From: Vladimir A. Panov/InterTrust/RU

To: Andrey A. Pirozhkov/InterTrust/RU@InterTrustCorp

Cc: Denis Mitavskiy/InterTrust/RU@InterTrustCorp, Roman E. Shilin/InterTrust/RU@InterTrustCorp, Ilya A. Tugushev/InterTrustCorp/SU

Date: 08.07.2013 18:29

Subject: Re: Права доступа

Добрый день.

Сегодня (08.07.2013) провели обсуждение замечаний в составе: Шилин, Пирожков, Панов.  
**См. комментарии ниже по тексту исходного письма**

С уважением,   
 Владимир Панов,   
 Главный архитектор,  
 Компания "ИнтерТраст",  
 Тел.: +7 (495) 956-79-28, +7 (495) 956-4392 доб.190  
 E-mail: panov@intertrust.ru ICQ:238023044 skype:Vladimir.A.Panov

From: Vladimir A. Panov/InterTrust/RU

To: Andrey A. Pirozhkov/InterTrust/RU@InterTrustCorp

Cc: Denis Mitavskiy/InterTrust/RU@InterTrustCorp, Roman E. Shilin/InterTrust/RU@InterTrustCorp, Ilya A. Tugushev/InterTrustCorp/SU

Date: 04.07.2013 22:49

Subject: Re: Права доступа

Добрый день.

В целом замечания не фатальные, скорее рекомендации, чем требования. Что-то уже обсуждали.

1. После прочтения 1-й страницы (первого описания динамических групп) был в шоке:   
   "при определении в конфигурации одной контекстной динамической группы пользователей ПРД создаёт множество реальных групп – столько, сколько есть подходящих доменных объектов"  
   Слишком легко это проецируется на "документы", которых миллионы, а соответствующих доменных объектов может получиться и миллиард. Ну и групп будет столько же. Но позже (на следующих страницах) всё разъяснилось, и наступило просветление :).  **Изменений в исходном тексте не требуется (т.к. идеальная для всех последовательность изложения не вырисовывается)**
2. ПРД - уж больно привычно как "правила разграничения доступа", а не "подсистема ....". Может лучше "подсистема управления доступом"? **Принимается. Заменяем ПРД на ПУД. А под ПРД понимаем "правила разграничения доступа".**
3. Тоже к 1-му абзацу: выглядит так, что объекты доступа - это операции, но это частный случай. А в основном у нас это "доменные объекты", а допустимые операции с ними - это "типы доступа". Надо будет точнее определить, что есть у нас объекты и субъекты доступа.  **Принимается. Есть сложность с "глобальными" (неконтекстными) операциями. Какой там объект доступа? Варианты:  
   1) Контекстом для них считаем всю систему (например, объект - система, тип доступа - создать доменный объект такого-то типа)  
   2) Объект доступа - тип создаваемого доменного объекта, тип доступа - создать...  
   3) Такие операции всё-таки считаем объектом доступа, а тип доступа - выполнить  
   Вроде остановились на первом.**
4. Еще туда же: субъектом доступа у нас является не только пользователь, но и процесс. Даже если у процессов априори полные права, всё равно они субъекты, по крайней мере их действия должны регистрироваться.  **Принимается: добавить в текст про это**
5. Предлагаю "динамические" группы не называть "контекстными", т.к.   
   1) путаются с контекстными ролями, хотя "контекст" как бы другой - у КР - "контекст объекта", а у ДГ - "контекст субъекта".  
   2) даже приведенные примеры неконтекстных ДГ, на самом деле контекстные: "все пользователи" это скорее всего в контексте конкретной организации. То есть, неконтекстные ДГ можно считать несущественным частным случаем (группа на всю корпоративную систему) **Предложение не принимается (остаются "контекстные динамические группы"). Но следует всё-таки еще раз проверить терминологию в тексте, вроде встречалась какая-то путаница**
6. Про контекстные роли уже обсудили, что они полезны не только для определения прав доступа. Они вообще определяют роли субъектов в отношениях с объектами, а значит будут полезны при формализации бизнес-логики системы. Я имею в виду в 1-ю очередь процессы. Контекстные роли контекстного объекта идеально подходят для определения субъектов - участников процесса, обрабатывающего этот объект.  **Принимается: добавить как дополнительную инф. в описание контекстных ролей.**
7. У меня был вопрос: как группе дать доступ сразу к множеству объектов, например, одного типа. Уж очень типовая задача, про нее не раз еще будут спрашивать, желательно упомянуть в документе. Обсудили, стало ясно, что в общем случае это был бы уже другой механизм, лучше обойтись без него. Конкретно доступ к объектам одного типа предоставляется описанным механизмом через дополнительную контекстную роль, которая может уже и не зависеть от контекста. **Пока ничего не требуется, считаем, что проблема решается исходным механизмом реализации ПРД**
8. На стр.5 - 1-й принцип реализации:  
   "**Проверка прав (авторизация) пользователя осуществляется кодом, расположенным в слое бизнес-логики (сервисов).**"  
   Это слой бизнес-логики - это в "платформе" или уже выше - в приложениях ("бизнес-решениях")? Надеюсь, что первое, но надо бы прояснить и уточнить в тексте.  **Принимается: следует более подробно раскрыть в тексте этот момент**
9. Никак не могу смириться с мыслью о том, что любой множественный атрибут доменного объекта реализуется тоже как доменный объект (множество дочерних объектов) другого типа. Очень напрягают примеры, для которых такой механизм - это как "из пушки по воробьям". Например, реквизит "адресаты" у документа - это список ссылок на субъектов документооборота. Использование описанного механизма приведет к тому, что у каждого "адресата" будет свой ACL, в котором будет указано, кто может именно этого адресата из документа удалить. А на самом деле достаточно правила в родительском объекте ("документе"), разрешающего удалять дочерние объекты типа адресат (по аналогии с правом создания таких дочерних обхектов).  
   Однако, тут может возникнуть противоречие, если права доступа к дочернему объекту будут определяться и в его ACL и в ACL родительского объекта. Но в данном, и уверен что во многих таких случаях, ACL у таких дочерних объектов не нужен в принципе, надо только как-то это формализовать. Я уже неоднократно предлагал разделять объекты на две категории, выделяя такие, у которых нет ни жизненного цикла (статусов), ни собственных прав доступа. А еще им не нужен внешний глобально-уникальный идентификатор, так как на них не бывает внешних ссылок.  **Принимается к решению на следующей (2-й) итерации (ориентировочно - через 2 недели).**
10. Обсуждали с Горностаевым тему управления доступом, особенно вот эти два требования  
    [Notes Link](Notes:///C3256D6000584BB2/48E3B729F7142E6EC3256B97002EF840/4CEECE0B17E11BCAC32577BD004EC35E)РД: СВТ. Защита от НСД к информации. Показатели защищенности от несанкционированного доступа к информации:  
    - Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).  
    - Дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.  
    Проблема в том, что пользователь CompanyMedia запросто распространяет права на доступ, например, к документу, просто выдав по нему поручение. И таких примеров множество. Решили, что честно на 100% реализовать эти требования мы не можем, но если "ограничение" понимать не как полный запрет, а как установление некоторых конкретных границ, то пусть выделенный субъект (админ) их устанавливает, а пользователь распространяет права в пределах этих границ.   
    Конкретнее, 1-й вариант решения такой: задаваемый администратором признак (атрибут) у пользователя, (не)дающий ему возможность выполнять операции, распространяющие права доступа. Такой пользователь не сможет выдать никому поручение, но вполне возможно что таких много.  **Принимается к рассмотрению (надо подумать), в том числе возможно и с участием аналитиков.**   
    Другой вариант исходит из типичной потребности (не)давать определенным пользователям доступ к целым приложениям ("бизнес-решениям"). Например, делопроизводство вижу, а договоры - нет. Основной механизм ПРД этим не отменяется, они должны действовать совместно, доступ дается, только если он дан всеми механизмами. Но если уж такой 2-й механизм делать, то имеет смысл обобщить его до "мандатного доступа". **См. следующий пункт**
11. Раз уж пошла речь про "мандатный доступ", то если делать его строго, архитектура управления доступом должна быть основана на "диспетчере доступа", а это для нас может быть затруднительно. Однако, официально на нашем уровне (1Г и 5 класс защиты от НСД) мандатов от нас не требуют, и диспетчер не обязателен. Он был бы полезен, но если сделать его трудно, можно обойтись. Ну и еще в мандатном доступе кроме нужных нам прав на чтение есть права на запись, которые нам ни к чему. **Предварительно принимается, но требуется дополнительное разбирательство:   
    1) С аналитиками - насколько это корректно и насколько востребовано.  
    2) Это всё-таки мандатный принцип или не совсем? (если без ограничений на запись, то не совсем, а если с ними, то для заказчиков/пользователей будет слишком сложно работать с разной (по уровню доступа) информацией в разных сеансах (с разным уровнем допуска).  
    3) Можно ли всё-таки сделать единый "диспетчер доступа", осуществляющий "перехват всех обращений субъектов к объектам"?   
    Если не получается, честно ставим на нем крест.**

С уважением,   
 Владимир Панов,   
 Главный архитектор,  
 Компания "ИнтерТраст",  
 Тел.: +7 (495) 956-79-28, +7 (495) 956-4392 доб.190  
 E-mail: panov@intertrust.ru ICQ:238023044 skype:Vladimir.A.Panov

From: Andrey A. Pirozhkov/InterTrust/RU

To: Vladimir A. Panov/InterTrust/RU@InterTrustCorp, Denis Mitavskiy/InterTrust/RU@InterTrustCorp

Cc: Roman E. Shilin/InterTrust/RU@InterTrustCorp

Date: 02.07.2013 21:42

Subject: Права доступа

Кажется, у меня в первый раз случайно попали разделы, которые я не успел обновить (конфигурационные объекты и далее). Просьба их игнорировать или взять эту версию:

[attachment "Права доступа.docx" - помещен в БД ДИТ [Notes Link](Notes:///C3256D6000584BB2/48E3B729F7142E6EC3256B97002EF840/97A8AB50DA0130BF44257B9E0060D92B)]

В репозитории: /Архитектура/Права доступа.docx

С уважением,

Андрей Пирожков

Главный конструктор

ЗАО «Компания "Интертраст"»

E-Mail: apirozhkov@inttrust.ru

Тел.: +7 (495) 956 7928