

Improving the TCPA Specification

Bill Arbaugh, University of Maryland at College Park

The Trusted Computing Platform Alliance (<http://www.trustedcomputing.org/>), an industry work group formed to create “a new computing platform for the next century that will provide for improved trust in the PC platform,” has recently received a great deal of negative press. At the same time that cofounder Microsoft announced plans to enhance the security of its next-generation operating system, Palladium, by leveraging TCPA technology, Cambridge University’s Ross Anderson critiqued many aspects of the specification (<http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>).

Without examining any of its technical details, the media was quick to condemn the organization’s effort as an attempt to further monopolies and destroy privacy. Unfortunately, until these sensational stories appeared, most people probably had no idea what the TCPA was or what it was doing. Compounding this problem is the fact that the specification is extremely complex and tersely worded.

Here I hope to explain in a balanced fashion what is both good and bad about the proposed industry standard and suggest ways that the TCPA technical committee can improve it.

ENHANCING TRUST

A consortium now consisting of more than 180 companies has created the TCPA specification to provide



We need better information security, but not at the price of the TCPA’s current draft.

strong configuration management for personal computers, operating systems, and applications through additional hardware and software in a component—the *trusted platform module*—that is tightly coupled with the CPU.

The TPM uses mathematical induction to increase a protected system’s functionality by building a *chain of trust*. It assumes that the hardware and a minimal portion of software are trustworthy—they work as expected and have not been modified since initial verification. The TPM confirms that the machine’s hardware configuration—additional boards and their settings—is in accordance with the platform’s policy and validates a stored *integrity metric* such as a cryptographic hash or digital signature for any additional software. If the integrity metric remains valid, the system executes the software. In this way, no unapproved software can execute on the host and the system remains trusted.

In addition to providing integrity protection, the TCPA defines a method for a trusted store external to the TPM

that, when coupled with a TCPA-enabled operating system, enables digital rights management (DRM) and provides *mandatory access control* (MAC). Documents that users create, whether as private individuals or members of an organization, can only be read on certain computers, by certain people, and during certain time periods.

The key point here is that the TPM alone cannot enable DRM. It requires OS support since it is not a reference monitor that mediates all security-relevant commands as some have claimed.

Beyond the bindings created while the platform is operational, several static bindings serve as the basis of trust.

- The TPM can only be bound to a single platform, and an endorsement key is bound to the TPM—thus binding the endorsement key to the platform.
- At least one public key certificate must serve as a root or base case of trust for measuring integrity metrics, and only one public key certificate can serve as the trusted store’s root of trust.
- A TPM endorsement identity public key pair must exist to uniquely identify the TPM.
- One or more user identity certificates issued by a conventional certificate authority or a special privacy certificate authority can exist in the TPM.

The current specification permits disabling almost all of the TPM’s functionality by the platform owner or user. The only functionality that cannot be

disabled is the `extend` command, which builds the chain of trust.

PRIVACY SUPPORT

The current TCPA specification provides a method for obtaining an anonymous user identity certificate from a privacy certificate authority over a secure channel. The TPM sends a public key—the key for which the user desires a certificate—and three credentials—a *public key certificate* and two *attribute certificates*—to the CA.

The public key certificate is the endorsement certificate issued by the entity that endorsed or verified the TPM. Under the current specification, this likely will always be either the manufacturer or a third-party testing lab. Among other things, the endorsement certificate contains a null subject and the TPM public endorsement identity's public key.

The first attribute certificate is the platform credential containing a pointer to the endorsement certificate that uniquely identifies the platform's endorser and the model—hardware and software revisions, TPM details, platform compliance with the TCPA specification, and so on.

The second attribute certificate is the conformance credential, which asserts that the named TPM complies with the TCPA specification. The specification clearly states that both the endorsement certificate and the platform credential should only be released to those with the “need to know” because the certificates contain sensitive information—they can be used to uniquely identify the platform and then possibly the user through product registration information.

Once the privacy CA receives these three certificates, it verifies the information, creates a TPM identity credential, and sends it to the client via the secure channel. The TPM identity credential contains a null subject and the public key sent by the user in the certificate request.

The primary purpose of this exchange is to ensure that anonymous

certificates are only issued to compliant devices.

A DOUBLE-EDGED SWORD

Broad, ambitious initiatives such as the TCPA specification are a double-edged sword. The universal application of robust authentication technologies—assuming that is possible—

A TCPA-enabled operating system could prevent a user from running an “unapproved” application.

might indeed prevent identity theft and a host of other problems, but it would also threaten privacy and add to marketing organizations' already formidable ability to data mine individuals' activities.

Among the many advantages of technology such as mandatory access control is that it makes espionage more difficult—significantly restricting access to information makes it far easier to trace the source of a leak. It also lets individuals limit who can see their personal data—a potential improvement over today's lack of any control. Finally, users and system administrators can specify only those applications that should run on a particular computer, preventing viruses and other malicious applications from executing.

However, as Ross Anderson has rightly pointed out, the TCPA specification presents several problems with respect to DRM and competition as well as circumvention of the open source GNU Public License (GPL). More broadly, and more ominously, it also threatens to eliminate privacy.

DRM and competition

Coupled with the 1988 Digital Millennium Copyright Act (<http://www.loc.gov/copyright/legislation/dmca.pdf>), DRM technology lets companies create proprietary file formats for their appli-

cations, preventing competitors from building cheaper and possibly better applications that interoperate.

A TCPA-enabled operating system could also prevent a user from running an “unapproved” application. Although such a capability might be highly desirable in environments such as a financial or governmental institution, it could limit application choices to those sanctioned by some entity beyond the average consumer's control.

DRM technology also erodes fair use exceptions to copyright law that courts have established over the years. For example, in the near future, a movie that you pay to download onto your desktop computer at home may become locked to that system, preventing you from copying or moving it to your laptop. In addition, copyright law differs throughout the world, and enforcing a single copyright policy by a combined TPM/OS is problematic.

Circumventing the GPL

Although one of the TCPA's stated objectives is protection of copyrighted material, the specification ironically creates a loophole to circumvent the popular GPL and exploit others' intellectual property. A company or individual could alter a GPL-protected program such as Linux, obtain a digital certificate permitting use of the program on TCPA-enabled equipment, and release the source code in accordance with the GPL.

Ross Anderson argues that home hobbyists and other less sophisticated users will not be able to reuse and extend released software because of the bureaucratic and financial barriers to obtaining approval of derived works. However, this is true if only one trusted root exists for integrity on the TPM, and the specification provides for multiple trusted roots.

As long as the TPM permits users to load additional trusted roots (which is admittedly unclear at the moment), they could obtain a certificate from anywhere, possibly creating it themselves, and install it. This

would allow them to load applications that they themselves approve. Of course, educating consumers so that they can fully exercise their rights is another matter.

Eliminating privacy

The current TCPA specification includes a *trusted third-party* system for preserving privacy. Unfortunately, it does not work.

If a user requests several anonymous credentials, the trusted third party can still link all of the anonymous credentials to the user because the user is uniquely identified in each certificate request. Also, if the trusted third party ever colludes with a true name certification authority or, more likely, companies possessing their registration information, it is easy to attach the user's real identity with the anonymous identities by matching public keys (the user's unique identity). TCPA proponents will argue, but cannot guarantee, that this will never happen.

RECOMMENDATIONS

Although the TCPA has operated behind closed doors, they have published their specifications and requested feedback. I believe that the following recommendations will eliminate most of the specification's unfavorable aspects while retaining its benefits.

Preserve fair use rights

Users should be able to continue copying and using copyrighted material for their own personal use. One way to protect fair use rights without drastically modifying the current specification is to let individuals become the root of their own certification tree and authorize various devices under their control to view purchased content. Users would need the ability to create their own tree and associate devices with it by loading new trusted certificates and possibly new roots.

Many content holders will argue that this approach would let thieves create unduly large certification trees

that they could use to create pirated copies. However, the TPM could reasonably limit the size of trees and offer users the option to request larger ones when needed.

Facilitate open source competition

Any technology that protects the rights of one group and infringes on those of another—as the current specification allows—is unacceptable. Giving users the freedom to choose their operating systems and applications encourages competition and benefits all of us in the long run.

The current TCPA specification has the potential to significantly erode privacy.

The TCPA should revise the specification to let users load their own trusted root certificates for both integrity and trusted storage. It should also provide documentation to open source developers to make the tools required to create and load such certificates readily available. Finally, the TCPA should let users completely disable the TPM, not just a subset of it as the current specification permits.

Enable true privacy

Some argue that true privacy cannot exist in the digital age. In January 1999, when questioned about privacy safeguards Sun Microsystems was considering for its forthcoming Jini network technology, CEO Scott McNealy infamously remarked that consumer privacy was a “red herring” and that people should “get over it” (<http://www.wired.com/news/politics/0,1283,17538,00.html>).

However, like many others, I believe that privacy is a right that should not be taken away without an individual's informed consent. The current TCPA specification has the potential to sig-

nificantly erode this right, but fortunately there are ways to ensure privacy for users who desire it.

Permitting users to completely disable the TPM is one sure remedy, but that would also prevent them from viewing protected content. A more practical alternative is to let the TPM have both a true name identity when users wish to reveal who they are and a pseudonymity when they desire privacy.

Such a mitigation strategy would prevent trusted third parties from colluding with others to learn the true name of a user based on the user's pseudonym but not from linking multiple pseudonyms of the same user. Eliminating this problem would require additional research into methods that let users or the TPM verify compliance without actually releasing the compliant device's identity information.

Improving information security is an important and timely goal, but not at the cost of further weakening fair use doctrine, encouraging anticompetitive behavior, or eliminating privacy. Unfortunately, the current specification does not meet this standard. However, I believe that the TCPA can rectify many, if not all, of the problems pointed out by Ross Anderson, myself, and others without having to make radical changes. ■

Bill Arbaugh is an assistant professor in the Department of Computer Science and the University of Maryland Institute for Advanced Computer Studies at the University of Maryland at College Park. Arbaugh's research contributed to the development of TCPA technology. Contact him at waa@cs.umd.edu.