RELATED KEYWORDS

- Santa Cruz

A road map to wardriving in these times

Hobbyists drive around looking for access, but efforts highlight systems' vulnerabilities

August 18, 2008 | By Matthew B. Stannard, Chronicle Staff Writer

Memorize this: *a5d1tmI#9DWSFX`/ksbo"RZ"l`SN`ito%b)Bel*B_EiCZ)q-h/`VF"3Gb_CM#TT.*

Got it? You might want to try because that's the kind of password you'll need if you really want your wireless network to be secure.

That's the word from Keith Maynard - who goes by the name Seric - and he should know. Not only is he a longtime computer security guru - when he isn't riding with the Vampire motorcycle club in Santa Cruz - Seric is one of the original wardrivers, hobbyists who deck out their cars with computers and sensitive antennas and go cruising the streets looking for wireless networks.

Wardriving got some bad ink earlier this month when federal prosecutors announced indictments against an international ring of hackers who allegedly used the technique to find poorly secured networks at several East Coast restaurants and stores. Secret Service investigators said Aug. 5 the thieves downloaded more than 40 million credit card numbers from those networks, which they used or sold online, netting millions of dollars and a condo in Florida.

But many wardrivers have nothing so nefarious in mind. Some just enjoy the Easter egg hunt of finding networks. Others, like Seric, use wardriving to draw attention to the scope of the emerging digital world. Their hope is that they can persuade people to think about their own wireless security by displaying the weakness they detect in articles, on panels and to professional clients.

"Once you buy a tool, you need to learn how to use it correctly," Seric said.

Original wardrivers

That was the idea that led Seric to join some of the earliest wardriving efforts with fellow enthusiasts from Berkeley's Dis.Org Crew - DOC - a group of self-described amateur troublemakers and professional consultants. The crew's Peter Shipley coined the term wardriving, which evolved from the term wardialing - finding open networks by randomly calling phone numbers with a modem - which itself came from the movie where the technique played a central role: "WarGames."

When the DOC started wardriving back in the early part of this millennium, wireless networks were difficult to find, but only about 15 percent of them, Seric said, featured any type of security.

RELATED KEYWORDS

- Santa Cruz

A road map to wardriving in these times

Hobbyists drive around looking for access, but efforts highlight systems' vulnerabilities

August 18, 2008 | By Matthew B. Stannard, Chronicle Staff Writer

(Page 2 of 6)

Wardriving eventually went mainstream, with Skyhook Wireless, the company behind the iPhone's location tracking abilities. Founder Ted Morgan said he stumbled upon wardriving in 2002, and today the company maintains a fleet of 500 scanning vehicles in Europe, Asia and the United States, all collecting data that allow the iPhone to find its user's location using the nearest Wi-Fi network as part of its mapping software.

Wardriving faded a bit as the networks went from being hard to find to being hard to miss, although enthusiasts - some of whom have recorded more than a million networks - still upload new finds to sites such as WiGLE.net. But on Thursday, at the request of The Chronicle, Seric dusted off his wardriving rig and took a spin around the Bay Area to look for potential vulnerabilities like the ones exploited by the ring indicted Aug. 5.

"I got like 135 (access points) off the freeway on my way up here from Santa Cruz," said Seric, as he adjusted his equipment - laptop, Wi-Fi antenna, GPS antenna - in the parking lot of Stanford Shopping Center.

After a five-hour cruise around the Bay Area - including residential and downtown sections of Palo Alto, San Francisco and Oakland before returning to Palo Alto across the Dumbarton Bridge - Seric's list included more than 2,600 individual networks, spotted at businesses, in homes, on campuses and within moving buses.

Open networks appeared every block or so, beaming from homes in West Oakland and near the Hewlett-Packard garage in Palo Alto, from Stanford University to Oakland's Federal Building and San Francisco's City Hall, along freeways, on tree-lined streets and in dusty industrial parks.

That's a crime?

Overall, about one-third of the networks found during the tour showed no encryption, although some might have featured some other forms of protection not visible without a more intrusive - and possibly illegal - probe. Attempting to access the network to find out could cause Seric to cross from legal wardriving, where networks are passively detected and recorded, into the legally gray area of computer trespassing.

That such a crime exists will come as disturbing news to the legions of iPhone and laptop users who have become accustomed to seizing the closest open network for their own use. But while legal experts say the law is murky, the Electronic Frontier Foundation in San Francisco has tracked a handful of cases where people have been successfully prosecuted for theft of service or computer trespassing for using open networks at libraries or cafes without permission.

RELATED KEYWORDS

- Santa Cruz

A road map to wardriving in these times

Hobbyists drive around looking for access, but efforts highlight systems' vulnerabilities

August 18, 2008 | By Matthew B. Stannard, Chronicle Staff Writer

(Page 3 of 6)

The sentences have included probation, suspended sentences and fines. But nobody, according to the EFF, has gone to trial, where a judge and jury could clarify the law.

"I think most people would presume that you have permission to access that open network, that's become the social norm. But it's a little unclear what the law is," said Jason Schultz, acting director of the Law and Technology Clinic at UC Berkeley's Boalt Hall School of Law. "The law has not yet had a definitive decision."

At the same time, security experts haven't made a definitive decision about how much security is enough, with some insisting upon maximum levels of encryption behind a 63-character hexadecimal password like the one at the top of this article - not memorized, but saved on a portable flash memory drive to be retrieved when needed.

Others, including Schultz, take the opposite extreme, advocating for leaving networks open unless they are used for some sensitive or confidential purpose.

"I think for most people, an open network is a nice neighborly thing to do," Schultz said. "Everyone gets more access to information."

Seric, like many security consultants, lands between the extremes, calling for making informed decisions - choosing your level of security based on your needs and your situation. A bank needs better security than a library; Joe Smith doesn't require the same level of protection as does Brad Pitt.

Unaware of the threats

The problem, Seric and other security consultants say, is that too many network owners - individuals and businesses alike - don't really know the potential threats posed by open or poorly secured networks so that they can make informed decisions.

Headline crimes like those announced earlier this month offer a red flag to big businesses that their customer-friendly wireless networks can give a malicious hacker entree to their sensitive financial data. Assemblyman Dave Jones (D-Sacramento) also has introduced legislation that would bar businesses and state agencies from sending payment data over open networks unless strongly encrypted.

But security experts say homeowners and small businesses, too, need to recognize that leaving their networks open could expose their computers, DVRs, printers, and other networked devices. Even a firewalled system can be compromised through an open wireless network - like locking your front door but leaving a bathroom window wide open.

RELATED KEYWORDS

- Santa Cruz

A road map to wardriving in these times

Hobbyists drive around looking for access, but efforts highlight systems' vulnerabilities

August 18, 2008 | By Matthew B. Stannard, Chronicle Staff Writer

(Page 4 of 6)

"People can walk right into your network," said Ed Skoudis, the author, with Tom Liston, of "Counter Hack Reloaded" and a fellow at the SANS Institute, a security research and training organization. "You've given that person access to your home. And he can hack your home."

The threat may be remote, but there are lesser concerns that security consultants describe. The local sex offender borrowing a neighbor's signal to download child pornography. The local teenager downloading terabytes of movies who would rather cripple a neighbor's bandwidth than Mom and Dad's. Or the random hacker or prankster looking for a server to send spam to millions or threatening messages to the White House.

In all of those cases, the trail followed by investigators would lead to the open network - your network.

"How much do you trust your neighbors? And how much do you trust, well, anybody that can get geographic proximity to your network?" asked Skoudis. "If a bad guy wants to commit a crime, he usually wants to avoid committing it in a place that it can be traced back to him."

Growing awareness of those threats may explain an increase in security since the early days of wardriving - early scans found as few as 15 percent of networks were encrypted, Seric said, while Thursday's scans found about two-thirds of sampled networks were encrypted in some fashion.

But in many cases, Seric and other security experts say, those networks are, in fact, effectively unprotected, using old code and outdated techniques that leave their owners living in an illusory bubble of security.

A thing to know about WEP

Then there is WEP - a form of encryption long in use and still used by many networks, either because the network owners don't know there's anything better or because there is older equipment on the network that can't understand newer encryption.

In other cases, homeowners or businesses set up their network five years ago and assume they were still secure. But while WEP once was the standard, type "hack WEP" into Google today and you'll get 170,000 responses, including instructional videos and step-by-step instructions.

Even a robust network, protected by the latest WPA2 encryption, internal and external firewalls, and alphabet soup passwords can be cracked in theory, Seric said. But for many home users and small businesses, that level of security is plenty, he said. And many people can get by with even lower security, if their comfort level allows - especially if their neighbor is doing even less.

RELATED KEYWORDS

- Santa Cruz

A road map to wardriving in these times

Hobbyists drive around looking for access, but efforts highlight systems' vulnerabilities

August 18, 2008 | By Matthew B. Stannard, Chronicle Staff Writer

"People are always going to look for the easy targets. ... If you're too much of a headache, unless there's something they specifically want from you, they're going to look for an easier target," Seric said. "It's really about making yourself tougher than the next guy."

Harvest of a wardriver
A map of networks identified during The Chronicle's wardrive is online at *sfgate.com/webdb/war driving*.

A glossary of wardriving terms
Wireless networking manuals use acronyms and obscure terms that can be daunting. But understanding at least some of those terms is required to properly secure an open network. A few of the more common and useful terms:

Encryption: Any process that uses a mathematical algorithm to transform information and make it useless to unauthorized users. Several forms of encryption are available for wireless networks (see below). Most Internet browsers can also employ SSL - secure sockets layer - that can encrypt communications on an open network. In addition, there are many programs for encrypting e-mail or the entire contents of a computer hard drive.

WEP: An older form of encryption. Many users still employ WEP, and some machines can't use other forms of encryption, but many security experts consider it so easily cracked - within two minutes, many estimate - that it is little better than leaving a network open.

WPA: Wi-Fi Protected Access, a newer form of encryption that is considered far more secure than WEP. A 2004 update, WPA2, is even more secure and is recommended by security experts - assuming the devices on your network can use it.

LAN: Local Area Network, a network of computers or other devices that share a wireless or wired network. Linking devices on a LAN allows the devices to share information and be centrally controlled, but also can allow one vulnerable device to be leveraged in an attack on another device on the LAN.

Firewall: A software or hardware "barrier" intended to prevent unauthorized intrusion onto a machine or network. Many everyday users fail to employ a firewall, or disable it for specific forms of communication, such as wireless networking. The problem is that an intruder who accesses openings through the firewall may be able to access all other devices on the network, unless the devices are protected by their own internal firewalls.

RELATED KEYWORDS

- Santa Cruz

A road map to wardriving in these times

Hobbyists drive around looking for access, but efforts highlight systems' vulnerabilities

August 18, 2008 | By Matthew B. Stannard, Chronicle Staff Writer

SSID: The Service Set Identifier is the name used by a wireless network to identify itself to compatible devices. Many users leave their SSIDs set to the default established by the vendor, but it is also possible to change the name or stop the network from broadcasting its SSID - though experts say neither of these steps contributes greatly to security.

MAC Address: Every device on a network has its own Media Access Control address, usually displayed as a set of six pairs of letters and numbers separated by colons or dashes. Theoretically each device has a unique MAC address, and it is possible to limit wireless network access to specific addresses. In practice, it is possible to spoof a MAC address, thereby fooling the network. For this reason, security experts say MAC address control contributes minimally to wireless network security.

Password: The first and in many ways the weakest line of wireless network defense. The best passwords use 63 random characters - letters, numbers, and punctuation - which some system administrators store on portable flash drives, to be retrieved when needed. Passwords using real words are vulnerable to hackers who can digitally throw an entire English dictionary at a network. And using a more complicated password for your credit card isn't much good if a hacker gets your simpler e-mail password - and then asks credit card sites to e-mail your "forgotten" credit card password.

- Matthew B. Stannard