Использование Технологии Доверительной Компьютерной Платформы для Повышения Безопасности Виртуальной Рабочей Среды Грид

Демченко Ю., University of Amsterdam
demch@science.uva.nl

Аннотация
В докладе рассматриваются проблемы обеспечения безопасности виртуальной рабочей среды Грид и предлагается 3-х уровневая модель безопасности для систем предоставления сложных сервисов и ресурсов (CRP - Complex Resource Provisioning) на основе Грид, которая включает доверительную компьютерную платформу, безопасную виртуальную рабочую среду, и пользовательские приложения. В работе приведены соображения по выбору технологий для всех уровней и более подробно рассмотрены возможности Доверительной Компьютерной Платформы (Trusted Computing Platform) для обеспечения доверительности всей виртуализованной рабочей среды.

1. Введение

Возможность широкого использования Грид для коммерческих приложений и предоставления специальных сервисов и ресурсов суперкомпьютерных центров и специального оборудования будет зависеть от того, насколько успешно программное обеспечение и инфраструктура общих сервисов Грид систем (обычно называемые общим термином Gird middleware) сможет обеспечить доверительную распределенную рабочую среду для выполнения пользовательских задач.

Под доверительной рабочей средой понимается такой способ обеспечения безопасности выполнения задач и приложений, при котором доступ к исполняемым задачам и данным может производится только для процессов или пользователей, входящих в ассоциацию безопасности, в которую входит пользователь, от имени которого запущена задача или приложение. Широко используемым механизмом обеспечения доверительности исполняемой среды является виртуализация, которая как минимум обеспечивает изоляцию множества исполняемых задач и процессов между собой и от операционной среды.

Одним из недавно предложенных решений, которое позволяет комбинировать виртуализацию сервисов, динамическое создание ресурсов или сервисов и безопасность, является платформа для создания виртуальной рабочей среды Virtual Workspace Service (VWSS), которая является частью популярной платформы для создания общих сервисов Грид Globus Toolkit version 4 (GT4) [1]. Очевидно, что VWSS разрабатывалась с точки зрения Грид сервис-провайдеров и предполагает, что компьютерная платформа, находящаяся под контролем провайдера, является безопасной для выполнения пользовательских задач. Однако существует множество ситуаций, когда пользователи не могут полностью доверять провайдеру Грид-сервисов или рабочей среды Грид, посколько фактически администратор вычислительной системы может иметь доступ ко всем пользовательским данным, временным и хранимым на диске, а также контролировать все процессы в системе.

Целью данной работы является дальнейшее повышение безопасности виртуальной рабочей среды Грид и разработка модели безопасности доверительной рабочей среды VWSS-UC (User-Controlled VWSS) [2, 3]. Предлагаемое решение использует Доверительную Компьютерную Платформу (Trusted Computing Platform), обычно называемую по имени рабочей группы, которая ее разработала TCG (Trusted Computing Group) [4, 5], и дополнительно средства обеспечения безопасности доступа пользователей к исполняемым приложениям и данным.

Дополнительной целью данной работы является предоставление краткого обзора новой технологии и попытка разьяснения базовых понятий TCG С этой целью в докладе предлагается определение базовых понятий и терминов TCG, которые сопровождаются также их английским эквивалентом. Дополнительная информация по теме предлагаемого доклада может быть найдена в работах автора [6, 7].

В качестве главных целевых приложениq для систем предоставления сложных сервисов и ресурсов (CRP - Complex Resource Provisioning) на основе Грид рассматривались три случая, которые требуют создание динамических пользовательских приложений: доступ к суперкомпьютерным ресурсам (Computer Grids), виртуальная среда для коллективной работы GCE (Grid-based Collaborative Environment), и предоставление сложных сетевых ресурсов по требованию BoD (Bandwidth on-Demand) или OLPP (Optical LightPath Provisioning).

2. Модель Безопасности Доверительной Виртуальной Рабочей Среды

Рисунок 1 иллюстрирует предлагаемую 3-х уровневую модель безопасности доверительной виртуальной рабочей среды VWSS-UC для выполнения пользовательских задач и приложений, которая обеспечивает комплексную защиту исполняемой среды и процессов на трех уровнях, которые включают доверительную компьютерную платформу (PC Platform) на основе TCG, виртуальную рабочую среду Грид (Grid Virtual VWSS), и пользовательские приложения (User Application Environment).

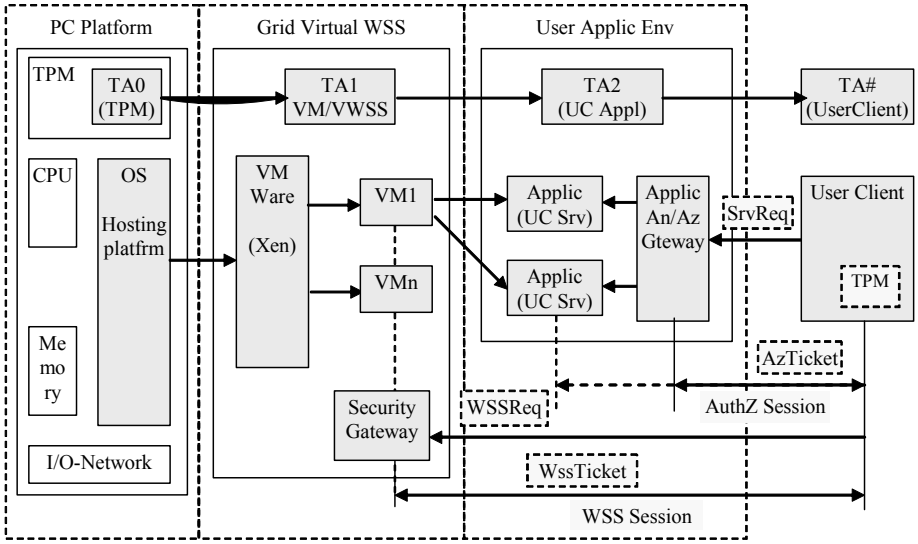

Рис. 1. Трех-уровневая модель безопасности VWSS-UC.

Мы предполагаем, что к моменту запроса на доступ к ресурсам и приложениям Грид эти ресурсы были резервированы и развернуты и пользователь, или пользовательское клиентское програмное обеспечение, могут ссылаться на запрашиваемый ресурс по идентификационному номеру резервирования ResID. В данном случае ResID служит своего рода ссылкой на контракт по предоставлению услуг, который обычно также содержит мандаты безопасности пользователя и провайдера в форме цифровых подписей и Сертификатов Открытых Ключей (СОК), которые могут быть использованы для создания и контроля “цепи” доверия.

Виртуальная рабочая среда создается после того, как пользователь посылает запрос к службе безопасности VWSS, которая проверяет пользовательские мандаты безопасности и категорию или права пользователя. Это выполняется службами аутентификации и авторизации соответственно, которые также производят контроль доступа к пользовательским приложениям и данным. VWSS позволяет создавать рабочую среду с параметрами, которые нужны для целевых пользовательских приложений.

Для обеспечения эффективного управления контекстом безопасности, мы выделяем два типа сеансов (или сессий) доступа: VWSS сеанс и сеанс приложения. Оба типа сеансов являются результатом положительного решения о доступе (или авторизации), однако сеанс VWSS может потребовать обработку более сложного контекста безопасности посколько может включать этап согласования требований к платформе или необходимым ресурсам, которые должны быть выделены на запрос пользователя.

В предлагаемой архитектуре доверительность компьютероной платформы обеспечивается при помощи специального Доверительного Платформенного Модуля (TPM - Trusted Platform Module), который является центральным компонентом TCG. TPM содержит аппаратно доступный секретный ключ, который служит одновременно уникальным идентификатором платформы и доверительным “якорем” (trust anchor), который позволяет “пристегнуть” (“bootstrap”) цепь доверия к апаратному доверительному якорю и создать непрерывную цепь доверия от доверительной платформы до пользовательского приложения или пользовательского сеанса: **TA#-TA2-TA1-TA0**., где **TAn** – соответсвует якорям, изображенным на рисунке.

Нужно отметить, что доверительность VWSS может также быть улучшена посредством использования предварительно сконфигурированных и свернутых образов виртуальных рабочих сред, которые хранятся в защищенных хранилищах и устанавливаются на платформе провайдера по запросу пользователя.

2. Доверительная Компьютерная Платформа

Доверительная Компьютерная Платформа TCG предоставляет основу для построения доверительной контролируемой рабочей среды для выполнения приложений и обработки данных [4]. Однако в самом начале предлагаемая модель безопасности TCG была немного противоречивой и поначалу направлена в основном на защиту прав провайдеров контента (IPR – Intellectual Property Rights), как-то электронной музыки или видео [8]. TCG должна была обеспечить соблюдение лицензий на использование или проигрывание музыкальных или видео программ и предотвращение пиратства. Однако в теперешнем ее состоянии развития, TCG может быть использована для обеспечения доверительной среды как для провайдеров приложений (где необходимо обеспечить доверительную рабочую среду), так и для провайдеров контента (где необходимо обеспечить соблюдение IPR). В обоих случаях мы имеем дело с расширением доверительности рабочей среды или среды потребления, что фактически может быть интегрировано в архитектуру VWSS-UC, описанную в предыдущей главе.

Архитектура TCG [9] включает 5 абстрактных уровней: платформа, система (включая операционную систему), сервис или приложение, и пользовательские мандаты. Основой для архитектуры TCG является Доверительный Платформенный Модуль (TPM - Trusted Platform Module) [10] – микросхема или аппаратный модуль, встроенный в компьютерную систему или пластиковую карточку (smartcard), который обеспечивает ряд аппаратных криптографических функций, обеспечивающих интегральность всех уровней модели TCG:

- Функция аппаратной генерации несимметричной пары ключей, которая использует аппаратный генератор случайных чисел, аппаратная генерация цифровой подписи, шифрование посредством открытого или секретного ключа.
- Подтверждающий ключ (Endorsement Key (EK)), который может использоваться владельцем платформы, чтобы доказать, что уникальный идентификатор платформы был создан посредством TPM и на основе аппаратного секретного ключа, который однако в открытую не предоставляется.
- Протокол и процедура Прямой Автономной Аттестации (Direct Autonomous Attestation (DAA)), которая позволяет безопасным образом передавать информацию о статической или динамической конфигурации платформы, которая может быть запомнена в TPM в хэшированной форме.
- Защита коммуникаций между двумья TPM.
- Монолитный счетчик и таймер, которые могут использоваться для контроля последовательности и временных параметров коммуникаций.

Таким образом TPM обеспечивает привязанную к платформе “вершину доверия” (“root of trust”), которая может быть использована для безопасной регистрации платформы в сеансе разворачивания сервисов по требованию или в процессе доверительного представления/инициации (“trusted introduction”).

Другие компоненты архитектуры TCG включают: разделенную память (“curtained memory”) центрального процессорного элемента (CPU); ядро безопасности в операционной системе; ядро безопасности во всех приложенях, которые хотят использовать TCG и TPM; а также поддерживающая инфраструктура онлайновых сервисов, которые обслуживаются производителями аппаратного и програмного обеспечения [11].

TCG также определяет отдельные стандарты для доверительной сетевой инфраструктуры (Trusted Network Connect (TNC)) [12], и архитектуру поддерживающего ПО (TPM Software Stack (TSS)). TSS определяет ряд программных интерфейсов (API) для поддержки удаленного доступа, управления идентификацией, обеспечение безопасности электронной почты, а также шифрование директорий и файлов.

Жизненный цикл доверительной платформы включает 6 этапов, которые поддерживаются тремья типами инфраструктуры: инфраструкутура предустановки/разворачивания (predeployment/provisioning) – поддерживает этапы производства, производственного контроля и доставки; инфраструкутура установки (deployment) - поддерживает этапы установки, регистрации и фактической эксплуатации; инфраструкутура вывода из эксплуатации или отставки (redeployment/retirement) - поддерживает этапы утилизации и отставки доверительных модулей и используемых криптографических идентификаторов .

TCG также определяет 3 типа мандатов безопасности [13]: описанный выше EK, платформенный ключ (platform key/credentials (PK)), и ключ аттестации идентификации (Attestation Identity Key (AIK)). EK и AIK имеют

формат сертификатов открытых ключей по стандарту X.509 (Identity Public Key Certificate). PK является сертификатом атрибутов по стандарту X.509 (Attribute Certificate).

4. Дальнейшее Исследования

Предложенная работа описывает общую концепцию использования TPM/TCG для обеспечения безопасности виртуализованных приложений, однако ее практическое внедрение потребует дальнейших исследований в направлении комплексного управления контекстом безопасности пользовательских задач и приложений.

Дальнейшие исследования будут также использовать последние достижения и результаты двух крупных проектов Daonity [14] и OpenTC [15], которые разрабатывают программные средства для интеграции TPM/TCG в Грид и другие приложения. Поддержка TPM введена также в последние версии популярной виртуальной среды Xen 3.0 [16].

Литература

[1] The Globus Toolkit. [Online]. Available: http://www.globus.org/toolkit/

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

[3] Keahey, K., I. Foster, T. Freeman, and X. Zhang. “Virtual Workspaces: Achieving Quality of Service and Quality of Life in the Grid”, Scientific Programming Journal, vol 13, No. 4, 2005, Special Issue: Dynamic Grids and Worldwide Computing, pp. 265-276

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

[5] Чеканов Д., Концепция Trusted Platform Module (TPM): первый практический взгляд. - http://www.thg.ru/howto/200510082/

[6] 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).

[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).

[8] Trusted Computing' Frequently Asked Questions, by Ross Anderson. [Online]. Available http://www.cl.cam.ac.uk/ ~rja14/tcpa-faq.html

[9] TCG Infrastructure Working Group Reference Architecture for Interoperability (Part I). Specification Version 1.0, Revision 1. 16 June 2005. [Online]. Available: I - https://www.trustedcomputinggroup.org/specs/IWG/IWG_Architecture_v1_0_r1.pdf

[10] Trusted Platform Modules Strengthen User and Platform Authenticity. TCG Whitepaper, January 2005. [Online]. Available: https://www.trustedcomputinggroup.org/specs/ TPM/Whitepaper_TPMs_Strengthen_User_and_Platform_Authenticity_Final_1_0.pdf

[11] TCG Design, Implementation, and Usage Principles Version 2.0, December 2005. [Online]. Available: https://www.trustedcomputinggroup.org/specs/ bestpractices/Best_Practices_Principles_Document_V2_0.pdf

[12] TNC Architecture for Interoperability. Specification Version 1.1, 1 May 2006. [Online]. Available: https://www.trustedcomputinggroup.org/specs/TNC/TNC_Architecture_v1_1_r2.pdf

[13] TCG Credentials Profile. Specification Version 1.0, 18. Revision 0.981. January 2006. https://www.trustedcomputinggroup.org/specs/IWG/Credential_Profiles_V1_R0.981-2.pdf

[14] Daonity Project. [Online]. Available: http://www.hpl.hp.com/personal/Wenbo_Mao/daonity/daonity.html

[15] Open Trusted Computing (OpenTC) Project. [Online]. Available: http://www.opentc.net/

[16] Users' Manual Xen v3.0. [Online]. Available: http://www.cl.cam.ac.uk/Research/SRG/netos/xen/readmes/user/