Global Grid Forum

Trusted Computing Research Group (TC-RG)

Notes of meeting held at GGF-14, Chicago

Wednesday 29th June 2005, 4.00pm – 5.30pm

These notes should be read in conjunction with the slides used at the meeting, which are archived on GridForge.

1. Housekeeping

Wenbo Mao opened the meeting and drew attention to the GGF IPR statement.

Andrew Martin and Wenbo Mao were to be note takers.

News regarding the setting up of the group was presented, together with a comment about the group having made contact with the relevant work group (Infrastructure) of the Trusted Computing Group (TCG). TCG is the standards body for trusted computing, and the infrastructure work group will be interested to receive the use case document which TC-RG is writing in GGF.

2. Progress

Wenbo Mao presented progress against implementation goals relevant to the TC-RG deliverable 1.

This relates to a secure client key repository, work being undertaken by HP Labs & ChinaGrid (Wuhan Univ, Huazhong Univ, China). The work uses a TPM as a client-side key repository. Crucially, it is using the TCG's Trusted Software Stack (TSS) implementation (TCG's counterpart to PKCS#11 & MS-CAPI). The project is on course to deliver an open-source augmentation to GSI (July 2006). Live research topics include:

- Backup server (what if a TPM breaks down?: which keys need to be exported/backed up? Clearly attestation keys must be non-exportable.)
- Usability (SSO with a MyProxy server?)
- Retaining proxy certificate (certificate with a short lifetime)?
- relationship to WS-I, OGSA?

Discussion suggested that the last of these is a medium-long term issue.

This work suggests a synergy with the CAOps group, where the use of smartcards for storing user keys is being discussed: a certificate request would go to the relevant CA tagged as having come from an hardware security module.

This work is part of a three-phase plan, the later phases involving distributed firewall implementation and multi-party/group-oriented security. A question arose as to whether these phases were sequential or overlapping; the answer is that they are progressive, but partly overlapping. Wider involvement in their implementation is welcome. At present they do not fall within the TC-RG charter scope, but could in future.

3. Use case document

Andrew Martin presented a possible outline for the use case document, deliverable 2. There is a danger of "creep"; trying to imagine trusted computing augmentation of every aspect of grid standards. It is important for the time being to explore use cases which offer immediate gains in

functionality, and to explore a manageable set, rather than trying to address everything possible. It is important that use cases be selected to inform a potential roadmap, rather than as simply possible but very long-term potentialities.

Thus it was suggested that a community group should grow out of the interests of the existing RG members – for example, by observing synergy with the activities of the firewall issues RG – and finding common ground.

The document should be positioned relative to the threats being addressed; it sholud ask what is being achieved/offered/improved; it should be about what can readily(ish) be achieved.

Of course, several GGF groups have collected use cases, and these are an obvious source of material for this document. The healthcare (life science) workshop at this GGF is an example.

The following headings may help to structure thoughts in this area, though considering multiple use cases for each is (too) ambitious:

1. securing the issue of credentials
2. helping users to secure their credentials
3. secure data storage
4. attested remote execution
5. infrastructure management

In addition, there is a pressing need for secure management of secret credentials for regular *servers*: servers must hold their secret keys online and unencrypted, in order to operate. This is a significant source of vulnerability.

Again, the present interests of the CAOps group in the area of credential storage were noted.

There was a digression here to consider what the TPM (and surrounding software) actually achieves, and the extent to which this is genuinely useful for the storage of user keys: clearly the surrounding infrastructure must support the use, so that the improved security is not illusionary.

On the subject of secured exection: it would be good to give some back-up to the statement about "tamper-proofing" of code. It will also be important for the document to account for a mixed-mode of operation, where some nodes have a TPM, and some do not.

In relation to infrastructure, the recently-published Trusted Network Connect specification of the Trusted Computing Group was noted as being very relevant.

The next steps are for Andrew Martin to create a framework for the document, and to invite other members of the group to contribute – based either on new material, or on their understanding of the existing GGF use case documents, as discussed.

4. Other business

The group will continue to explore synergies with other GGF groups, both as a source of use cases and more generally. In particular, we will help to arrange a joint security/life-sciences workshop at GGF-16 in Athens.