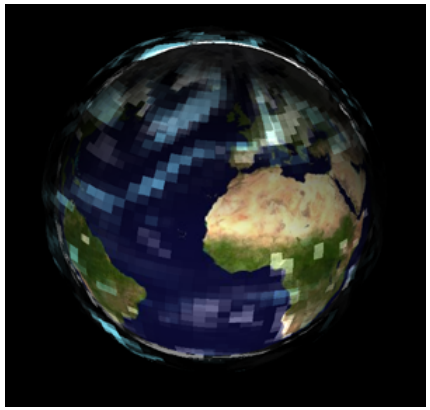
Opportunities for using Trusted Computing Platforms with Grid/Web Services

Andrew Martin
Oxford University Software Engineering Centre
Oxford e-Science Centre

Use Case: climate*prediction*.net clients



- distributed computing using BOINC (SETI@home)
- climate model distributed to 60 000 participants
- Monte Carlo simulation: each gets subtly different parameters or initial conditions
- builds probabalistic forecast for 2050, using IPCC scenarios etc.

Security of climate*prediction*.net clients

Principal project risk: integrity of results

- are the clients really running the selected model instance
- simulation is very different from search
- duplication not worthwhile?
- estimate number of tainted jobs (compare with halving accuracy of ensemble)

- guarantees impossible with standard architecture
- relatively simple attestation problem for TC
  - = able to ensure code and parameter integrity
  - = able to sign results etc.

Use case: Climate*prediction*.net servers

Generated data is held on donated resources around the globe.

- more recognisable 'grid'
- integrity of stored data is crucial (cannot afford to collect an archival copy)
- integrity of computations on that data is also crucial
- fully remote attestation in TC would be of value here

Related requirements

- data confidentiality on servers
- query confidentiality
- code secrecy

Use case: trusted distributed applications

- many TC detractors are concerned about DRM
- the same technologies can be used for 'socially desirable' purposes too
- enforce non-disclosre rules for electronic patient records
- able to do genuine end-to-end security (avoid requirement for separated networks)

Challenges

- configuration management: manageable integrity measurement
- tying that information to grid information services
- virtualisation as a means of achieving this
- in principle can extend the trusted platform to a distributed trusted platform: secure storage, identity/integrity measurement, etc.
- huge amount of detail to be worked out

Index