Re: Can a computer virus kill the CPU?

Source: http://www.derkeiler.com/Newsgroups/comp.security.misc/2006−11/msg00053.html

- *From*: mike4ty4@xxxxxxxxx
- *Date*: 16 Nov 2006 17:33:07 −0800

w_tom wrote:

> For a longest time, satellites, et al did not have computer
> (microprocessors) or even encryption. Satellites were a gentleman's
> game even during the Cold War. Most processing was performed on earth.
> A satellite had only enough intelligence to maintain itself for short
> periods. Electronics was the simplest and the least complex possible.
>
> Later, simple processors were installed only for station keeping −
> only to increase reliability. I suspect TDRSS (NASA's communication
> satellite system) may have been a first to use intelligent processing
> for data − satellite operating as a switch and not as a repeater.
> However that is the trend. Electronics in aerospace is the simplest,
> old, and well understood because reliability and being 'fully
> qualified' are so critical. To put something more advanced means there
> was no alternative. Only then was massive money spent to qualify a new
> part.
>
> When more processing power is required, an expensive process would be
> used to qualify a newer and yet well proven processor. So designers
> kept most intelligent functions on earth. Yes, slowly more robust
> processors make it into space. But rarely is anything 'state of the
> art' in aerospace. 'Reliability' is a far larger consideration which
> often means old and well proven hardware. Processing power of one
> astronaut's laptop is far more powerful than all Shuttle computers
> combined. That laptop need not be reliable. Those shuttle computers
> must be extremely reliable − and still they sometimes fail. Therefore
> the Shuttle has five computers making flight decisions. A poll
> determines which three will be believed. Again, it's about
> reliability and why those computers have so little processing power.
>
> Viruses that attack firmware have even been shipped (unknowingly) by
> the computer manufacturer. Such viruses, although rare, have been
> observed (and manufacturers don't like to talk about it). But again,
> no hardware damage.
>
> Cited previously was the case where a monitor signal too high in

> frequency could cause monitor damage. So yes, sometimes a designer does make a mistake, the lessons learned, and hardware fixed so that software cannot cause damage.
>
> We also built customized equipment where a software bug could cause relay damage. But again, this was customized equipment AND restricted users also had no access to embedded software. Software was embedded so that damage could not result from user programming. Even customized equipment makes hardware as resilient as possible to software failure or malware.
>
> The context is not such custom equipment. This context is consumer computers. Consumer electronics is designed so that software cannot harm hardware. Consumer equipment must be that 'idiot proof'.
>
> More complex and custom equipment can be harmed if the attacker has very specific engineering knowledge of that item; a specific item targeted. Specific engineering knowledge is what a virus writer must have to specifically attack firmware for a specific machine. These customized machines were designed so that software could not cause hardware damage. But then some functions might not be so robust because costs would be so high and because of the unique customized nature of its function. It is possible to put a virus into a robot so that robot destroys its own arms. But then good luck trying to do it. It is possible, but ....
>
> Supercomputers are a different environment. The days of customize hardware (ie Cray XMPs) are gone. Same processor chips built for commercial purposes now are used in supercomputers where numbers of processors − not specialized functions − are the objective. Most 'souped up' chips are sold in the market. An example: Sony Playstation 3. This new hardware is also challenging how software can utilize the power − creates a massive challenge to software engineers.
>
> Don't assume that because it is a nuclear missile, then it must have the most advanced electronics. Instead, it will have the most 'reliable' electronics. Each market has different parameter requirements. Sony Playstation 3 would be far too unreliable for aerospace use.

And nuclear missiles do not need gigantic high−power computers, so it would be a waste of cash to get a "reliable", high−power processor built, right? And everything is determined by the amount of available money, and that money has to be spent wisely. Spending it on getting a super−tough Pentium built would be a waste, when one could do fine with something much slower.

> But consumer electronics is carefully designed so that software will not damage hardware. Computers are legacy designs where most of the machine is simply a faster version of the same thing done a decade ago. That legacy requirement is important because of what the market demands of consumer electronics − where everything is a black box and the retail 'computer expert' does not even know what a power supply does. In such markets, hardware is designed so that software (viruses, bugs, and mistakes) cannot damage hardware.

But in aerospace, etc. is the hardware used also just as impervious, if not
more so, to software−induced destruction?

> mike4ty4@xxxxxxxxx wrote:
>
> > So then, basically, it would be very difficult to write a virus that could attack 95% of the firmware out there and thus require 95% of infected systems to be sent back to the factory (which is what I had in mind when I asked the original question −− a virus that would demand factory return.), or have parts replaced, etc., and almost impossible to damage hardware physically with the virus, right?
> >
> > You mentioned about spacecraft not using advanced Pentium processors, only 8086s. But what if they needed more computing power? 8086 is a very slow processor and is only useful for relatively simple things. Even though they might not need it now, what if they do in the future?
> >
> > I also needed to know about the motivation to make the virus thing, where I asked about the military. Could it be possible that the military has a virus that can damage hardware or otherwise mandate physical repair procedures?
> >
> > Also, though, for military computers used for doing complex calculations or other intense activities, including supercomputers, is it possible that the chip companies manufacture "souped−up" chips for THOSE computers?

.