Security and Dynamics in Customer Controlled Virtual Workspace Organisation

Yuri Demchenko
University of Amsterdam
demch@science.uva.nl

Frank Siebenlist
Argonne National Laboratory
franks@mcs.anl.gov

David Groep
NIKHEF
davidg@nikhef.nl

Leon Gommans
University of Amsterdam
lgommans@science.uva.nl

Cees de Laat
University of Amsterdam
delaat@science.uva.nl

Oscar Koeroo
NIKHEF
okoeroo@nikhef.nl

ABSTRACT

This paper proposes the security infrastructure for user-controlled Virtual Workspace Service (VWSS-UC) that comprises of three layers: trusted computing platform, secure virtualised workspace, and user aplication. The suggestions on the technology selection are provided for the first two layers: industry adopted Trusted Computing (TCG) platform, and Virtual Workspace Service (VWSS) developed in the framework of the Globus Toolkit. Solutions and implementation are proposed and discussed for the application authorisation session security context management. The paper is based on experiences gained from major Grid based projects such as EGEE, Globus Toolkit, and Phosphorus.

Categories and Subject Descriptors

C.2.4 [**Computer Systems Organization**]: Computer Communication Networks – *distributed systems, distributed applications.*

General Terms

Design, Security, Standardization

Keywords

Virtualisation, Virtual Workspace Service, Complex Resource Provisioning, User-controlled security model, Authorisation Session, Trusted Computing Platform.

1. INTRODUCTION

Business acceptance of virtualised Grid-based services will depend on how successfully the Grid middleware will solve creation of fully user-trusted distributed/remote execution environment for user tasks.

One of recently proposed solutions that attempts to combine services virtualisation, dynamic resource creation and security is the Virtual Workspace Service (VWSS) being developed in the framework of the Globus Toolkit version 4 (GT4) [1]. The current VWSS security model has been developed from the point of view of Grid services providers and considers the computing platform as trusted. However, for more complex and security concerned use cases the VWSS should be completed with means to ensure user-centric and user-controlled secure environment.

The goal of this paper is to further advance the development of the security model and infrastructure for building user-controlled secure virtual workspace environments (VWSS-UC) that enable user trusted services and/or execution environments. The paper proposes a high-level model that combines the GT4 VWSS with the industry adopted Trusted Computing platform [2] to provide higher trustworthiness of the remote computing platform, and adds the session based user security context management using Authorisation (AuthZ) session management tools being developed in the framework of the GAAA Authorisation Framework (GAAA-AuthZ) [3]. Background information on the proposed solutions can found in the recently published paper [4].

2. VWSS-UC SECURITY MODEL

Figure 1 depicts the proposed 3-layer VWSS-UC environment for running user tasks and applications that provides integral protection of user tasks/applications at all three layers. It is capable of scaling over multiple administrative and trust domain and allows for running multistage user tasks or complex resource provisioning. The three layers include: a TCG based computing/hosting facility, a Grid based Virtual Workspace Service, and a User Application Environment.

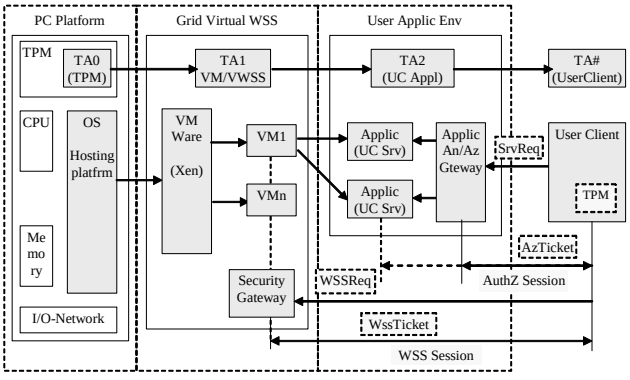

Figure 1. Three-layer Security Model of the VWSS-UC.

We assume that at the time of requesting access to the service or application, the resource reservation and allocation have been done and the user can reference it with the reservation ID.

Reservation ID actually means a kind of contract based on which a service can be deployed on the remote platform in the VWSS container/environment.

A virtual workspace is created after a user request is sent to the VWSS security gateway, which checks user credentials and deploys the VM based workspace with characteristics that meet the request's requirements. Such a virtual workspace creates a trusted environment where users can run their tasks or applications. User applications and/or tasks are protected by basic security services to avoid potential data compromise or interruptions. This is first of all achieved by user Authentication (AuhtN) and Authorisation (AuthZ) provided by the Application AuthN/AuthZ Gateway. In the case of complex/multi-component services, their combinations should be secured through the applications level security context management.

For the dynamic security context management, we distinguish between a WSS session and an application/service AuthZ session that is related to the user task or application. WSS session may have wider security context but still both of the session types are based on the positive authorisation decision and will require a similar AuthZ context management. WSS sessions that includes VWSS request may also need to incorporate a negotiation stage and possibly want to verify the platform security configuration and/or integrity, which could be achieved through the TCG Trusted Platform Module (TPM) based mechanisms.

In the proposed architecture/model, the TPM with its hardware-based secure ID allows for "bootstrapping" a chain of trust to the TMP and hardware platform. This creates a continuous chain of trust from the user to the workspace environment and hosting platform: TA#-TA2-TA1-TA0., where TAn – are trust anchors as shown on the picture.

Note that the VWSS trustworthiness may also be increased by using a trusted VM-repository, which stores pre-configured VM-images that are cryptographically bound to a user or to a trusted third party.

3. AUTHZ SESSION MANAGEMENT

To provide described above functionality of the dynamic VWSS and application authorisation sessions security context handling, special features should be added to existing Grid oriented AuthZ frameworks such as Globus Toolkit 4.0 AuthZ Framework (GT4-AuthZ) [5] or gLite Java Authorisation Framework (gJAF) [6].

Important component of the AuthZ session management is the AuthZ Ticket (AuthzTicket) that is supported by the special module TriagePDP that provides an initial evaluation of the service or application Request against assertions contained in the AuthzTicket and configured as the first Policy Decision Point (PDP) in the "permit-override" AuthZ chain [7].

An AuthzTicket is generated as the result of a positive PDP decision. It contains at least the PDP decision and all necessary information to identify the requested service. Extended AuthzTicket content may include additional information about the policy decision, such as Obligations and Delegation, and other information to preserve all AuthZ session context data. When presented to the TriagePDP, its validity can be verified and in the case of a positive result, access will be granted without requesting a new policy decision that can be slow.

Current AuthZ Ticket format and its implementation [7] support extended functionality for distributed multidomain complex resource provisioning. The semantics of AuthZ Ticket elements is defined in such a way that allows easy mapping to related elements in other XML-based and AuthZ/AuthN related formats, like the Security Assertion Markup Language (SAML) and the eXtensible Access Control Markup Language (XACML).

If considered for extended user session management and binding with the VWSS and TCG layers the additional functionality should be added to support TPM-based platform trust anchors, VWSS public keys or other security credentials, mutual user client and VWSS authorisation, and additionally accounting data.

4. FUTURE DEVELOPMENTS

More research and modeling are required to identify additional functionality to address wider security context management in the VWSS and application sessions. We plan to investigate in details what existing service provisioning frameworks and protocols could provide the required functionality and how they can be used in VWSS-UC (at different stages of the VWSS-UC operation).

Suggested further development will include more detailed investigation how the TCG and TPM can be practically integrated into the proposed VWSS-UC architecture and with the current Grid middleware. This work will also rely on the recent developments in the Daonity and OpenTC projects that provide practical examples of using TCG for improving security of user credentials and security context management in Grid applications, including fine-grained client-side VM policies management.

5. REFERENCES

[1] Virtual Workspaces. [Online]. Available: http://workspace.globus.org/index.html

[2] Trusted Computing Group (TCG). [Online]. Available: https://www.trustedcomputinggroup.org/home

[3] Generic Authorization Authentication and Accounting. [Online]. Available: http://www.science.uva.nl/research/air/projects/aaa/

[4] Demchenko Y., L. Gommans, C. de Laat. Extending User-Controlled Security Domain with TPM/TCG in Grid-based Virtual Collaborative Environment. Accepted paper. *The 2007 International Symposium on Collaborative Technologies and Systems (CTS 2007)* (Orlando, FL, USA, May 21-25, 2007).

[5] GT 4.0: Security: Authorization Framework. [Online]. Available: http://www.globus.org/toolkit/docs/4.0/security/authzframe/

[6] Developer's guide for the gLite Java Authorisation Framework - https://edms.cern.ch/document/501718

[7] Demchenko Y., L. Gommans, C. de Laat. Using SAML and XACML for Complex Resource Provisioning in Grid based Applications. Accepted paper. *IEEE Workshop on Policies for Distributed Systems and Networks (POLICY 2007)* (Bologna, Italy, 13-15 June 2007).