Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump (Ed.):
(24th June 2003)

Digital Rights Management

Technological, Economic, Legal and Political Aspects

digital-
rights-
management.org

Contents

1 Introduction
Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump 9

2 Digital Rights Management: Technological Aspects 11

2.1 Definition, Aspects and Overview
Niels Rump 11

2.2 Requirements for DRM Systems
Richard Gooch 24

2.3 Components of DRM Systems 34

2.3.1 Identification and Metadata
Norman Paskin 34

2.3.2 Authentication, Identification Techniques and Secure Containers — Baseline Technologies
Gabriele Spenger 70

2.3.3 Digital Watermarking
Fabien A.P. Petitcolas 89

2.3.4 Content Based Identification (Fingerprinting)
Jürgen Herre 101

2.3.5 Rights Expression Languages
Susanne Guth 109

2.3.6 Electronic Payment Systems
Ahmad-Reza Sadeghi, Markus Schneider 121

2.3.7 Mobile DRM
Frank Hartung 146

2.4 A Sample DRM System
Susanne Guth 158

2.5 DRM and Standardization — Can DRM be Standardized?
Spencer Cheng, Avni Rambhia 170

2.6 Trusted Platforms, DRM and Beyond
Dirk Kuhlmann, Robert A. Gehring 186

2.7 DRM Under Attack: Weaknesses in Existing Systems
Tobias Hauser, Christian Wenz 214

2.8 If Piracy is the Problem, Is DRM the Answer?
Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan 232

3 Digital Rights Management: Economic Aspects 242

3.1 The basic Economic Theory of Copying
Tobias Bauckhage 242

3.2 Facing the Music: Value–driven Electronic Markets, Networks and Value Webs in Economic Integration of Digital Products
Rolf T. Wigand 258

3.3 Creating a Framework for Business Models for Digital Content — Mobile Music as Case Study
Willms Buhse, Amélie Wetzel 279

3.4 Impacts of DRM on Internet based Innovation
Arnold Picot, Marina Fiedler 296

3.5 Evaluating Consumer Acceptance for Protected Digital Content
Marc Fetscherin 309

3.6 Lessons from Content–for–Free Distribution Channels
Michel Clement 329

3.7 Standardization in DRM — Trends and Recommendations
Oliver Bremer, Willms Buhse 342

3.8 The Darknet and the Future of Content Protection
Peter Biddle, Paul England, Marcus Peinado, Bryan Willman . . 352

4 Digital Rights Management: Legal and Political Aspects 374

4.1 Protection of Digital Content and DRM Technologies in the USA 374

4.1.1 Protection under US Copyright Law
Mathias Lejeune 374

4.1.2 The Copyright Wars — A Computer Scientist's View of Copyright in the U.S.
Barbara Simons 391

4.2 Protection of Digital Content and DRM Technologies in the European Union 413

4.2.1 European Copyright — Yesterday, Today, Tomorrow
Jörg Reinbothe 413

4.2.2 Digital Rights Management and Privacy — Legal Aspects in the European Union
Lee A. Bygrave 426

4.2.3 Private Copying and Levies for Information– and Communication–Technologies and Storage Media in Europe
Constanze Ulmer–Eilfort 455

4.2.4 Tipping the Scale in Favor of the Right Holders: the European Anti–Circumvention Provisions
Séverine Dusollier 470

4.3 Protection of Digital Content — Germany 487

4.3.1 The German Copyright — Yesterday, Today, Tomorrow
Thomas Dreier, Georg Nolte 487

4.3.2 Copy Protection by DRM in the EU and Germany: Legal Aspects
Bettina Goldmann 510

4.3.3 Implementation of the European Info Directive in German Law and its Consequences for Teaching and Research
Bettina Böhm 528

4.3.4 New Copyright for the Digital Age: Political Conflicts in Germany
Dirk Günnewig 536

4.4 Copyright Dilemma: Access Right as a Postmodern Symbol of Copyright Deconstruction?
Thomas Hoeren 582

4.5 Business, Technology and Law — Interrelations of three Scientific Perspectives on DRM
Johannes Ulbricht 595

4.6 The Present and Future of DRM — Musings On Emerging Legal Problems
Stefan Bechtold 605

A Getting insights: DRM Conferences 2000 and 2002
Eberhard Becker, Dirk Günnewig 663

A.1 DRM Workshop 2000: Summary 665

A.2 DRM Conference 2002: Summary 672

A.3 Conference Programmes 675

B Authors 677

C References 693

D Index 789

2.6 Trusted Platforms, DRM and Beyond

Dirk Kuhlmann[416], *Robert A. Gehring*[417]

I Introduction

It is not immediately obvious why a book on Digital Rights Management should include a chapter about Trusted Computing, although a number of publications have investigated the suitability of trusted systems as rights management platform. Until recently, however, they have been of little more than remote interest for DRM as well as for typical business or consumer environments, as they were considered to be inflexible and cumbersome to manage.

This has changed dramatically with the advent of the technology developed by the Trusted Computing Platform Alliance (TCPA). Although this technology has primarily been propagated as security improvement of networked end systems, multiple observers were quick to point out that some basic features were similar to mechanisms that allow to support DRM. In some extreme cases, TCPA has literally been equated with DRM, this is, as a thinly veiled attempt to introduce ubiquitous control mechanisms on formerly open PC architectures.

As an introductory remark, it is sufficient to point out that the apparent contradiction between "openness" and "full user control" on the one hand and "closedness" or "constrained user behaviour" constitutes a similarity between requirements of DRM and system security. Consider computers in organisational and corporate environments: once a machine is part of a collaborative network and processes data that is subjected to external policies, full user control gives rise to a number of problems. It allows users to install and run arbitrary software for both corporate and private purposes. This can easily create security vulnerabilities, something network administrators are very aware of keen to prevent.

Copyright holders are facing a similar problem. Personal computers can include software media players to display digital content, but as the user has full control, they can also be used for storing, duplicating, and disseminating the content in ways not endorsed by copyright regulations. The proliferation of cheap and powerful multimedia PCs and the convergence of digital storing technology (e.g., compact disc) has created a situation where copyright owners have effectively lost control over digital copies of their works.

These and other dilemmas have renewed the interest in mandatory control mechanisms and trusted systems. These systems can enforce rules users have to adhere to when interacting with resources that have multiple stakeholders. In other words: the user can not override the policy while maintaining access to the resource subjected to this policy. This can significantly improve confidence in the expected behaviour of an IT system as it allows fine-grained control over what

[416] Hewlett Packard Laboratories, Bristol.
[417] Technische Universität Berlin.

computers and their users can do at any given time. TCPA and Trusted Platform technology claim to address the problem of how to gather and communicate indicators about what behaviour to expect.

This paper is an attempt to scrutinise arguments that concern TCPA's potential as DRM technology. We will start with an outline of TCPA (v. 1.1b) in terms of its context, basic features, and critique it has encountered, followed by an overview of trusted systems in general that discusses both the traditional concept of 'trust' in IT security and more recent attempts to apply this approach to digital rights management. This allows us to analyze commonalties and differences between traditional and DRM–focused trusted systems. We conclude with a discussion of the future of Trusted Platform technology and some thoughts on technology regulation.

II Trusted Computing Platforms

IT security vulnerabilities have become an increasing problem during the recent years. As of 2003, an average of 11 new bugs are reported every day[418], and this number is rising. As a consequence, security remains a major concern for both corporate and private IT users.

There are a number of factors that contribute to this situation. To name only three of them:

- Most users have little if any idea about what is going on behind their graphical user interface. Even administrators frequently do not have a comprehensive understanding about what is actually happening on their machines.
- All software can be tampered with before or while it is running. As a consequence, systems whose security relies on software alone ultimately can not vouch for their own status and integrity.
- Even if our current IT systems were more secure, they could not communicate this fact in a trustworthy manner to remote peers. Trust relationships between technical systems currently have to be established out of band by their owners.

The current lack of confidence the security of IT can at least partially be attributed to two major advantages of today's end systems and networks — namely, their openness and flexibility, which are often considered as fundamental values. However, one might argue that the extent to which a system should be flexible and open depends finds its natural limitations in the purpose it serves to its owner and his communicating peers at any given point in time. In some situations, maximum openness and flexibility are desirable. In others, the exact opposite might be true.

Systems that put emphasis on security rather than on versatility have traditionally been designed for environments where concerns of confidentiality, integrity and separation of roles are prevalent under almost all conditions, e.g. for the

[418] See: CERT (2003).

military and financial sector. They tend to be governed by rigid polices, and much research has been done to find suitable access control mechanisms, in particular for operating systems[419]. Unfortunately, these designs tend to counteract the aforementioned advantages of openness and flexibility while simultaneously imposing a penalty of additional system management.

Trusted platform technology as discussed in the following sections claims to combine the advantages of both worlds. It starts from the understanding that in everyday situations, security is a flexible notion rather than an absolute goal: in order to be trustworthy, a system just has to be secure enough to be fit for purpose. Trusted platforms do not insist on provable security for all conditions – even less so since the user may not understand and therefore not trust the proof. It is deemed more important that a trusted party vouches for the fact that a particular system configuration and policy is fit for a particular purpose.

Apart from enforcing policies, Trusted Platforms address two other problems mentioned above. The design sets out to provide for a mechanism to reliably record the system state and to report it upon request. This allows to communicate state information from a local machine in a way that is trustworthy to a remote party.

II.1. The Trusted Computing Platform Alliance

The Trusted Platform Computing Alliance (TCPA) was created in 1999 by Compaq, HP, IBM, Intel, and Microsoft, all of which became members of the organization's steering committee. Since its creation, the TCPA has been joined by more than 170 other companies and organisations. Apart from the major platform and software companies just mentioned, the consortium includes, amongst others, chip and BIOS producers, vendors of authentication or security technology and services, and financial or content service providers.[420]

Although the alliance started out with a PC specific agenda, TCPA design characteristics now cater for other a wide range of networked IT such as servers, network appliances, mobile phones, PDAs, and consumer electronics. This has broadened TCPA's appeal even further, and while this article is written (March 2003), the consortium is undergoing a major process of reorganisation that accommodates a wider and more diverse membership.

Since its formation, the alliance has created the current TCPA "Main Specification" 1.1b[421] and a PC–oriented "Implementation Specification"[422]. For the TCPA hardware component, the "Trusted Platform Module" (TPM), was defined, and its version 1.9.7[423] has since been certified by NIST according to the Common Criteria Evaluation Assurance Level EAL3+[424].

[419] Overviews can be found, e.g., in Pfleeger (1996); Anderson (2001); Bishop (2003).
[420] For details. see the TCPA membership list at: http://www.trustedcomputing.org/tcpaasp4/members.asp.
[421] See: TCPA–Spec.
[422] See: TCPA–SpecImpl.
[423] See: TCPA–TPMProf.

II.2. TCPA — Motivation and approach

The IT industry sees itself under increasing pressure from government, businesses and consumers to improve security aspects their products and services. So far, the success of respective efforts has been quite limited. This can partially be explained by the fact that neither the Internet protocols nor the PC have originally been engineered for the purposes they are used for today.

The common Internet Protocol (IP) ignored security aspects almost completely, The same is true for many transport, signalling, and management protocols that constitute the building blocks of today's infrastructure and have been built on top of IP. As a consequence, deployment of security enhanced systems becomes difficult as soon as contributing nodes are part of different organisational domains and subjected to different policies. This situation is increasingly typical for today's Internet: current practices of outsourcing, contracting and collaborative work make it desirable to allow access to precisely defined subsets of system resources, and there is an increasing need to support policies even across organisational and corporate levels.

PCs and their operating systems were originally designed for standalone purposes. Over the last two decades, they have been continuously extended to make them usable as network nodes. Workstations and other end systems now include features that would previously have been considered as elements of networked servers. This has made them more vulnerable to remote subversion and more suitable as tools or launching platforms for hostile attacks. This problem of end point security and trustworthiness is the one TCPA has set out to address.

Given that it was possible to create such a broad industry alliance to tackle end point security, one can safely assume the existence of major technical, economical and political drivers behind the agenda of trustworthy computing. Existing technical deficiencies and continued governmental pressure are likely to play an important role here. Apart from this, there are straightforward economic factors that may motivate support of TCPA's agenda. Depending on their respective commercial activities, consortium members could be motivated by the following considerations:

- TCPA requires an additional hardware component to be embedded on motherboards, which makes this technology interesting for chip producers.
- TCPA relies on security validation and certification, which makes it attractive for evaluation laboratories and PKI vendors.
- Lack of adequate security for end systems has been named as a major inhibitor for ubiquitous e–business and e–government, and e–service providers may see TCPA as enabling technology.
- Last, but not least, content providers and software vendors are likely to view TCPA as a promising technology to protect their rights on digital content[425].

[424] See: NIST (2002).

[425] Content protection is not copyright protection since the copyright laws do not acknowledge mere "material" and/or "metadata" as subject matter for copyright protection. The paradigmatic change hidden behind this chosen terminology ("content") is broadly discussed in: Bechtold (2002).

Given the extent of TCPA's intended usage, security requirements will vary widely due to different usage contexts and platforms. To comprehensively cover this variety in a technical specification is close to impossible, which is likely to be the reason why TCPA steers makes minimal assumptions about usage scenarios. It assumes little more than that every platform has an owner. In addition, the specification reflects the common situation where users do not own the platforms they are working with.

One of TCPA's most emphasised features is a set of mechanisms to reliably record and report the configuration and state of a platform. Since trustworthiness is a multilateral problem in the networked world, reliable reporting not only has to satisfy the local user of a machine, but also peers he is communicating with. Trusted platform technology provides a number of building blocks to address this problem.

There are two ways how users can convince themselves that a system is adequate for an intended action. They either base their decision on their own understanding of technology or they trust a third party that vouches for the system's "fitness for purpose". It should be emphasised that "fit for purpose" is a pragmatic notion and different from "secure". Trusted platforms can support judgements about the level of risk that they might not behave as expected. Secure systems are designed with the goal to minimise or exclude risk. Clearly, secure systems can be built on top of Trusted Platform technology.

Systems that are built on top of TCPA technology can exploit its features to ensure the integrity of the system configuration once it has been accepted. This includes enforcement of any particular policy that is part of this configuration. How they do this is not defined by TCPA; Trusted Platforms technology as such is oblivious to any specific policy or configuration.

II.3. TCPA technology and infrastructure

The TCPA architecture consists of three principal elements: hardware, software, and infrastructure (see figure 1).

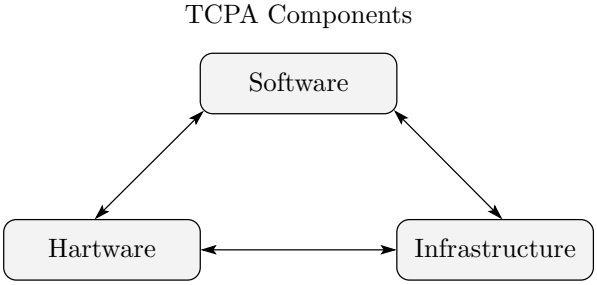

Fig. 1. TCPA Components[426]

The interaction between these components is quite complex and can only be outlined in this section. For a more comprehensive overview, the reader is referred to

[426] Unless stated otherwise, all figures are © 2003 Robert A. Gehring.

Pearson[427] and the specification proper[428]. A number of common misconceptions are addressed by TCPA[429] and Safford[430], and this article, respectively.

Hardware

The hardware component (Trusted Platform Module or TPM) provides functionality that is roughly equivalent to that of a state of the art smartcard. It includes a random number generator, a generator for RSA key pairs, and a limited amount of non–volatile storage. The non–volatile memory on the chip is considered shielded: at the level of the chip's tamper–resistance, it is protected from interference and prying.

Some of the non–volatile memory on the TPM is used to store two 2048 bit asymmetric key pairs. One of these key pairs, the Endorsement key, is generated at the vendor's premises during production time and is the single unique identifier for the chip. The second pair, the Storage Root Key, is generated when a customer takes ownership of the TPM.

During the process of taking ownership, the prospective owner defines an authorization secret that he has to provide to the TPM from then on to enable it. The private parts of both the Endorsement and the Storage Root keys are stored exclusively inside the TPM. The owner can not use the private part of endorsement key to sign or encrypt data. In order to decrypt data that has been encoded using the public part of the endorsement key, knowledge of the authorization secret is required.

The remainder of the non–volatile memory on the TPM is organised as two sets of registers. A Platform Configuration Register (PCR) is designed to store values that represent the complete history of its modifications; a Data Integrity Register (DIR) has the same size as a PCR. It can hold an arbitrary value of up to 160 bit length that typically reflects the expected value of a corresponding PCR.

Most TPM commands are essentially combinations of the basic functions mentioned above: authorization secret, key protection, key generation, shielded configuration registers and integrity registers. Amongst others, the TPM supports to:

- employing asymmetric key pairs that can not be used by software, but only by a TPM,
- logging system events in a non-reversible manner, supporting reliable auditing of the system's bootup and configuration,
- binding the capability to decrypt data to a specific platform state

Most operations are not provided by the TPM on its own, but need operating system and application software support.

[427] See: Pearson, Balacheff, Chen, Plaquin, Proudler (2003).
[428] See: TCPA–Spec.
[429] See: TCPA–QA.
[430] See: Safford (2002a).

Software support

TCPA compliant end user systems require two types of software. The first type, the Trusted platform Support Service (TSS), implements a number of complex functions that need multiple invocations of the TPM and symmetric encryption functionality. The second type, called "Core Root of Trust for Measurement" (CRTM), is part of the platform firmware. It will typically reside in a BIOS or chipset and executed at an early stage of the platform bootup. Its task is to generate hash values of all binary code that is about to be executed and to log these values into the PCRs of the Trusted Platform Modules.

The core idea is to extend this type of "software measurement" from the firmware and the BIOS to the operating system (OS), OS services and applications. TCPA defines the chain of integrity verification up to the OS boot loader. Specific boot loaders or operating systems are not covered by the specification. As of the current specification, TCPA is OS–neutral.

Infrastructure

TCPA based systems include indicators that help to determine the level of confidence users can have in a given software environment. This judegment can be based on trusted statements of other parties. In order to communicate these statements, TCPA needs support of digital signatures, certificates, and public key infrastructures.

The first certificate concerns the unique identifier inside the TPM, the endorsement key. It attests that the private endorsement key resides on a TPM of a specific type, on this TPM alone and that it has never been disclosed to anyone.

The second certificate attests that a specific TPM with a specific endorsement key has been properly integrated on a motherboard of a specific type.

Platform credentials include a reference to a third kind of credential, the conformance certificate. It vouches for the fact that the combination of a TPM and a specified type of motherboard meet the TCPA specification, e.g., because both meet the Protection Profiles mentioned in section II: *The Trusted Computing Platform Alliance* on page 188.

The last certificate type can combine all aforementioned credentials in a single statement. The TCPA specifications envisages these "identity certificates" to be issued as identifiers for Trusted Platforms. It is noteworthy that:

- identity certificates do not need to reflect attributes of human users in any way, as they identify platforms;
- a single Trusted Platform can have an arbitrary number of identity certificates, hence multiple identities;
- requests for identity certificates do not require to prove platform ownership to a remote party.

Figure 2 shows the composition of TCPA components and their infrastructural dependence on Certification Authorities[431].

[431] See: TCPA–TPMProf; Pearson et al. (2003).

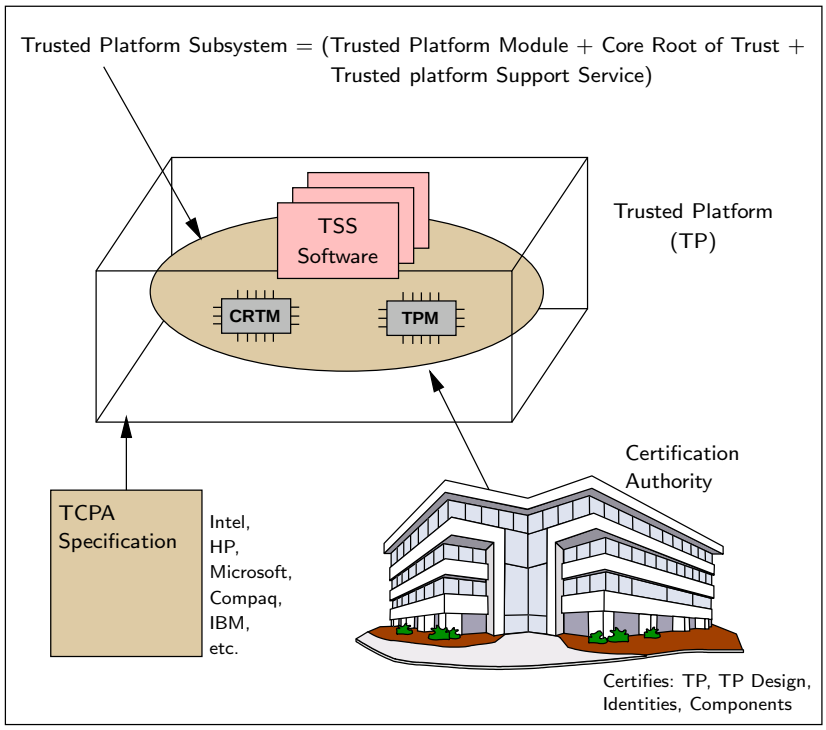

Fig. 2. Composition of TCPA Components[432]

Certification Authorities (CAs) that issue TCPA identity certificates may follow arbitrary policies since the specification is agnostic about particular CA policies and platform configurations. CAs may require a specific protection level attested as by the conformance certificate.

In principle, all TCPA mechanisms can be used without involving *external* certificate authorities. Platform owners, be it organisations or individuals, can issue identity certificates for themselves.

II.4. Critical reactions

The concept of "Trusted Computing Platforms" as proposed by TCPA has drawn heavy criticism from security experts, computer scientists and consumer protection organisations even before its deployment.

An impartial observer will, at least in part, blame the TCPA itself for the criticism: The development process of the TCPA specification was not open to contributions or comments from the public and statements of some TCPA members regarding their intentions to deploy the technology raised suspicion of hidden actions and intentions.

[432] Source: Pearson et al. (2003): 7.

This section gives a cursory overview of the main arguments of the critique. They can not all be scrutinised for their merits here. However, the most common point, namely, the equation of TCPA with DRM, deserves an in–depth exploration. This will be done in section III of this paper.

The objections[433] against TCPA can be roughly categorised as follows:

TCPA means DRM
A number of critics maintain that the main purpose of TCPA is to embed hardware support for Digital Rights and Software management on end user platforms. They question the motives and intentions of the TCPA consortium and, in particular, the large corporations that constitute the steering committee, on principal grounds.

TCPA means less freedom
Critics have pointed out the potential for misusing TCPA technology, e.g. for censorship and customer lock–in. The warnings that TCPA could put restraints on free speech are derived from the same warnings directed against DRM technology.

From a consumer protection point of view, it is claimed that TCPA solves the providers' rather than the users' problem. By supporting to constrain what users can or cannot do with their computers, more consumer value could be destroyed than is created by better trustworthiness.

TCPA means less privacy
Since TCPA is widely equated with DRM, reproaches for undermining privacy directed against DRM technologies are regularly applied to TCPA too. The most important reproach refers to the impossibility of consuming media content in privacy due to the built–in feature of many available DRM systems to collect media usage information and to transfer it to content owners.

TCPA means less security
It has been claimed that TCPA based technology could make reverse-engineering of DRM and security components harder. In conjunction with legal prosecution of reverse-engineering, this may lead to a situation of less rather than more trustworthiness.

TCPA means less competition
Concerns have been raised with respect to potential negative consequences of TCPA in economical, social or political terms. Without objecting to TCPA as such, these critics argue that this technology will inherently cement current quasi-monopolies in the hardware and software sector and may create new ones in the content industry.

[433] More detailed criticism can be found, e.g., in: Anderson (2003); Arbaugh (2002); Green (2002); Cryptography (2002); Cypherpunks (2002) (from June 22, 2002 onwards).

TCPA means more security–relevant problems

A number of issues have been named that are linked to TCPA's hardware- and infrastructure based approach. They concern e.g. problems of (a) proving the trustworthiness of the on–chip random number and RSA key generators; (b) consequences for virtualisation layers and emulators; (c) potential large–scale abuse of the mechanism by bogus endorsement and identity certificates dissemination or revocation.

Summary

To wrap up: TCPA critics object the technology on the grounds that Trusted Platforms mean DRM, less competition,[434] less freedom — including less freedom of choice, and less control[435] Supporters of TCPA have upheld that much of the critique is based on speculation and limited understanding of the technology, and that mutual assurance for IT systems is a real and pressing issue that is independent of any given political and economic context and has to be addressed where it crops up: at the level of technology.[436]

A cautionary observer may conclude that both critique and rebuttals are dissatisfying and that further discussion is in place.

III Trusted systems vs. DRM systems — deblurring the lines

That TCPA should be considered as some kind of DRM is a key part of almost every critical statement about the concept.[437] The reasons for this assumption can be traced back to different motives, some obscure ones and some meritorious ones. We find technical arguments mangled with conspiracy theories and ample speculation based on misunderstandings. To make a serious judgement on these issues, we first have to deblur the lines between the concepts of trusted systems, trusted computing platforms, and DRM systems. We focus here on trusted systems and trusted computing platforms because DRM systems are exhaustively treated in this book.

For reasons of historical developments, we start with a portrayal of trusted systems.

---

[434] Most recently Anderson (2003a).

[435] According to prominent critic Ross Anderson, they are probably even less secure, because a "trusted system or component" is defined as "one which can break the security policy", implying that a "trusted computer" is one "that can break my security" Following this line of logic, the only computer where our security can not be broken is an untrusted one (since no one would expect security in first place). See: Anderson (2003): par. 24, 25.

[436] More detailed answers to the critics can be found, e.g., in: TCPA–QA; Safford (2002a).

[437] See, e.g.: Anderson (2003); Yodaiken (2002); Weber (2003); Grassmuck (2002).

III.1. The classic approach to trusted systems

Trusted systems are neither new nor invented by the TCPA. Actually, research on trusted systems dates back to the 1960s and was driven by government and military needs for effective protection of information. The development of the Trusted Computer System Evaluation Criteria (TCSEC) from 1983 to 1999, also known as the Orange Book, was the first culmination of those research activities. Since its development was driven by governmental institutions, confidentiality is the main focus of the TCSEC. Data integrity and system availability, usually goals of information security, [438] are of less importance within the TCSEC framework [439].

Two research approaches were particularly influential on the formulation of the classic concept of trusted systems:

- The reference monitor concept introduced in 1973 by James Anderson;[440] and
- The Bell–LaPadula (BLP) model as introduced in the same year by D. Elliott Bell and Leonard J. LaPadula.[441]

BLP was developed for a military environment, Anderson's reference monitor has been conceived as a proposal for governmental establishments. BLP is a *policy model*, describing a specific way of controlling access to system resources. It is primarily concerned with restricting the information flow between formally distinguished security levels and compartments. The reference monitor concept, on the other hand, models a *system architecture* suitable to enforce policies. The monitor can be regarded as container to be filled with a rule set of choice (which could follow the BLP model as well as completely different ones). This concept is more generic, as it allows to employ arbitrary policies that might be better suited to meet modern business requirements for sharing information than the rather restrictive BLP.

The following short discussion may help to understand some peculiarities of the TCPA approach to evolve ordinary computers into trusted computing platforms. We start with pointing out some basics of the reference monitor concept.

The reference monitor concept

According to Bishop[442], "a reference monitor is an access control concept of an abstract machine that mediates all accesses to objects by subjects." Figure 3 shows the schematic structure of the reference monitor concept[443].

Conceptually speaking, a reference monitor is nothing more than a container for a security policy. If we "fill" this container with a certain security policy, i.e. with defined subjects, objects and relations between them (e.g., security clearances

[438] See, e.g.: Pipkin (2000): 14; Stallings (1999): 5).
[439] See: Bishop (2003): 574.
[440] See: Anderson (2001): 140.
[441] See: Anderson, Stajano, Lee (2001): 189.
[442] See: Bishop (2003): 502.
[443] See: Stallings (1999): 530.

and classifications), it will enforce the policy (what is allowed, what is forbidden) circumscribed thereby.

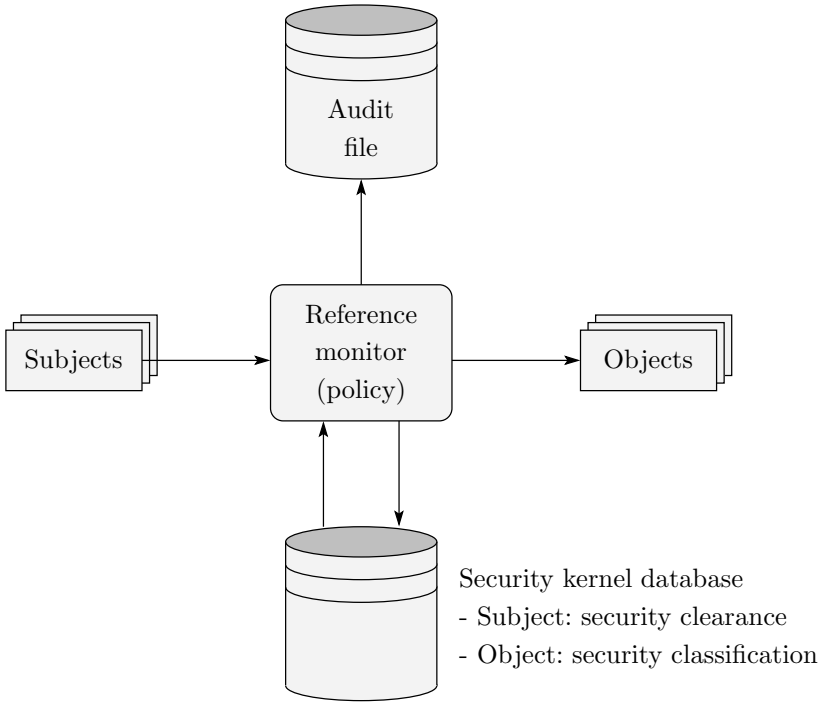

Fig. 3. The Reference Monitor Concept[444]

The implementation of a reference monitor concept is called a "reference validation mechanism" (RVM) and shows the following properties[445]: (1) It is tamper resistant;[446] (2) it cannot be bypassed; (3) it is small enough for complete validation[447]. Around the RVM, the "trusted computing base" (TCB) is built. "*A trusted computing base (TCB) consists of all protection mechanisms within a computer system — including hardware, firmware, and software — that are responsible for enforcing a security policy.*"[448]

[444] Source: Stallings (1999): 530.

[445] See: Bishop (2003): 502.

[446] In fact, Bishop uses the term "tamper proof" here. For some critical analysis of so–called "tamper proof" devices, see: Anderson, Kuhn (1996/1997); Bao, Deng, Han, Jeng, Narasimhalu, Ngair (1997).

[447] In practice, however, the third criterion quite often cannot be fulfilled due to "size or complexity of the reference validation mechanism", as the Orange Book acknowledges. Nevertheless, we speak of a TCB in such cases too. Cf. http://www.kernel.org/pub/linux/libs/security/Orange-Linux/refs/Orange/OrangeI-II-6.html.

[448] See: Bishop (2003): 502.

The intention of his verbal take–over was to transform a standard computer technology into a "copyright box"[456]. And so he describes the new understanding for trusted systems:

> "*A trusted system is a system that can be relied on to follow certain rules. In the context of digital works, a trusted system follows rules governing the terms, conditions and fees for using digital works.*"[457]

Stefik pursued his approach further and discusses trusted systems in the context of the Internet as:

> "*systems, which protect digital works using a set of rules describing fees, terms, and conditions of use. These rules, written in a machine–interpretable digital–rights language, are designed to ensure against unsanctioned access and copying and to produce accurate accounting and reporting data for billing.*"[458]

A quite simple concept designed to enforce, in principle, freely selectable security policies is thereby transformed into a concept for the enforcement of "digital rights" — "machine–governed rules of use" for content such as "[c]*reative works.*"[459]

If we try to precisely identify all the parts of Stefik's approach to trusted systems, we can list them as follows: (a) access restriction; (b) copy restriction; (c) use control; (d) accounting; (e) reporting for billing.

In analogy to figure 3 showing the reference monitor concept, we can sketch Stefik's design as shown in figure 4.

Two additional databases (dashed boxes) complement the database and audit file used by the reference monitor (renamed to DRM monitor for the sake of explanation). One database is needed to store the digital rights[460] and one for the accounting and billing data generated during the subject's use of protected objects.

To prevent any manipulation by the user, neither of the additional databases will be stored on the user's system. Since the DRM monitor is at least in part managed by a source outside of the system's boundaries, the objects are not under full control of the subjects anymore.

From the user's point of view, the crucial issue is the concurrent implementation of two different access control mechanisms: one as described in the digital rights database and one as described in the security kernel database. According to

book "Code and Other Laws of Cyberspace", quotes well known cryptographer Ralph Merkle with a Stefik–like statement (1999: 127). Nevertheless, many commentators consider Mark Stefik being the inventor of "trusted systems". Cf., e.g., Griffith (1999) and Gimbel (1998).

[456] See: Stefik (1999): 55.

[457] See: Stefik (1997): Sect. II (A) Para. 1.

[458] See: Stefik (1999): 55.

[459] ibid.

[460] For the sake of simplicity, we assume the implementation of the digital rights storage as a database. In practice, the necessary information is stored in part in a database and in part tied to the objects (e.g. as digital watermarks).

Stefik and other proponents of DRM systems, the thereby enforced DRM policy will have higher priority than the security policy under the user's control.[461]

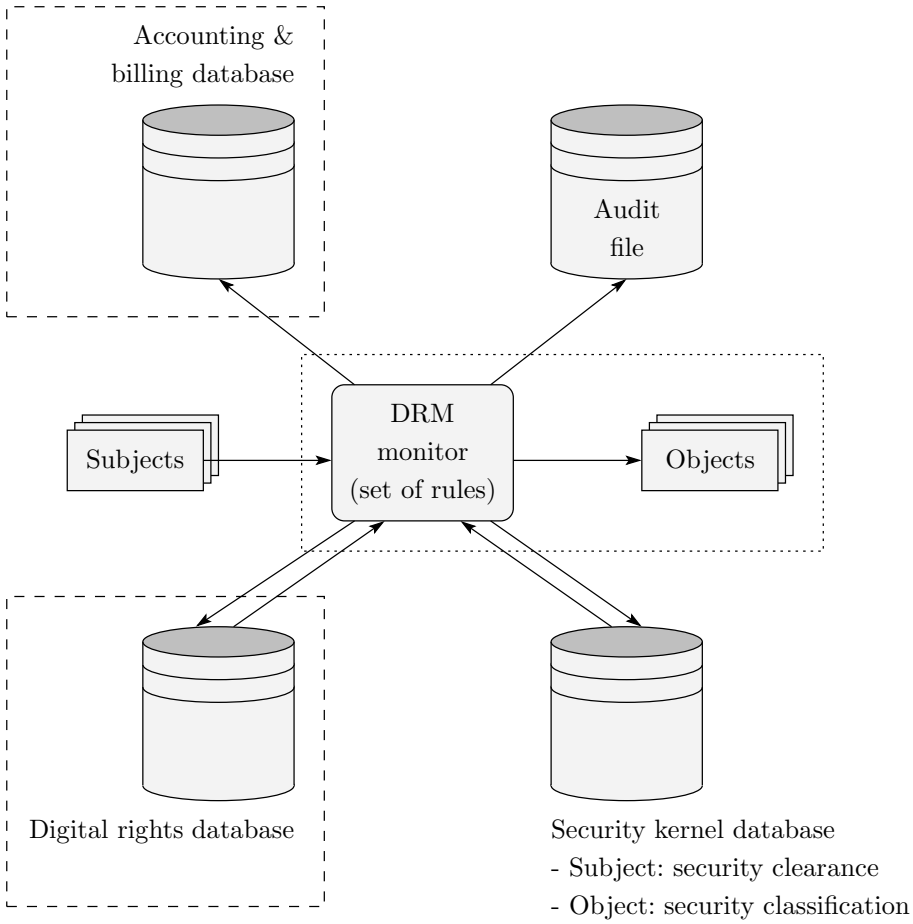

Fig. 4. Stefik's Design for trusted systems[462]

The main difference between trusted systems designed according to the classic concept and Stefik's trusted system is that the first ones are conceptually policy–neutral while the last one is clearly policy–specific.

Many people express their disagreement with these DRM systems by spelling them as "Digital Restrictions Management". As long as definitions of policies addressing digital rights are not in line with copyright law as well as with reasonable user expectations regarding freedom of speech, and protection of privacy,

[461] This is exactly the meaning of the laws giving legal backing to such "trusted systems". Recent heavily disputed legislation — the Digital Millennium Copyright Act (DMCA) in the U.S., and the EU Directive 2001/29/EC in Europe — pinpoint the principle of primacy for digital rights management systems.

[462] Figure based on Stallings (1999): 530.

criticism of systems built to enforce DRM will remain widespread. Nevertheless: simplistically applying the same criticism to the Trusted Computing Architecture means to overshoot the target.

III.3. From Trusted Systems to the Trusted Computing Platform Architecture

The description of trusted systems given above made a clear distinction between their (conceptually) policy–neutral and their (conceptually) policy bound appearance. How do Trusted Computing Platforms fit into this picture?

Compared to Stallings (see section II: *The classic approach to trusted systems* on page 196), Bishop[463] defines trusted systems from a more practical standpoint:

> "*A trusted system is a system that has been shown to meet well–defined requirements under an evaluation by a credible body of experts who are certified to assign trust ratings to evaluated products and systems.*"

Certified authorities apply existing metrics (evaluation criteria) to an existing system (a constellation of hardware and software) in This yields a "*measure of trustworthiness, relying on the evidence provided*"[464]. Since it is practically in feasible to create perfectly secure systems[465], this measure has no absolute meaning, but reflects the relative level of faith or belief one can put in it. In the real and imperfect world, we therefore talk in terms of trust rather than those of security when making judgements systems based on this measure.[466]

It has already been mentioned that this approach is quite static. Changing requirements and/or modification of the system configuration that affect its security property may invalidate the assurances established in a previous evaluation process and can make it necessary to re-certify the system.

Today's systems tend to be highly dynamic. New attributes can be added on the fly. Many of them are capable to interact: mobile phone with laser printers and cameras with computers. The requirement to continuously monitor, "measure", and signal "fitness for purpose" (see section II: *TCPA — Motivation and approach* on page 189) goes beyond what the traditional trusted systems approach had to offer and has motivated the Trusted Platform concept.

Trusted Platforms come with small, embedded hardware elements delivering low–level functionality to the operating system and applications. Once initialised, the behaviour of these elements can not be changed other than by full reset: they can be relied upon behaving as specified. Using a very simple layer model, the architecture can be sketched as shown in figure 5.[467]

[463] See: Bishop (2003): 479.

[464] See: Bishop (2003): 478.

[465] See, e.g.: Bishop (2003): 477.

[466] There are many definitions of trust and trustworthiness and not all are consistent, whereby discussions about this topic are easily mislead. For a short description of the problem see: Anderson (2001): 9 f. The overloading of the wort "trust" is confusing even for experts; some scientists argue that it will do more harm than good when applied to computer systems and transactions. For a discussion see, e.g.: Nissenbaum (1999); Friedman, Kahn, Howe (2000).

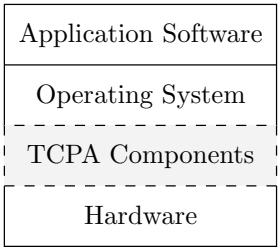

Fig. 5. A Layer Model for TCPA

The TCPA components (hardware and software) are inserted between the standard hardware and the operating system, and activated by "opt–in".[468] Taken on their own, the TCPA components do not provide more than a number of "bricks" to build a trusted computing platform[469] from a conventional computer. The "mortar" comes from outside, from trusted third parties (TTPs[470]) that declare the trustworthiness of the "bricks". To reflect this dependence on different stages from TTPs we enhance the above layer model. (The use of an index x for TTPs indicates the dependence from different TTPs.[471])

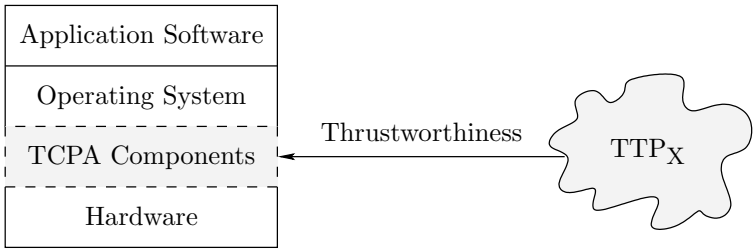

Fig. 6. TCPA layer model with TTPs

The layers above the TCPA layer, i.e. operating system and application software, can make use of the functionality provided in order to operate in a "trustworthy" manner. How far this goes depends on both operating system and application software. Relying on the TCPA components means: an access control policy will be enforced without unexpected interference — as long as the declaration of trustworthiness for the TCPA components holds.[472] Thus, step by step, a trusted system configuration can be build up without the need to certification of the system as a whole. Compared to the classic approach to trusted systems, the trusted computing platform architecture provides much more flexibility.

[467] One of the earliest descriptions of a TCPA–like architecture, the article by Arbaugh, Farber, Smith (1997), also argues along a layered approach.

[468] In practice however, the borders are blurred.

[469] See: Pearson, Balacheff, Chen, Plaquin, Proudler (2003): 44.

[470] The trusted third parties (TTPs) are called "certification authorities" (CAs) in the TCPA terminology. See: Pearson et al. (2003): 298.

[471] See *Infrastructure* in section II on page 192.

[472] Due to lack of experience, it is hard to judge if this approach is feasible on a large scale.

The integration of TCPA functionality into the operating system and/or the application software requires the use of additional TTP support in order to retain the trust model. Again, certification of trustworthiness is provided by the TTP. A multi–user operating system, for example, could make use of certified identities. The integrity of system components will be certified accordingly. The actual level of trust is then derived from the level of trust before the integration of the new system component and its certificate, as shown in the next figure.

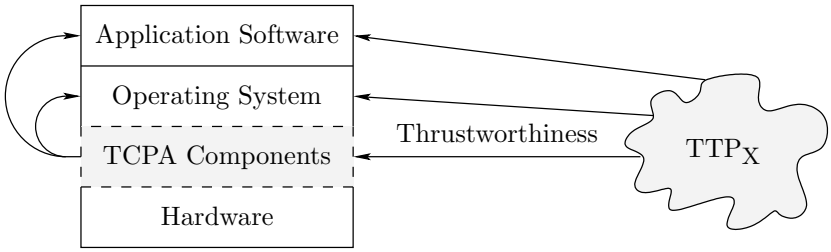

Fig. 7. Promoting Trustworthiness

Thus, trust is propagated through composition of the knowledge of an existing system configuration and authorised statements about new components. In the TCPA terminology, a "chain of trust"[473] is build.

In order to enable "trustworthy interaction" with other systems, the actual state of the system can be signaled to other systems. This is called "remote attestation"[474].

By evaluating this state, the remote system can decide whether the level of trustworthiness signaled by the local system is consistent with its own security policy. If the remote system decides to accept the level of trust signaled by the local system, for example, transactions initiated by the local system can take place.

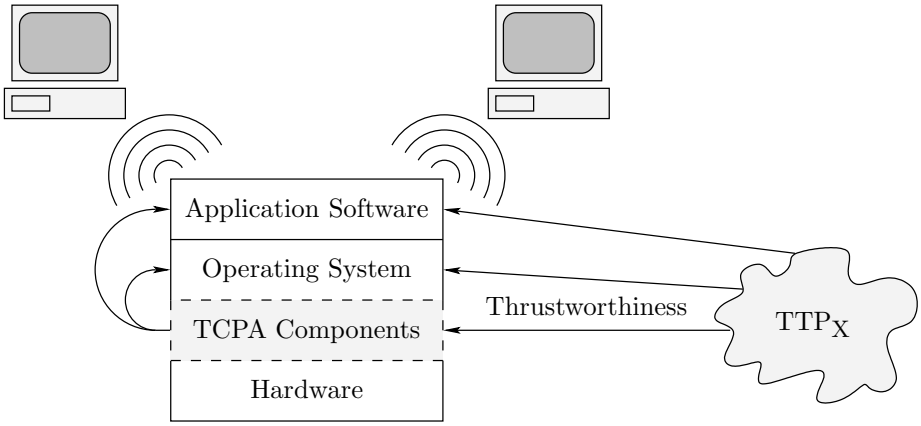

Fig. 8. Remote Attestation

[473] See: Pearson et al. (2003): 75.
[474] See: Pearson et al. (2003): 49.

TCPA provides "*a special wrapping process that permits the caller to state the software environment that must exist in the platform before the TPM will unwrap a secret.*"[475]

> "*Taken together,* [enhanced protection of secrets and enhanced signatures] *improve confidence for the owner of data that resides on remote computer systems. It becomes possible to store data on a remote computer and restrict the conditions under which that data can be used.*"[476]

A wealth of possibilities to handle information according to different security policies is enabled by this TCPA functionality.[477] There can be no doubt that DRM is one of the possibilities.

Although Pearson et. al do not explicitly refer to DRM, they write of "digital content delivery"[478]. "Digital content delivery" plus "restrict the conditions under which that data can be used" is a description of what DRM does. To put it bluntly, although TCPA does not define a DRM system, "trustworthy" DRM systems can be built using the TCPA components.

And here we can draw the line between DRM technology and TCPA technology. DRM technology, by definition, is policy–specific, built "to police copyright"[479], while TCPA technology is conceptually policy–neutral, as was the classical concept of trusted systems before. At least from a strictly technological point of view, this statement holds.

Both proponents and opponents of DRM technology should realise this difference. When discussing the pros and cons of TCPA technology, or *whether* and *how* to regulate the deployment of this technology, the focus has presumably to be directed towards the other elements of the whole communication infrastructure: hardware, operating system, application software levels (local and remote), and certification services.

III.4. A short Comparison of DRM and TCPA

Digital Rights Management (DRM) systems can be understood as follows:

> "*Digital Rights Management (DRM) technology has emerged to protect and manage the commerce, intellectual property ownership, and confidentiality rights of digital content creators and owners as content travels through the value chain from creator to distributor to consumer, and from consumer to other consumers. In an enterprise environment, DRM is related to policy management, which controls access and management of information based on policies.*"[480]

[475] See: Pearson et al. (2003): 46.
[476] See: ibid: 47.
[477] For an overview see: Pearson et al. (2003): 48–56.
[478] See: Pearson et al. (2003): 7, 44.
[479] See: Chris Hoofnagle in: Gaither (2002).
[480] See: Duhl, Kevorkian (2001).

Based on the above made explications on the concept of trusted systems and the peculiarities of the TCPA approach, the following comparison between DRM and TCPA technology can be made:

Criterion	*DRM*	*TCPA*
Relation to DRM	is DRM	enables DRM (1)
Direction	"content"–centristic	"resource"–directed
Policy	policy–specific (enforce "digital rights" policies)	policy–neutral (enforce any access control policy)
Legal status (protection against circumvention)	protected by copyright laws (DMCA, Directive 2001/29/EC)	not specially protected (2)
Optional	(increasingly) no choice for "opt–in" or "opt–out"	specified as "opt–in" technology
Hardware switch	no hardware–based switch–off	hardware–based switch–off specified
Standardisation	different systems from different vendors (3)	standardised technology
Privacy	undermines users' privacy (4)	can be used to undermine as well as to protect users' privacy
Security	insecure (5)	(probably) hard to break
Availability	different systems available	almost ready for market (6)

Remarks

(1) DRM is one technology, and only one, that can be based on the components provided by TCPA.

(2) Since TCPA alone — as it is specified — is not capable of functioning as a "Copyright Protection and Management System" (as described in the DMCA), only *TCPA–derived technology* intended to be used as a DRM system is protected by copyright law against circumvention etc. Otherwise, by specifying a switchable "opt–in" solution, TCPA would possibly offend against the DMCA rules. Every switch disabling TCPA functionality had to be interpreted as "circumvent[ing] a technological measure that effectively controls access to a work protected under this title."[481] Additionally, TCPA will control access to computer resources that by no means, not even under the indistinct declarations of the DMCA, qualify for copyright protection.

(3) See also the article from *Chang* and *Rambhia* (discussing DRM and standardisation) in the present book on page 170.

(4) To protect users' privacy is usually not a design goal for DRM developers, what draws continuing critique.[482]. Even the EU Commission, while pushing development and deployment of DRM systems, raises concerns that "[f]rom the individual's perspective, the unlawful collection and processing of personal data

[481] Title 17, United States Code, Chapter 12, §1201 (a)(1)(A).
[482] See, e.g.: Cohen (2003/a).

for customer profiling and other uses by a DRM provider would constitute a threat to their privacy and could affect the willingness of consumers to accept DRMs."[483].

(5) As different studies have shown, contemporary DRM systems provide only a medium level of security and, in fact, many systems do not even resist unsophisticated attacks.[484]

(6) IBM is already delivering some of its notebooks with a security chip and according software support. This *proprietary solution*, however, is not to be confused with TCPA. Nevertheless, it can be considered as some kind of a prototype of a trusted computing platform according to the TCPA specification.

IV The Future of TCPA

An updated version of the TCPA specification is currently under development. It can be expected to address well–known shortcomings of the current specification such as the simplistic audit mechanism[485]. As for the alliance itself, it has become obsolete after the formation of its successor, the Trusted Computing Group (see below).

TCPA has met a fair amount of criticism. Much of it, such as the notion of "TCPA–certified" operating systems and software, is based on misconception or mere speculation and has been dismissed as such by parties with vested interests[486], but also by apparently independent analysis[487]. Other arguments, however, require careful consideration, not least because successful deployment of TCPA technology will critically rely on customer acceptance.

Many debates were actually centred around potential implications of "Palladium" — this is the old label for Microsoft's efforts to build its own trusted platform (the name "Palladium" has since been replaced by the slightly more cumbersome one of "Next Generation Secure Computing Base" or NGSCB).

In the following, we give a brief overview of the Palladium / NGSCB approach and the hardware that underpins this architecture: Intel's LaGrande technology. We will close this sections with some considerations about TCPA and Open Source and a first glimpse at the freshly founded Trusted Computing Group.

IV.1. TCPA and Microsoft's Palladium / NGSCB

Although TCPA and NGSCB share some basic features, e.g. the TPM, Microsoft has made it clear that both have fundamentally different architectures.[488]

[483] See: EU–COM (2002): 14.
[484] See, e.g.: TÜViT (2002); EU–COM (2002); Pfitzmann, Sieber (2002).
[485] See: Pearson et al. (2003): 71.
[486] See: Safford (2002a): TCPA–QA.
[487] See: Anonymous (2002).
[488] The following discussion is based on Microsoft's Technical FAQ for the Next Generation Secure Computing Base. See: Microsoft Corp. (2003).

NGSCB's scope is much broader and it requires hardware support that goes far beyond what TCPA has to offer. such as those of Intel's LaGrande architecture (see below), as Intel security architect David Grawrock admitted[489].

Palladium relies on a hardware component called "Security Support Component" (SSC), which has features that are very close, but not quite identical, to those offered by the TPM of TCPA. As of writing of this article (March 2003), it is still unclear whether the additional functionality required by the SSC (symmetric AES encryption) might be offered by a future version of TCPA, the chipset, the CPU, the BIOS, a combination thereof, or by a completely separate component.

NGSCB creates a new environment that runs alongside the OS, the so–called "nexus". In combination with the CPU this component allows to "wall off" and hide parts of the memory from other applications and the operating system as shown in figure 9.[490]

According to Microsoft's FAQ, anyone can write a nexus for a nexus–aware system, users will be in control of what nexus runs on their machines, and dual–boot will be possible in the future. It is less clear, however, whether Microsoft's operating systems and nexus–aware applications will run with an arbitrary nexus, whether emulators and virtualisation layers will be affected, whether applications will employ persistent storage shielded by a particular nexus, and how attestation of applications will be obtained.

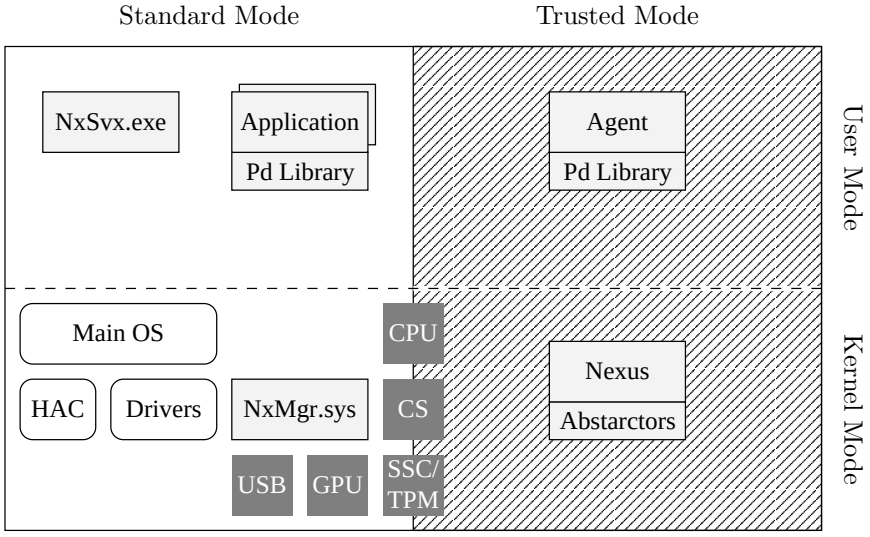

Fig. 9. MS Palladium/NGSCB structure[491]

[489] See: Plura (2003).

[490] This figure shows the Palladium components before the concept was renamed to Next Generation Secure Computing Base. It is drawn after a picture shown in Himmelein (2003): 88.

[491] Source: Microsoft.

Considered that TCPA has carefully avoided to include mechanisms for symmetric bulk encryption into the Trusted Platform Module (TPM) in order to avoid issues of export restriction, it seems quite astonishing that the SSC should contain such a capability in the first place.

IV.2. TCPA and Intel's LaGrande Processor Architecture

As of March 2003, Intel has disclosed very little information about its LaGrande architecture other than it will be released during the second half of the year[492]. Microsoft's plans to "wall off" parts of the memory suggests modifications of the CPU and the memory controller, e.g., by introducing a new capability that is similar, but orthogonal to the well–known "memory ring" concept of the Intel processor architecture. Secured communication between the CPU and the keyboard is likely to require support from a modified chipset.

Intel has declared that LaGrande will be an opt–in technology[493], at least if the new features don't find acceptance in the first place[494]. This has not dispelled concerns about secondary effects such as customer lock–in and loss of privacy, in particular in conjunction with Palladium[495]. It is relatively safe to assume, though, that LaGrande can be used in conjunction with arbitrary operating systems.

IV.3. Open Source and TCPA

Whether or not TCPA leads to strengthening of customer lock–in to proprietary solutions remains to be seen. If future TCPA based software severely impedes consumers, lack of usability might actually push them to look for alternatives.

IBM as well as HP have shown commitment to both TCPA and Open Source[496], and we can expect to see TCPA–supporting Linux versions hit the market in the near future.[497] Both vendors will probably address the enterprise sector first. Other TCPA members declared their support for TCPA–based Linux solutions as well[498].

There are, nevertheless, compelling questions about the impact of TCPA on Open Source software and its particular development model.

---

[492] See: Ortelli (2002).

[493] See: Kanellos (2002).

[494] See: Bonnert (2002).

[495] See: Gaither (2002).

[496] To recall the core idea of software being "Open Source":

> "*The source must be available for redistribution without restriction and without charge, and the license must permit the creation of modifications and derivative works, and must allow those derivatives to be redistributed under the same terms as the original work.*"

Throughout this article, we use the term Open Source in the generic manner quoted above. See: O'Reilly (1999): 34.

[497] See, e.g.: Jaeger, Safford, Franke, (2002), discussing the integration of TCPA, Linux, and the Linux Security Modules (LSM).

[498] See: Krill (2003).

Impact on Free and Open Source software developers

Since it seems reasonable to assume that the certification process for TCPA–supporting software will be neither costless, nor without expense of time, three peculiarities of the Open Source community require particular attention:[499]

1. Important parts (approximate 25%) of the developer community do not have significant amounts of money at their disposal. Even small charges of fees for certification may have a de–motivating effect.
2. About two thirds of the community spend between 0 and 10 hours per week developing Free and Open Source software. Every amount of time spent for certification procedures will, presumably, be deducted from the time invested for developing, testing, and debugging code.
3. Many developers are not paid for developing Open Source code. It is hard to imagine those voluntary "hackers", i.e. sophisticated programmers with strong commitment to pushing information technology to its limits, to invest time and money in order to support business models of industry giants such as IBM and HP.

If a split of the Open Source community is to be avoided, a working model of a TCPA/OS certification process has to be shaped along the sociological structure of the community.

Impact on the GPL

A more puzzling problem is whether Trusted Platform technology will undermine the GPL and other Free Software and Open Source licences,[500] destroy Free Software, allow the GPL to be "hijacked" for commercial purposes and thereby de–motivate idealistic programmers. The original argument put forward in Anderson[501] is based on the notion of a "TCPA operating system" and assumptions that full use of TCPA features require proprietary certificates, neither of which is backed up by the specification. On a more general level, however, a valid point has been raised: does the attestation of security properties for Open Source software have implications for its status, flexibility, production process, and distribution?

The attestation of security properties is external to the source code and therefore not subject to the GPL. Attestation can only ever refer to a particular version of the source code: if the code is altered, the attestation of the original code loses its validity.

[499] We refer to the findings of the "WIDI" study (Robles, Scheider, Tretkowski, Weber 2001) conducted by the Technical University of Berlin, Germany. A follow–up study (Ghosh, Glott, Krieger, Robles 2002) called "FLOSS" and conducted by the International Institute of Infonomics, Maastricht, The Netherlands and Berlecon Research GmbH, Berlin, Germany, showed — with minor differences — similar results.

[500] See, e.g.: Arbaugh (2002): 78 f.

[501] See: Anderson (2003).

Evaluators might claim that security validation of Open Source simply adds value to it. However, the validation of this very source code is only possible because it is "there" in the first place and is open to everyone. The source code to be evaluated is "there" by virtue of liberal copyright licenses that allow for a flexible development process, but the assurances that result from evaluations introduce a formerly unknown element of inflexibility. Flexibility as envisaged, e.g., by the GPL seems to be at odds with assurances provided, e.g., by a Common Criteria evaluation.

This presents a serious dilemma, as there could be clear benefits of an Open Source approach to security in general and Trusted Platforms in particular. In order to combine the flexibility of the Open Source development model[502] with the growing demand[503] for security assurances, new technical and organisational models have to be found.

TCPA, Open Source, and Software Patents

The extent to which TCPA technology and components that can be built on top of it are protected by patents is currently unknown. As far this concerns software patents, it must be emphaissed that they have long since been considered incompatible with Free/Open Source software development.[504]. A "source code privilege" as proposed by Lutterbeck, Horns, Gehring[505] could prove an essential element for enabling the integration of TCPA and Open Source software.

IV.4. The Trusted Computing Group

The formation of the Trusted Computing Group (TCG) was announced [506]. while we were finishing this text. The TCG has been set up as successor organisation of the Trusted Computing Platform Alliance "*to advance the adoption of open standards for trusted computing technologies*". AMD, HP, IBM, and Intel are aboard again, as is Microsoft after temporarily having left the TCPA path. In addition, many consumer electronics companies have joined the TCG, e.g., Sony, Philips,[507] and Nokia.

---

[502] For recent advances in the field of "Open Source security" see: Ott (2003a/b); Wright, Cowan, Smalley, Morris, Kroah–Hartman (2002); Pourzandi, Haddad, Levert, Zakrzewski, Dagenais (2002).

[503] E.g.: from July 1st, 2002 on, all U.S. government acquisitions of IT systems processing sensitive data must be evaluated and validated according to the Common Criteria or equivalent. See:
http://www.oracle.com/corporate/press/1623351.html.

[504] See, e.g.: Gehring (2003).

[505] See: Lutterbeck, Horns, Gehring (2000).

[506] See: Fisher (2003).

[507] In fall 2001, Sony Corp. of America, Philips, and Stephens Acquisition LLC jointly bought Intertrust, holder of many trusted systems and DRM technology based patents. In the aftermath, the EU commission investigated potential negative impacts of this new joint venture for the DRM market and concluded "*that the transaction raises no serious competition concerns.*" Cf. Monti (2002): 5.

Jim Ward, chairman of the TCG, describes the aim of this organisation as follows:[508]

> "*Open standards, widely supported, will accelerate the design, use, management, and adoption of standards–based trusted systems and solutions that are urgently needed to meet the challenges of an increasingly interconnected world.*"

In order to promote this approach, the TCG will continue where TCPA has stopped.[509] Microsoft is founding member of the TCG, which indicates that its NGSCB plans are compatible with whatever the TCG will pursue.[510]

> "*TCG has adopted existing trusted computing specifications from the Trusted Computing Platform Alliance (TCPA) and will extend and enhance these specifications.*"

TCG and DRM?

While the TCG has dismissed any intention to develop DRM standards, [511] Bill Gates has made it clear that Microsoft's future operating systems will support DRM functionality,[512] and Microsoft, who considered the TCPA specification as being not comprehensive enough to support their security architecture not too long ago, has decided become a member of the TCG consortium. Given the TCG's focus to further develop the TCPA specification, we may assume that DRM based on trusted platform technology à la Microsoft is coming closer. This time, however, it may not merely embrace personal computer systems[513], but "multiple platforms, peripherals and devices"[514] as well.

V Summary

Given the complete lack of experience with ubiqitous Trusted Platform technology, difficulties of categorisation and a shortage of independent expertise, many open questions remain. However, it is possible to summarised some preliminary observations.

TCPA and Trusted Platform technology is not identical to DRM technology, although both have a common forerunner in the Trusted Systems concept developed in the 1970s. On the other hand, TCPA offers functionality that can be a used to build DRM systems.

[508] See press release "TCG announced April 8, 2003", at: http://www.trustedcomputinggroup.org/home. Last visited: 10 April 2003.
[509] See TCG FAQ at: http://www.trustedcomputinggroup.org/about/faq/. Last visited: 12 April 2003.
[510] See supra note 509. See also: ComputerWire Staff (2003).
[511] See supra note 509.
[512] See: Schulzki–Haddouti (2003).
[513] See: Merritt (2003).
[514] See press release "TCG announced April 8, 2003", at: http://www.trustedcomputinggroup.org/home. Last visited: 10 April 2003.

Albeit members of the TCPA consortium, Microsoft and Intel appear to have staged a parallel effort to put the vision of a Next Generation Secure Computing Base into action. It is unclear whether this was a contributing factor to finally declare "[d]*eath to the Trusted Computing Platform Alliance*"[515] while simultaneously having the TCG raise from the ashes. Equally unclear are the consequences for a PC market already dominated by Microsoft and Intel. They could be severe, given TCPA's wide support by the industry. Trusted Platform technology is likely be deployed on a very wide scale. Large IT users such as big enterprises and the civil service are might well be the pioneers here.

Microsoft's announcement to make the source code of its nexus "widely available for review"[516] indicates that a huge problem might be lurking at the core of Trusted Computing: Who guards the guardians? How can one be sure that trusted software components are trustworthy indeed and not Trojan horses undermining the system's or user's security instead?

Combining TCPA technology with Open Source software might offer the potential to provide more trustworthiness in electronic transactions. Since the code can be subjected to scrutiny, its potential to foster trust is arguably greater than any combination of TCPA and proprietary, closed source software. The accessibility of the source code as such may not be sufficient to give a convincing answer, but its main virtue "openness" suggests itself as a necessary element to arrive at one.

The proliferation of Trusted Platform technology could change the way information technology is used. If Trusted Platform technology such as TCPA wants to be successful in delivering on its promises of bringing about more security, more privacy, and better customer confidence in electronic transactions, good answers have to be found to well–founded critique. Some of these answers may lie in imparting knowledge about the technology to the users.

In other cases, conceptual, technological or legal changes might be necessary. The Internet revolution has demonstrated that values we take for granted can quickly come under pressure in computer–mediated environments. To sustain constitutional values may well require re–regulation of technology, and it may force us to rethink intellectual property protection.[517]

The need for a political debate

Western democracies protect freedom of speech, freedom of information, freedom of trade, and other values we attribute to an open society. Technology that mediates the social discourse influences how we think about these values. Over the last years, politicians all over the world have shown remarkable reluctance to acknowledge this fact. Laws crafted behind closed doors and enacted to favor

[515] See: Lemos (2003).

[516] See: Microsoft Corp. (2003).

[517] Most recently, Alan Greenspan (2003) contributed to the debate about how to put intellectual resources to most efficient use. He questioned, whether the existing system of intellectual property protection is "*appropriate* [...] *for an economy in which value increasingly is embodied in ideas rather than tangible capital.*"

particular interest instead of the public one undermine the commitment of the majority of people to the "common good" (John Locke) in the long run. A broad, qualified, political debate[518] about how the information society is shaped by technology like TCPA and Palladium is urgently needed.

About this document

This text documents an ongoing discussion between the authors. Should inconsistencies occur in the argumentation, they are likely to be an unavoidable result of different points of view. In many cases, we had to confine ourselves to short descriptions of important technological aspects and to forego a plethora of details.

The opinions expressed in this article are those of the authors and do not necessarily represent the positions of their employers.

[518] And here we do not mean a salon debate among professional politicians but rather a social discourse of all stakeholders, including the 'users'.