УДК 004.4’2

ЗАДАЧИ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ И ПОДХОДЫ К ИХ РЕШЕНИЮ

А.И. Кучеров, А.В. Петухов, Е.А. Левчук, О.М. Демиденко
Гомельский государственный университет имени Франциска Скорины, Беларусь

Рассматривается решение задачи идентификации и аутентификации с использованием профессиональных средств защиты информации. Большинство исследований механизмов защиты компьютерных систем от несанкционированного доступа посвящено различным способам хранения и ввода идентификационной информации о пользователе. Однако, когда речь заходит о компьютерной безопасности, задача идентификации и аутентификации в своей постановке значительно шире, чем задача контроля входа пользователя в систему.

1. Требования к механизму идентификации и аутентификации

Идентификация – это процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации (каждый субъект или объект системы должен быть однозначно идентифицируем). Аутентификация – это проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

Требования к механизму идентификации и аутентификации состоят в том, что комплекс средств защиты информации (КСЗ) должен:

- требовать от пользователей идентифицировать себя при запросах на доступ;
- подвергать проверке подлинность идентификации – осуществлять аутентификацию;
- располагать необходимыми данными для идентификации и аутентификации;
- препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась, т. е. выдвигается требование, состоящее в необходимости идентификации и аутентификации пользователя именно при запросах на доступ;
- проверять подлинность идентификатора субъекта - осуществлять аутентификацию;
- располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в вычислительные средства неидентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

Что же представляет собою запрос на доступ к ресурсу? В общем случае подобный запрос может быть охарактеризован тем, какой пользователь обращается к ресурсу (идентификатор пользователя, определяющий, кому нужен ресурс), какой процесс (приложение) обращается к ресурсу (идентификатор процесса, определяющий для решения каких задач пользователю нужен ресурс), и, собственно, к какому ресурсу осуществляется обращение (идентификатор объекта доступа) [1].

Естественно, возникает вопрос, с какой целью необходима какая-либо идентификация и аутентификация субъекта и объекта доступа при запросах на доступ к ресурсу. Ведь в любой системе защиты предполагается, что реализуется механизм идентификации и аутентификации пользователя при входе в систему. Результатом этого является однозначная идентификация пользователя, запускаемые им процессы наследуют этот идентификатор, т. е. именно от лица идентифицированного пользователя и обращаются

к ресурсу, на чем и строится в своей основе разграничительная политика доступа к ресурсам.

2. Задача идентификации и аутентификации пользователя при запросах на доступ

Примерный перечень мероприятий по идентификации и аутентификации пользователя можно описать следующими шагами [2].

Первый шаг идентификации, поддерживаемый режимом аутентификации, реализуется при входе пользователя в систему. Здесь следует выделить возможность входа в штатном и в безопасном режиме. Принципиальным отличием безопасного режима является то, что при запуске системы в безопасном режиме можно отключить загрузку сторонних по отношению к системе драйверов и приложений. Поэтому, если в системе используется добавочная система защиты информации от несанкционированного доступа, можно попытаться загрузить систему в безопасном режиме без компонент дополнительной защиты. С учетом же того, что загрузить систему в безопасном режиме может любой пользователь, то система защиты должна обеспечивать возможность входа в систему в безопасном режиме (после идентификации и аутентификации) только под учетной записью администратора.

Второй шаг состоит в запуске пользователем процессов, которые уже, в свою очередь, порождают потоки и процессы. Все работающие в системе процессы и потоки выполняются в контексте защиты того пользователя, от имени которого они так или иначе были запущены. Для идентификации контекста защиты процесса или потока используется объект, называемый *маркером доступа* (access token). В контекст защиты входит информация, описывающая привилегии, учетные записи и группы, сопоставленные с процессом и потоком. При регистрации пользователя в системе создается начальный маркер, представляющий пользователя, который входит в систему, и сопоставляет его с процессом оболочки, применяемой для регистрации пользователя. Все программы, запускаемые пользователем, наследуют копию этого маркера.

В общем случае пользователь имеет возможность запуска процесса, как с собственными правами, так и под учетной записью другого пользователя. Запуск пользователем процесса под другой учетной записью возможно только после выполнения процедуры аутентификации – пользователь должен ввести идентификатор и пароль, соответствующие той учетной записи, под которой им будет запущен процесс.

С одной стороны, это очень полезная опция, которая может быть использована в корпоративных приложениях, когда на одном компьютере требуется обрабатывать конфиденциальные и открытые данные. При этом предполагается, что для обработки данных различных категорий создаются различные учетные записи. Данная опция предполагает, что одновременно (без перезагрузки) можно обрабатывать данные различных категорий. Естественно, что реализация данной возможности выставляет и дополнительные требования к системе защиты информации.

Однако важнейшей особенностью рассматриваемого способа запуска процесса является то, что при этом система начинает функционировать в многопользовательском режиме – в системе одновременно зарегистрировано несколько пользователей. Как следствие, может возникнуть проблема однозначной идентификации пользователя при доступе к ресурсу, что характерно для решения задачи реализации разграничительной политики доступа к устройствам.

Третий шаг состоит в порождении процессом потоков, которые собственно и обращаются к ресурсам. Система предоставляет разработчикам приложений сервисы олицетворения. Сервис олицетворения предоставляет возможность отдельному потоку

выполняться в контексте защиты, отличном от контекста защиты процесса, его запустившего, т.е. запросить олицетворить себя с правами другого пользователя, в результате – действовать от лица другого пользователя. Как следствие, именно на этом этапе и возникают вопросы корректности идентификации и аутентификации пользователя при запросе доступа к ресурсам, а задача идентификации и аутентификации пользователей при запросах на доступ сводится к контролю корректности олицетворения.

3. Реализация механизма идентификации и аутентификации при запросах доступа к ресурсам

В общем виде решение задачи должно состоять в следующем. При запросе доступа к ресурсам должны выявляться факты произошедшего олицетворения (соответственно, субъектом доступа здесь выступает процесс, для которого анализируется наличие олицетворяющего маркера доступа) и проверяться их корректность в соответствии с заданными разрешениями (запретами). Очевидно, что проверка прав субъекта доступа к ресурсу должна осуществляться уже после проверки корректности его идентификации [3].

Таким образом, в качестве субъекта доступа выступает процесс (в том числе, это обусловливается и тем, что различные процессы (приложения) могут затребовать и различных правил разрешенных (запрещенных) олицетворений, а это невозможно обеспечить, если в качестве субъекта доступа принять пользователя – учетную запись).

4. Ограничения возможности корректного решения задачи

Ограничения, о которых пойдет далее речь, в первую очередь относятся при реализации разграничительной политики доступа к устройствам. Разграничение доступа к устройствам – это задача противодействия внутренним ИТ-угрозам (в частности, решаемая для защиты информации от санкционированных пользователей).

КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется с выделенным ему конкретным устройством.

Проблема здесь состоит в том, что многие устройства предполагают возможность взаимодействия с ними приложения не напрямую, а через драйвер. В этом случае запрос доступа к устройству осуществляется от лица пользователя System. Возникает вопрос, а откуда взять идентификатор пользователя, который инициировал это обращение к устройству? Можно, конечно, «посмотреть», какой пользователь зарегистрирован в системе, и фильтровать запросы доступа, применительно к его учетной записи (кстати говоря, подобный подход и реализуется некоторыми специализированными средствами защиты). Но не будем забывать, что современные операционные системы многопользовательские. В таком режиме в системе одновременно зарегистрировано несколько пользователей, при этом выявление учетной записи, от которой осуществлен запрос доступа к устройству, становится неразрешимой (или, по крайней мере, весьма сложно корректно решаемой) задачей.

Таким образом, задача идентификации пользователя может решаться некорректно именно в тех приложениях, для использование в которых и предназначено средство защиты.

Возникает вопрос – как решить данную задачу (речь идет о корректном разграничении доступа пользователей к устройствам, доступ к которым осуществляется через драйверы), если архитектурная особенность реализации обращения к ресурсу такова, что он осуществляется от имени пользователя System.

При этом будем учитывать, что для обращения к подобным устройствам, как правило, необходимо приложение (отдельная программа), взаимодействующая с драйвером устройства. С учетом сказанного, можем сделать вывод, что данная задача решается с использованием механизма обеспечения замкнутости программной среды, разрешив/запретив пользователю запуск приложения для работы с устройствами.

5. Вопросы корректности идентификации объекта доступа

Здесь, на первый взгляд, проблем вообще не существует. Однако, если внимательно рассмотреть архитектурные принципы реализации и возможности современных универсальных операционных систем, то точка зрения на этот вопрос радикально меняется. В порядке примера рассмотрим предоставляемые современными Windows возможности идентификации файлового объекта при запросе доступа.

В NTFS файловый объект может быть идентифицирован различными способами:

- файловые объекты, задаваемые длинными именами, характеризуются той отличительной особенностью, что к ним можно обращаться как по длинному, так и по короткому имени, например к каталогу “\Program files\” можно обратиться по короткому имени “\Progra~1\”;

- файловые объекты, задаваемые русскими (либо в иной кодировке) буквами, также имеют короткое имя, которое формируется с использованием кодировки Unicode (внешне они могут существенно различаться); например короткое имя для каталога C:\Documents and Settings\USER1\Главное меню будет C:\Docume~1\USER1\5D29~1\; к этим объектам можно обратиться как по длинному, так и по короткому имени;

- файловый объект идентифицируется не только именем, но и своим идентификатором (ID) – индекс объекта в таблице MFT, причем некоторые программы обращаются к файловым объектам не по имени, а именно по ID.

Если установленная в вашей информационной сети система защиты информации от несанкционированного доступа не перехватывает и не анализирует лишь один подобный способ обращения к файловому объекту, то, по большому счету, она становится полностью бесполезной (рано или поздно, злоумышленник выявит данный недостаток средства защиты и воспользуется им).

Заключение

Защита информации – это очень сложная научно-техническая и инженерная задача. Некоторые разработчики систем защиты в средствах массовой информации говорят, что средство защиты может быть простым в использовании и в администрировании.

В корпоративных приложениях, где конфиденциальные данные являются потенциальным товаром, т. е. обладают потребительской стоимостью, к вопросам компьютерной безопасности нужно относиться серьезно, необходима соответствующая квалификация лиц, отвечающих на предприятии за защиту информации. В этом случае потребитель уже должен ожидать от разработчика средств защиты не простых, а эффективных и обоснованных решений. Поэтому следует разрабатывать более новые эффективные программные комплексы по защите информации от несанкционированного использования.

Список литературы

1. Воруев, А.В. Удаленный контроль и управление процессами в локальных сетях / А.В. Воруев, О.М. Демиденко, А.И. Кучеров // Изв. Гомельского гос. ун-та им. Ф. Скорины. – Гомель. – 2007. – № 5 (44). – С. 98-100.

2. Дробышевский, С.В. Функциональные возможности приложения для анализа работы пользователей в сетевой среде/ Дробышевский С.В., Винглевский Д.Б., Кучеров А.И. // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: матер. XII Респ. науч. конф. студ. и аспир. (16-18 марта 2009 г, Гомель) – Гомель: изд-во ГГУ, 2009. – Т. 2. – С. 195-196.

3. Шуман, Е.А. Проверка идентифицированного пользователя на предмет соответствия личности / Шуман Е.А., Кучеров А.И. // Новые математические методы и компьютерные технологии в проектировании, производстве и научных исследованиях: матер. XII Респ. науч. конф. студ. и аспир. (16-18 марта 2009 г, Гомель) – Гомель: изд-во ГГУ, 2009. – Т. 2. – С. 259-260.