Eliminating some possible sources of hardware Trojans from PCs

No tags yet. + Add Tag

Sort replies by: Oldest first Newest first Most popular

Nick Jacobs . 10 days ago

When you buy a new PC, it comes with a lot of firmware that is generally hidden from the user. You have no simple way of knowing whether it contains Trojans.
There is a company that replaces many of the chips containing "opaque" firmware and replaces them with open-source firmware: Link . I've never used their product, and know nothing about them except what is available by googling. What they sell is basically a ThinkPad X200 with the firmware removed and replaced. The downside is that the ThinkPad X200 isn't exactly the latest tech in laptops; it was introduced in 2008. Of course it takes time to reverse-engineer the firmware and re-write it.

0 · flag

Chuck Gollnick . 12 hours ago

How, pray tell, does replacing the FIRMware guarantee that there are no HARDware trojans?

If IBM was not involved to give the new firmware authors the functional specifications for its chips, I would be much more concerned about errors and omissions in the reverse-engineering of the old firmware and hardware resulting in functional errors in the new firmware than I am about any trojans in the old firmware.

This raises an interesting dilemma, a bit of a Hobson's Dilemma in fact: is it more important for a computer to be secure or to function properly? The practical answer, of course, is somewhere in the middle. We want our computers to be secure, yes... but we also want them to function properly. Of what use -- other than academic curiosity -- is a computer that is completely secure, but doesn't function?

Low-level firmware that is based on somehow "black-box" reverse-engineering the hardware doesn't strike me as a good idea... as a path to reliable computing.

0 · flag

Nick Jacobs · 6 hours ago

Chuck,
Three points here:
1. Replacing the firmware isn't about a "guarantee that there are no trojans", it's about eliminating **some** possible sources of trojans. Of course there are other possible sources.
2. Every PC in the world today that runs Windows contains reverse-engineered firmware. That's because the original BIOS introduced by IBM more than 30 years ago contained a BIOS written by, and copyrighted by, IBM. To produce "IBM-compatible" PCs, other vendors had to reverse-engineer the original BIOS. Functionality from that 30-year-old BIOS is still present in modern PCs. So you're already using reverse-engineered firmware.
3. As far as I know, IBM no longer produces PCs or any of the chips used in them. (If it does, it's now a very minor player in the PC market.)

0 · flag

+ Comment

New post

To ensure a positive and productive discussion, please read our forum posting policies before posting.

B | I | Link | <code> | Pic | Math | Edit: Rich | Preview

Make this post anonymous to other students

Subscribe to this thread at the same time

Add post