



## Trusted Computing

**R. Jason Weiss**

**Development Dimensions International**

Trusted Computing (TC) is a set of related technologies that have the potential to profoundly affect how I-O psychologists work among ourselves and with our clients. In this issue of *TIP*, I review Trusted Computing and consider some of the ways in which I-O may look to benefit from it, provided there are solutions to some of the significant concerns that it might present. Let's start by considering where TC comes from and what exactly it is.

### Who Can You Trust?

Trusted Computing owes a good part of its origins to the rampant file sharing that was so famous during the Internet bubble years. The most common (or at any rate the most notorious) use of file sharing was among computer users who shared songs copied from CD with anonymous others across the Internet. Naturally, it alarmed the music companies that good copies of their saleable products were being given away free for the asking. The Recording Industry Association of America promptly used the courts to chase after the file sharers, but this was only a reactive solution. A more proactive solution, building technology into the computers to enforce the copyright-holder's rights, was up to the hardware and software companies. Seeing the potential for new streams of income as computers and entertainment merged, companies such as Intel, AMD, IBM, Sun, and Microsoft formed the Trusted Computing Group to devise a solution.

If TC were only about preventing the unauthorized sharing of music files, then this column would be my shortest and most misguided. However, though digital rights management (DRM) for entertainment media may have been a critical inspiration for TC and remains a critical component of it, TC is a much larger framework dedicated to creating a secure computing environment. In short, TC aims to create a secure environment within your computer for the software that runs on it. It does this through a combination of software and hardware, including a security chip with a unique ID called a Trusted Platform Module (TPM) that is mounted inside the computer and securely stores digital keys, passwords, and certificates. The software side is a combination of a TC-enabled operating system and applications with associated security-sensitive programming.

When TC is working in all of its glory, applications are effectively safe from outside attack. Memory used by secure programs will be inaccessible to other programs. Even the connections between the keyboard, computer, and monitor will be secure. The TPM safeguards passwords and other digital identification and is impervious to software-based hacking. Importantly, through a feature called remote attestation, some level of communication with remote computers can offer further security by, say, verifying the legitimacy of the software running on the computer. For example, a test vendor can automatically ensure that a given installation of test administration software is an authorized copy and has not been hacked. If the software is legit, the test vendor can have increased confidence in serving tests to it.

Trusted Computing is therefore a two-way street. With TC, the computer user can feel confident that the software installed on the computer is running as designed and, further, that no nefarious third party is capturing the information that passes between the keyboard and computer, such as passwords, e-mail content, and so forth. The software vendor, similarly, can trust that the software on the computer has not been reverse engineered or disabled in any way as to enable activities that exceed the user's stated rights as specified in the end-user license agreement (EULA). The EULA lays out—often in mind-numbing detail—the user's rights as associated with the software. For example, it is common for the EULA to restrict the installation of the software to a single computer at a time and to permit the user to make one copy of the software media for back-up purposes. The principles behind remote attestation make it possible to enforce certain aspects of EULAs, such as the number of active installations of the software, which have traditionally been clumsy to police.

What is interesting about TC is that it has generated considerable debate and concern before any business-related applications have even been rolled out. Indeed, TC is not going to be available at the operating system level until Microsoft's next OS, *Windows Vista*, is released in 2006. The loudest arguments center on the remote attestation feature and its potential for use and abuse. Remote attestation brings a third party into the relationship between user and computer by enabling software to communicate with an outside server and potentially take action outside of the user's control. Indeed, the reaction to this prospect among some in the technology community has been nothing short of alarm. Is this justified? Let's take a look at some of the ways in which TC may benefit I-O and consider whether the concerns raised should give us pause as well.

### **Will Trusted Computing Help or Hinder I-O?**

There are two ways to consider the potential for TC as it relates to I-O, and these relate to our roles as developers and vendors of technology and as consumers. Let's address each of these separately.

*Vendors.* In many ways, TC is a boon for developers and vendors of technology. In the case of testing and assessment applications, we can have greater confidence that our applications are delivered securely. Indeed, the Trusted Computing Group has expanded beyond end-user computers to consider trusted servers and trusted networks as well, so there will be a day in which we can have strong confidence that the potential for foul play at any point in the process is minimized. As well, with remote attestation we can verify that our applications are being deployed in accordance with the licensed terms.

Remote attestation actually gives us additional tools beyond simple license monitoring. For example, through remote attestation, it is possible to verify the identities of other applications on the user's system. This enables us to ensure that any supporting applications that are required by our software are present and, thus, safeguards the user's experience. For example, it is not uncommon to require access to Adobe Reader to view PDF files or Windows Media Player to view media files. Because these applications are updated frequently and add new features with each update, being able to verify remotely that they are present and of sufficiently recent vintage would represent a considerable benefit. Although a client's IT department should be able to confirm these details according to its reference platform (a standard configuration of hardware and software), it is often my experience that users independently make substantial changes to the installed software on their computers. In deployments of sufficient size, it's unreasonable to expect the client IT department to manually verify specifications on each targeted computer. Remote attestation, then, offers us a necessary safeguard.

It is important to note, especially around applications associated with testing and assessment, that TC only targets the computer at which the user sits; all it can do is confirm the identity of the computer. The TC specification has no intrinsic method to verify that the person sitting at the computer is indeed who we expect, and so the need for proctoring will not be directly eliminated. However, TC will work with other methods such as biometrics (e.g., fingerprint scanning) to support such a level of security.

*Consumers.* As consumers of technology, TC offers us particular benefits as well. One of the more controversial applications of remote attestation is that it could support much more sophisticated document security than we have seen in the past. For example, it could be possible to make sure that a given document is only viewable on computers within a department, accessible within a particular time frame, or editable by selected users. The need for this is illustrated in an anecdote from the book *21 Dog Years: Doing Time @ Amazon.com* by Mike Daisey (2002). Toward the end of his career at Amazon and during a particularly turbulent time, Daisey found a printout of the compensation schedule for everybody in his department. For reasons known only to himself, he then photocopied and distributed the document, which caused considerable additional turmoil. With remote attestation, it could be

possible to secure such a sensitive document and prevent it from being printed, which certainly would have helped prevent the drama that undoubtedly ensued. Given the extremely confidential nature of the information managed by HR departments, the capability to institute stronger access controls could represent a significant benefit.

Clearly then, TC holds significant promise for I-O, some of which can be leveraged almost immediately once the supporting hardware and software are in place. There are, however, significant challenges to be considered as well. Remote attestation, by definition, enables a third party some level of access to a computer's files, or at least to information about them so as to allow the enforcement of rules around how, when, and by whom a file may be opened. However, this also creates significant concerns around privacy, security, and the potential for censorship. What happens if, for example, the third party managing authorization is hacked or its access is used irresponsibly? Alternately, what happens if a software vendor determines that files created within its software applications must only be accessed using those applications? This results in being locked in to a vendor's software for all future use of those files and eliminates the capacity to share the files with others who may have different software.

These issues alone represent no small concerns, both from a general business perspective and from a more specific HR data perspective. They are the subject of much of the furor around TC, and the reader interested in greater detail is directed to the documents listed in the Additional Resources section at the end of this article. There are yet other issues that represent additional cause to stop and consider the potential ramifications of TC. One is the carelessness with which users already treat many aspects of computer security. The use of common or easily cracked passwords is only one example. Document security is something that must necessarily be considered on a document-by-document basis and may need to be configured to a minute level of detail such as the names of those permitted to access the document, where it may be accessed, and an expiry date after which the document may not be accessed at all. It is not a "set it and forget" type of feature. It is quite likely that the extra work necessary to configure security for any given document will scare away most users for any but the most obviously valuable documents. This leaves at risk a vast middle ground of documents that could benefit from some level of security but for which setting appropriate security would appear too onerous of a process.

Another concern is how TC will handle the lifecycle of hardware within organizations. Remember, the Trusted Platform Module is an integral part of the computer's hardware and includes a unique ID key that is a core element of TC. What happens when, for example, a computer is handed down from a manager to an administrative assistant? Undoubtedly, there will be processes to ensure that the document rights accorded that computer when it belonged to the manager would not follow it to the administrative assistant,

but there is no reason to believe that these would be uniformly applied. For example, it is not uncommon to see news stories of used computers sold with confidential personal and/or business information left on the hard drives, despite the easy availability of software that could erase all traces of data. The problem does not stop there, however. How easy will it be for managers' access rights to follow them to a new computer? How will it be possible to decommission an old computer and transfer its documents and all rights pertaining thereto to another computer? These and other questions must be answered in a way that supports the processes and exigencies of modern organizations before TC can be adopted with any hope of seeing its benefits.

### **Conclusion**

Trusted Computing is coming, and the technology side of it will be here very soon. As argued above, TC offers I-O distinct benefits across a range of applications. It makes sense to apply safeguards to our data and information, provided we do so responsibly and with a clear understanding of the ramifications of our choices. Clumsy deployments, on the other hand, will only create frustration and highlight a lack of security where it is most needed. As such, the challenges associated with effectively implementing TC, not to mention the concerns around use of remote attestation by third party software, clearly require a great deal of consideration before widespread adoption can be recommended.

As TC rolls out, it may make the most sense for us as a field to consider its implications and develop a set of recommendations for how features of TC should be implemented for HR data. As I've argued before (Weiss, 2001), such a standard will likely be created whether we are involved or not. By taking the initiative, we can shape the discussion around the concerns we know to be present.

### **References**

- Daisey, Mike (2002). *21 dog years: Doing time @ Amazon.com*. New York: Free Press.
- Weiss, R. J. (2001, October). Six things you should know about XML. *The Industrial-Organizational Psychologist*, 39, 30–34.

### **Other Resources**

Further detail on the privacy and other concerns associated with TC can be found in the following documents.

Anderson, R. (2003, August). *"Trusted Computing" frequently asked questions, Version 1.1*. Retrieved July 31 from <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>.

New Zealand State Services Commission (n.d.). *Trusted Computing technologies: Briefing*. Retrieved July 31, 2005 from <http://www.e-government.govt.nz/docs/trusted-200410/drm-200410.pdf>.

Schoen, S. (2003). *Trusted Computing: Promise and risk*. Retrieved July 31 from [http://www.eff.org/Infrastructure/trusted\\_computing/20031001\\_tc.php](http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php).

Thompson, B. (2005). What price for 'trusted PC security'? *BBC News*. Retrieved July 31 from <http://news.bbc.co.uk/1/hi/technology/4360793.stm>.

I welcome comments, suggestions for future articles, notes of errors of omission or commission, and any other communications with the possible exceptions of offers to hide millions of dollars in my bank account, for which I will receive a generous commission, provided I maintain the utmost secrecy. Please contact me at [jason.weiss@ddiworld.com](mailto:jason.weiss@ddiworld.com). This article is archived with my previous *TIP* columns at [SIOP.org](http://SIOP.org) and [jasonweiss.net](http://jasonweiss.net).

## Powerful NEW EEO Software

### Adverse Impact & Test Validation

Industry-first  
software  
programs that  
address current  
employment  
standards

**Ask Us For  
Free Demo  
Software!**

Established in 1974



Biddle  
Consulting  
Group, Inc.

(800) 999-0438  
[staff@biddle.com](mailto:staff@biddle.com)

#### ▶ **Adverse Impact Toolkit™**

Uses new multi-year **adverse impact analyses** being used by the U.S. Department of Labor and includes **"exact" tests supported in litigation**.

AI Toolkit includes tools for virtually every adverse impact analysis possible - **single event, multiple events, pools analysis, selection rate comparisons**

#### ▶ **Test Validation & Analysis Program™**

TVAP™ uses a step-by-step **validation process for written tests** that has been supported in numerous litigation settings.

Includes **new statistical techniques** endorsed by the *Principles and Standards*.

**[www.biddle.com](http://www.biddle.com)**