SECURITY NOW!

Transcript of Episode #6

# Mechanical & Electromagnetic Information Leakage

**Description:** Triggered by a recent report of three UC Berkeley researchers recovering text typed at a keyboard (any keyboard) after simply listening to ten minutes of typing, Leo and I discuss the weird realm of "alternative information leakage" - from CRTs glowing, to radio emissions, to LED lamps on the front of network equipment...to a microphone listening to anyone typing.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-006.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-006-lq.mp3

**Leo Laporte:** This is Security Now! Episode 6 for September 22, 2005. Steve Gibson is with us, our security wizard from GRC.com, author of SpinRite, ShieldsUP!, DCOMbobulator, LeakTest, and all those great security programs, as well as, of course, as I mentioned, SpinRite, which is a fabulous disk recovery program. Steve's back in Irvine, I'm back in Petaluma, so we're home safe and sound. And we're going to talk today about electronic eavesdropping and how people can spy on you.

**Steve Gibson:** Well, there's been a lot of dialogue in the last week because three researchers at Berkeley wrote some software which, after just recording the sound of someone typing, not a prepared text, just random English language - they need to assume that it's English because they use English dictionaries and something called Markov modeling which allows you to determine the probability of one letter following another - which is language based, but not requiring that their system be trained with a previously prepared text, just recording the sound of someone typing. They record ten minutes of the sound of someone typing. Then their machine, which is running a 3GB Pentium IV, takes 30 minutes to process that sound. And they are able to, with 96 percent accuracy, determine what was being typed, just from the sound of someone typing.

**Leo:** How have they done that? Have they mapped - does each key sound different?

**Steve:** Well, it turns out, yes. There are enough - they use the energy content of the keystrokes as opposed to the frequency domain content. Some of this has been done before using fast Fourier transforms, which determine essentially the spectrum. These guys use the energy content that is represented by the sound. And there's enough variation in keys that they are able to record that. Then through processing this, they group the keys that they are unable to differentiate into similar groups. But then, by presuming that English is what's being typed - that is, words that they have in a dictionary - they're able to process that information and disambiguate the keys which sound indistinguishably different and figure out what they are. Basically sort of running a speller and a grammar check on this, they're able to break it apart and figure out what was done.

The chilling thing is that, once they've done that, they can, for example, they're able to determine passwords which are not in the dictionary - that is, random characters that are being entered - with a 90 percent probability. They end up with a list of possible passwords that were typed. And with very good probability, the correct password is in this list of, like, a hundred passwords that it could be, based on what they heard being typed.

**Leo:** So someone could put a recorder in your cubicle at work and basically see everything you're typing. You don't need a keystroke logger, in other words.

**Steve:** Well, exactly. Now, if you had that kind of physical access to someone's cubicle, what you'd really do is you'd stick one of those little in-line keystroke loggers into their keyboard connection. You know, that's a real risk from that kind of physical proximity. But I think the real danger here is, for example, if you had a parabolic microphone that was aimed at someone's keyboard from, you know, across a hall or some distance away, where for whatever reason you didn't have direct access, or maybe, for example, you could bounce a laser off of their window in order to pick up the sound of them typing in their office...

**Leo:** The window makes kind of an audio transducer, so you could actually see the vibration of the window? Is that...

**Steve:** Oh, exactly.

**Leo:** From the typing, just like a microphone.

**Steve:** And that technology exists pretty well. Now, well, what's interesting is this is another in a long series of security and information leakage which is a function of electrical or mechanical or electromagnetic leakage from a computer. You know, we've all heard, you know, years ago there was this technology called Tempest, which was - it attempted to, and apparently successfully, determined what image you had on your screen based on the electromagnetic leakage from a CRT.

**Leo:** "Van Eck freaking" they call that, yeah.

**Steve:** Exactly.

**Leo:** So, I mean, Tempest was an attempt to - that was the military spec to avoid it by shielding. And I remember PGP used to have a Tempest mode where, instead of displaying the characters in crisp black and white on your screen, it would do as a very light blue that apparently was supposedly more difficult to freak.

**Steve:** And so the point would be, exactly, that the scanning beam, in displaying that light blue, it was enough low contrast, and there wasn't enough difference...

**Leo:** Right.

**Steve:** ...that it didn't put out a signal that was able to be picked up.

**Leo:** I notice they've - as far as I know, they've taken that out of recent versions of PGP. Maybe not something in great demand. How serious is this stuff?

**Steve:** There's also been some other research recently that is able to do this using the ambient light generated from the CRT...

**Leo:** Right.

**Steve:** ...and also even from an LCD, apparently.

**Leo:** Yeah, Bunnie Huang, who was the guy who cracked the Xbox ["Hacking the Xbox: An Introduction to Reverse Engineering" by Andrew "bunnie" Huang], I remember, told us that he could, for the screensavers, build us such a device that would - you could see around corners, in effect, because if you could see the flicker, the strobe coming off a CRT, you could reconstruct it into this visual on the screen. That's all it took.

**Steve:** But not easy to do. You know, the work I did years ago was to create a high-resolution light pen for the Apple II computer...

**Leo:** Oh, I remember that, yeah.

**Steve:** ...that used a photo diode. You'd need an extremely fast response photo detector in order to pick up the scanning beam on a CRT. But it's certainly possible to do. I mean, that technology exists now, and it's been refined a lot because, of course, that's how we move information through fiber optics is by having very, very high-performance photo reception at the receiving end of a fiber optic. Which brings to mind another issue, and that was about a year ago people suddenly got concerned that the LEDs which were showing the activity of their routers was a similar sort of electromagnetic, in this case optical, leakage of what was going on in their networks.

**Leo:** And it was strobing fast enough that you could see data?

**Steve:** Well, I mean, that's the thing...

**Leo:** I don't think so.

**Steve:** ...is that it was one of these sort of urban legends that made the rounds through the Internet community about a year, maybe a year and a half ago, to the point where ISPs started putting black electrical tape...

**Leo:** Ohhh.

**Steve:** I'm not kidding you - over the lights on the front of their networking equipment because they were afraid that people were going to suck the information out somehow.

**Leo:** I don't think you have the resolution. Maybe for 300 baud, but not for 10 megabits.

**Steve:** Well, I was immediately skeptical because all of the LEDs that I've seen...

**Leo:** They can't switch fast enough.

**Steve:** Well, they're showing you packets...

**Leo:** Right.

**Steve:** ...not bits.

**Leo:** Right.

**Steve:** And so they're only meant to be information illumination and not actual data being moved.

**Leo:** If they were showing you bits, they'd be on constantly because the bitrate is so fast.

**Steve:** Right. So what's interesting about all of these is that, I mean, based on all the email that we've received, people being concerned now about people listening to them typing on the keyboard, it seems to me that it's an interesting issue for security, and that is that it's important to recognize that not just the traditional means of information leakage, but even these nontraditional approaches - optical leakage and now acoustic - are things that, you know, at the far end of the spectrum, it is a way for information to get out of your computer, something that people need to be concerned about. Well, or at least, you know, NSA sorts of people.

**Leo:** Yeah. Did the Berkeley researchers come up with any recommendations?

**Steve:** Well, this is a preprint from their paper that they'll be publishing in the November issue of the Communications of the ACM for Computers, Communications, and Security. So they did experiment with, like, softer, quieter keyboards. They actually used a couple Dell specifically, like, low-noise keyboards for these experiments. And those keyboards generated enough noise that they were able to perform with 96 percent recognition of what was being typed.

**Leo:** I suppose if you had one of those white noise generators in the background, or something like that, you might be able to mask it.

**Steve:** Well, and certainly, if you were doing anything yourself to deliberately obfuscate this kind of problem, like deliberately hitting, you know, every other key harder, you know, clearing your voice while you're typing your password...

**Leo:** [Humming]

**Steve:** Right. They did talk about the notion of two-factor security, that is, for example, you know, using some other technology than just a password, which would not be typed at the keyboard. And, in fact, some of the people that responded to our second podcast, No. 5, about passwords, also talked about the idea of onscreen keyboards, where you would use your mouse and click the password on the screen in order to completely avoid the keyboard and the problem with keystroke loggers and so forth.

**Leo:** And of course biometrics, thumbprint recognition and the like, would have the same benefit.

**Steve:** Yeah, it's interesting that they have to take these keystrokes, the sound of these keystrokes, in context. That is, you know, you need to use English, and they largely improve the accuracy by figuring out what, you know, based on the sounds, there were many possible combinations because acoustics wasn't perfect. Not every key sounded unique. So they ended up with groups of keys that they were able then to say, okay, here's all the words in the dictionary that are possible, versus based on what we've seen, here's the groupings of keys that could be pulled out. Now, you know, what of these groupings map into the words, they did that. Then they figured out, okay, which words make sense from a grammar context, based on the assumption that English is being typed?

**Leo:** Don't you think, Steve, though, that worrying about these kinds of things is kind of ignoring the larger danger of the fact that your stuff is being sent over the Internet and, you know, that, I mean, frankly, the password, the weakest point is the storage on the other end. I remember IBM did a study a few years ago where they discovered that something like eight out of ten of the big e-commerce sites had poor password security on their end.

**Steve:** Well, or poor storage of the data.

**Leo:** Right.

**Steve:** Like, for example, unencrypted databases at the other end.

**Leo:** Right. So that that's really the greater risk.

**Steve:** Yes, I completely agree that this is sort of in a far out end of what any real normal user needs to be concerned about. But again, you know, the people that listen to this podcast, who are surprisingly security concerned, were, you know, sending me links to this story that I have now seen a hundred times by the end of the week. And I was thinking, okay, well, let's just talk about this and put it into context, which is something I'm glad you're doing because it is clear that, you know, this is, again, it's the sort of thing where, in order to record the data and the sound of someone's keyboard, you would have to have, you know, either a parabolic mic which is somehow aimed at their keyboard, or plant a microphone or a recorder of some sort near them. Well, if you're going to have that kind of physical access, there's way easier ways to get the information, far more reliable ways to get it.

**Leo:** That's right, yeah, yeah. And Van Eck freaking, while, I mean, I've seen demonstrations that kind of work. I don't know if anybody's really demonstrated that you could, you know, through a hotel room wall, for instance, see what the other guy is doing on his screen.

**Steve:** Well, what is a little annoying is that, based on the paper, which I've read and studied carefully, this was really some serious number crunching and a lot of work.

**Leo:** Yeah.

**Steve:** But they're going to post the source code for this...

**Leo:** Oh, great. Oh, great.

**Steve:** ...on their site. Keyboard-emanations.org will be the name of the site. And on our Security Now! page I've got a link to a page of links of various information.

**Leo:** Very interesting.

**Steve:** Now, one other aspect of this which is sort of interesting is that, from a legal standpoint, this is not illegal.

**Leo:** Really.

**Steve:** Yeah.

**Leo:** It's not eavesdropping. It's not...

**Steve:** Well, it's not eavesdropping because it's not covered by the law because this is not considered deliberate communication. So even though the law has been amended so that, even if you don't have an expectation of privacy, there is sort of a presumed privacy in the law, this is not considered communication. So the sound of your keyboard being typed is not protected under the law because there's no expectation that this is communication.

**Leo:** Mm-hmm, it's just incidental sound.

**Steve:** Whereas, of course, you know, Internet communication or telephone communication and so forth, there you're protected. But not any kind of, you know, optical, electromagnetic, or acoustic emanations from your system. So, you know, these guys are going to post the source code for this. Who knows what kind of tools the open source community will generate from that. And it may be at some point that, in the same way that we have now cracking tools that allow wireless communications to be cracked far more easily just by downloading them and running them, at some point you can foresee in the future that there will be freely downloadable software that will process the sound of keyboards being typed and figure out what people are typing.

**Leo:** Well, I only have one thing to say to that [typing sounds]. And there. You detect that, huh?

**Steve:** Right.

**Leo:** All right. Steve Gibson, fascinating conversation. And I'm sure people will have more to say about it. And we encourage their feedback. How do you like people to get a hold of you?

**Steve:** We've got a response form down at the bottom of the Security Now! page on GRC.com, and that's how lots of people are sending their comments and thoughts and questions.

**Leo:** Great. So that's at GRC.com/securitynow.htm. And of course we thank AOL Podcasting at AOLmusic.com for providing the bandwidth for Security Now!. We couldn't do it without them. But their contribution makes it possible for us to do this for free. And Steve also puts transcripts of each Security Now! up on his website. Steve, how long does it take to get a transcript out, about a week later?

**Steve:** No, I've got this great gal who's into computers and knows the moment these things go up. It normally takes only a few hours.

**Leo:** Wow. Wow. Again, that's at GRC.com/securitynow.htm. Can you come up with a little redirect for that to just make it so much easier for me to say?

**Steve:** We always have a link at the top of our home page.

**Leo:** GRC.com, okay.

**Steve:** But just GRC.com, and that'll get them to it.

**Leo:** That's easy enough to remember. And this time - I didn't put up the show notes last week, so I will put dual show notes up this week. For those of you who use RSS readers or professional-style podcast clients to get this, you'll see the show notes have links in it, and there's more information. But for those of you using iTunes or less capable podcatchers, the web page will have that information. Again, GRC.com/securitynow.htm. And be careful what you type. I'm more concerned really about the NSA with spy satellites looking in at my windows and watching the strobe from my monitors and reconstructing what I'm looking at. You know what they'd see right now? A picture of you...

**Steve:** [Laughing]

**Leo:** ...on Skype. Steve Gibson, thanks a lot.

**Steve:** Thank you, Leo.