Trust Management of Dynamic Virtual Organisations in XtreemOS

Adam Barker, Benjamin Aziz, Alvaro Arenas, Ian Johnson, Brian Matthews, Erica Yang

e-Science Centre, STFC Rutherford Appleton Laboratory, Oxford OX11 0QX

1 Dynamic Virtual Organisations

The notion of *Virtual Oranisations (VOs)* is widely used in computational Grids to manage large numbers of users and computing nodes. A VO is defined as a set of users and real organisations that provide resources they want to exploit for a common goal. In Grid computing, physical machines, services, applications, and data sets can all be seen as resources. *Dynamic VOs* are created on-demand in response to requests from users. They tend to be short-lived and are characterised by the possibility of users and resources joining and leaving during their lifecycle. The underlying environment for the creation of dynamic VOs consists of a large number of resource providers, which have interests in pursuing common future goals and share compatible infrastructures and technologies. Such environments are usually termed *virtual breeding environments* [**?**], out of which VOs emerge. In such environments, resource access and usage across multiple administrative domains becomes challenging given the dynamic nature of VOs. Even the most basic authentication and identity management are no trivial tasks.

This paper describes the management of dynamic VOs, and the underlying trust model, when using the XtreemOS Grid-based operating system.

1.1 A Virtual Market Place of e-Learning Resources

In order to illustrate the requirements of a dynamic VO, consider the following use case scenario taken from the e-Learning domain [**?**]. The main actors are: *End Users*–learners who wish to acquire or complement their skills in a given domain of knowledge; *Portal Operator (PO)*–acts as an integrator, building bespoke training packages and co-ordinating their delivery to the end user. Finally, *Leaning Content Providers (LCPs)*–organisations providing training packages built from modular *Learning Resources (LRs)*.

In a typical use case, the end user accesses the portal and starts interacting with the PO in order to define their training requirements. Based on these requirements, the PO issues invitations to selected LCPs to offer bespoke courses that meet the requirements. The LCPs respond with training packages constructed from LRs. The PO dynamically creates a VO consisting of a set of LRs in order to deliver a learning service which meets the requirements of the user. The PO monitors the user's progress and advises the user on changes to the programme. At the end of the course, payments are distributed to the various service providers subject to user satisfaction and fulfillment of obligations.

This e-Learning scenario highlights a number of interesting challenges for trust and security in dynamic VOs:

- **Trust and security management:** The scenario highlights the classical need for hiding the management of the trust and security infrastructure underlying applications as much as possible from the end users. The learners could be students of any topic (e.g. arts and humanities etc.) who do not necessarily have the necessary technical expertise for managing trust and security in their applications. For example, in current Grid middleware technologies, such as Globus [1] or gLite [2], a user must explicitly acquire and manage at least two independent identities: a local OS identity and a Grid identity, which are used for authentication at the two different levels. These identities are usually issued by separate institutions and supported by different security technologies, such as Kerberos and Public Key Infrastructure (PKI). Manually configuring and managing multiple credentials can be a daunting task for the non-technical learners.

[1] http://www.globus.org/

[2] http://glite.web.cern.ch/glite/

- **Dynamic VO topologies:** The fact that the learning requirements of end users may change frequently over time implies that the topology of the VOs representing their training packages may also change frequently. Therefore, it is important that the management of the change in trust relationships resulting from this dynamicity of VO topologies be carried out as transparently as possible to the end users.
- **Trust modularity:** The commercial aspect of the e-Learning application scenario implies that LRs could belong to different LCPs that do not necessarily share a single root of trust or are affiliated to a single organisational domain. One could envision some notion of *trust modularity*, in which multiple roots of trust can come and go in any single learning module. Therefore, these multiple roots of trust must be able to coexist within the same dynamic VO and be useful to the end user.

2 The XtreemOS Trust Model

XtreemOS (www.xtreemos.eu) is an open source OS that supports Grid applications and runs on a range of platforms: PCs, clusters and mobile devices. The core aim of XtreemOS is to provide an abstract interface to remote as well as local resources, the way a traditional OS does for a single computer and to provide users with the capabilities associated with Grid middleware. Unlike traditional middleware approaches, XtreemOS provides seamless support for VOs [**?**], on all software layers involved, ranging from the OS of a node, via the VO-global services, up to direct application support. XtreemOS supports a trust model, as shown in Figure 1, between users and resources in a system through trusted online means to obtain end entity certificates (users' or resources') and root Certification Authorities (CAs) certificates.

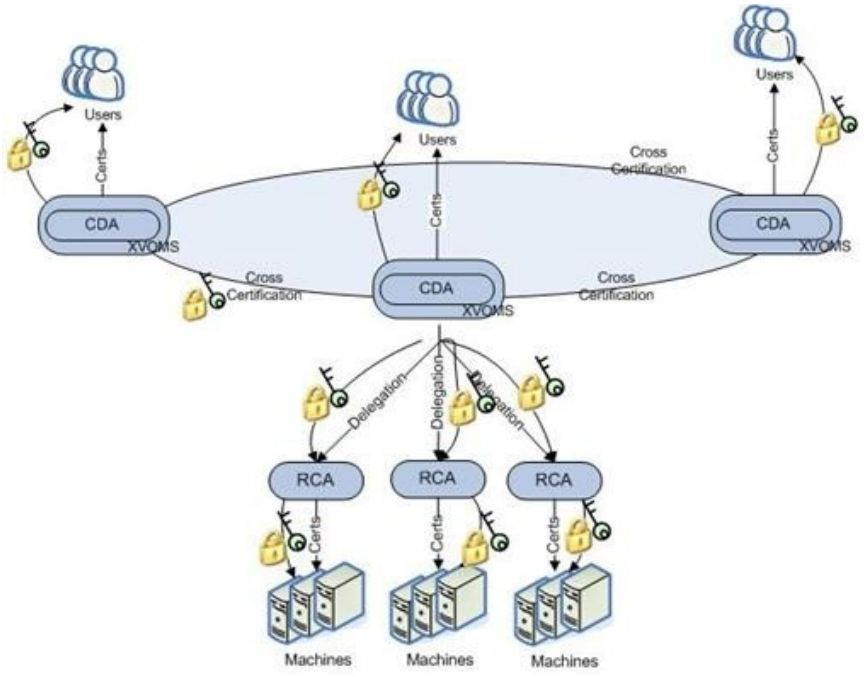

Figure 1: The XtreemOS Trust Model

At the heart of this model are the online Credential Distribution Authorities (CDAs), which distribute credentials to users in the form of identity and attribute certificates. These CDAs exist as part of a larger component known as the XtreemOS Virtual Organisation Management (XVOMS) component [**?**]. CDAs also delegate trust to subordinates called Resource Credential Authorities (RCAs), which could represent individual trust domains characterised as being stable so not evolving frequently over time. Finally, RCAs certify individual resources, which could be machines or nodes running multiple services. These resources are characterised as being dynamic; they may be removed, added or replaced in the VO at any point in time.

Based on the functionality of the XVOMS service, XtreemOS facilitates trust management in dynamic VOs in the following sense:

- **Trust and security management:** XtreemOS provides native support for VOs [**?**] and takes a flexible approach in order to support a wide range of applications: from long-lived collaborations with several users (as in large-scale scientific applications) to short-lived, dynamic ventures among a few participants to achieve one task (such as in commercial scenarios, e.g. the e-Learning use case discussed in Section 1.1). This native support means that XtreemOS also eases the task of managing trust and security for users and resource administrators. Users can register themselves with the XVOMS using their passwords and later use single-sign to access resources. They do not need to install certificates nor corresponding private keys. The same can be said about resource administrators setting-up their resources.

- **Dynamic VO topologies:** The concept of RCAs in the XtreemOS trust model allows for trust to be *localised* when it comes to registering and managing resources and their certificates. From the trust perspective, there is a clear transparency between the users and the highly dynamic entities in the VO, which are the LRs. Users have only to trust the more static RCAs in order for them to avail of the LRs.

- **Trust modularity:** The XtreemOS trust model is fundamentally a cross certified hierarchical Public Key Infrastructure (PKI) trust model [**?**], like the Globus Security Infrastructure (GSI)[3]. This means that LCPs do not necessarily have to have a single root of trust. Such cross-certified models are common in PKI systems. However, there is a key difference between the PKI trust model and that of XtreemOS in the manner in which trust is set up. In the former, trusted root CA certificates are distributed through *offline* means whilst in the latter, these certificates are disseminated through *online* protocols. XtreemOS provides a set of such protocols, which facilitate its online operation. This means that: a) users do not need to worry abut the errors associated with offline root CA certificate installation and configuration, and b) there is no need for users nor resource administrators to generate certificate signing requests. This approach promotes the notion of the *modularity of trust*.

3 Deploying the e-Learning Market Place into XtreemOS

This section demonstrates how XtreemOS provides seamless support from the operating system level to the application level for dynamic VOs in large-scale Grids by describing how the e-Learning market place can be deployed into XtreemOS. In particular, we extract a set of requirements for dynamic VOs not currently supported by Grid middleware.

References

[1] L. M. Camarinha-Matos and H. Afsarmanesh. Elements of a Base VE Infrastructure. *Comput. Ind.*, 51(2):139–163, 2003.

[2] M. Coppola, Y. Jegou, B. Matthews, C. Morin, L. P. Prieto, O. D. Sanchez, E. Y. Yang, and H. Yu. Virtual Organization Support within a Grid-Wide Operating System. *IEEE Internet Computing*, 12(2):20–28, 2008.

[3] S. Le Goff and S. Ristol. MetaCampus Marketplace and the Challenge for Next Generation eLearning Platforms. In *eChallenges Conference*, 2004.

[4] A. Qin, H. Yu, C. Shu, and X. Yu. Operating System-level Virtual Organization Support in XtreemOS. In *9th International Conference on Parallel and Distributed Computing, Applications and Technologies, PDCAT'08*, 2008.

[5] J. Turnbull. Cross-Certification and PKI Policy Networking. Technical report, Entrust Technical Report, 2000.

[6] E.Y. Yang, I. Johnson, B. Matthews, and A.E. Arenas. VOHost: A Secure and Flexible VO Hosting System for Grids and Beyond. Poster at the UK e-Science 2008 All Hands Meeting, 2008.

[3] http://www.globus.org/toolkit/docs/latest-stable/security/GT4-GSI-Overview.pdf