TC-RG Use Cases Document

Progress so far

Andrew Martin

GGF-15, Boston

Document Structure

1. Trusted Computing

   Three paragraphs, with a reference to a tutorial introduction.

2. Use Cases

3. Glossary

4. Housekeeping and BoilerPlate

   Security Considerations; Authors Contacts; Contributors; IPR Statement; Copyright

5. References

Use Cases

Is *Use Cases* the right phrase?

1. Server Credential Storage
2. Centralised user credential storage
3. Secure data isolation
4. Process isolation (sandboxing)
5. Trusted information services
6. Distributed firewall; application-aware firewall
7. Secured Audit/Logging Service

Server Credential Storage

Threat/Issue: server keys have to be online without passphrase etc.: very vulnerable

TC Contribution: place in protected storage; make non-migratable

Implementation Ease: natural modification to OpenSSL; similar libraries?

Centralised user credential storage

Threat/Issue: users are poor at managing their own secret keys; want access from several locations

TC Contribution: key repository; non-migratable; capable of issuing proxies

Implementation Ease: c.f. Wenbo

Secure data isolation

Threat/Issue: some users of Grid resources require strong guarantees about controlled access to their data (e.g. rivals using the same resource)

TC Contribution: allows storage to be sealed to particular applications

Implementation Ease: substantial challenge to work out the model; and to build it. 'Mixed economy' will mean that some Grid resources support this and others do not. How does the user tell between them?

Process isolation (sandboxing)

Threat/Issue: like secure data isolation, only more so

TC Contribution:

Implementation Ease:

Trusted information services

Threat/Issue: (vague) many TC activities rely on having accurate meta-data (hashes, version numbers, …). Can we build this on top of existing information services infrastructure?

TC Contribution:

Implementation Ease:

Distributed firewall; application-aware firewall

Threat/Issue: 'Perimeter' for some Grid activities is poorly defined. Best perimeter would be around the VO. Implies need to trust other sites to be protecting the VO — and an implementation strong enough to trust without other firewalls.

TC Contribution: Able to give guarantees of distant software configuration.

Implementation Ease:

c.f. FI-RG.

Secured Audit/Logging Service

Threat/Issue:

TC Contribution:

Implementation Ease:

Questions

- Heading in right direction?
- Mundane/Resonable/Imaginative/Speculative/Out there ?
- Is *Use Cases* the right phrase?
- Is the "Threat/Issue ; TC Contribution ; Implementation Ease" break-down a good one? Other headings?
- Contributions?