An introduction to Trusted Computing

Contribution to the United Nations' Internet Governance Forum

Vittorio Bertola <vb@bertola.eu.org>
31 July 2006

1. Introduction

"Trusted computing" is a new technology that is being introduced in these very months into computers and most other consumer electronic devices. It has been designed by the industry to reduce dangers and threats to which users are subject while using PCs and other electronic devices over the Internet, but also to prevent users from executing unauthorized operations with their computers. While industry strongly believes in the benefits of this technology and is set to add it to every new device sold in the near future, civil society and Internet user groups have been complaining about the potential endangerment of their rights caused by this technology.

Thus, different stakeholders have very different views on whether this technology is "good" or "evil", and whether it needs to be adopted, regulated, or totally rejected. However, such a deep technological change clearly affects all issues deriving from the usage of the Internet; as such, it is a very interesting, urgent and important matter for consideration by the Internet Governance Forum.

This is why this paper is provided to the participants to the Internet Governance Forum, with the purpose of briefly describing the technology and its impacts. Hopefully, the Forum will be able to start a discussion on this matter, bridge the disagreements and help establishing common best practices that could act as guidelines for the implementation and regulation of this new technological and social development, while facilitating its deployment in a way that respects the rights and needs of all stakeholders, and thus is fully supported by all of them.

2. What is "Trusted computing"?

Trusted computing (TC) is the name used by the industry to indicate the practice of including, inside PCs and other consumer electronic appliances, special hardware pieces designed to use cryptography to certify the source and authenticity of the software running on the device, and protect the flows and storage of data inside the device.

This practice is designed to fight viruses and piracy; it has the advantage of preventing the execution of malicious code, but also the disadvantage of potentially giving to a few manufacturers and ICT companies a significant degree of control on what can and cannot be done with electronic devices in the world.

Global technical and policy standards for this matter are defined by the **Trusted Computing Group** (TCG), formerly known as **Trusted Computing Platform Alliance** (TCPA), an industry consortium including all primary manufacturers of electronic devices and software (Microsoft, IBM, HP, Intel, AMD, Nokia, Philips, Samsung...). Users have formed groups to ask for regulation of the matter, or to fight for the rejection of the idea at all. There is no global regulation of the matter yet, and also few or no national initiatives at all.

The first TC-enabled devices are currently being introduced into the market; this makes the discussion of the issue even more urgent.

3. The technicalities of trusted computing

It is very hard to really understand the technicalities of trusted computing, both because it still is a work in progress where different efforts are being merged and fixed, and because of industrial confidentiality requirements. However, the specifications that were already released by the TCG require TC-enabled systems to implement four main technical functionalities, which, in a very simplified way, can be described as follows:

1. **Secure I/O**: Information typed onto the keyboard, or images shown onto the screen, or sound sent to the speakers, are to be encrypted so that they cannot be captured or read by applications other than the current one.
2. **Memory curtaining**: Data stored in the memory of the computer are to be encrypted so that only the application that generated them is able to read them.
3. **Sealed storage**: Data can be saved on the computer's hard drive in a "sealed" form, that is encrypted so that it can only be read by the original application on the original device. If moved to another device or accessed with another application, the data are unreadable.
4. **Remote attestation**: The device is able to automatically certify to third parties in enciphered form, over its Internet connection, which software it is running, and whether it has been modified (either by a malicious attacker or by the owner of the device).

All these functionalities are implemented by a piece of hardware named **Trusted Platform Module** (TPM), and nicknamed "Fritz", that is being added to newer PC motherboards; in the near future, a TPM will be integrated inside the microprocessor.

According to the specifications, a system will be "trusted" if all its components (hardware and operating system) support TC functionalities. The user will still be able to disable them, but by doing so, the system will become "untrusted", and TC-enabled services and applications might refuse to run. In other words, depending on the actual policies used in the implementation, users might have to renounce accessing "trusted" applications, services and data if they want to use other applications, services or data that are not marked "trusted" by the TCG or by the system itself.

4. Current implementations of trusted computing

The most famous instance of trusted computing is Microsoft's new component of its Windows operating system, originally nicknamed **Palladium** and then named **Next-Generation Secure Computing Base** (NGSCB), which will be included in the forthcoming releases of Windows.

Also, both major manufacturers of PC microprocessors, Intel and AMD, as well as one of the main manufacturers of PDA microprocessors, ARM, have announced the integration of a TPM in their next generation of products.

The TCG has also recently released specifications to include TPMs in mobile phones and other Internet-ready mobile devices; and inside Internet routers and network access systems, to use TC to allow or deny access to the network.

5. Governance impact of trusted computing

The widespread introduction of trusted computing could completely change the relationship between the ICT industry and end users; most, if not all, of the control on what users can or cannot do with a computer would shift from the owner of the computer to its manufacturer.

This is specifically due to the fact that remote attestation does not make a difference on whether the software being used was changed by a malicious third party (e.g. a virus) or knowingly substituted by the user; both kinds of alterations are considered a security attack by the device.

This would in turn have an impact, positive or negative, on many different issues and policy sectors:

- Antitrust: Through the examination of remote attestations, the manufacturer of the PC and/or of the operating system would be able to prevent specific applications, for example by its competitors, to work on the device, or to access data that were created or acquired with TC-enabled applications. Also, content or service providers could refuse to provide content or service to users running specific applications or operating systems, including applications that behave identically to theirs (i.e. are fully "compatible" or "interoperable"), but were developed by competitors[1].

- Industry development: By being able to prevent the use of specific applications, the biggest service or content providers might start to request software makers to undergo licensing costs or other fees and clauses, in exchange for letting their applications access the service; similarly, operating system manufacturers might require fees to let third party software work on the PCs that use their OS, or discriminate "untrusted" software in other ways. If this kind of policy became commonly used, small players, individual software writers (especially of free software) and developing country actors might be cut out from the software development market.

- Electronic security: The introduction of TC could speed up the detection and removal of viruses, trojans, and other malicious software commonly spread over the Internet. It could significantly enhance the safety of the average Internet usage experience, especially for less experienced users, and thus induce greater usage of the net. On the other hand, since TPMs are going to be embedded deep into hardware and encipher the data they compute, it will be more difficult for users and governments to verify what they actually do, and ensure that they do not contain bugs and backdoors and do not deviate from the published specifications and policies.

- Consumer rights: Consumers could lose the ability to do whatever they want with their computer; in certain cases, the owner of a PC might be considered an attacker, at the sole judgement of the manufacturer of the hardware, operating system or service, and thus he could be denied full access to his own computer. Without regulation, there is no warranty that this technical possibility will not be used arbitrarily against consumers; for example, consumers might potentially be required to pay fees to update or maintain their software and hardware, or else it would stop working; their documents and content, which would be stored in a manner that is only readable by that PC, could not be movable to a new PC or operating system without authorization by the manufacturer of the current one; and other similar behaviours.

- Privacy: TC systems are uniquely identified and recognizable, when performing the remote attestation mechanism; thus it is possible to track which software a specific PC is running, and perhaps also acquire further information. Potentially, if TPMs are not implemented in a publicly screened way, they could communicate back to manufacturers and other parties any kind of information and data from the user's PC, without the user even knowing it. This could allow manufacturers and other parties to spy what the user does with the device.

- Intellectual property: TC can prevent the execution of illegally duplicated software, or access to content that has not been properly licensed to the user; it can be the platform over which to implement DRMs (Digital Rights Management systems) that cannot be circumvented. However,

[1] Even if manufacturers and content/service providers, already today, can require specific applications for access in the present "untrusted" environment, users still have the ability to use "compatible" applications by third parties that behave like the one required by the provider; this still allows for competition. With trusted computing, even if the behaviour of the applications were identical, manufacturers and providers would be able to tell original applications from compatible ones and disallow access to the latter, thus effectively preventing any competition.

these systems can also prevent users from exercising their rights, such as fair use or backup copies, or discriminate against the use of non-DRM-protected content, even if legal.

- Freedom of expression: Potentially, manufacturers of trusted software might embed arbitrary censorship provisions in their applications (for example, deny access to certain websites or content); users might not be able to replace this software with "compatible" but uncensored ones without losing the "trusted" status of their system, and thus being denied access to TC-only services and data.

- National security: The presence of opaque hardware parts on PCs, on mobile phones and on all electronic devices can potentially allow mass surveillance of all electronic communications and activities in a country, not necessarily by the government of that same country.

- National sovereignty: As rules for what can or cannot be done with a PC or electronic device would be defined by manufacturers and service providers – mostly private companies residing in a few developed countries –, other countries could lose part of their practical ability to regulate the matter.

It is thus clear that trusted computing is a wide issue that impacts on many of the themes that were identified and addressed in the Tunis Agenda from the WSIS.

6. Conclusions

Trusted computing is not bad or good per se, but it can have devastating effects on market competition, privacy, and consumer rights, depending on the policies that will be adopted in its deployment. It can also significantly slow down the development of ICTs in the developing world, by increasing the control and the competitive advantage held by the current market leaders, and by causing arbitrary increases in costs due to the reduction in competition.

The situation is still extremely unclear, both from the technical and from the policy point of view; for this reason, it is necessary to start an open and public process involving all stakeholders, to have a frank discussion on the merits and disadvantages of the widespread introduction of trusted computing, and on whether some practices and rules can be agreed among all stakeholders, to protect the interests and views of all of them.

This is why this matter is being put to the attention of the Internet Governance Forum, that, given the breadth and horizontality of this matter, is the most adequate international venue for this discussion.