

# Preface

Attacks on computer platforms are unrelenting. Governments, businesses, organisations, and consumers are battle fatigued. They cope the best they can and carry on regardless.

Successful attacks disclose the secrets and private information stored and processed by computers. At the turn of the century, the computer industry responded by starting to design Trusted Computing platforms with built-in security mechanisms and built-in trust mechanisms. The security mechanisms are reasonably conventional but the trust mechanisms are novel.

Security mechanisms in computers protect data by isolating data and constraining access to that isolated data. In principle, Trusted Computing enables computer users to select a spectrum of isolation and access controls from non-existent up to the level of the strongest mechanisms implemented in a particular platform.

- The security mechanisms provided by real trusted platforms are anticipated to be somewhat inferior to those of conventional secure platforms traditionally used in critical infrastructures, albeit far superior to those provided by ordinary mass-market platforms.

One doesn't always need to protect data, however, and there is always a balance between convenience of access to data and the level of protection afforded to that data. Sometimes one just doesn't care; or some information in a platform might not need any protection, but other information might need a lot of protection; or the level of protection might vary with time and other circumstances.

The real question for most computer users is whether one trusts a computer platform enough to perform the current task. In other words, is a given platform doing what the user expects it to be doing, and is that behaviour adequate for the user's current purposes? Trusted Computing addresses this question via trust mechanisms that help to determine whether a computing service is trustworthy enough for the current task, instead of just hoping that it is.

Thirteen years on (at time of writing), the greatest difficulty in Trusted Computing has been determining a compromise between incompatible consent, privacy,

protection, and ease-of-use requirements whilst meeting legal, commercial and manufacturing constraints. The greatest business difficulty has been continually solving the chicken-and-egg business problem of introducing new technology for services that don't exist because the technology doesn't exist. The next significant business hurdle may well be avoiding a "race to the bottom", where trusted platforms are implemented in the cheapest but weakest possible ways, to reduce costs to the bare bones.

Speculative criticism of Trusted Computing has probably delayed its adoption, despite the fact that there is no known technical alternative to Trusted Computing for protecting customers' data in mass-market platforms, short of constraining customers' choice of software. The reader may decide for themselves whether this delay has unnecessarily exposed people and organisations to certain types of attack, or has encouraged development of closed computing ecosystems or platforms that constrain the choice of software.

The computer industry has continued to put components of Trusted Computing in place, one by one, even though the components couldn't (and can't) be used to their full potential until all the components are in place. Trusted Platform Module (TPM<sup>1</sup>) chips have been installed in literally hundreds of millions of computers. To assuage initial concerns, TPMs were shipped in an "off" state, so that customers had to opt in in order to use Trusted Computing. Initially, however, the only computer users who understood what a TPM might be were enthusiasts who feared the technology because they had read sensationalist speculative descriptions. Ordinary computer users (whom Trusted Computing is intended to protect) neither knew nor understood, nor wanted to understand, what Trusted Computing is or does. Eventually corporate customers came to appreciate that trusted platforms are safer platforms, but complained that the technology had to be turned on before it could be used. Then it transpired that application developers were reluctant for their software to have any reliance on the TPM, lest the TPM be "off" and hence unavailable. The net effect was that some TPMs were used to protect "data at rest" (when a platform was turned off), via Microsoft's BitLocker™ technology, for example, but the overall level of TPM usage was very low. This has (so far) eliminated the business case for development of a Trusted Computing infrastructure.<sup>2</sup>

Despite everything, Trusted Computing has gained credibility amongst those who have studied the technology. Universities<sup>3</sup> have started teaching and researching the technology, and it has emerged that governments encourage use of the technology to help protect government information. The UK government, for

---

<sup>1</sup> It is a coincidence that TPM is also the acronym for Technical Protection Measure, which is a legal term for a technique used to prevent illegal copying of computer programs.

<sup>2</sup> Albeit the USA's NIST does maintain a National Software Reference Library (NSRL [www.nsrll.nist.gov](http://www.nsrll.nist.gov), visited April 2014), which contains "a collection of digital signatures of known, traceable software applications", including applications that may be malicious.

<sup>3</sup> Including Birmingham University (UK), Royal Holloway College - University of London (UK), IAIK (Graz, Austria), Oxford University (UK), Bochum (Germany), Darmstadt (Germany), Hochschule Hannover (Germany).

example, has published the recommendation “CESG IA Top Tips – Trusted Platform Modules” [CESG01].

The Trusted Computing Group (the industry organisation that promotes Trusted Computing) has become a rallying point for manufacturers to build information protection into their products, and the initiative has expanded to cover other aspects of computers and computing. Besides the Trusted Platform Module chip, new platform firmware, new platform chip sets, self-encrypting hard disk drives (SEDs), trusted networks (Trusted Network Connect, TNC), and more secure parts of the pre-OS platform have been developed. In fact, SEDs and TNC are arguably becoming important and successful in their own right.

The first proper trusted platform is arguably a Personal Computer running Microsoft’s Windows 8™ operating system, which has a Trusted Platform Module (TPM) in its Trusted Computing Base (TCB). This TCB manages the TPM, uses the TPM’s functions to help protect the platform, and enables applications to use the TPM to protect their data. There are as yet no mobile phones that support Trusted Computing because they are arguably really needed only for compatibility with services built for trusted platforms, but there are currently no such services. There’s currently a dearth of trusted hypervisors.

There is no avoiding the fact that mass-market computing needs improved data protection. It’s indisputable that secrets and private information are increasingly stored as data in commercial networked computer platforms, which are under continuous and escalating attack. Improving the level of protection in mass-market computers and computer networks is an enormous task and (given a choice) the ICT industry would have started afresh, instead of with computer and network architectures that were not designed to protect information. The task is complicated by incompatible stakeholder requirements. Providing protection for computer platforms is much simpler if platforms have less flexibility, users have less control, and privacy is irrelevant, but these easy options are incompatible with many existing types of computer platform. Consequently manufacturers have had to devise a compromise that gives almost everyone almost everything they wanted.

The Trusted Computing initiative has forced everyone involved to think about what trust means, who and what is trustworthy, and whether they themselves are trustworthy. Some commentators found the conclusions disturbing and were upset by the effect on the status quo. Some are still upset because, if nothing else, Trusted Computing:

- complicates the way that a platform boots and shuts down,
- complicates access to data, and can prevent existing tools and services from working,
- can help prevent the platform state from being rolled back,
- can be used to implement digital rights management systems, which are anathema to some commentators,
- prevents some repurposing of platforms.<sup>4</sup>

---

<sup>4</sup> At some point, imaginative use of a platform becomes an attack on that platform.

Trusted Computing requires evidence that products are trustworthy, and the technology is undoubtedly an obstacle for those who want to repurpose platforms. Fundamentally, however, no one can dispute that better protection is beneficial for mass-market communicating computer platforms, or that any credible data protection mechanism involves constraining the environment that has access to programs and data. The most liberal constraint is to allow whoever has an unprotected copy of software or data to choose the environment to protect that software or data, and that is exactly what Trusted Computing enables.

Trusted platforms and Trusted Computing will no doubt change with time but this book should continue to provide a record of origins and justifications. The authors have worked in the field of trusted platforms and Trusted Computing for many years. Chapters 12 and 13 were written by Liquan Chen and Chris Dalton respectively. The rest of this book was written by Graeme Proudler with some input from Chen and Dalton.

Bristol  
May 2014

Graeme Proudler  
Liquan Chen  
Chris Dalton

Naturally, this book also draws upon the expertise of many other people over many years. The authors are particularly obliged to colleagues for information on the Federal Information Processing Standard and on export/import regulations; to Paul Waller of CESG for comments and information about certification; and to Dirk Kuhlmann of HP Labs-Bristol for compiling this book's index.

## Reference

[CESG01] "CESG IA Top Tips - Trusted Platform Modules" (April 2014) [http://www.cesg.gov.uk/publications/Documents/ciatt-01-11-trusted\\_platform\\_modules.pdf](http://www.cesg.gov.uk/publications/Documents/ciatt-01-11-trusted_platform_modules.pdf)

Trusted Computing Platforms

TPM2.0 in Context

Prouder, G.; Chen, L.; Dalton, C.

2014, XVIII, 382 p. 9 illus., 2 illus. in color., Hardcover

ISBN: 978-3-319-08743-6