In Our Trusty Cage

Aaron Weiss

Admittedly, the term "Trusted Computing" isn't as conspiratorial as it sounds. Within computer security circles, to "trust" a system has a long and legitimate history describing available degrees of credentials. Indeed, the Trusted Computing Group, a Who's Who list of major technology vendors from Microsoft to Intel to IBM, consciously emphasizes the security pedigree implied by their name. But don't let the name fool you. Ultimately, it isn't the machines the TCG aims to make trustworthy. It's their customers.

The trusted computing pitch is simple. With today's computers, bad things can happen. General purpose machines are like an open society where evildoers can spread viruses, steal identities, and raid bank accounts. The only way to safeguard computers—and therefore ourselves—is to lock them down. Close their borders. Sure, you the computer owner and operator lose some freedom with how you can use the machine. But it's for your own security. It's for our own good. Whoa—déjà vu! Where have we heard this before?

It's certainly true that the security technologies in place today for the average computer owner are inadequate. Software defenses, like many popular anti-virus packages, are burdensome and unwieldy. E-mail authentication technologies to minimize malware distribution and phishing attacks are still immature. Protection of assets in a popular operating system like Microsoft Windows is weak. Even in a world where all of these tools improve—and they should—bad things will sometimes happen because there are no 100-percent guarantees.

What these defenses share in common, and where they differ from trusted computing initiatives, is that the individual opts-in to their own level of security. You choose a balance between security and practicality that meets your interests. Any time it is proposed that these choices be imposed, we're duty-bound to raise questions. Perhaps we accept that airlines must impose a minimum level of uniform security and effectively make our choices for us. Precisely what that entails is a legitimate subject for public debate, because the rules affect us all.

The Trusted Computing Group, however, endeavors to impose choices without public accountability. These are, after all, private enterprises. But these are enterprises which design and manufacture most of the technologies we rely on daily. The trustworthy computer, as they see it, acts upon all data—and by association, its users—as guilty until proven innocent. This perversion of justice should be just as unacceptable in front of the keyboard as it is anywhere else in our civic lives.

Much of the vitriol aimed at trusted computing so far has come from the intellectual property crowd. Their ire is raised by how TC can and will be used in an attempt to strengthen Digital Rights Management, the

Continued on page 39

Continued from page 40

content industry's elaborate and desperate attempt at copy protection. But bashing TC by way of DRM is actually a poor strategy.

It is easy for corporations to play the victim card when it comes to intellectual property rights. Many ardent opponents of DRM accuse content providers of overreaching when protecting their movies and music from being copied freely. The problem is, their content *is* being copied freely. Often by those very opponents of DRM.

Of course it's true that DRM is a waste of time and money. If people can see it, or hear it, they can copy it. However obtuse your encryption scheme and however many elaborate cryptographic keys you employ to unlock content, ultimately the technology for unlocking it has to be given to the end user. Or else they can't play it. Wrap those keys in as many layers of obfuscation as you want, but eventually someone will figure out how to unwrap them and millions of dollars of investment in securing your content is undone like an unfurled sweater.

Despite this reality, opponents of DRM too often sound like people who want to justify stealing. And even if they are not, it is too easy for DRM and trusted computing lobbyists to make them look that way. Fighting DRM is a legitimate cause, but it's not the way to harpoon trusted computing.

The undoing of trusted computing as an imposed exchange of freedom for security should be that it's bad for business. (Well, unless you're in the TC business.) Sure, they'll tell you that business will benefit from trusted technology. It will be harder for thieves to compromise your data, for example. But that will be true because responsibility for and access to your data will be shifted, under TC, from your hands and into your technology vendor's.

You can enjoy defenses against data theft today by hiring competent IT professionals, and maintain control of your resources to boot. Should IT staff need permission from your vendor to modify or repair your in-house technology? They would in a TC environment where each component is married, at the hardware level, to every other component in an individual computer. What if your vendor decides not to provide said permission, and instead requires customers to purchase outsourced maintenance?

In fact, vendor lock is one of the greatest threats of trusted computing. Today, an increasing number of organizations and public institutions are realizing the dangers of single-vendor solutions. Consider document creation. The State of Massachusetts is planning to require state agencies to create documents in ODF, the Open Document Format, rather than a single vendor's proprietary format. Governments at various levels around the world are taking similar steps. If a single vendor controls access to your hardware, your software, and the data created with it—your future options begin to look rather limited.

Trusted computing technologies can be useful taken individually, and optionally. Hard drives with built-in encryption, for example, absolutely have their place in the right context. A TPM cryptography chip that distributes access keys to authenticate system components' right to access data is a really good idea for computers that need to be "trusted" in the legitimate sense of the word. Like in the military.

Trusted computing initiatives aim to achieve their goals by not trusting anything. Aside from the distasteful creepy factor of becoming consumers of technology, which is designed to distrust us, we face the same fundamental decision point as in domestic and international security. Can we collectively prevent many bad things from happening by locking ourselves in a steel cage? Absolutely. Remember not to throw away the key. ~