Bluetooth Leaves Cellphones Exposed

By JEREMY WAGSTAFF

If you spot someone tailgating you on the road or standing next to you wearing a backpack, then watch out: You may have been spied on. All the data on your cellphone, including addresses, calendars, whom you called and who called you, may now be in that person's computer.

Many cellphones use Bluetooth technology, which allows them to communicate wirelessly with other Bluetooth-equipped devices—computers, personal digital assistants and other cellphones. This means you don't need a cable, for example, to synchronize the address books on your laptop and your cellphone. It's convenient, but that makes it possible for someone to steal your data, or even hijack your cellphone for their own purposes.

Last year, London-based security consultant AL Digital spotted flaws in the way some Bluetooth cellphones swapped data with one another—flaws which could be used to gain unauthorized access to everything stored on that phone without the user ever knowing. AL Digital's Adam Laurie, who discovered the problem, shared his findings with cellphone manufacturers and with the public (leaving out the detail which might allow ne'er-do-wells to copy his experiments at street level). He termed the trick Bluesnarfing.

Not a lot has happened since then. Nokia Corp., the market leader in the cellphone industry, acknowledges the flaw but says it is not aware of any attacks against Bluetooth-enabled phones. Sony Ericsson, a joint venture of Telefon AB L.M. Ericsson and Sony Corp., didn't reply to an e-mail. Even those highlighting the danger say they haven't heard of specific attacks.

But these attacks are nevertheless possible. Mr. Laurie cites a scenario in which a paparazzo could steal celebrity data. He says he was able, with permission, to sniff from a friend's phone details of her company's shops, door codes and safe combinations. "There's any number of angles you can look at, and they are all bad as far as I'm concerned," he says.

Martin Herfurt, a 27-year-old German student at Salzburg's Research Forschungsgesellschaft mbH last year set up a laptop at a technology trade fair in Hannover, Germany, and ran a sniff attack. He found nearly 100 cellphones from which he could have stolen data, sent text messages or even made calls. He has published his findings to prove that this kind of thing can be done easily.

How does it work? The attacker can use a Bluetooth-enabled laptop to discover other Bluetooth gadgets within range. Anything with Bluetooth activated will show up, usually identified by its default device name. Being "discoverable" means your gadget is visible to anyone searching, but even if it isn't, an attacker can still find it, using software freely available on the Internet. The attacker can then use more software to take, delete, change or add data.

So what's a consumer to do? Turn off Bluetooth on your phone unless you really need it to communicate with your other gadgets. In most cases, phones that have Bluetooth will have prominently displayed the fact on the box the phone came in, or you can expect to find "Bluetooth" in the index of your phone's manual. Otherwise, the Bluetooth settings can usually be found in the "Communications" or "Connections" menu on your phone. If you do find something called "Bluetooth," there will also be an option for switching it off. If you're still not 100% sure, take it to a store and have them do it for you.

More importantly, there shouldn't be anything on your phone that you don't want someone else to have. Whether the attack is via a high-tech wireless method from across the station platform, or the more common grab-a-handbag-and-run method, you'll feel happier if they didn't get hold of the good stuff.

THE MART

By DON CLARK

Santa Clara, Calif.

Companies in Silicon Valley say their technology is set to revolutionize the look of games. Hsu Huang, chief executive of Nvidin Corp., here, is showing off something that really is.

It is a computer-generated model of a character named Nalu, with a cloud of golden hair that realistically seems to reflect the light and flow with the water. Nalu's skin is rosy, unusually lifelike, and she is displaying generous quantities of it as she flirts with the player.

More than 3,000 kilometres away in a suburb of Toronto, executives at rival ATI Technologies Inc. are preparing a coming-out party for Ruby, another computerized creation who also has a skin texture unusually detailed for a videogame character, along with a shock of red hair and pensive glances.

The two characters are unlikely soldiers in a fast-moving technology battle helping to shape the evolution of digital entertainment. Nvidin and ATI, the two leading providers of chips that control graphics on personal computers and other gadgets, developed the animated figures to demonstrate the power of the improved technology each company is unveiling this month. The real animation increases as images of greater number of geometric blocks, called polygons, to create. Nalu is composed of 300,000 polygons; Ruby has 80,000—both far far in the future of real-time interactive movies.