Proposed Trusted Computing Research Group TC-RG: BOF at GGF13

Notes of the meeting. 14th March 2005.

1. Wenbo Mao introduced the session and drew participants' attention to the GGF intellectual property statement. Andrew Martin volunteered to take notes. Cees de Laat was present in place of the Security Area directors, and would make a report.

   Slides for the following are available from the temporary web site http://www.softeng.ox.ac.uk/Andrew.Martin/TC.

2. Presentation: Wenbo Mao - overview of Trusted Computing;

   There were questions and discussion of tamper-proofing (and the relative cost of tampering), unique and multiple keys, trusted peripherals (keyboards)

   On the subject of secure key storage, there was discussion of whether the signing entity is able to access secure time, and discussion of the extent of the benefit gained by secure storage of private keys.

   Another question arose about whether curtained memory is strongly enforced down to BIOS (this was believed to be the case, but no one had certainty).

3. Presentation: Andrew Martin - use cases for TC platforms with web/grid services

4. Presentation: Prof. Hai Jin, "Security Requirements for ChinaGrid"

5. Mike Helm spoke briefly about running CA for DoE Grids. They have experience with using hardware security modules. This is add-on hardware which offers secure storage of a CA's signing key and is mandatory for on-line CA use. It is expensive, in contrast to the TPM, which is intended to add almost nothing to a platform's cost. He wondered whether CA operators could help issue identities for more secure systems, or help offer secured identities? TCPA [now TCG -ed.] could be very valuable for CAs in providing services such as trusted OCSP responders etc. and various kinds of assertion authorities. Having experience of a like technology, he would be interested in helping people to use these technologies. [Mike subsequently sent a longer note, which is archived with the presentations.]

6. Discussion of charter

It would be good to have a staged view of how to use TC. This is both an input (an outline in the charter) as well as an output (a roadmap document). Host identity and secure storage are already useful.

Milestone 2: re-phrase as a profile for a TC-enhanced GSI, offering greater security for long-term keys. This will not remove the need for proxy certificates as they play a role as authorisation certificates, but has the potential to simplify and improve the security of their use.

Five people (beside the chairs) were willing to work on the use cases/requirements document (milestone 3). These included Mike Helm, Frank Siebenlist, and Hai Jin, and Dejan Milocijici.

At most, milestone 4 should be a roadmap for future development (without suggestion of design, or *a priori* connection to OGSA). It may be best to defer planning of this for the future, perhaps following a re-charter.

The next steps, then, are for the chairs to refine the charter and discuss it on the mailing list and with the area chairs. Attention was drawn to the document GFD-34.