

Trusted Computing



Lisa Thalheim¹

The widespread use of the term “intellectual property” in the discussion on access to knowledge and information is a fortuitous circumstance for those who profit from the sale of nonphysical goods. The term suggests that texts, music, and know-how are exactly the same as cars, houses, or televisions. There are clear rules for defining ownership of material goods, the rights of the owner, and what we understand as theft of such a good.

The mantra of intellectual property cannot, however, belie that there are important differences between a digital piece of music and a vehicle. One such difference is that the musical piece – in contrast to the vehicle – can be shared simultaneously among any number of users without anyone incurring a damage. Another difference is that a vehicle cannot be copied any number of times and the copies distributed – which is possible in the case of a digitally available piece of music. We have already witnessed how those wishing to sell music respond to the possibility of reproducing musical pieces at virtually no cost. One need only look, for example, at the criminalization and vigorous prosecution of file-sharing network users by the music industry. The term “pirated copy” itself serves as an example of how public perception is influenced. It relates the unauthorized reproduction of music and text to the criminal offense of robbery, which, by definition, is linked to the use of force. There are also efforts at the technological level to quash unlimited reproduction by preventing the copying of musical pieces using software and hardware. This method has the advantage that the interested parties – mostly international corporations – do not have to rely on policy makers and the legal system.

Trusted computing is a technology that attempts to broadly implement this kind of artificial restriction on the possibilities of digital products, even though its creators vigorously dispute having had this intent in its development.

Trusted computing in itself is difficult to grasp. Not only is it complicated from a technological point of view but it also combines various features, some of which are desirable and useful, others of which are problematic and dangerous – depending on who is deploying the technology and for what purpose. Advocates praise trusted computing as a solution for protecting against computer viruses and other attacks. Opponents vocally and energetically criticize the damage potential – because industry associations, manufacturers, and possibly also governments are usurping the user’s control over his own computer. What is it about this technology that causes such a stir? And who is right – the advocates or the opponents of trusted computing?

In 1998, some of the major computer industry corporations founded the Trusted Computing Platform Alliance (TCPA). This industry alliance was then renamed Trusted Computing Group (TCG) in 2004. The founding members were chipmakers AMD, Infineon, and Intel; hardware makers AMD, Hewlett-Packard, IBM, and Sun Microsystems; and software maker Microsoft. The Trusted Computing Group’s website meanwhile lists over 140 member companies.

Trusted computing can be viewed as an approach to solving problems that we have with our globally linked and ubiquitous computer systems: computer viruses, attacks on servers and private PCs, and, consequently, the loss of confidential information.

¹ The author is a student of computer science and philosophy at Humboldt University in Berlin and a freelance consultant for computer security.

Lisa Thalheim: Trusted Computing

Some of the founding companies developed their own projects. Microsoft initially called its project Palladium and then NGSCB, which stands for *Next Generation Secure Computing Base*. This project covers both hardware and software. NGSCB attempts to develop fully trusted computer systems, including software and hardware. It thus differs from Intel's *Safer Computing Initiative*, which is mainly concentrated on the hardware aspects of trusted computing.

Simultaneous to this effort, the TCG members are developing TCPA specifications: a series of documents detailing how trusted computer systems are to be implemented.

With these specifications, the TCG has proposed a de facto standard for how the basic security problems of computer systems are to be solved in the future.

The centerpiece of the TCPA is the Trusted Platform Module (TPM), a small chip that is cheap to build and is supplied as an integral component of computers, printers, network hardware, and entertainment electronics. That means that anyone who purchases hardware is simultaneously buying the TPM – whether consciously or unconsciously. Most current notebooks already contain such a TPM. Both the U.S. Army and the U.S. Department of Defense require that every newly purchased computer contain a TPM.²

The function of a TPM can be compared to that of a notary public. The TPM can store data confidentially and only distribute it under certain, predetermined conditions and it can certify information about the status of the computer system.

It can reliably determine whether the computer has uploaded a predetermined set of programs, whether the licensing provisions are being observed for those programs, or whether they have been manipulated – whether by a virus or knowingly by the user. The TPM can then present this information to the computer user.

However, it also offers the possibility of providing this information to third parties – say, the operator of a website or an online music provider with whom the user interacts.

The latter feature is one of the main criticisms of opponents of trusted computing because this function enables online content providers to determine, for example, whether a user is working with a “trusted” software environment. From the provider's perspective that would be a software environment, say, that makes it impossible to copy legally acquired content – a document, a piece of music, a video – onto a computer or to burn it onto a CD. So it is conceivable that providers might view only Microsoft Windows with Microsoft's MediaPlayer as trusted and simply deny its services to anyone who does not use such a software environment. While the user would be free to deactivate the TPM – this fact could, in turn, be determined by the provider and serve as a reason to exclude the user from the service in question.

The other criticism of the TCPA specification is that the user is granted only limited control over his computer. The TPM works on the basis of a secret key that is cryptographically different for each TPM. Practically all TPM functions are built on this key and, as no two TPMs in the world have the same key, it, in turn, makes possible to identify a TPM. Users, however, are unable to gain knowledge of or change this key; the manufacturer burns the key onto the TPM during production. The TCG justifies this decision with the argument that it

² <http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf> and <http://www.army.mil/ciog6/news/500Day2006Update.pdf>

serves to protect the user himself. If the user does not know the key, he cannot erroneously reveal it to an attacker.

A TPM, in principle, offers some useful functions that can help users better prevent important data from being lost or compromised. Yet it still seems too early to be able to estimate the mid-term effects of implementation of trusted computing. The technology is very complex and so far has not been discussed in the public. It will also take some time before applications begin using TPMs on a broad basis. What these applications will look like and what they will actually perform still remains widely unclear.

What is clear, however, is that trusted computing by no means offers the promoted patent solution to all the problems of computer security. Instead, the cited risks associated with the deployment of trusted computing are already becoming evident.

A technological assessment of the TCPA specification leads to the conclusion that the technology is unlikely to have a dramatic impact on the PC software market. It is likewise difficult to predict whether trusted computing will have significant negative effects on free software. But the existence and widespread use of TPMs in all computers weakens the hand of the individual (the user) vis-à-vis the computer and media industry. The technology has considerable potential to shift the power relationship further in favor of major corporations and industrial alliances.

Even if trusted computing does have less influence in the PC sphere, we will tentatively see a greater influence in the area of specialized devices, especially entertainment electronics. Here, it is already now practical to allow the user only minimal control over the device. That has recently been shown in devices such as the Apple iPod, iPhone, and Amazon's Kindle. The TCPA specification is ideal for bringing to market reliable and near unavoidable digital rights management³ (DRM) applications on devices. Trusted computing is no longer a technical framework that can be used in a variety of ways. Rather, the companies behind trusted computing are primarily representing their economic interests by advancing this technology. These interests coincide in part with those of the user; in part, they are also intended to restrict the freedom and rights of the user (and hardware owner) as much as possible.

Last but not least, the TCPA can also be understood as an attempt to technologically ingrain social acceptance of the concept of "intellectual property" without concern for the outcome of current, political, social, and legal discussions.

It is up to users to reject the loss of control associated with the TCPA and to demand a technological alternative that treats users not as opponents or defenseless victims but as partners and citizens.

³ Digital Rights Management is a catch-all phrase for technological measures undertaken to guarantee the enforcement of rights to digital content, such as copyrights to documents or music. A frequent application of DRM technologies is, for example, protection against the copying of document or music files.