.

Sinha opened his laptop and launched a Wi-Fi detection program to demonstrate his point. Using equipment any 10-year-old could wrangle, Sinha generated a list of more than 250 Wi-Fi access points and associated devices inside the company's building.

Well over half of the access points either had no encryption or an outdated version that the most basic of hackers could crack within minutes. From the comfort of our car, we could see the type of devices people were using inside — iPhones, laptops, printers — and the names of the networks they were connecting to.

With just a couple of clicks, Sinha could have been surfing around the company's network and probing many of these devices. A less benevolent person could easily grab passwords, copy sensitive documents or plant viruses.

It only took about an hour with Sinha, a chief technologist for Motorola Enterprise Mobility Solutions, and his wireless detective kit to leave me horrified. Motorola has a financial interest here, of course; it is in the business of selling mobile security solutions. But Sinha and Motorola are not alone in pointing out the lack of public awareness about the gaping hole in wireless security.

Patrick Martin, a senior product manager in Symantec's security response group, said he didn't have data on the numbers or percentages of wireless access points that are vulnerable to hackers. But, he added: "Certainly it's quite common. I've seen cases myself where my laptop can see

wireless networks in the houses adjacent to me and there's always at least one that's insecure. "... Unfortunately, there are a lot of folks who just don't understand that these vulnerabilities exist."

I am, admittedly, like many of those folks when it comes to issues of security. Which is to say, I'm careless. I couldn't even tell Sinha offhand what — if any — type of encryption I used on my Wi-Fi router at home.

Still, it's astonishing to see that when it comes to wireless security, even a savvy high-tech region like Silicon Valley essentially has its pants down. And if you don't think hackers everywhere know this, think again.

Whether it's at work, at home or at the local coffee shop, these hackers know that for some reason, people don't think twice about logging onto whatever Wi-Fi signal they can find and sharing all sorts of sensitive information. Both individuals and companies are careless with wireless security in ways they would never be with wired connections to networks.

"The problem for consumers is that wireless is promiscuous connectivity," Sinha said.

And as our appetite for Wi-Fi grows, and new wireless devices flood the market, there seems to be little thought given to security.

"These threats are only very real if the users fail to configure their wireless access point securely," said William Hau, a vice president at security firm McAfee. "A significant proportion of the vulnerabilities in the public arena can be attributed to insecure installations by the end users."

So this has left us vulnerable to hackers who could be right at this moment patrolling the streets of our fair city, plucking packets of data from the air and spinning them into digital gold.

By the end of our hour together, Sinha had me scared straight. I updated my security settings at home that night.

And now, I am a bit wiser, thanks to Sinha. But somehow, all those signs on coffee shops advertising "Free Wi-Fi Inside!" seem more ominous than inviting.

Mercury News staff writer Steve Johnson contributed to this story. Contact Chris O'Brien at 415-298-0207 or cobrien@mercurynews.com. Follow him on Twitter at <http://twitter.com/sjacobrien> and read his blog posts at www.siliconbeat.com.

HOW TO STAY SAFE

For everyone:

1. Don't use the security setting known as Wired Equivalent Privacy, or WEP. Instead, be sure to use Wi-Fi Protected Access, or WPA2, the latest and greatest protocol.

2. Don't just leave security settings on default. When installing Wi-Fi access points, check the settings and place them on the highest level.

For consumers:

1. Don't perform sensitive activities, such as banking or purchasing with a credit card, at public Wi-Fi hot spots.
2. If a box appears asking you to accept a security certificate while using Wi-Fi, don't accept it. If hackers are trying to hijack your Wi-Fi connection, they need you to accept one of these to do so.
3. Make sure you have good firewall software on your laptop.

For businesses:

1. Install wireless sensors around your building that scan your internal Wi-Fi access points and probe for intruders. All it takes is one employee plugging in a rogue Wi-Fi router and your network can be compromised.
2. If you have a lot of company laptops in the field, have strong security policies for using them. For instance, require employees to initiate a virtual private network connection with your office network before they start surfing.

THREE WAYS TO ATTACK

Hackers can use insecure wireless access points in several ways. Here are three:

Scheme 1: "Packet Sniffing"

Sitting outside a building, Motorola engineer Amit Sinha ran a program that made copies of all the packets of data being transmitted between Wi-Fi devices and networks. Using a free software tool, Sinha could then decode the packets. What might he find inside? Passwords. Social Security numbers. And loads of other personal and corporate secrets.

Scheme 2: "Middle Man" (or "Evil Twins")

The hacker's laptop finds the name of a wireless access point that devices are trying to connect to. Using special software, the laptop can disguise itself as that access point, so that these devices connect to the Internet through the hacker's laptop. All the activity of those devices can then be captured on that laptop. This allows the hacker to capture more information for longer periods than during packet sniffing.

Scheme 3: "Network Intruder"

The hackers use a weak Wi-Fi access point to get inside a company's network, where they plant viruses or retrieve copies of sensitive information. If printers are on Wi-Fi networks, the hackers could get copies of documents in a queue to be printed and print their own hard copies.

These schemes were taken to their extreme in recent years by Albert Gonzalez, a Miami-based hacker who recently pleaded guilty to stealing more than 100 million credit card numbers. How did he get most of them? Through the Wi-Fi systems of various retailers.

Source: Amit Sinha, Motorola engineer

Dan Muñoz | [A&R Edelman](#) | 650.762.2918 (Mobile: 650.533.5836) | dmunoz@ar-edelman.com