Meditations on Trusted Computing

Fred von Lohmann

In 1641, in his Meditations on First Philosophy, mathematician and philosopher Rene Descartes asked how it is that we can trust our senses. What if, he asked, everything we experience is actually part of a delusion created by an omnipotent demon bent on deceiving us?

It turns out that a similar question has been weighing on the minds of Microsoft, Intel, and a number of other computer companies. How do you know that your computer is actually what it seems? After all, hackers could have broken into your computer and replaced the software on it with software that imitates, in every particular, the software that was on your computer before. To you, things would appear unchanged. But now your computer is under the hacker's control, logging your every keystroke, copying your most sensitive information, and sending it out over your Internet connection.

This points to another nagging epistemic doubt—how can any software on your computer trust any other software running on your computer? For example, when you run an anti-virus program, how can it be sure that the operating system hasn't been subverted somehow? After all, software installed by the hackers could intercept any warnings before they were output to your display, replacing them with screens announcing "no problems detected."

In short, how can you be sure that everything you experience on your computer is not part of a delusion created by hackers bent on deceiving you?

These are not idle questions. Today, computer users are increasingly besieged by malicious, hard-to-detect software designed to subvert computers—viruses, Trojan horses, worms, and spyware, to name just a few. This specter haunts not only individuals, but also a wide variety of companies, including health care providers, movie studios, intelligence agencies, and others who routinely entrust valuable or sensitive information to computers.

Enter the Trusted Computing Group, comprised of Microsoft, Intel, AMD, and several other large computer technology companies. The TCG companies are working on technology that will let you trust that your computer is what it appears to be.

Trusted computing: What is it?

First, you'll have to buy a new computer (did you think for a moment that a plan hatched by the world's largest software, chip and computer companies could start any other way?) that will include a special chip containing cryptographic hardware and keys.

You can choose to ignore the new chip, and your computer will behave just like the one you have now. You are free to install any operating system you like, and any software. The chip remains dormant until you decide to take advantage of it.

If you elect to activate the "trusted computing" features made possible by the chip, and if your operating system has been updated to take advantage of it, then your computer is "virtually" split in two, divided into "untrusted" and "trusted" sides. Both "sides" share the same CPU, the same hard drive, the same keyboard, and the same display, but the trusted side has an additional, very special property—it cannot be subverted by other software running on your machine. In other words, on the trusted side of your computer, you can run software with a high level of confidence that the software is what you think it is.

How? Well, the story depends on a great deal of sophisticated cryptography. When the trusted side of your computer saves data to the hard drive or to memory on behalf of a particular trusted software application, it does so in a secure, encrypted format. This encrypted data can only be read by that software application, running on the trusted side of your computer.

Malignant software that may be running on your computer (whether on the trusted or untrusted side) will not be able to read the encrypted data that belongs to another trusted application. In addition, the trusted side has a secure, encrypted channel to your keyboard and display, so malignant software cannot intercept data or interpose itself between you and the trusted application.

All of this allows you to trust the integrity of the software that is running on the trusted side, and that data saved by this software will not be accessible to subverted software that may be running on the untrusted side. (You are still vulnerable if a hacker has access to your hardware, however, as the security can be breached by hardware-based attacks.) So far, so good.

Trusting computing: Troubling implications

Trusted computing, however, does more than allow you to trust your own computer; it also aims to enable *others* to trust your computer. The key to this capability is in a feature called "remote attestation." This allows another person to ask the software running on the trusted side of your computer to identify itself. Because the answer comes from the tamper-resistant hardware on the motherboard of your computer, the "attestation" is relatively reliable. This feature certainly has some desirable uses (for employees logging into corporate networks from offsite locations, for example).

But there is a dark side. If others are able to verify that particular software is running on the trusted side of your computer, then some may refuse to communicate with you at all *unless* you are running their software. In other words, companies may begin demanding that you install and run the software *of their choice* on the trusted side of your computer. This would effectively give them control over a portion of your computer. You would be free to refuse, but then you would not be able to do business with them.

In a competitive market, this might not be a problem, as vendors would avoid anything that might alienate customers. In a market where competition is compromised, however, trusted computing can dramatically increase the power of a monopolist or cartel to impose "take it or leave it" terms on the public, by giving them the capability to insist on a relatively unassailable beachhead inside your computer.

For example, imagine that Hollywood movie studios decide to release their movies in formats that can only be played by certain trusted media player software. "Remote attestation" would be used to verify that the media player software was, in fact, running on the trusted side of your computer and that it had not been tampered with. This would give the movie studios unprecedented control over how your computer interacts with their movies. Your continued ability to make copies, take excerpts, fast-forward and mute would all be entirely within Hollywood's control, and part of your computer would now answer to Hollywood, rather than to you.

The implications, however, reach far beyond "digital rights management" schemes pushed by entertainment companies. Other industries may also eagerly embrace the idea that they can demand a beachhead inside your computer as a condition of doing business with you. For example, the dominant vendor for a particular software application (like Microsoft Word for word processing) could modify a future trusted version to prevent you from migrating your documents to a competing application.

As with many technologies, trusted computing has uses both for good and for ill, and thus should be viewed with a critical eye, lest the users end up, in Descartes words, “as the captive, who, perchance, was enjoying in his dreams an imaginary liberty, when he begins to suspect that it is but a vision, dreads awakening, and conspires with the agreeable illusions that the deception may be prolonged.”