NEVER MIND THE HAT'S COLOUR: Unlike their ill-reputed black-hat counterparts, white-hat hackers like Brad Haines use their talents for the forces of good. Well, at least they don't break the law

Security and Emergency Preparedness

WIRELESS INSECURITIES

Brad Haines, 28, seems like a normal guy. He's tall, has slight features and never leaves home without his favourite hat. One more thing. Haines is also a "white-hat hacker" who knows a thing or two about computer security and he's ready to talk shop

By Jennifer Cockrall-King
Illustrations by Eric Gravel
Photography by 3Ten

IDLING IN A PARKING LOT ON EDMONTON'S JASPER AVENUE, BRAD HAINES FIRES UP his laptop. It's connected to a global positioning system and some crazy-looking, Cold War-era antennas strapped to the back of the headrests in his car. The antennas are hooked into an amplifier, as is the omni-directional antenna on the roof. Not to worry though, he says to reassure me, he's only receiving, not transmitting, so our brain cells won't get nuked. Good to know. Within moments the laptop's screen starts to cycle through rows of data – not quite the indecipherable gibberish of the *Matrix* movies, but seemingly random words and numbers, except to Haines. Hardly able to contain himself, he blurts out, "From a total restart and not moving, we're seeing 106 wireless networks!"

Haines notes that 78% of the networks are encrypted; that is, they have some security settings enabled. This is actually good news. It used to be about 30% just a few years ago. But it also means that tonight, 22% are happily broadcasting every bit of data that is passing between the computer and the network in the clear, as if the user was shouting it out over a bullhorn for all to hear, or in this case, for us to see.

In tech talk, a network is a system of interconnected computers that work together to pass information back and forth via an Internet cable or a wireless connection. The link lets businesses share files, directories and information on various hard drives. It's also used to simplify Internet access and therein lies the problem. When it comes to wireless networks, there are several security standards that are used to control how information flows between computers. The first and most common is the default setting, which has no security features. That means any schmuck with a compatible wireless device can basically walk by, log on and gawk at the nifty nuggets of information being passed around.

On average about 70% to 75% of networks these days are secured. "The big thing," Haines says, "is the number of wireless networks we're seeing broadcasting on default. No one has bothered to change the network's name or default settings. They opened up the box, plugged it in and it worked. I call this the low-hanging fruit."

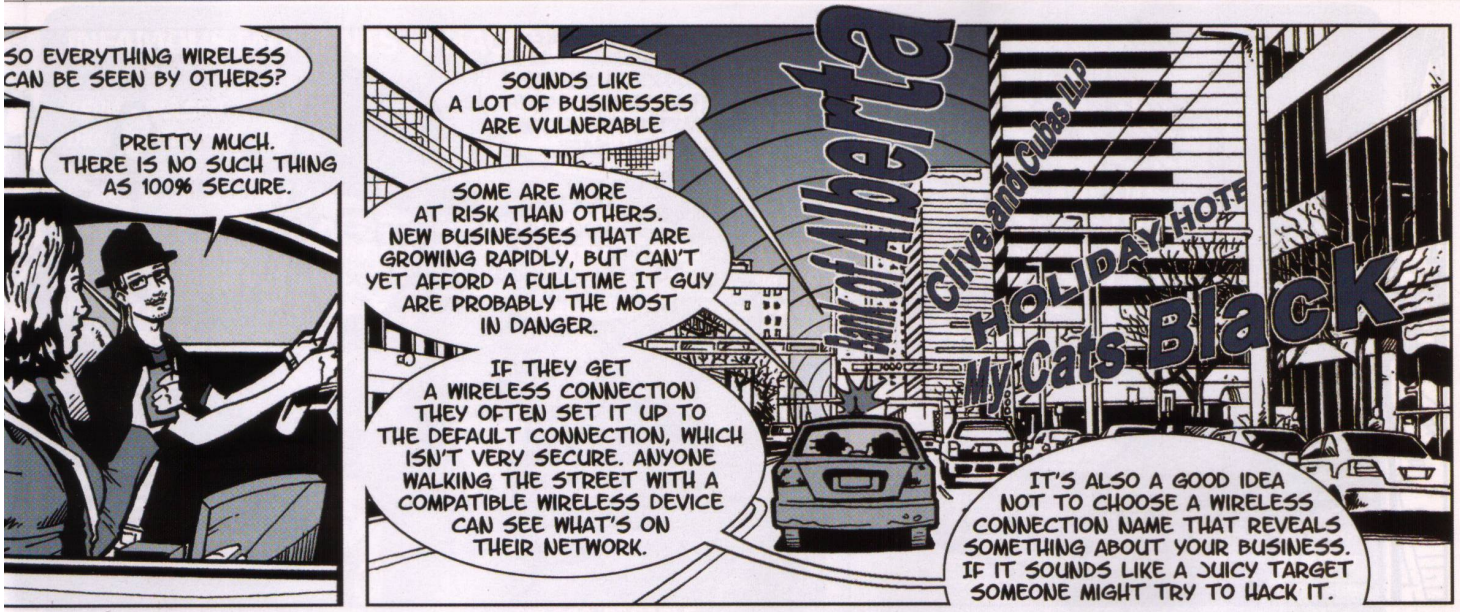
Haines has been on the prowl for unsecured wireless connections in Edmonton and Calgary since 2002. In 2004 he was part of an incident that caught the attention of both the Canadian Security Intelligence Service and the national media, when he helped organize a survey of the wireless networks in Red Deer. CSIS got wind of the move and fired off a warning to businesses in the area to be ready for a possible hacker attack, but Haines' intentions were benign and no attack came.

The activity of mapping wireless connections is called wardriving, deriving its name from the 1983 movie WarGames. (A plucky computer kid played by Matthew Broderick sets his old-school PC to automatically dial every phone number in his California area code. Looking for another modem connection, he inadvertently connects to NORAD's computer thinking it's a gaming software machine. He cracks the password and almost sets off World War III. Remember?) Wardialing became popular in the computer world after this movie and hackers would use automated dialing programs to find other computer modems or fax machines. Around 2001, wardriving began. It's the act of scanning for wireless networks from a moving vehicle. On foot, it's warwalking. By bike, it's warriding.

Is it geeky? Hell, yes. But it's also very telling about our current obsession with all things wireless. And Haines, 28, is a regulation-savvy version of Matthew Broderick who likes the thrill of mapping out these networks. Think of it as a hobby, the hacker thing to do on a Friday night. It's information gathering for the sake of information gathering. Pre-emptively, Haines declares that it's totally illegal to hop onto any of these networks. "It's felony theft of service from a computer," he says flatly. "We won't be doing that."

Haines is what's known as a "white-hat hacker," someone who is relentlessly curious about new technology. He likes to take it apart, find out how it works, modify it and come up with uses for it that no one else has. But really this is just the definition of a hacker, plain and simple. Guys have been tinkering with engines ever since cars were invented, he points out. "Hacker is just easier than saying 'electrical engineer wannabe or computer security enthusiast,'" he laughs. He knows, though, that the term has largely been tinged with negative and criminal connotations in the media and movies. Black-hat hackers are a huge thorn in the much larger world of hackers. These are the few who use their resourcefulness to steal information for personal gain. They're also known as crackers, and Haines says that even a whiff of suspicious activity gets you kicked out of the tight-knit hacker community pretty quickly. "You have to be responsible with the knowledge. Push the limits but don't break the law. I'm not going to do anything because if anything goes on in Edmonton, I'm the guy they come looking for."

As it turns out, Haines, who also goes by his hacker handle, RenderMan, is a rather prominent figure in the very niche, but global, community of wardrivers. His "Stumbler Ethics" text is widely considered the wardriving community's bible and rule book. It's posted for free on his site www.renderlab.net. Haines is thin and fine-featured, with shoulder-length brown hair. He dresses all in black and always wears his trademark black fedora. He looks very much the part of a "computer enthusiast." In a bit of geek-chic self-awareness, his black T-shirt has a periodic-table-esque white square with the letters Gk in the upper left corner. His website notes that he "does clean up nicely for working in offices" and juggles various contracts for clients who hire him to set up and trouble-shoot their company's wireless network systems, or to do threat analyses. He's also a regular speaker at international hacker conferences.



IT'S BEEN A WHILE SINCE HAINES has done any wardriving in Edmonton. He's pumped to see if, and how, things have changed. Other than wires and gear, the inside of his car is neat and tidy, not strewn with old fast-food bags and rattling with Red Bull empties that most movies insist young "computer enthusiasts" live off. As we roll east along Jasper Avenue in the heart of Edmonton's downtown core, wireless network names begin to pop up on his laptop.

He pokes at a few keys and explains that we are now looking at unencrypted data flowing by on networks. Most of this information is websites people are navigating and e-mail messages. "One time turning onto Highway 2, I think I saw a credit card transaction going by," he says when I ask what sort of information you can look at with these off-the-shelf programs. Frankly, it's shocking to think that someone can just intercept that kind of information, but these users are basically broadcasting this unencrypted data over a public frequency. "People might not like it that I can look at it, but it's the sort of thing that makes you want to smack people across the head. You don't walk around naked with all your blinds up, do you?"

Just then a police car cruises by in the opposite direction. I ask if he's ever been stopped, and he says he hasn't. "But you could imagine, a guy dressed in black with all this computer equipment in his car..." he trails off.

Surprisingly, even the highest level of computer protection doesn't guarantee your network is safe. "There is no 100% secure network," Haines says in true hacker fashion. But every step a bad guy has to go through to get to you or your company's private information makes it less and less appealing, especially given all that other low-hanging fruit. One of the big mistakes, says Haines, is relying on old technology that uses outdated security encryption codes. "It's a situation where you get enough guys cranking away on something, they'll find enough ways to poke holes in it."

> THE PROBLEM IS THERE IS NO I.T. PERSON OR DEPARTMENT, MERELY AN EMPLOYEE IN MARKETING OR ADMINISTRATION WHO VOLUNTEERS TO TAKE ON THE TASK OF SETTING UP THE NETWORK.

Yet, that doesn't mean all security breaches come by the hands of merciless black hat hackers. Most stem from nothing more than human ignorance. Take the example of Alberta's first major personal information security breach of a wireless computer. In March 2007 an unprotected computer server in a downtown Edmonton law office allowed access to hundreds of clients' files that included personal information such as criminal records, work histories, driver's licences and social insurance numbers.

A lawyer with the firm had set up a wireless system. He thought it was secured by an encrypted password, but a person in a nearby building with a laptop and a wireless card was able to connect to it without even being asked to enter a password. The network then invited him to connect to one of the lawyer's databases making the breach complete.

Shaun Sturby, technical services manager for the network specialist firm Optrics Engineering, says the Edmonton case points to the lack of tech savvy that's often at the root of these types of problems. "That lawyer thought he had set it up correctly," Sturby notes, "if a professional like a lawyer can get it wrong, the implication is that everyone can get it wrong."

Alberta's Information and Privacy Commissioner, Frank Work, has since ordered an investigation into the incident and believes it's important that companies take the necessary precautions to lessen the chance of having such problems. The cost of remediating a loss that involves missing personal information can be devastating, Work says. There's the possibility of lawsuits by customers who have been harmed. Nevertheless, he continues philosophically, "we're far more captivat-

ed by what the technology can do than what its vulnerabilities are."

BACK ON JASPER AVENUE, Haines and I break off our conversation as yet another pimped-out, stereo-blasting muscle car passes, drowning out our words. The lineups of hooting tube-topped girls are just starting to form at the bars this Friday night. It's a prime time to wardrive.

As we move deeper into the downtown core, I giggle at some of the names of the wireless networks: The $10,000 Crackhouse, Desperately Seeking Porn, just to name a couple. Then there are the names that make you wonder if their mothers know they've named their wireless networks that. While the creativity is amusing, Haines points out that common mistake people make with their wireless connections is that they give away too much information with the name they choose. As if on cue, a number of network names to businesses pop up, ones that clearly state they are an investment house, a financial company or a law firm, most of which we imagine have juicy customer databases or financial information. "Those are the ones that some people might find worth their while to spend some time on," warns Haines.

With smaller companies, Haines says the main security problem lies in the fact that there is no IT person or department, merely an employee in marketing or administration who volunteers to take on the task of setting up the network. Sometimes it's just the fact that companies don't budget to be proactive, he says. Either way many companies don't have a plan in place if or when they do have a problem.

ABOUT 22% OF THE WIRELESS NETWORKS OUT THERE ARE HAPPILY BROADCASTING EVERY BIT OF DATA PASSING BETWEEN THE COMPUTER AND THE NETWORK IN THE CLEAR, AS IF THE USER WAS SHOUTING IT OUT OVER A BULLHORN FOR ALL TO HEAR AND SEE.

We enter the zone of downtown hotels, and the subject of wireless connections in hotel rooms comes up, literally, on the screen. How many business travellers are sending all sorts of data across the wireless room-link networks? Generally, these networks are encrypted, says Haines, but adds, if you have the choice of logging in with your wireless card or plugging a cable into your laptop, go for the wire. "It's kind of hard to screw up a wire."

We then turn south and head across the river to the university area. This, Haines says, is traditionally the most dense area for wireless networks. Indeed, driving the length of one block, we find over 100 networks. As we slowly creep along, our numbers rise to more than 700 networks in four blocks. Given that it's just a numbers game, with the number of unsecured networks hovering at that 25% mark, a lot of people are not just allowing strangers to use their Internet connections, they're allowing people to potentially take files and information off of their computers, to download files onto their computers and to send spam from their network. "I usually equate that with running a network cable out to the parking lot and letting anyone connect. Would you do that? No. So take the time to separate yourself from the foolish masses."

We end our drive after 50 minutes. With an off-the-shelf program, a laptop and a mangle of wires, we've seen over 5,400 networks. Over one quarter of them are metaphorically shouting their activity from rooftops. Sure, this is a much better scenario than Haines was detecting even a couple of years ago, but the wireless explosion seems to cancel out any gains, leaving lots of low-hanging fruit. I ask Haines whether he ever gets technology overload and wants it to stop changing so rapidly. He thinks about it for a second and then says, "I want it to slow down because the rest of society needs to catch up." AV