

Trusted Computing and the Integrity of Government-held Information

A New Zealand Perspective

Andrew McEwen Mason
BSA Limited

Trusted Computing (TC)

- An emerging class of technologies with great potential to improve security in a number of areas
- Heralds a sea change in the way:
 - Software will be written and delivered
 - Digital content will be created and accessed
 - Users will be able to control their own information
- Expected to become ubiquitous in a wide range of devices (PCs, PDAs, mobile phones...)
- Involves many of the largest technology companies such as AMD, HP, IBM, Intel, Microsoft, Sony, Sun.....
- Investment already totals hundreds of millions of \$\$\$

What is Trusted Computing?

- Objective is to provide confidence that the software environment in a platform is operating as expected
- Achieved by measuring and reporting information about the platform
- Will use a special chip mounted in PCs (the basis of the *Trusted Platform Module – TPM*)
- TPM will allow users, software & devices to authenticate themselves over a network
- TPM will check what programs are being loaded, & only approved software will be permitted
- Already in products – e.g. X-Box, IBM ThinkPad T-30 notebooks
- Will offer full integration with MS Windows Vista
- Digital Rights Management (DRM) features are already in MS Office 2003, Adobe “Policy Server” (NB Acrobat Reader user base is >500 million)

Some Potential Uses of TC

- **Financial Transactions:**
 - Safer storage of passwords, PINs, account numbers
 - Prevention of spoofing by false inputs
- **Malware**
 - Offers potential to reduce (eliminate??) threat posed by malicious software
- **Digital Rights Management:**
 - Protect intellectual property rights
 - Enforce rules set by rights holders
 - DRM is currently available in early release (see next slide), will be strengthened when used with TC
- **Software Licensing:**
 - Software licensed to one user/machine would not work on another without specific permission from licensor

Microsoft Digital Rights Management

- Available as *MS Information Rights Management (IRM)* with Office 2003, Outlook 2003 (& a “Rights Management” extension to Internet Explorer)
- “Owner” of a file specifies who may do what with it (read, copy, forward etc.)
- Requires involvement of MS Rights Management services (root CA & Activation Service)
- Appears to be a first step into providing technology for consumers to manage content such as movies, music and electronic books
- At current release, seems to be generally limited to sharing documents within the content-producer’s organisation
- Still at an early stage and thus unproven
- Not currently seen as suitable for Government use
- NZ Government has recommended that Agencies do not enable IRM

Potential Concerns re TC – Economic/Privacy

- Potential to strengthen monopolies, enforce supplier “lock-in”
- Limit interoperability and competition
- Danger that one vendor controls the client and server software, the protocols, and the trust infrastructure
- The TPM may “call home” with user data, unknown to the user

NZ Government's Position

- Primary concern is the **integrity of Government-held information and processes**
- Information available to date about TC & DRM indicates that:
 - ⊗ It is designed for commercial use within corporations & protection of intellectual property rights (music, movies etc)
 - ⊗ It has not really taken into account governments' requirements in managing information
- Two main issues:
 1. Ensuring Government's long-term access to its own information
 2. Possibility of information being communicated to external entities without explicit knowledge or permission

Potential Concerns (1)

- Access to data:-
 - ⊗ Access permitted only according to terms & conditions set by a third party (creator of the data or software company)
 - ⊗ Could potentially preclude NZG from access to its own data
- Privacy:-
 - ⊗ For 'attestation', a user's computer will report to a remote system
 - ⊗ Unique ID assigned to each computer – further potential for breaches of user privacy
- Long Term Management:-
 - ⊗ Long term management/access could be dependent on continued use of the technology
 - ⊗ If switch to another technology, historical records might not be able to be decrypted

Potential Concerns (2)

- Permanence of Records:-
 - ⊗ DRM enables creator to specify 'life' of each copy of a digital record, who may do what with it
 - ⊗ Government's access to its own records could be "turned off", intentionally or accidentally
- Legal Obligations of Agencies:— e.g. NZ agencies are subject to legislation including:
 - Official Information Act
 - Archives Act
 - Privacy Act
 - Evidence Act
 - National Library Act
 - Agency-specific acts (e.g. Income Tax Act)

Other Jurisdictions

- NZ Government has contacted other Governments:-
 - ⊗ Little evidence to date of other Governments giving consideration to TC
 - ⊗ Seen as important, but have not begun to address the issues
- Exception is Germany – Federal Office of IT (BSI) has issued "Comments on the TCG and NGSCB in the Field of Trusted Computing" (see URL in final slide)
- Active international liaison to find shared opportunities to develop collective government policies & positions on TC-related issues
- This should include co-operation with TC developers (TCG etc.)
 - it is NOT a "vendor beat-up"!

Actions to Date

- In Nov 2003 the E-Government Unit issued advice to NZ Government agencies not to enable Microsoft IRM. *This advice remains valid.*
- Communicated with other governments, research organisations & other experts (*cf* previous slide)
- Engaged a technical expert to evaluate the technologies & explore some of their implications (report is available on website – see URL in final slide)
- Engaged with Microsoft to (a) check understanding & (b) have the technical expert's work peer-reviewed
- Established Trusted Computing Working Group to develop government-wide principles for use of TC technologies in NZ under the e-Government Interoperability Framework (e-GIF).

Next Steps – Trusted Computing Working Group

- Investigate practicable means for agencies to filter out DRM from files & records received (or return to sender) – in short term
- Co-ordinate work on long-term implications of TC & DRM
- Develop principles for NZG use of TC
- International consultation & co-operation re TC & integrity of government information – continue to share work via channels such as OECD (& APEC?)
- Continue engagement with key ICT industry players – ensure that government requirements adequately considered

Summary

- TC will have a profound effect on whole ICT landscape
- Currently quite immature:-
 - ⚙ Focussed on intra-corporate use & IPR protection
 - ⚙ Doesn't seem to have taken Government needs into account
 - ⚙ Not 100% reliable
- Governments internationally don't seem to be active in evaluating impact of TC
- NZ Government is taking proactive steps and wishes to work with other governments
- Vital to work with – not against – vendors
- TC has great potential to improve security aspects of ICT – governments need to ensure that public sector information management requirements are accommodated

References

<http://e.govt.nz/trusted/index.asp>

<http://e.govt.nz/docs/irm-200202/index.html> (*review of MS IRM*)

http://www.bsi.bund.de/sichere_plattformen/trustcomp/stellung/StellungnahmeTCG1_2a_e.pdf (*German Government's "Comments on TCG & NGSCB"*)

andrew@bsa.co.nz

Ph. +64 21 466 181