Информационная безопасность грид-систем

А. О. Мелащенко, О. Л. Перевозчикова

Институт кибернетики НАН Украины, проспект академика Глушкова 40, Киев, Украина

dep145@gmail.com

Аннотация. *Рассмотрены подходы к построению информационной безопасности грид-среды на основе национальных стандартов, гармонизированных с международными. Эти стандарты именуются общими критериями (CC). Задействование профилей защиты и методов оценивания, основанных на общих критериях, позволит достичь международного уровня информационной безопасности грид-среды, а также выполнить требования национального законодательства по защите информации.*

Ключевые слова

информационная безопасность, общие критерии оценки ИТ-безопасности, грид-системы, стандартизация, смарт-карточки

1 Введение

Сегодня от разработчика требуется умение отлаживать распределенный программный продукт (РПП), зачастую некорректно работающий ввиду ненадежной среды. Кроме того, использование качественно разработанного программного продукта на поврежденных данных обычно нивелирует результаты длительных расчетов, особенно в грид-средах. Эти проблемы связаны с отсутствием двух свойств информационной безопасности (ИБ): целостности и доступности данных. Ввиду специфики обрабатываемых данных третье свойство конфиденциальности не столь актуально в академическом гриде, особенно учитывая соотношение цена/потребность. Также следует учесть другие свойства ИБ: аутентификацию, аудит, неопровержимость, достоверность [1] для надежного функционирования грид-среды.

Цель доклада обосновать подход к спецификации требований к инфраструктуре ИБ грид-среды с акцентом на целостности и доступности обрабатываемых данных.

2 Идентификация цели/объекта оценивания

В типовой архитектуре грид-среды, (рис. 1) свойство аутентификации достигнуто с использованием ПП NorduGrid [2] и задействует сертификат открытого ключа X.509 [3] инфраструктуры открытых ключей [4]. После аутентификации ПП NorduGrid от имени пользователя NorduGrid запускает на идентифицированном кластере РПП. Исполнение РПП на конкретном кластере отображено на рис. 2. Обычно РПП задействует MPI [5] для организации обмена сообщениями в распределённой среде, а конкретный экземпляр РПП исполняется в ОС конкретного узла.

Рис. 1. Типовое взаимодействие в грид-среде

Первые три уровня РПП, NorduGrid и MPI как инновационные составляющие имеют высокую динамику изменений, поэтому для них нецелесообразно жестко фиксировать требования ИБ. С другой стороны, операционные и сетевые среды имеют традиционные функции и составляют основу ИБ, для них целесообразно жестко регламентировать требования, поскольку от них зависит функционирование грид-среды в целом. Один конкретный РПП может завершиться крахом, но не должен повлиять на работу грид-среды. Необходимо регламентировать требования к вычислительному узлу и каналам коммуникации.

Типовые требования ИБ поддержаны восьмью принципами [6].

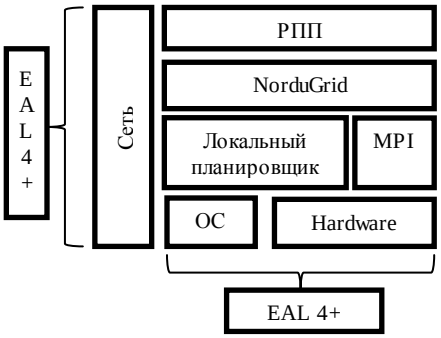

Рис. 2 Типовое взаимодействие в грид-среде

1) Непрерывное совершенствование – непрерывная оценка качества достижения целей и изменений для улучшения результатов.

2) Наименьшее количество привилегий – предоставление людям или другим объектам минимального количества полномочий, необходимых для выполнения им своей роли в системе.

3) Глубокая защита – создание системы из независимых уровней безопасности, чтобы нападающий в успешной атаке преодолел сопротивление множества независимых мер безопасности.

4) Открытая архитектура – создание механизмов защиты, архитектура которых не должна быть секретной.

5) Цепочка контроля – гарантирует исполнение надежного программного обеспечение или его поведение ограничено навязанной политикой безопасности, обойти которую невозможно.

6) Запрет по умолчанию – обеспечение полномочий, определенных правилами задействованной политики безопасности, остальные полномочия запрещены.

7) Транзитивность доверия – если А доверяет В, а В доверяет С, то А доверяет С.

8) Разделение обязанностей – декомпозиция критической задачи на отдельные элементы, выполняемые разными людьми или ИТ-сущностями.

С одной стороны, эти принципы (особенно 1, 3, 8) предполагают формальное изложение требований, не привязанных к технологии. С другой стороны, согласно Закону Украины № 80/94 [7] национальная грид-среда должна иметь сертификат комплексной системы защиты информации (КСЗИ). Формализация требований к вычислительным узлам грид-среды позволит их типизировать и сертифицировать согласно Закону Украины [8], в том числе получить сертификат КСЗИ.

Формально изложить типовые требования ИБ к вычислительным узлам и каналам коммуникации как целям оценивания грид-среды можно согласно серии стандартов ISO/IEC 15408 (Общие критерии, CC).

3 Роль общих критериев ИБ

CC позволяют сгруппировать функциональные требования безопасности, описанные на формальном языке, в профили защиты (PP), соответствие которым оценивается. Стандарт гибок в предмете оценивания и поэтому не привязан к разновидностям ИТ-продуктов. В контексте оценивания в стандарте использован термин "TOE" (цель/объект оценивания).

Философия ISO/IEC 15408 обеспечивает гарантию, основанную на оценивании (активном исследовании) IT-продукта, которому по определению нужно доверять. Оценивание – традиционное средство обеспечения гарантий и основание для предыдущих документов критериев оценивания. В выравнивании существующих подходов ISO/IEC 15408 принимает ту же философию. В ISO/IEC 15408 предложено измерять законность документации и полученного ИТ-продукта опытным (авторитетным) и независимым оценщикам с растущим акцентом на сфере применения TOE, глубине и строгости ее методов.

ISO/IEC 15408 не исключает и при этом не комментирует относительные достоинства других средств извлечения гарантий. Продолжается исследование альтернативных способов получения гарантий. Поскольку зрелые альтернативные подходы появляются из этих исследовательских действий, их рассмотрят для включения в ISO/IEC 15408, который настолько структурирован, чтобы допустить их будущий ввод.

Применение CC в грид-среде рассмотрим в двух аспектах:

– технологический – обеспечение ИБ через аудит качества программного продукта;
– организационный – построение КСЗИ с встроенным механизмом самосовершенствования.

3.1 Технологический аспект CC

Большинство подходов к ИБ подразумевают использование надежных ИТ-продуктов, но вопрос оценки «надежности» программных или программно-технический комплексов (ПТК) оставляют экспертам ИБ.

Показательный пример – Национальная система электронных цифровых подписей, в которой аккредитованный центр сертификации ключей должен построить КСЗИ. Первый этап построения КСЗИ – получение «позитивного экспертного заключения», оценивающего реализацию набора документов в ПТК. Большинство заключений имеют формулировки «алгоритм реализован правильно», сама формулировка не корректна, поскольку зачастую эксперты не столько оценивают качество программного продукта, от которого зависит надежность КСЗИ, сколько беседуют с обслуживающим персоналом.

Для процедуры оценивания CC необходимы методы оценивания соответствия цели/объекта установленным требованиям (PP) в зависимости от потенциала атаки. Введено 7 уровней оценивания: от функционально проте-

стированного EAL1 до формально верифицированного и протестированного проекта EAL7. Уровень EAL4 обеспечивает наилучшее соотношение цена/качество; большинство европейских и американских организаций, включая правительственные, требуют от всех ПТК наличия сертификата соответствия EAL4 на основе зарегистрированного профиля. На уровне EAL4 гарантировано высокое качество продукта и его способность гарантированно обеспечивать ИБ.

При задействовании в грид-среде продуктов, сертифицированных на соответствии профилю защиты OSPP (Operating System Protection Profile, соответствует EAL4+ [9]), можно гарантировать, что данные РПП не сможет модифицировать и/или использовать неавторизированная ИТ-сущность. Пример ПТК, соответствующего OSPP, – операционная среда Red Hat Enterprise Linux Ver. 5.3 для семейства серверов Dell 11G.

3.2 Организационный аспект СС

Текущая процедура построения КСЗИ подразумевает «замораживание» номенклатуры аппаратного и программного обеспечения, что противоречит 1-у принципу ИБ. Чтобы «сохранить» сертификат КСЗИ при модернизации аппаратной и/или программной составляющей, целесообразно регламентировать требования к ПТК в терминах СС. Так, ПТК вычислительного узла должен соответствовать профилю защиты OSPP или CAPP (Controlled Access Protection Profile). Поэтому любой вычислительный узел сможет использовать на выбор:

– Microsoft Windows Server 2008 R2;
– Oracle Enterprise Linux Version 5 Update 1;
– Red Hat Enterprise Linux Ver. 5.3 on Dell 11G Family Servers;
– SUSE Linux Enterprise Server 10 SP1.

Профиль защиты OSPP допускает, имея разную архитектуру (рис. 3), рассматривать TOE как единую систему, действующую для всех внешних сущностей. Примеры TOE:

- один компьютер с одним экземпляром ОС;
- несколько аппаратных компонентов (NUMA-системы), на которых исполняется одно ядро ОС.
- несколько аппаратных компонентов, каждый со своей ОС, а любая внешняя сущность имеет один способ получения доступа к этой системе и "видит" множество систем как единую. Примеры: высокопроизводительный вычислительный кластер, где различные узлы решают разные системные задачи (скажем, один узел выполняет вычисления, один узел – хранилище, один узел – гейтвей для кластера, один – предоставляет интерфейс для других ИТ-сущностей), но узлы работают совместно для предоставления функциональности кластера.

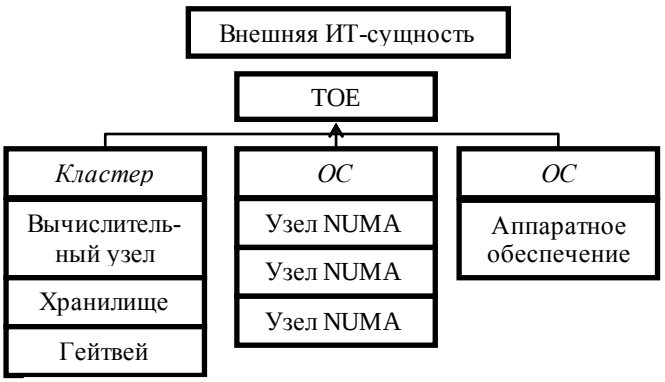

Рис.3 Виды TOE

Требования к вычислительным узлам грид-среды на соответствие профилю защиты OSPP противостоит атакам, когда агент угрозы может:

1) прочитать или изменить данные функциональности безопасности TOE (TSF) без необходимой авторизации при хранении и передаче данных;

2) получить доступ к данным пользователя, хранимым, обрабатываемым или передаваемым TOE без авторизации в соответствии с политикой безопасности TOE;

3) использовать или модифицировать функциональность TSF без необходимых полномочий или получить неавторизированный доступ к данным TSF или пользователей;

4) получить доступ к надежному каналу связи между TOE и другой удаленной надежной ИТ-системой или замаскироваться под нее;

5) получить доступ к информации или передать ее другим получателям по каналам связи, без авторизации согласно политике контроля за информационными потоками;

6) замаскироваться под авторизированную сущность (в том числе TOE или часть TOE) для неавторизованного доступа к данным пользователя и TSF или ресурсам TOE;

7) получить доступ к данным пользователя и TSF или ресурсам TOE, за исключением публичных объектов, без идентификации и авторизации.

Такая политика подразумевает наличие двух организационных политик, гарантирующих, что:

1) пользователи TOE отвечают за действия, связанные с ИБ в рамках TOE;

2) авторизовать необходимо только надежных пользователей, способных корректно использовать TOE.

В основе OSPP лежит система авторизации, которая в грид-среде основана на инфраструктуре открытых ключей.

4 Задействование CC и смарт-каточек в грид-среде

В рамках проекта «Разработка методов и инструментов информационной безопасности грид-технологий на основе международных стандартов» для «Государственной целевой научно-технической программы внедрения и применения грид-технологий на 2009-2013 годы» разработаны проекты 3-х национальных стандартов, гармонизированных с международными. Они лягут в основу технологической ИБ грид-среды.

Ввиду гетерогенной природы аппаратно-программного обеспечения грид-узлов, планируется привести существующие вычислительные узлы к требованиям профиля защиты OSPP. Речь идет об организационной политике, целях безопасности и программном продукте для максимального приближения свойств ИБ грид-среды к требованиям EAL4.

Сейчас в грид-среде задействуют файловые носители личного ключа, защищенного 15-символьным паролем для авторизации, но отсутствуют требования на запрет записи этого пароля, что угрожает ИБ. Для грид-среды гармонизирован стандарт по требованиям безопасности (EAL4+) к смарт-карточкам, которые планируется задействовать как носители ключевой информации (личных ключей) пользователей грид-среды. Это позволит надежно управлять пользователями грид-среды, что особо актуально ввиду значительно прироста (в 3 раза), на примере кластера СКИТ-3, доли грид-задач в общих кластерных вычислениях. Потребность в надежном контроле следует из потенциальной возможности задействовать один личный ключ многими людьми для запуска разных задач, что при ограниченных вычислительных ресурсах нерационально. Например, под одним личным ключом разные пользователи могут запустить две задачи. Первая – подбор паролей некоего домена для выявления слабых паролей пользователей (задействует 128 вычислительных узлов), а вторая – моделирование оползня в районе Мариинского дворца (задействует 140 вычислительных узлов). Первая задача несет менее весомый результат, чем вторая, но при попытке заблокировать личный ключ будут блокированы обе задачи, важная и менее важная.

Невысокая стоимость сертифицированных смарт-карточек поможет задействовать 4-символьные пароли для доступа к личному ключу и его единоличный контроль пользователем. Как показал зарубежный опыт, смарт-карточки целесообразны для целей электронного делопроизводства в институтах НАН Украины.

5 Выводы

Использование профилей защиты, основанных на национальных стандартах критериев оценивания ИТ-безопасности, позволит формально описать требования к ИБ без привязки к технологическим решениям. Это приведет к возможному получению для множества программных продуктов и/или программно-технических комплексов сертификатов оценки соответствия согласно Закону Украины [8]. Продукты с сертификатом соответствия можно задействовать в грид-среде не только для гарантий ИБ и КСЗИ, но и удешевления услуг обеспечения ИБ.

Для достижения целей информационной безопасности грид-узлов, целесообразен профиль зашиты OSPP, в котором цель/объект оценивания рассматривают как один компьютер и/или кластерный комплекс, а также имеет модульную структуру, позволяющую доуточнить требования профиля зашиты. Примером такого уточнения в грид-среде, являются требования к взаимодействию глобального и локальных планировщиков.

Список литературы

[1] ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary

[2] NorduGrid http://www.nordugrid.org/

[3] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[4] *Мелащенко А.О., Перевозчикова О.Л.* Організація кваліфікованої інфраструктури відкритих ключів. – К.: Наукова думка, 2010.

[5] MPI-2: Extensions to the Message-Passing Interface

[6] Jerome H. Saltzer, Michael D. Schroeder The Protection of Information in Computer Systems // Fourth ACM Symposium on Operating System Principles (October 1973)

[7] Закон України від 05.07.1994 № 80/94 «Про захист інформації в інформаційно-телекомунікаційних системах»

[8] Закон України від 01.12.2005 № 3164 «Про стандарти, технічні регламенти та процедури оцінки відповідності»

[9] Operating System Protection Profile (OSPP) //Режим доступу: http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf