How Can You Trust the Computer in Front of You?

Siani Pearson
Trusted E-Services Laboratory
HP Laboratories Bristol
HPL-2002-222
November 5th , 2002*

E-mail: Siani.Pearson@hp.com

trusted platform, trusted computing platform, TCPA, root-of-trust, privacy

In this article the issues that lead us to trust - or not trust - the computers that we use every day are examined.

* Internal Accession Date Only
Approved for External Publication
www/informit.com, September, 2002

How Can You Trust the Computer in Front of You?

Siani Pearson

Trusted Systems Lab,
HP Laboratories,
Filton Rd, Bristol. BS34 8QZ. UK.
Siani.Pearson@hp.com

Abstract

In this article the issues that lead us to trust – or not trust – the computers that we use every day are examined.

Introduction

Most dictionaries define at least one use of the word *trust* in wording similar to the following: "a firm belief in the reliability or truth or strength, etc., of a person or thing." However, this is not the end of the story. To date, we have no universally accepted scholarly definition of trust, although "confident expectations" and "a willingness to be vulnerable" are usually viewed as critical components.

In this article, I'll attempt to provide a succinct analysis of trust, including consideration of both behavioral and social components. This provides important context for explaining the sense in which you can trust your computer.

Trust: A Complex Notion

Pinning down the meanings of many words is difficult. *Trust* is particularly tricky because it's not a simple notion. Typically, we think in terms of entity A trusting entity B for something, which is complex for the following reasons, among others:

- **Not always transitive.** If A trusts B and B vouches for C, does A trust C in this case? In other words, is trust a transitive notion? The answer is *not always*, although it can be transitive under specific circumstances.

- **Dynamic.** Trust is dynamic rather than static; there can be differing phases in a relationship, such as building trust, ongoing trust (a stable relationship), and declining trust. Trust can be lost quickly.

- **Varying degree and scope.** Trust levels differ both in the sense of varying degree and scope of trust: Entities typically trust—or don't trust—each other to fulfill selected obligations or for a particular purpose, rather than for everything. On

the other hand, trust in certain areas can transfer to more general trust, as shown by major brands having an advantage when moving into new areas of business.

It's useful to have a succinct definition of trust if at all possible, however, particularly if you're claiming to provide an increased level of trust in something.

When "trust" is applied in an online business context, these facets include the following:

- **A technological basis**—that's the main concern of this article.
- **A contractual side**—including both laws and underwriting or contracts.
- **Customers' image**—built up via previous interactions with a company, brand image, publicity, and so on.

Trust in Technology: Delegation of Trust

It's very probable that some dictionary definitions of trust will mention law, and this is no accident. Indeed, one reason why trust is necessary is because we don't have the resources on a personal level to analyze all the information that we need during our working life. Therefore, as societies become more advanced, such delegation increasingly requires trust in functional authorities and institutions, particularly in the area of knowledge (and technology).

As far as the technological basis of trust is concerned, people can't always be expected to work things out for themselves, particularly when technology is involved. They'll look somewhere else for an example—for example, a consumers' association or role models. Because of a lack of information and time, together with the huge complexity of IT security, it's impossible for users of IT products to identify the level of security offered by individual products. They need to rely upon a product being assessed accurately by experts through evaluation and certification procedures, such as using criteria catalogues. Such criteria catalogues are widely used; for example, the "orange book," ITSEC, Common Criteria in ISO/IEC. I'll explain later how delegation of trust can be used in order to enable you to trust your computer.

Trusted Platforms

A Trusted Platform in the latest jargon is a computing device that has a trusted component, probably in the form of built-in hardware, and uses this to create a foundation of trust for software processes. The computing platforms specified in the Trusted Computing Platform Alliance (TCPA) specification are one such type of Trusted Platform. (For further information about the TCPA specification and its use, see http://www.trustedcomputing.org/.)

TCPA Trusted Platforms are designed to provide enhanced identification and data storage and to maintain user privacy. Another central feature is that they have mechanisms that provide information about their software state with a high level of assurance, so that you can decide whether to trust a platform's behavior for your intended purpose. In particular, you can judge whether it's safe to use the platform for sensitive processing. The information can be made available over the Internet to anyone who wants to interact with the platform. These trust mechanisms are a new feature of TCPA Trusted Platforms, and I'll describe below how they work.

How Can Platforms Be Said To Be "Trusted"?

As noted, there are different aspects to trust. The TCPA definition of trust is that something is trusted "if it always behaves in the expected manner for the intended purpose." A similar approach is adopted in the third part of the ISO/IEC 15408 standard: "A trusted component, operation, or process is one whose behaviour is predictable under almost any operating condition and which is highly resistant to subversion by application software, viruses, and a given level of physical interference."

In this section I'll give a description of the TCPA trust mechanisms and argue that categorizing trust in terms of behavioral and social components helps in understanding how Trusted Platforms enhance trust.

The way in which you (as a local user or third party) know whether a platform can be trusted is as follows:

- When you want to trust that platform for some particular purpose, you ask for measurements (called *integrity metrics*) about the platform, digitally signed by the trusted component on that platform. You then compare these integrity metrics with expected values that represent software that you would trust sufficiently to interact with the platform for whatever purpose you have in mind. (The actual measurement values that are compared could differ according to the particular intended use of the platform.)

- If the measured values are the same as the expected values, you can safely interact with the platform for the desired purpose. Anomalous integrity metrics indicate that the platform is not operating as expected, and you'll need to judge whether to proceed with the interaction based on this information.

In order to trust a computer platform, it's necessary to use both behavioral and social elements of trust; mechanisms provide information about the behavior of a platform, but you'll only trust that information if you trust the people who vouch for the mechanisms themselves, as well as for the expected value of such information.

Behavioral Components

A TCPA Trusted Platform provides trust mechanisms to generate reliably, store, and report measurements about its software environment. These trust mechanisms dynamically collect and provide evidence of the platform's post-boot behavioral history.

There are two minimal roots of trust for these mechanisms:

- The *root of trust for measurement* (RTM) starts the measurement process.
- The other root of trust stores the results of the measurement processes as they happen, in such a way that measurements cannot be "undone." It cryptographically reports the current measured values and prevents the release of a secret if the current measured values don't match the values stored with that secret. This second root of trust is implemented as a hardware chip rather like an internal smart card chip, called the *Trusted Platform Module* (TPM). The TPM is protected by being tamper-resistant, so that what goes on inside the chip cannot be tampered with by the platform, by the user, or by a third party. The TPM is something that's trusted by everyone.

This evidence of behavior is the behavioral component of trust, since it provides the means of knowing whether a platform *can* be trusted.

Social Components

The social component of trust relates to what it is to be *trustable* (capable of behaving properly); that is, trustworthy in a social sense, when people agree that the trusted item is *bona fide* and will do the right things.

Social trust in a Trusted Platform is an expression of confidence in behavioral trust, because it's an assurance about the implementation and operation of that Trusted Platform. Such information provides the means of knowing whether a platform *should* be trusted. Trusted Platforms use social trust to provide confidence in the integrity collection and reporting mechanisms mentioned above via delegation of the analysis of such mechanisms. They also use social trust to provide confidence that particular values of integrity metrics published by another organization or individual indicate that the platform can safely be used for a particular purpose.

A specific TPM relies on social trust—you can inspect its platform certificate, which is a trustable assertion by the company that made it. Other elements of a Trusted Platform also have certificates that vouch for the design of a Trusted Platform—that a specific TPM was incorporated into a Trusted Platform, that the design of the RTM and TPM meet the TCPA specification, and so on.

In summary, social trust underpins why a Trusted Platform can be said to be "trusted"; third parties are prepared to endorse the platform because they've assessed the platform and are willing to state that if measurements of the integrity of that platform have a certain value, it can be trusted for particular purposes. Whether you're a local or a remote user, so long as you trust the judgment of the third parties, if the platform proves its identity and the measurements match the expected measurements, you'll trust that the platform will behave in a trustworthy and predictable manner.

In this section I've given a brief introduction to the trust mechanisms provided by TCPA. Unfortunately, these trust mechanisms are inherently difficult and can't be directly managed by individual (human) users; they require cryptographic operations and complex comparisons. As a consequence, you always need a computing engine to challenge a Trusted Platform, even when that Trusted Platform is right next to you. Challenging a remote Trusted Platform involves a straightforward use of the trust mechanisms described above, so long as you trust that your challenging device will convey its findings to you and make its analysis about the integrity of the platform in a trustworthy manner. But what if you can't trust it? And what about checking a platform in front of you that you want to use but that you don't necessarily trust?

So How Can You Trust the Computer in Front of You?

As well as a system authenticating a user, it's sometimes necessary for a user to authenticate a system. Let's imagine that you're using a system other than your own, in a frequent flyer lounge at the airport, for instance, or at another desk. The work you're doing on that computer is confidential, but you're faced with using a machine that runs unknown software and that could possibly be set up to take information and send it to someone else or store it for misuse. You need to ensure that the computer can be trusted to behave in the manner you expect for the particular use you want to make of it. In addition, you need to know that when you're told this is the case, it's not malicious software giving you a message that's merely *pretending* to be trustworthy!

To solve this problem, a smart card can be used to make it easy and non-intrusive for you to establish that you can trust the use of a computing platform for a particular purpose. The smart card will carry out the challenge of the Trusted Platform on your behalf. You therefore only need to trust that your smart card will behave as expected—something that we've already become used to with banking cards. A smart card can be programmed with secret information that only you know—for example, a drawing that your child made. You put the smart card close to the computer's smart card reader, or into a smart card reader with a contact card. If it picks up the drawing and displays it onscreen, you know that the computer is safe because it has been interrogated and checked by the smart card on your behalf. This secret image can't be reused indefinitely, and needs to be changed periodically in case it's compromised.

Another way for the smart card to communicate the result of the Trusted Platform challenge to you would be to implicitly deny access to functions of the smart card (in other words, the smart card would deny authentication information required for access to a specific service, on the basis that integrity verification of the platform has failed).

As an alternative, a portable security challenger with a proper user interface could be used to enhance your confidence in Trusted Platforms. The portable challenger could be a mobile phone, personal digital assistant (PDS), smart card reader, biometrics reader, or other device. The portable challenger would challenge the local platform to obtain integrity metrics, as described above, and communicate its findings to you through its own user interface.

These ideas are not discussed at all in the TCPA specification, and they can be applied to a wide range of scenarios, including using terminals in public places to carry out confidential business.

Once you're convinced that it's safe to use a platform, you can safely present your authentication information to the platform, knowing that it won't be stolen or subverted. This authentication information can take the form of simple passwords or biometrics.

Once authenticated, you can use the platform to digitally sign data with increased confidence. You can use Trusted Platforms to give you greater confidence that the document you believe you're signing is *actually* the document you're signing, which is particularly important as digital signatures gain in legal status. For example, your smart card could be programmed to refuse to sign data created by the platform unless the smart card trusts the platform. Or, using a specially modified Trusted Platform where the TCPA chip is integrated into the display circuitry, your special secret image that's stored on your smart card could be used as a background or border to an image that represents the data to be signed, and so you can be sure that you're signing a digest (compressed version) of what actually appears marked by this image on the computer screen.

Summary: Trust and Trusted Platforms

The concept of trust in computing involves myriad issues, all of which are important for business. TCPA has taken the approach of addressing the issue of trust (confidence) for businesses rather than just trying to improve the level of information security *per se*, although security improvements do form part of the solution. Trust is a fundamental concept in the business world, and information security is an important—even vital—enabler.

A genuine Trusted (Computing) Platform is a platform that's trusted by local users and remote entities, including users, software, web sites, and all third parties. To enable you

to trust a computing platform, a trusted relationship must be built between you and your computing platform that can tell you that an expected boot process, a selected operating system, and a set of selected security functions in the computing platform have been properly installed and operate correctly. You then make your own judgment as to whether you trust the boot processing, operating system, and security functions. By using your trusted PDA or smart card, you can also check out computers that you think might be untrustworthy or that you haven't used before.

Acknowledgements

This article is based on technology developed by a variety of people within the TCPA organization and within HP Labs' Trusted Systems Lab; the technology is described further in "Trusted Computing Platforms: TCPA Technology in Context", edited by Siani Pearson, written by Boris Balacheff, Liqun Chen, Siani Pearson, David Plaquin and Graeme Proudler, pub. Prentice Hall, 2002.