The TCPA; What's wrong; What's right and what to do about[1]

William A. Arbaugh[2]
Department of Computer Science and UMIACS
University of Maryland
College Park, Maryland 20742

July 20, 2002

We are all aware of the criticisms that the TCPA has received. Ross Anderson did a good job of explaining the problems in an abstract fashion, but I felt that there were some things left out (Privacy concerns). I also wanted to see if the TCPA could provide the good things- mandatory access control, integrity protection, and secure storage without the bad things. What I found will appear in an article in my security column of IEEE Computer next month. However, I wanted to briefly mention the findings before hand.

The Trusted Platform Module (TPM) is the core of the TCPA specification. Ross calls this "Fritz" in honor of Senator Hollings. The TPM is really nothing more than a cryptographic co-processor tightly coupled to the CPU that requires software support from the BIOS, and host operating system. The TPM provides two classes of functionality: integrity protection ("integrity metrics in the specification"), and trusted storage. Both require a basis for their security guarantees, and both use trusted root certificates as this basis. The security guarantees are then provided through the application of induction as the system boots and subsequently operates. One point that should be made is that it is not a reference monitor as Ross has suggested. However, it could operate as one with the appropriate OS hooks.

The potential evil of the specification comes from three distinct points. The first is a non-malleable "trusted root" for trusted storage. The second is the inability to disable ALL of the functionality of the TPM, and the third is the inability to provide a reasonable degree of privacy.

Currently, the specification does not permit the owner (the consumer in a home use situation, and likely an enterprise in the business case) to load an alternate trusted storage root. This, coupled with the inability to disable the "extend" capability, would prevent anyone from running an operating system of their choice. It could also prevent the use of "free" operating systems because the OS kernel would have to be signed by a entity which is a descendant of the trusted root. The difficulty and cost of obtaining such a certificate is unknown at this point. It is this capability that Ross has argued, correctly, can potentially be used to circumvent the GNU Public License (GPL).

---

[1] This article is an overview of a slightly larger article with a different title in the Information Security column of IEEE Computer in August 2002.

[2] Ross Anderson credits myself, and my co-authors for the ideas behind the TCPA because of my dissertation research on securely initializing an information system. The two conference papers on the subject are here and here.

The current specification provides a method for obtaining an anonymous user identity certificate from a privacy certificate authority over a secure channel. The user (or actually the TPM) sends a public key and three credentials to the CA: a public key certificate, and two attribute certificates. The public key is the key for which the user desires a certificate. The public key certificate is the endorsement certificate issued by the entity that endorsed or verified the TPM. This will likely always be the manufacturer or a third party testing lab under the current specification. The endorsement certificate amongst other things contains a NULL subject and the public key of the TPM public endorsement identity. The first attribute certificate is the platform credential which contains a pointer to the endorsement certificate which uniquely identifies the endorser of the platform and the model, i.e. the revision of the hardware and software, details of the TPM, and that the platform complies with the TCPA specification. The second attribute certificate is the conformance credential which asserts that the named TPM complies with the TPCA specification. The specification clearly states that the 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, i.e. they can be used to uniquely identify the platform and then possibly the user through product registration information.

Once the privacy CA receives the three certificates from the previous paragraph, the CA verifies the information and 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 user now has a presumably private identity.

The privacy aspects of the TCPA implement a "trusted third party" system where the user presents their identity and receives an anonymous credential from an anonymity certification authority (the trusted third party), see the above technical discussion. There are two major problems with this approach. The first is that if a user requests several anonymous credentials—the "trusted third party" can still link ALL of the anonymous credentials to the user because of their knowledge of the user's identity. The second problem is that if the "trusted third party" ever colludes with a true name certification authority (or more likely companies along with their registration information) then it is easy to attach the user's real identity with their anonymous identities by matching public keys. While the proponents for the TCPA will argue that this will never happen, they can not guarantee nor prevent it.

But rather than throw stones at something that might actually help improve security, let's see if we can keep the "good" and lose the "bad". Please note, that this might not be doable in all cases because security is a "double edged sword". Just as it is required to provide anonymity; it can eliminate it. Just like the sword- it all depends on how you use it. As such, the following are suggestions to the TCPA technical committee:

1. *Allow owners to load their own (or others) trusted root certificates, and provide the source code for tools that do so*. This eliminates the ability to circumvent the GPL and permits owners to use any operating system and applications of their

choice. It may, however, prevent the owner/user from viewing content that is protected.

2. *Allow the TPM to be completely disabled*. This will permit users to utilize the information device completely free of any TCPA capabilities.
3. *Allow for complete privacy*. Doing this, unfortunately, requires more research into zero knowledge systems, or group keying mechanisms.
4. *Work with the open source community to enable the use of TPM features*. Ideally, this would include the release of example source using the TPM under an open source approved license.
5. *Hold a technical workshop for open source, privacy advocates, and security researchers*. This will allow the community to better learn about the TCPA and provide better input.

The TCPA as it stands now is unacceptable. But, technology such as TCPA offers great promise for improving information security. I hope that the TCPA technical committee listens to these suggestions and/or others, and takes action to improve the specification so that we can have the good, but not the bad.