ON THE BENCH

PROJECTS, REVIEWS, TIPS & TECHNIQUES

This is your equipment page. Monitoring Times pays for projects, reviews, radio theory and hardware topics. Contact Rachel Baughn, 7540 Hwy 64 West, Brasstown, NC 28902; email editor@monitoringtimes.com.

Cordless Phones - Let the Buyer Beware

By Lee Badman

Here's a typical scenario – you need a new telephone at home, so off you go to the neighborhood department store. Most stores offer several models, with a range of accompanying prices. Many people tend to look first at price, then maybe consider how the phone might look hanging in the kitchen or sitting on the desk. Perhaps the appeal of a system that lets you use a couple of handsets comes into play. Some mental gymnastics are done, a shiny new phone in its excellent packaging gets rung up, and a new phone goes into service in your home for a couple of years. No news here, right? Unfortunately, it very well might be a big deal – if thoughts of security are left out of the cordless phone purchase process.

Many of us are getting ever more wise to the increasing number of various threats to our privacy that pervade modern life. We know enough to not let the guy behind us see our PIN get entered into the ATM. We are more mindful of email scams, Internet-borne worms, and spyware that might contribute to identity theft as we use our computers. Even in traffic, our every move may be on video – so we buckle up and slow down to stay legal. But the simple act of talking on the phone is easy to take for granted – yet using the wrong phone may be giving away the farm when it comes to personal information and details of our lives that we may not want the general public to know about.

Even *MT* readers could use the reminder that cordless telephones are radio devices. As such, signals are transmitted, and it's often anybody's guess where those signals go (I personally have never seen an antenna pattern diagram for cordless phones). But there are some assumptions that most consumers – including many in the radio hobbies – share about cordless phones. For example, it's a safe bet that most people envision that the base and handset of their cordless phones can only "talk" to each other. It's also assumed that the interaction between the handset and base of a given cordless phone is somehow "protected" from casual eavesdropping. And most folks – if asked – would probably assume that their cordless phone signals are not going much farther than the walls of their home or apartment.

The uncomfortable reality is that many consumer-class cordless phones contradict all of these assumptions. And it gets worse: Many phones are flat-out misrepresented in both packaging and available technical literature, so it's hard to tell what you might be getting "under the hood," even when trying to shop smart.

Fundamental Problem #1

Most consumer devices that rely on transmitted signals – from wireless networking components to garage door openers – play in unlicensed spectrum. Cordless phones are no different. And all communications-oriented devices in the unlicensed spectrum sandbox are pretty much at each other's mercy. We're talking about baby monitors, wireless intercom systems, FRS radios, cordless phones, wireless microphones, and more. If one device can pick up another's signals, well, that's just the way it is… and most users assume that limited range (and perhaps some unnamed technical magic) will make the products safe to use.

The onus is definitely on the consumer to use these devices with care, and little in the user guide jumps out to tell us as much. Chances are that the typical consumer is probably unaware that scanners, ham radios, and wideband communications receivers can often receive every single frequency in use by all of these communications products – at a far greater range than might be expected.

One day while working at Syracuse University, my Uniden BCT-246T scanner was doing its stuff in the background. Even though my office is in the basement of an old fortress-like building with walls of several-feet-thick concrete, the scanner picked up a phone conversation from the next building over with its "Close Call" feature. In this case, the call belonged to a faculty member who I work closely with on occasion – so I was comfortable sharing my findings with him for his own good – especially since he is a "wireless guru" who teaches and writes about wireless networking and related topics. The revelation made for some lively chat – more on this story in a bit.

Fundamental Problem #2

So far, nothing discussed here is big news to most scanner enthusiasts – we've known about the listings for baby monitor and cordless phone frequencies all over the Internet for years. So, you'd think that when we look to purchase cordless phones, our knowledge would make us better shoppers. Conventional wisdom would dictate that if we don't want to be eavesdropped on in the same bands that pick up baby monitors and FRS radios, then we should buy phones that operate in other bands – maybe 2.4 GHz or 5.8 GHz, where the typical scanner or wideband receiver have no "ears."

Now for the problem: Even phones that are labeled as 2.4 GHz or 5.8 GHz often work at the lower frequencies with little or no notification to the user. In other words, a 5.8 GHz cordless phone might also be a 900 MHz phone – and unless you're monitoring, you'd never know.

❖ Real-World Cases

Back to my professor friend – in this case he had the Panasonic KX-T9000, an older cordless phone that works in the 900 MHz range. The Professor was in disbelief – one of the foremost experts on wireless networking and security was talking business daily – often sensitive business – on a phone that could obviously be listened to by a relatively low-cost consumer receiver!

Yes – the act of listening to cordless phone conversations is illegal – but it's also 100% passive and in most cases undetectable, so unless the eavesdropper brags about what he's hearing, the law is irrelevant. One of the Prof's first questions as he tried to take it all in was "…yeah, but how many people really have scanners?" After we talked of volunteer firemen, news reporters, NASCAR fans, and ham radio operators with rigs that have extended receive functions, the potential for his personal and business-related conversations falling on many unintended ears became very clear.

The icing on the cake? The fact that with a mouse-click, I could have recorded his conversation with the ARC246 scanner control software running on my computer. (Sound files can be manipulated, forwarded, or used for a slew of nefarious purposes.) Finally, a Google search of "Cordless Phone Frequencies" turned

up frequencies for many phones, including the KX-T9000. It was quickly replaced by a new model in hopes of better security, after the full gravity of the situation was finally impressed upon the good professor.

Closer to home, I was shocked one day to pull into my driveway as my Yaesu FT-90R mobile dual-band amateur radio was scanning through its programmed channels, and it settled on the unmistakable voices of my wife talking with her mother. A check of the channel showed she was booming through on one of the FRS radio channels (between 462.5625 and 467.7125), despite the fact that she was talking on a General Electric 2.4 GHz cordless phone!

I purchased this phone after reading of the eavesdropping dangers of phones NOT in the higher frequencies – and so was quite taken aback to see a unit labeled 2.4 GHz was even capable of working in another slice of spectrum altogether. After reviewing both the box that the phone came in and the "manual" (a one-page how-to), I could find no mention of this phone being equipped with circuitry for other bands, yet I could demonstrate the effect at will by using the phone and monitoring it with the FT-90R, my BCT-246T scanner, or the Icom R3 receiver – all were in agreement that the GE Model 27998GE6-C 2.4 GHz phone was indeed operating far from the 2.4 GHz spectrum I expected it to use.

Chalking up the GE phone to a malfunction or other anomaly, it was off to WalMart for a replacement. Looking over all the offerings (and carefully reading the packaging), I settled on the modestly priced Uniden EXAI5580. With a box that was plastered with "5.8 GIGAHERTZ" all over it – and no mention of lesser frequencies anywhere on the feature list – I went home feeling good about replacing the traitorous GE for this new super-sleek phone.

After charging the unit, I had my son make a call while monitoring with the BCT-246T. My blood boiled – there in the 900 MHz range on my scanner was my son's entire conversation with one of his buddies – the full-duplex happy banter of a couple of young teenagers – that wasn't supposed to be on that frequency. My mind filled with dread – are all cordless phones like this?! Is the conspiracy that widespread?

I went to Uniden's web site, to reread the list of specifications, which confirmed that this was supposed to simply be a 5.8 GHz phone. I went through the manual page-by-page. Surely there must be some explanation, some narrative about how and why this phone would ever use frequencies other than the 5.8 GHz that was touted online and on the box it came in. Finally – 51 pages into the manual, I found a single reference that the phone used frequencies between 925.181 MHz and 927.451 MHz – but no explanation as to when or for what. It was time for a phone call to Uniden.

❖ Even the Manufacturers Seemed Confused

My first call to Uniden was downright bewildering. The first customer service rep I spoke with told me that she didn't understand the frequency issues I was describing. After putting me on hold, she came back and said that the base of the phone talks to the handset at 5.8 GHz, but the handset talked back to the base on the 900 MHz. When I told her that the scanner was picking up both halves of the conversation on a single discreet 900 MHz frequency, her supervisor got on the phone and echoed what she had told me and insisted that my particular phone must be malfunctioning. Though I was skeptical, I swapped the phone for another one – and found the same condition.

Another call to Uniden – and this time another story – but one that at least made more sense. It turns out that indeed the 900 MHz frequencies are used – for "extended range." Unfortunately for me, this seems to mean anywhere in my house, including a foot from the base of the phone. When I mentioned that the packaging does not say that 900 MHz is used, the rep I spoke with disagreed, and told me it was stated very clearly on the box.

After looking the box over again, I still could not find reference to 900 MHz – until I turned to the side that was printed in Spanish, where I found in very, very small letters *"Este producto combina las frecuencas de 5.8 GHz y de 900 MHz, las cuales aumentan la claridad."* That was it: the only reference that product was not 100% 5.8 GHz, and it wasn't even in English. (At least the second Uniden rep agreed that the labeling left much to be desired.)

Back to the GE phone – calls to Thompson (who handle service on GE Cordless phones) were not free, nor productive. After lots of time on hold at my cost, I could not find anybody willing to spend any time on the issue, or who would address that the packaging and manual left out the fact that in this case, 2.4 GHz means "2.4 GHz and the easy-to-eavesdrop 462.5625 – 467.7125 MHZ range."

Finally, after looking at many phones on many shelves from several manufacturers, I found that most cordless phones being sold today do not make mention of anything other than their "primary" frequencies of 2.4 GHz and 5.8 GHz – which can certainly give consumers a false sense of security when shopping based on frequency alone.

❖ Spread Spectrum (and privacy codes) to the Rescue

By now, we know that 2.4 GHz is not always 2.4 GHz, and 5.8 GHz is hardly 5.8 GHz exclusively when it comes time to sell cordless phones. Maybe the truth is too technical for the masses, so it just gets left out.

Whatever effect or philosophy is at work, there is a solution for safely buying a cordless phone. Sticking with 2.4 and 5.8 GHz is where it starts – but make sure any phone bought is using Digital Spread Spectrum (DSS) between both the base and the handset and back.

This "breaking up" of what would otherwise be a narrow-band signal adds greatly to security, as evidenced by the military's long-running use of spread spectrum. But, the security brought by spread spectrum does little good if your neighbor has the same phone and picks up your conversations (or makes outgoing calls on your dime) because the hardware is the same. This is where privacy codes, addressable phones, or whatever else the manufacturer chooses to call the mechanism comes in – you want a base-handset pairing that doesn't allow other uninvited phones to participate. Other benefits of Digital Spread Spectrum are less susceptibility to interference (same holds true for wireless networks built on spread spectrum), and usually slightly better realized power.

Remember – Digital Spread Spectrum is not the same thing as "Digital" – digital cordless phones might prevent eavesdropping, but some digital phones "switch over" to analog for increased range, unbeknownst to the user. If security is your goal, don't settle for digital – go for Digital Spread Spectrum. Also, "frequency hopping" is not spread spectrum – it simply means the handset chooses between available frequencies for the clearest signal.

Cordless phones, like wireless networks and radios, give amazing flexibility and portability to communications. Unfortunately, to the unwise, cordless phones can be as dangerous as Internet scams or losing your wallet for identity theft and similar problems. Know the score on cordless phones, and if there's any doubt on the radio goings-on with a given phone, leave it and move on. Finally – use that scanner or receiver and audit your home or office cordless telephones. What you find might shock you.