



Trusted Computing technologies: Briefing

Trusted Computing and the Integrity of government-held Information

Purpose

Trusted Computing is a class of technologies that have implications regarding the integrity of government-held information. The E-government Unit has been investigating these implications, and has prepared this briefing paper to provide an update on what has been learned, and to signal what further work we will be doing in this area.

Summary

A quick summary of our advice about trusted computing is that it:

- is an emerging class of technologies with significant implications for government
- heralds a sea change in the way software will be written and delivered, digital content¹ will be created and accessed, and users will have control over their own information
- is available now in only a limited range of products, but while it is very early days for these technologies, their use will become ubiquitous in a wide range of electronic devices
- offers benefits related to protection of intellectual property and the security of online transactions, but also offers risks including:
 - external parties monitoring a user's information without permission
 - software companies controlling access to data generated with their software
 - external parties controlling access to electronic records, including provision for them to disappear after being sent.
- should not be used by the government until and unless it can be satisfied that:
 - it will continue to have access to its own information

¹ Increasingly, digital content is the main medium of storage for all created items, including learning materials, books, music, designs, games and video materials.

- that such access will be under its exclusive control
- that sensitive information will be protected from disclosure to unauthorised third parties.

What is this issue about?

A new generation of computer technology, called “Trusted Computing”, is entering the market. It is expected to address many computer security concerns and enable better enforcement of rights over digital content.

The complexity of the issue derives from the fact that Trusted Computing:

- is highly technical and difficult for a lay audience to understand (it is also poorly understood by the majority of people working in information technology)
- holds promise for the development of further new technologies and applications not yet thought of
- like many emerging technologies, has apparent potential for both great benefit or great harm depending on how it is deployed, regulated, and managed
- is being promoted by a group of international corporations, and the scope for New Zealand to influence what will happen may be quite limited
- is seen by a number of reputable commentators as having wide-ranging and potentially damaging implications for government.

What is Trusted Computing?

Trusted Computing (TC) refers to the ability to feel confident that the software environment in a computing platform is operating as expected. This is to be achieved by reliably measuring and reporting information about the platform.

The scale of deployment of TC is potentially so great, that it could eventually be included within most electronic devices that are used for information storage, delivery or use – including PCs, PDAs and mobile phones.

The organisations and institutions involved in developing and deploying these technologies have been some of the most significant technology companies in the world, including AMD, Hewlett-Packard, IBM, Intel, Microsoft, Sony and Sun Microsystems. Hundreds of millions of dollars have been spent over the last three years in developing these technologies. This is a significant collective endeavour.

How will TC work?

A special security chip will be mounted in PCs that will be able to guarantee security, and will allow users, software and devices to authenticate themselves over a network. The security chip, together with new software designed to work with it, will look to see what programs are being loaded, and will only allow approved software to be used.

When will it become available?

The technology has already been included in a number of products, including the X-Box, and IBM’s Thinkpad T-30 notebook computers.

The technology is expected to be widely available by 2007, including full integration with Microsoft's next Windows version, called Longhorn, anticipated in 2006. The supporting hardware environment will emerge in future generations of PCs and servers.

Digital Rights Management features of the technology are currently available through software such as Microsoft Office 2003, and Adobe's "Policy Server". Adobe's Acrobat Reader software has a user base of more than 500 million copies used for reading PDF files.

What are the potential uses of the technology?

As TC is an emerging technology, many uses for it are at the early stages of development. Some of these are identified below:

- **Financial transactions** – TC would allow financial applications to run in a far more secure environment. For example, it would allow safer storage of passwords, PINs and account numbers; stored data could be isolated from potential viruses; and spoofing by false inputs could be prevented.
- **Digital rights management (DRM)** – DRM technologies protect intellectual property rights, and enforce rules set by rights holders on the use of digital content. DRM is currently used to control access to and use of digital content, and will be further enhanced and strengthened when deployed in combination with TC.
- **Software licensing** – software licensed to a particular user for a particular machine would not work for another user or at another machine, unless specific permission was secured from the licensor.
- **Online elections** – TC could overcome risks inherent in running online elections with election software on an individual's PC. It would allow the voting server to make sure that the user's voting software had not been altered.

Potential concerns

There are concerns regarding TC that have been raised about a wide range of issues, including economic-based concerns (such as the potential effect of TC to strengthen monopolies and limit interoperability and competition). However, the focus for this paper is on issues related to the integrity of government-held information and processes.

Because the technology is at an early stage of deployment, it is not possible to determine the consequences of individual aspects of the design – these will only become apparent when the use of the technology is widespread. When this occurs (expected to be over the next 3-5 years), it will be clear how the behaviour of individuals, businesses and governments are changed.

At this stage, we have identified the following five areas of potential concern:

- **Access to data** – DRM, integral with TC, will allow a user to access software and data on their machine only to the extent that such use is consistent with terms and conditions set by a third party – these conditions can be set by the creator of the data and by the software company. Such control could potentially preclude the New Zealand government from having access to its own information.

- **Privacy** – The remote attestation feature of TC will entail a user’s computer reporting to a remote system in a reliable and trustworthy fashion. This technology will work only by having each computer assigned a unique identity, which will also provide the potential for breaches of user privacy by software developers.
- **Long-term management** – Long term management of government information produced using TC systems could be dependent on continued use of the technology. If at some stage in the future, one vendor’s technology was abandoned in favour of a different system, then historical records may not be able to be decrypted.
- **Permanence of records** – DRM features within TC technology will enable the creator of a digital record to specify that content will disappear after a specific period of time. This is one of a very wide range of controls that will be able to be applied to documents, even after a document has been distributed, and regardless of how many copies were distributed. The implications of government’s access to its own records being able to be “turned off”, whether intentionally or by accident, are significant.
- **Legal obligations of agencies** – The advent of TC is expected to affect the business processes and legal obligations of agencies in many ways. Issues that need to be considered include legal obligations under legislation such as the Official Information Act, Archives Act, Evidence Act, National Library Act and Evidence Amendment Act.

Annex 1 contains examples, which illustrate some of these risks.

What is happening in other jurisdictions?

There is very little evidence to date of consideration being given by other governments to the implications of TC on government-held information and processes. From the contacts we have made with various governments, the feedback we have received is that the issues are important, but that they have not begun to address them.

At this stage, the only country known to have publicly addressed policy issues related to TC and the integrity of government information is Germany. In March 2004, the German Federal Office of Information Technology released its “Comments on the TCG² and NGSCB in the Field of Trusted Computing” – which set out the government’s requirements for the technology to meet if it is to be acceptable. These comments were taken into account in the drafting of some potential requirements for adoption in New Zealand, included Annex 2 to this paper.

New Zealand government officials are currently in the process of liaising with their colleagues internationally to find shared opportunities to develop appropriate collective government policies and positions on issues related to Trusted Computing.

Actions to date

In November 2003, the E-government Unit issued advice to agencies to not enable DRM features of recently available software called “information rights management” which is part of Microsoft Server 2003 and Office 2003. This message is also still posted on the E-

² TCG is the Trusted Computing Group, an organisation that is working to promote the trusted computing specification. See: http://www.bsi.bund.de/sichere_plattformen/trustcomp/stellung/StellungnahmeTCG1_2a_e.pdf

government web site. The reasons for this advice are still relevant today, and this advice is reconfirmed.

Research and analysis has been undertaken by the E-government Unit to keep informed about the latest TC developments and to better understand their implications for New Zealand. This work has included:

- communicating with government agencies, research organisations and various technology and policy experts around the world
- having preliminary discussions with representatives of various New Zealand government agencies, including the Ministry of Economic Development, National Library, Archives New Zealand, GCSB, and the Office of the Privacy Commissioner
- engaging a technical expert to evaluate the technologies and explore some of their implications for New Zealand government agencies
- engaging with representatives of Microsoft to test whether our understanding of the technologies is in accord with their latest thinking, and to have drafts of our consultant's work peer reviewed by them.

Next steps

The E-government Unit will be undertaking further work in this area which will include:

- Investigating appropriate and practicable means for agencies to configure their systems to actively filter out DRM from any files or records that are received, or to return such files to the sender – in the short to medium term.
- Coordinating the process through which government agencies should consider and report on the long term implications of the use of TC and DRM for their own agency.
- Developing principles regarding New Zealand Government use of trusted computing, and consulting with various parties about them including New Zealand government agencies, other governments, and members of the Trusted Computing Group.
- Monitoring what other countries are doing with regard to trusted computing and integrity of government information, and continuing to share our work with them through channels such as the OECD.
- Continuing to engage in dialogue with key ICT industry players in the field of TC.

Annex 1

Examples that Illustrate Risks to the Integrity of Government Information from Trusted Computing

Note: These examples are presented only to illustrate the scale and range of potential risks from implementation of trusted computing technologies. They reflect worst case, but legitimate, scenarios. The extent to which they eventuate will be dependent on how the behaviour of individuals, businesses and governments change as a result of the technology.

These risks may be mitigated through development of appropriate government policies and practices, combined with some (limited) opportunity to influence the way these technologies may be designed and deployed by software and hardware companies.

Access to Data

If DRM were to be permitted in emails or other documents – without adoption of appropriate policies and practices – the myriad of interactions and vulnerabilities may result in a loss of certainty as to what content can be accessed through what software, on what terms it may be accessed, by whom it may be accessed, and for how long it can be accessed.

The complexity of these issues can be illustrated by the following example:

- An agency receives an email from an outside party. It has two attachments. The first is a Word document from an outside party and the second is a PDF document from yet another party
- The email and the documents were all created with DRM enabled but with open permissions for guests
- Continuing access is limited with each document having different controls by time, by the number of accesses and the number of times copies are made from the document
- Recipients are unaware of the permissions, as the guest access and the limitations are ‘silent’
- The email is forwarded on to many. Additional comments are provided. The email and its attachments become evidentially important
- The guest permissions expire with varying effect (some users have saved one or more of the attachments). The originator of the email dies. The PDF is authored outside the jurisdiction and the author cannot be contacted. The author of the word document is not co-operative
- The DRM permissions mean that it is not possible for anyone to obtain access to the email or either of the attachments.

Privacy

Trusted computing will work by assigning a unique identity to each computer, and each computer will report its configuration to a remote system in a reliable and trustworthy fashion. However, this will also provide the potential for breaches of user privacy. Concerns have been expressed about the fact that information about the configuration of a

user's computer, and work being done on it, may be communicated to a software owner (or others) without the user's permission or knowledge.

Examples of these concerns include:

- externally held registers of information about a user's machine or software, with potential for abuse (data matching)
- external monitoring of a user's computer to determine what software and data is held there.

Although software developers may be encouraged to build applications that use personally identifiable information in ways that inform users of what is being shared and how it will be used – there is no guarantee that this will happen. These aspects of the technology, therefore, increase the significance (for the end user) of:

- the risk that a user may grant such permission (to enable disclosure of personal identity and information) without realising that they have done so (e.g., by clicking on “I agree” to a complex end user licence agreement), or without understanding the implications of doing so
- the future potential for software companies to collect and report on a user's personal information without even seeking permission from the user, and without the user's knowledge.

In response to concerns about privacy, “trusted third parties” may be established and used for the purpose of associating particular communications with any specific computer. The reliance on a trusted third party, however, will introduce its own privacy risks, as that party could disclose its knowledge of a user's identity and communications. Thus, the independence, reliability and integrity of any trusted third parties that may be established would become critically important to the integrity of government-held information.

Long term management

Software enabled to work with trusted computing will have its security policy administered remotely by a server. Such remote policy enforcement could lead to “remote control” of software running on a user's trusted computing system.

For example, if a program were to be written to receive a “revocation list” of banned documents it is no longer permitted to display, this would be downloaded from time to time and used to screen all files that the application opens. Files could be revoked by content, by the serial number of the application that created them, and by a number of other criteria – and would be impossible for the user to override.

In that case, a remote authority could revoke documents already resident on computers around the world; those computers would, despite the wishes of their owners, comply with the revocation policy.

A foreign organisation (or government), with access to the TC certification master keys, could prevent the New Zealand government from having access to its own information when that information is held electronically.

Annex 2

Requirements to Be Adopted by New Zealand Government Agencies with Respect to the Use or Deployment of Trusted Computing Technologies

Draft for Consultation Purposes

Agencies should not use trusted computing technologies, unless they can be satisfied that the following criteria will be met:

Transparency and disclosure of interfaces and specifications

- 1 Documentation should be available for all the functionality within the Trusted Platform Module (TPM). The application scenarios for the expected use of the TPM should be documented in an easy-to-understand manner. They should illustrate the effects of the TPM in practical use and should identify the end applications concerned.
- 2 The algorithms and key lengths used for encryption and signature functions should be documented. They should be approved by GCSB for IN-CONFIDENCE material.

Certification of the security system

- 3 The TPM should be certified at least to Common Criteria EAL4. The security and strength of the mechanisms used to generate keys should also be independently validated.

System security, data backup and migration

- 4 The TC solution should allow transfer of the information stored in an existing security module to a new hardware platform in such a manner that users can continue using their software and data on the new hardware platform. It must be possible to migrate any cryptographic keys of the TPM from one hardware platform to another.
- 5 Any TC applications considered - including DRM solutions - should cater for the user's right to copy data and programs for private purposes.
- 6 If data that is not copyrighted is processed with the involvement of the TPM, it must be possible to transfer and use that data on other systems which do not include a security module.

System check by the user

- 7 System owners and/or users must be able to decide whether the TC functions are to be used. This means that it must be possible to fully deactivate the security module. Deactivation of the security module should not affect the functionality of any hardware and software components that do not use the TC functions.
- 8 System owners must have full control of their TC keys, and they should be able to delete these keys and to generate new keys when necessary. They must be able to re-initialise any keys other than those that serve the unambiguous identification of the security module (such as the endorsement keys). It should be possible to delete

any information previously stored in the TPM and to cancel its functionality (for example, when scrapping the PC).

- 9 Where possible, the use of personalised programs, data and online services should be linked to a personalised smartcard rather than the TPM. This will enable more flexible user-related access to data and significantly reduce migration problems.
- 10 The TPM should not hinder the use of any software by requiring validation by an external online service once initial one-off licensing requirements for the software have been satisfied.
- 11 If the use of a certification authority is offered or required, users should have a choice as to which CA they wish to use. Government users should only use government-approved CAs.
- 12 Using the security functions of the TPM must be possible even without an online connection (Internet).

User awareness and consent of data protection and transmittal

- 13 Data protection functions must be transparent so that users can at all times exercise their right of freedom of information and deactivate these functions for the information and files that they 'own'.
- 14 If personal data is transmitted in conjunction with the use of the TC, the user must have the possibility to consent to such transmission in each and every case.
- 15 The user must be informed of the type and extent of data transmitted to the application vendor or any other third party, if any, in connection with the use of the TC.