Reed Electronics Group

MICROPROCESSOR REPORT

www.MPRonline.com

THE INSIDER'S GUIDE TO MICROPROCESSOR HARDWARE

THE EDITORIAL VIEW

MICROPROCESSOR CONFUSION

By Tom R. Halfhill {10/30/06-03}

Relatively few people in the world know much about microprocessors—what they are, what they do, how they work. This ignorance may seem harmless. Merely learning how to use an electronic device is challenging enough. Why should ordinary folks get bogged down in low-level technical details that couldn't possibly matter to them?

Unfortunately, as microprocessors become ubiquitous, knowing something about them is becoming not only desirable but necessary. Those who are familiar with microprocessors—including everyone who writes for this newsletter and everyone who reads it—should help educate the general public about an important technology that can seem as mysterious as string theory.

Recently, three incidents made me realize that lay people need to learn at least a little about microprocessors. Two of those incidents may seem funny, but they are troubling when you consider the implications. The third incident made me think hard about the long-term role of microprocessors in our world.

In the first incident, I brought a malfunctioning digital camera to the service desk of a camera shop. This particular shop is in Silicon Valley, and it has an uncommonly competent staff that is knowledgeable about the store's large inventory of advanced-amateur and professional equipment. In other words, these people aren't dummies. That's a high compliment in an era of rapidly evolving photographic technology and generally poor customer service at retailers.

After I described the camera's problem to the person at the service desk, he asked how I transferred photos from the camera to my home computer. I told him that usually I remove the camera's memory card and insert it into a card reader. "Hmmm," he said. "Maybe a virus from your computer has infected your camera."

I rolled my eyes and tried not to laugh. I wanted to explain that an executable program written for a particular microprocessor architecture (the x86) and operating system (Windows XP) couldn't possibly infect the camera's embedded microcontroller and system firmware, which are based on a completely different microprocessor architecture (in this case, Fujitsu FR-V) and embedded operating system. But where would I start? So I ducked the problem by explaining that I usually reformat the memory card after moving it back to the camera (true), which would erase any virus. He accepted my explanation and changed the subject. Whew!

More recently, a similar incident hit the news. Apple inadvertently shipped an undetermined number of video iPod players with the Windows RavMonE virus lurking on their hard drives. A headline in my local newspaper said, "Windows Virus Infects iPods." The article didn't clarify that the iPods were merely carriers—their ARM embedded-processor cores are as immune to RavMonE as they are to smallpox. The iPod might spread the RavMonE virus when attached to a computer, but the iPod isn't "infected" in a way that could harm the player.

To engineers and others familiar with microprocessors, those two incidents might seem funny—at first. But the more I thought about them, the more concerned I became. These kinds of misunderstandings can cause unnecessary

grief for people who don't know better. For them, it's no laughing matter. They might return, or stop buying, the electronic products that your company or customers spend years designing. Or they might convince the government to pass another stupid law. Not funny.

The third incident that sparked my thinking on this subject was at the ARM Developers Conference in October. ARM's keynote speaker was inventor Ray Kurzweil, author of *The Singularity Is Near: When Humans Transcend Biology* (Viking Books, 2005). Kurzweil's talk was fascinating and included a demonstration of his latest invention, a portable text-to-speech reader for the blind. No matter what you think of Kurzweil's controversial theories on immortality, one thing is certain: microprocessors are rapidly moving from desktop PCs to portable devices, from portable devices to wearable devices, and from wearable devices to microsystems implanted in the human body. This trend brings a whole new meaning to the industry term "embedded processor."

Already, millions of people are frantic about the foods and drinks entering their bodies. Is our spinach and lettuce carrying deadly E. coli O157:H7 bacteria? Do the benefits of omega-3 fatty acids in fish outweigh the risks of environmental mercury absorbed into the ocean's food chain? Are the chlorine, chloramine, and fluoride in tap water more harmful than the natural bacteria in bottled water?

Some American cities and states—including New York, Chicago, Los Angeles, and New Jersey—are considering laws that would ban transfats in restaurant food. It's not hard to imagine the same kind of attention and legislation aimed at electronic devices implanted in humans. People might be terrified that a computer virus hiding in RFID tags at Wal-Mart could wirelessly infect and disable their pacemaker, insulin pump, or C-leg. Shop till you drop!

You can see where I'm going with this. First, those of us who understand microprocessors shouldn't miss an opportunity to educate our fellow citizens, as I neglected to do at the camera shop. We don't have to deliver a crash course in engineering. Just a brief explanation can help, especially if it's not condescending.

Second, the engineers designing new products must make security their top priority. Although conventional computer viruses can't bridge incompatible microprocessor architectures, some cross-platform languages and file formats may pose a risk of "cross-species" infections. And any electronic device that interacts with another electronic device could become a vector for spreading malware that remains inert until it finds a vulnerable host. So be careful now, or be sorry later. ◇