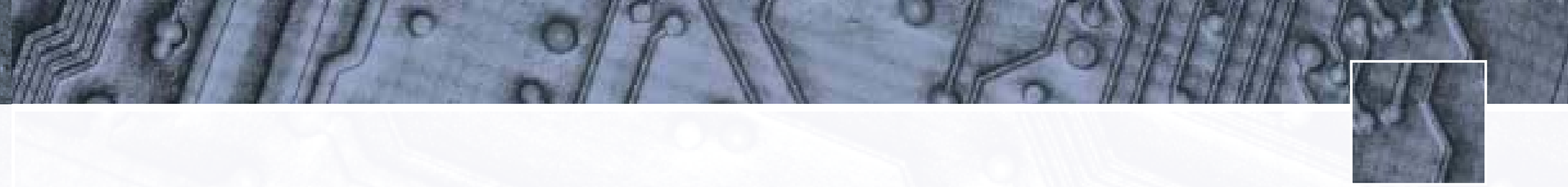

one online 24/7. This "around the world geek network" can come in quite handy when needing advice on a technology issue and your Googling skills are failing.

So where's the hitch? VOIP systems and IM systems still suffer from outages and the quality of the phone call. When Wayne (remember him from our first example?) needed to call his wife on a very critical issue, he switched to a traditional phone to ensure that the call would be connected and clear. And currently, you cannot make location-aware calls to emergency numbers; if you call 911, the system will think you are still at your home base and not at your current location.

Bottom line — we now can communicate in ways other than POTS (plain old telephone service). New ways of connectivity also mean new opportunities of communication for you and your clients. We're now used to cell phones to the point of them being a normal everyday item you own … it won't be much longer before communicating won't be just with a device that has the word "phone" in its name. As a *BusinessWeek* article recently said, "it's not about connecting places, it's all about connecting people."

**Susan E. Bradley, CPA/CITP, MCP, GSEC, is a principal with Tamiyasu, Smith, Horn and Braun in Fresno, Calif. Contact her at *sbradcpa@pacbell.net.*** ●

## Letter to the Editor

### WEP an Unsecured Connection?

**Dear Editor,**

**I read with interest the article by Michael R. Dickson, "Understanding Wireless Technologies for Maximum Benefit" (Sept/Oct 2004). I would like to clarify the security issue with Wireless Encryption Protocol (WEP). Even though WEP uses 128 to 154 bit encryption, at a start of a session, WEP in protocols 802.11a and 802.11b passes identifying key information in the "clear." This means that a hacker who listens to the frequency may obtain WEP keys from a station initiating a session. Subsequently, hackers can authenticate themselves as a legitimate user of the wireless router.**

**In addition, I could not find in the article discussions of interference of wireless routers that are located in proximity and more importantly, "signal leakage" of wireless signal outside the perceived perimeter of an organization.**

**In conclusion, so far, WEP should be considered an unsecured connection.**

**Yigal Rechtman, CPA.CITP, CFE, CISM**

*Dear Yigal:*

*You are correct! Wireless Encryption Protocol (WEP) has weaknesses, one of which you describe. In fact, nearly every single security strategy has a weakness or flaw; that is why a layered approach to information technology is always recommended. Wi-Fi Protected Access (WPA), unveiled in late 2002 as the replacement for WEP, also has some weaknesses when users select short pass phrases, although this weakness is harder to exploit than the one you mentioned.*

*In the specific case you cited, an additional 5th layer of control (in addition to the four suggested controls in the article) could be implemented to offset or mitigate this risk by requiring specific identification of every wireless device authorized to use the network by its Media Access Code (MAC address). While it is possible to spoof a MAC address, it requires a lot of time and costly equipment making it unlikely except for the very competent and very determined hacker.*

*I don't in any way want to diminish the importance of having "fail-safe" security for wireless networks, but few of us have the expertise or resources (people and dollars) to implement a 100% secure network; wireless or not.  Therefore, a security program that is designed to keep out 1) casual unintended users who may discover the existence of your wireless network just because they visit your office (or the home or office next door), and 2) technically competent hackers looking for open networks to exploit, should be considered to be the minimum level of security employed on a small business or home wireless network.*

*Thanks for your feedback.*

*Michael R. Dickson, CPA.CITP* ●