For a computer scientist, I suppose I’m a bit of a Luddite. Unlike nearly all the computer science sorts I know, not to mention a huge fraction of professionals in all walks of life, I’ve resisted the move toward increasingly capable (and increasingly expensive) mobile devices such as the Apple iPhone, BlackBerries, and so on. I haven’t felt the need to be attached to my email 24/7, and I haven’t felt the compulsion to have easy access to all the other applications that are available. Well, maybe that last statement is getting less and less true, as increasingly interesting applications become available. Also, of course, consolidating my various devices would have advantages.

The one device I always take with me on trips is my laptop. I know I can rely on security between my browser and the various Internet servers I access, even if the networks I use are, well, dodgy. This doesn’t mean I’ll willingly connect to the “Free Public Wi-Fi” hotspots (see, for instance, http://onemansblog.com/2007/10/23/the-threat-of-free-public-wifi/). Given that I read mail via a secure connection and don’t do an awful lot else, I should be okay. There’s always my desktop firewall of course.

But what if I didn’t want to take my laptop? I recently had dinner with an old friend who had taken a trip around the world. I was really surprised to hear him talking about the great Internet cafés in various countries, such as India, and even more surprised when he mentioned using them to do his banking. Was he daft? Shouldn’t he assume that every “public” computer he accesses has been infested with a dozen keystroke loggers, all competing for the chance to let someone follow him into his account and clean him out?

As he explained it, he established a bank account in the US. He entrusted that bank with account information for other companies that he might wish to access, and the “point” bank provided an automated tunneling system to connect him to those other institutions. So, if he could access his “point” bank securely, he could access anyone with whom he might have to do business. (The technology is provided by Yodlee; see www.yodlee.com/solutions_pfm_ymfpf.shtml.) To access the bank in a way that wouldn’t let others follow his tracks, he had to log in with both a regular password and a temporary credential he received via SMS to his cell phone. That credential was good only for a few minutes and, once used, couldn’t be reused. So, the window of vulnerability for someone else to access his account was extremely brief. What if someone was actively monitoring his kiosk and could present him with a fake interface while draining his accounts using the real connection he had just himself established? Basically, he was willing to take that chance, assuming the threats were from capture and replay rather than real-time rip-offs. (Note that his bank did provide a customized SiteKey image to him when he presented his login name and before he presented his passwords — a feature that provides some assurances but is still vulnerable to man-in-the-middle attacks.)

I think I’m a bit more paranoid than my friend — perhaps not; I learned my friend left only a relatively small amount of money in any of the accounts accessible through this service, with weekly automatic transfers from another account; the account with most of the money wasn’t accessible remotely — and would figure that even if the real-time corruption of a public access point wouldn’t happen today, it would be close to happening tomorrow. In fact, I went online to look into this issue a bit; I found such items as http://preview.tinyurl.com/yb8g7rw, which discusses hackers using a particular old-fashioned phone to clone a phone number and receive the SMS messages intended for it. This would let a hacker get access to the bank at any arbitrary time after obtaining the login credentials from the Internet café, and, from there, the hacker could actually access all of my friend’s other accounts with no special controls. Even the
controls that many banks place on accesses from "new" locations would fail when the accesses all come from the "point bank" that’s been accessing them all along. (And remember, even if the other organizations challenged these accesses, the hacker would have seen how those challenges were answered in the café and could repeat the answers back.)

Looking around, it seems mobile Transaction Authentication Numbers (mTANs; see en.wikipedia.org/wiki/Transaction_authentication_number) are becoming commonplace in areas of the world such as Europe, even if the US is as usual slow to catch on (my friend’s example notwithstanding). As they become more popular, they, of course, become more enticing to hackers.

One alternative to the simple SMS interface is an RSA SecurID system (en.wikipedia.org/wiki/SecurID), or similar methods for two-party authentication. With SecurID, a customer could carry a small device with a number that changes every few seconds, so physical possession of the device is an indication that someone is entitled to access an account. That device can be useful for someone without mobile phone access in a locale, or as an extra guard against lack of mobile phone security, though it has its own threats.

I n the end, though, I think the era of the Internet café as a means to conduct personal business is over, mTANs or otherwise. You use your smart phone, or, if you’re a Luddite like me, you lug your laptop … and you hope your laptop hasn’t been infected by a parasite!

**Acknowledgments**

I would like to recognize the helpful input of my “old friend,” the intrepid traveler Bob Mayo, who provided not only the initial tale of his remote banking exploits but many additional comments on my description of them. The opinions expressed in this column are my personal opinions. I speak neither for my employer nor for IEEE Internet Computing in this regard, and any errors or omissions are my own.