Trusted Computing for Grid Security Research Group

Global Grid Forum, SEC Area

DRAFT Charter

Administrative Information

Name and Acronym:

Trusted Computing for Grid Security research group, TC-RG

Chairs:

Wenbo Mao, Hewlett-Packard Laboratories wenbo.mao@hp.com
Andrew Martin, University of Oxford andrew,martin@comlab.ox.ac.uk

Secretary/Webmaster:

The chairs will fill these roles.

Email list:

to be hosted by GGF. anticipated as tc-wg@ggf.org

Web page:

[hosted by HP or gridforge]
temporary web page: http://www.softeng.ox.ac.uk/Andrew.Martin/TC

Charter

Focus/Purpose

The Trusted Computing (TC) initiative developed by Trusted Computing Group (TCG) represents a major shift in the design of computing hardware, offering substantial benefits in host identity, secure storage, and software integrity measurement. Many of the descriptions of this technology envisage applications in distributed computing, but the work necessary to achieve them largely remains to be done. The purpose of this research group is to evaluate how the capabilities of TC can be used in a grid context.

Scope

In the short-term, enough TC hardware and drivers are already available to achieve valuable results in secure long-term cryptographic credential storage and management. Therefore, there is immediate scope for the definition of a TC-enabled GSI: in the currently available TPM commercial tools (eg, HP ProtectTools), a user's private key is in the tamper-resistant TPM and can never be extracted (not even by a system admin). Such a capability could hugely improve the security both of long-lived user secret keys and short-term job credentials. Secured storage could also be made available to applications.

More advanced hardware will soon be available, corresponding to version 1.2 of the TCG specification. Integrity measurement and attestation are in the TCG Spec 1.2, and the earliest commercial tool would probably be MS Longhorn in 2006, though HP and IBM are also working on Linux-OSs. Such capabilities could be put to an enormous range of uses in Grid middleware and applications – from ensuring that encryption is performed only for known applications, to permitting remote measuring of whether a nominated piece of software is really running; from code and data secrecy, to applications which are incapable of disclosing confidential data to unauthorised users.

As such, TC-RG will collect and document use cases from Grid applications which could either be enhanced through use of TC, or which have sufficiently stringent security requirements that they cannot presently be implemented but might be realised using TC.

The group will then re-charter to produce one or more roadmap documents for the introduction of TC in grid contexts. A working group may be formed to take forward those principles into detailed specifications.

Goals

Deliverable/Milestone 1: Profile for a TC-enabled GSI

First draft by GGF14; complete by GGF16

Deliverable/Milestone 2: Use case/requirements document

Outline by GGF14; draft by GGF15; complete by GGF16.

Deliverable/Milestone 3: Charter for creation of a research group to deliver roadmap document, and/or working group for detailed specifications.

Prepared in advance of GGF16; BOF at GGF16, with expectation of approval soon thereafter.

Management Issues

The group will meet at each GGF, and may meet face-to-face at other times. Most of its work will be carried out by email. A workshop may be held to elaborate themes in milestone 2.

Evidence of commitments to carry out RG tasks

Wenbo Mao and others at HP are already considering applications of TC technology. Andrew Martin has a project running at Oxford considering the design of TC-enabled middleware. Five other people at the BOF expressed willingness to contribute. They included: Mike Helm, Frank Siebenlist, and Hai Jin, and Dejan Milocijici.

Pre-existing Document(s) (if any)

- *Innovations for the Grid Security from the Trusted Computing,* Wenbo Mao
- [presentation at GGF12 by Dirk Kuhlmann (HP Laboratories Bristol, UK) http://grid.ncsa.uiuc.edu/ggf12-sec-wkshp/panel4/kuhlman.ppt]
- *Opportunities for using Trusted Computing Platforms with Grid Services,* Andrew Martin, October 2004

Any other relevant information

The Trusted Computing Group (TCG) is the standards body for TC. The research group will maintain contact with the relevant technical committee(s) of the TCG. https://www.trustedcomputinggroup.org/home

Seven Questions (From GFD-34)

1. Is the scope of the proposed group sufficiently focused?

The scope of the group covers an application of existing deployed technology, and the applicability of well-defined technology presently being implemented. Many authors have suggested Grids as a likely application area for trusted computing but details have been sketchy hitherto.

2. Are the topics that the group plans to address clear and relevant for the Grid research, development, industrial, implementation, and/or application user community?

Some use cases are quite evident already – as discussed in the pre-existing documents. Others will emerge through the work of the group.

3. Will the formation of the group foster (consensus based) work that would not be done otherwise?

The group should accelerate consensus-building, and enable a coherent direction to be taken by interested parties at a critical point in the roll-out of these technologies.

4. Do the group s activities overlap inappropriately with those of another GGF group or to a group active in another organization such as IETF or W3C?

No other GGF group is addressing these issues at present. The Trusted Computing Group has working groups on Infrastructure and Trusted Network Connect. Neither is particularly focussed on Grid issues, but contact will be maintained with them.

5. Are there sufficient interest and expertise in the groups topic, with at least several people willing to expend the effort that is likely to produce significant results over time?

The BOF would indicate yes.

6. Does a base of interested consumers (e.g., application developers, Grid system implementers, industry partners, end-users) appear to exist for the planned work?

The BOF attracted interest from a cross-section of the community, and the research group has potential to bring together technologists, vendors, and application scientists.

7. Does the GGF have a reasonable role to play in the determination of the technology?

The documents proposed will provide a substantial input to the Trusted Computing Group, and help to shape the development of the technology. In the fullness of time, there is almost certainly a role for GGF in defining higher layers of middleware which exploit Trusted Computing Platforms, but these will follow the re-charter of the group.