УДК 004.056(06)

М.В. Ларченко, М.М. Кучеров

Универсальная идентификация – важное средство борьбы с киберпреступностью

Предложено использование полученной модели в качестве эффективного механизма для поддержки универсальной идентификации объектов. Рассмотрена необходимость введения системы универсальной идентификации и на основе различных моделей доступа предложен возможный вариант ее поддержки.

Мандатный контроль и управление доступом, закон Гроша, эффективность доступа

Введение. Всемирная сеть является идеальной средой для деятельности террористов, поскольку доступ к ней крайне легок, в ней легко обеспечить анонимность пользователей, она никем не управляется и не контролируется, в ней не действуют законы и не существует полиции. «Традиционное» преступление происходит «на земле», в осязаемом физическом мире, где есть государственные и таможенные границы, устоявшиеся административные режимы и т.д. В телекоммуникационном же пространстве границ нет, события там развиваются молниеносно и сразу в масштабе планеты. Ныне в Сети представлены абсолютно все террористические группы, которые публикуют свои материалы, по меньшей мере, на 40 различных языках. Террористические группы создают и многоязычные сайты, чтобы оказать влияние на людей, напрямую не вовлеченных в конфликт. Особое беспокойство вызывает то, что экстремистские группировки, сепаратистские силы, проповедники идей, противоречащих общечеловеческим ценностям, стремятся интенсивно использовать современные передовые информационные технологии для пропаганды своей идеологии и достижения своих целей.

Чаще всего поддержка сайтов террористической и экстремистской направленности осуществляется из-за рубежа. Создать сайт в Интернете на территории любого государства сегодня очень просто. На это уходит примерно 50 мин времени плюс средства, перечисляемые электронным платежом. Причем зарегистрировать сайт можно на любое имя и разместить на нем любую информацию [1].

На сегодняшний момент не решен вопрос о правилах размещения информации в Интернете, чем и пользуется преступный мир. Хотя в области информационной безопасности и существуют базовые принципы и законодательные документы, но они действуют только в пределах границ отдельно взятого государства. А взаимодействие между странами в области решения проблемы финансового мошенничества, хищения персональных данных, распространения компьютерных вирусов, спама и детской онлайн-порнографии оставляет желать лучшего. Для борьбы с этим нужно искать тех, кто распространяет подобные программы и сайты, а не тех, кто их использует. Не так-то просто удалить сайт из Всемирной сети. Для этого мало того, что он кому-то не нравится, необходимо решение суда: контент незаконный, закрыть.

Главное – это создание международного механизма, поскольку Интернет глобален. Ведь сайты, которые вытеснили из российской зоны Интернета, благополучно существуют в иностранных зонах. Тут сталкиваются религиозные, национальные и прочие вопросы. К тому же правозащитники много рассказывают про свободу слова и право на информацию. Получается, что у наших детей есть право на просмотр порно, ознакомление с прелестями наркомании, изучение фашистской идеологии и т.д.

Решение проблемы может быть только одно – отказ от анонимности в Сети! Присвоение каждому пользователю ID должно стать нормой так же, как ИНН, номер паспорта, прав, персональный код в пенсионной системе и системе медицинского страхования и т.д. Человек, пользуясь Интернетом, будет авторизовать свои действия при помощи этого номера и, соответственно, будет отвечать за них [2].

Необходимо обеспечить общее понимание проблемы кибербезопасности и объединение всех заинтересованных сторон в деле противодействия Интернет-преступности. В этом должно помочь создание универсальной системы идентификации [3]. Также как каждый имеет уникальный национальный паспорт, который используется, чтобы путешествовать в различные страны, должен быть единственный идентификатор (ID), чтобы обращаться к множеству приложений и сервисных шлюзов. Хотя сторонники многочисленных идентификаторов и заявляют, что опасно иметь единственный ID, который может быть взломан и затем использоваться, чтобы обращаться к многочисленным учетным записям, тем не менее для конечных пользователей весьма трудно создавать одинаково защищенные многочисленные пароли для разных идентификаторов. И в большинстве случаев пользователь назначает один и тот же пароль нескольким идентификаторам.

Уникальный ID может быть прикреплен к системному идентификатору вычислительных устройств или к биометрическому отпечатку пальца пользователя. Или это могла бы быть комбинация обоих. Цель здесь состоит в том, чтобы удостовериться, что операция системы аутентична пользователю и его вычислительному устройству. Поэтому если кто-нибудь сумеет захватить пользовательский ID и пароль, то он не будет по-прежнему функционировать на другом вычислительном устройстве или/и пользовательской комбинации.

Как только пользователь регистрируется в системе, ему предлагается защищенная среда, из которой пользователь может обратиться к разнообразию приложений и служб. В любом случае доступ к

приложению или службе внутренне прикреплен к системному ID. Хотя такое понятие идентификации обеспечивает меньше мобильности, поскольку нельзя обратиться к приложениям и службам с другого вычислительного устройства, оно обеспечивает более стабильную защиту конечному пользователю.

Если пользователю требуется обращение к приложениям, службам и данным из нескольких мест, используя тот же самый ID, система позволяет прикрепить его системный ID к его биометрическому профилю и выполнять аутентификацию, используя биометрическое устройство или другие подобные устройства. Мобильность данных доступна в соответствии с предложением по размещению данных на сетевом сервере или синхронизацией данных с хранением на других устройствах. Пользователь, чтобы обратиться надежно к любому обслуживанию в Интернете, ориентированному на универсальный ID, может использовать свой ID вместе с паролем или биометрическими данными. Он может использоваться в международных критических по безопасности областях, чтобы произвести доверенную идентичность и надежно представить личные детали без необходимости заполнения форм.

Приведем пример того, как пользователь может получить свою электронную почту (которая сохранена локально на офисном или домашнем рабочем столе) из вычислительного устройства (ВУ) мобильного телефона.

Для этого пользователь должен настроить браузер на ВУ мобильного телефона, а также зарегистрировать и применить один и тот же системный ID. Затем пользователь должен или интерактивно поддерживать офисный или домашний рабочий стол (где расположены почтовые папки), или синхронизировать почтовые папки с сетевым обслуживанием хранения, которое доступно только через пользовательский системный ID. Пользователь может тогда войти в ВУ мобильного телефона и обратиться к электронной почте на своем домашнем/офисном компьютере. Это пример использования одного и того же ID для нескольких устройств и приложений/служб.

В случае если пользователь хочет поддерживать разные идентификаторы доступа для различных устройств и приложений/служб, он может обратиться к многочисленным ресурсам разных устройств, формируя личную сеть и обеспечивая полный доступ к различным идентификаторам доступа. Эта система при предложении большей мобильности не обеспечивает такую же защиту, как уникальный идентификатор доступа.

В более широком контексте идею универсальной идентификации можно распространить на весь «материальный Интернет» (Интернет of Things), в том числе и на объекты, которые не могут иметь собственного коммуникационного поведения, такие как абстрактные документы. Такие объекты не общаются, но они могут быть упомянуты другими агентами, такими как мощные централизованные серверы, действующие по запросам пользователей. Идея столь же проста, как трудно ее приложение. В материальном Интернете должны быть представлены 50–100 000 миллиардов объектов и, возможно, необходимо следовать за изменением этих объектов. Каждый человек окружен 1 000–5 000 объектами.

Базы универсальной идентификации

Чтобы обеспечить международную инфраструктуру для доверенной универсальной идентификации через Интернет, используя существующие ресурсы, каждой участвующей стране необходимо установить национальную базу данных и серверную систему и импортировать данные из локальных, официальных источников ID, которые индексируются уникальным идентификатором. Прикрепляя код страны ISO-3166 к этому идентификатору, получают всемирный уникальный идентификатор. Связь кода группы с универсальным идентификатором расширяет возможности, чтобы идентифицировать другие объекты. Каждая страна подключает свою базу данных к Интернет и действует как центр идентификации и авторизации по отношению к обладателям универсальных ID по всему миру.

Для реализации универсальной идентификации необходимы высокопроизводительные СУБД, которые могли бы иметь минимальные накладные расходы по обработке многочисленных запросов. Большинство доступных в настоящее время систем основываются на технике, называемой блокированием [4]. Главная идея блокирования заключается в том, что если транзакции нужны гарантии, что некоторый объект (обычно запись базы данных), не будет изменен каким-либо непредсказуемым образом в течение требуемого промежутка времени, то она устанавливает блокировку этого объекта. Результат блокировки заключается в том, чтобы изолировать этот объект от других транзакций и, в частности, предотвратить его изменение средствами этих транзакций. Для первой транзакции, таким образом, имеется возможность продолжения предусмотренной в ней обработки, располагая определенными знаниями о том, что объект запроса будет оставаться в стабильном состоянии до тех пор, пока данная транзакция этого пожелает.

Для пользователей представляют интерес, в основном, блокировки двух типов: монопольные и совместные.

Если транзакция A устанавливает, например, монопольную блокировку записи R, то запрос из транзакции B на любого типа блокировку записи R приведет к тому, что B перейдет в состояние ожидания. Транзакция B будет находиться в этом состоянии до тех пор, пока не будет снята блокировка, установленная транзакцией A.

Напротив, если транзакция A устанавливает совместную блокировку записи R, то запрос из транзакции B на монопольную блокировку записи R заставит B перейти в состояние ожидания, и B будет находиться в этом состоянии до тех пор, пока не будет снята блокировка, установленная транзакцией

A. С другой стороны, запрос из транзакции *B* на совместную блокировку записи *R* будет удовлетворен, т.е. теперь обе транзакции будут удерживать совместную блокировку записи *R*. Сказанное можно удобно резюмировать с помощью матрицы совместимости (табл. 1).

Таблица 1

Матрица совместимости типов блокировки

Тип	Монопольная	Совместная	–
Монопольная	Нет	Нет	Да
Совместная	Нет	Да	Да
–	Да	Да	Да

Когда транзакция успешно осуществляет выборку/обновление записи, она автоматически устанавливает совместную/монопольную блокировку этой записи. Блокировки удерживаются до успешного или неудачного завершения транзакций.

Этот простой протокол порождает возможность тупиковых ситуаций.

Предложение по решению проблемы

Управление транзакциями – это задача диспетчеризации исполнения транзакций таким образом, чтобы каждая транзакция могла рассматриваться как высказывание типа «все или ничего» даже при условии, что возможны произвольные сбои на части любой отдельной транзакции или самой системы, и при условии, что множество независимых транзакций может выполняться параллельно и обращаться к одним и тем же данным. Подобная задача изоляции транзакций решается также в мандатной модели информационной безопасности. Для того чтобы обеспечить безопасность информации, необходим процесс управления информацией и разграничение доступа внутри и за пределами каждой организации. Необходимо проанализировать протокол и дополнить его с учетом модели мандатного управления доступом.

Вначале дадим необходимые определения [5–8]. Мандатное управление доступом есть разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Под уровнем конфиденциальности будем понимать иерархический атрибут, который может быть ассоциирован с сущностью компьютерной системы для обозначения степени ее критичности в смысле безопасности. Этот атрибут может обозначать, например, степень ущерба от нарушения безопасности в компьютерной системе, или чувствительность (чувствительность – характеристика ресурса, которая определяет его ценность или важность и может учитывать его уязвимость).

Степень доверия – это атрибут, определяющий уровень конфиденциальности субъекта. Чем выше степень доверия субъекта, тем к более секретной информации он имеет доступ. Чем выше конфиденциальность объекта, тем более секретная информация хранится в нем.

Определим функции, отображающие субъектов и объекты системы, на уровни конфиденциальности – допуск (*clearance*) и гриф (*classification*). Областью значений каждой из этих функций является решетка уровней конфиденциальности *L* с линейным отношением частичного порядка. Функция *clearance* определена на множестве субъектов *S*, а *classification* – на множестве объектов *O*. Эти функции записываются следующим образом:

$$\text{clearance}(s) = l_s, \quad (1)$$

$$\text{classification}(o) = l_o. \quad (2)$$

Кроме уровней конфиденциальности, можно ввести множество категорий. Каждая категория описывает соответствующий тип информации. Примерами категорий могут служить: «Для прессы», «Основной», «Стратегический» и т.п. Объект, которому присвоено несколько категорий, содержит информацию, соответствующую этим категориям.

Множество уровней конфиденциальности образуют решетку по отношению к операции (<). Решетка (SC, ≤) определяется следующим образом: SC – конечное множество уровней конфиденциальности; ≤ – бинарное отношение частичного порядка для уровней конфиденциальности SC.

Отношение (≤) рефлексивно ($A \le A$), транзитивно ($A \le B$ & $A \le C \Rightarrow A \le C$) и симметрично ($A \le B$ & $B \le A \Rightarrow A = B$). При этом существует наибольшая верхняя граница в SC, т.е. для каждого A и B в SC существует класс $C = \max(A, B)$ такой, что:

$A \le C$ и $B \le C$;

$A \le D$ и $B \le D \Rightarrow C \le D$ для любого D из SC.

Для каждого непустого подмножества $S = \{A_1, A_2, \ldots, A_n\}$ из SC существует единственный элемент $S = \max(A_1,\ldots, A_n)$.

Можно определить также наименьшую нижнюю границу в SC. Для каждого A и B в SC существует единственный класс $E = \min(A, B)$ такой, что:

$E \le A$ и $E \le B$;

$D \le A$ и $D \le B \Rightarrow E \le D$ для любого D из SC.

Для каждого непустого подмножества $S = \{A_1, A_2, \ldots, A_n\}$ из SC существует единственный элемент $S = \min(A_1,\ldots, A_n)$.

Приведем пример мандатного управления доступом. Рассмотрим систему информационной безопасности предприятия. Здесь можно ввести концепцию качества информации. Качественная производственная информация обладает некоторыми характеристиками. К ним относятся полнота, своевременность и конфиденциальность.

Решения относительно качества информации следует принимать на основе формальной модели, которая основана на следующих двух критериях: субъективной и объективной ценности.

Субъективная ценность соотносится с размером нанесенного ущерба в случае, если информация окажется известной лицам, не авторизованным для ее получения. Здесь ущерб возникает из качеств, присущих самой информации. Объективная ценность соотносится с размером нанесенного ущерба в случае, если информация окажется недоступной или имеет ненадлежащую целостность. Это – объективный критерий, зависящий от событий или спецификаций вне самой информации. Например, если финансовые документы, которые по закону должны храниться в течение ряда лет, окажутся утраченными, предприятие может быть подвергнуто штрафу.

Отдельные элементы информации согласно этой модели попадают в обе категории. Например, ведомости по персоналу, в которых указаны суммы компенсации сотрудникам, имеют субъективную и объективную ценность.

В табл. 2 приведен образец классификационной политики.

Таблица 2

Пример классификационной политики в области информации

Субъективные классификации	Метка конфиденциальности		
	Для служебного пользования	Конфиденциальная	Персональная
Определение	Раскрытие может нанести в перспективе ущерб экономике предприятия	Раскрытие может нанести серьезный ущерб экономике предприятия	Раскрытие может негативно повлиять на сотрудников или претендентов на должность
Объективные классификации	На хранении	На текущем контроле	
Определение	Ненадлежащее качество может привести в перспективе к серьезным правовым или экономическим последствиям	Ненадлежащее качество может нанести серьезный ущерб экономике предприятия	

Модель эффективного доступа

Дополним это описание с учетом доступности. Закон Гроша утверждает, что увеличение в n раз отдачи от инвестиций в компьютерное оборудование возможно при увеличении в n^2 раз скорости обработки информации, т.е. сокращении в соответствующее число раз времени доступа к информации [9, 10]. В таком случае необходимо размещение субъектов и объектов с высокой доступностью на высшей ступени иерархии целостности. В результате субъекты и объекты с высокой доступностью являются также и высокоцелостными, а компоненты с низкой доступностью не всегда являются таковыми, т.е. могут быть модифицированы. Таким образом, правила NWU (нет записи вверх) и NRD (нет чтения вниз) в структуре модели Биба соответствуют решеточной модели безопасности Белла и Лападула, так как чтение снизу высокоцелостных файлов в иерархии модели целостности Биба происходит быстро. Аналогично быстро происходит и запись информации вниз, т.е. «на хранение». В свою очередь, противоположно направленные информационные потоки, такие как перевод информации из категории «на хранении» в категорию «на текущем контроле», и доступ высокоцелостных субъектов, в том числе компьютерных процессов, к программам и данным ненадлежащего качества подлежат контролю.

На рис. 1 разрешены два информационных потока: поток по записи (*write*) снизу вверх, и поток по чтению сверху (*read*) – это работа с файлами операционной системы, официальными утвержденными отчетами, справочными данными и тому подобной информацией с высоким уровнем целостности. Перезапись официальной информации должна быть ограничена и строго контролироваться (NWD), поскольку она препятствует высокопроизводительной работе.

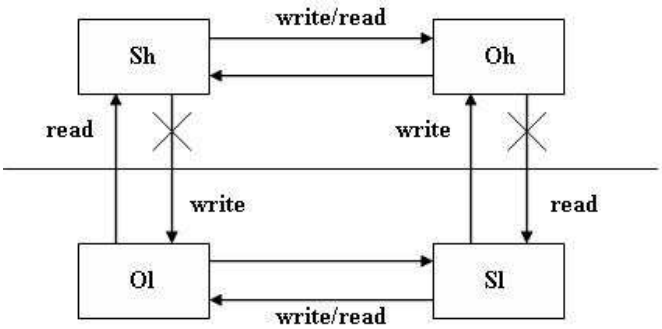

Рис. 1. Дополнение модели Белла и Лападула с учетом доступности. Высокий уровень конфиденциальности объединен с низким уровнем доступности, а низкий уровень конфиденциальности – с высоким уровнем доступности

Точно так же должен быть ограничен поток по чтению снизу (NRU) в модели Белла и Лападула, поскольку он не только приводит к НСД к информации, но и замедляет высокопроизводительную обработку данных.

Процедуры коррекции информации с высоким уровнем доступа должны инициироваться записью вверх, на более конфиденциальный уровень. Таким образом, достигаются две цели: информация становится недоступной для рядовой обработки и на более секретном уровне к ней получают доступ субъекты, которые могут ее редактировать.

Перевод информации с низкого на более высокий уровень доступности означает деклассификацию информации, т.е. ее санкционированное распространение, и должен проводиться на основе, во-первых, установления правильного форматирования и представления вновь публикуемой информации, во-вторых, проверки ее своевременности и соответствия реалиям деловых процессов и, в-третьих, под ответственность принципала, от лица которого выполняется эта операция.

Необходимо отметить, что процесс редактирования информации должен осуществляться по завершении любой иной ее обработки, в противном случае в системе одновременно окажется два «официальных» источника данных, что является нарушением.

На практике это позволяет разместить важные системные файлы в верхней части иерархии модели Биба. Это защищает доступность эталонных файлов и проверенных данных от обычных пользователей, поскольку правило NWU не позволяет им осуществить запись в важные документы и тем самым исправлять официальные данные. Кроме того, если рассматривать исполнение как чтение, то высокопроизводительные процессы компьютерной системы, к которым и относится закон Гроша, не могут оперировать документами и данными вне высшего круга целостности. Это обеспечивает дополнительную защиту целостности в компьютерной системе.

Данная схема обеспечивает защиту системных файлов от троянских программ. Если троянская программа находится на одном из нижних уровней в иерархии модели Биба, то она не сможет исказить системные файлы за счет правила NRD. Таким образом, осуществляется защита производительности и целостности от троянских программ. Очевидно, что такое объединение моделей может также осуществлять защиту конфиденциальности для верхних уровней определенной иерархии и защиту эффективного доступа для нижних уровней в модели Белла и Лападула.

Обсуждение предложенного решения

Модель эффективного доступа позволяет повысить эффективность работы СУБД. Если транзакция *A* устанавливает, например, монопольную блокировку записи *R*, то уровень транзакции *A* является конфиденциальным; запись *R* получает метку «конфиденциально» и становится недоступной для низкоуровневой транзакции *B*. Запрос из высокоуровневой транзакции *C* на любого типа блокировку записи *R* приведет к тому, что *C* перейдет в состояние ожидания. Транзакция *C* будет находиться в этом состоянии до тех пор, пока не будет снята блокировка, установленная транзакцией *A*.

Напротив, если транзакция *A* устанавливает совместную блокировку записи *R*, то уровень транзакции *A* не является конфиденциальным; запрос из транзакции *B* на монопольную блокировку записи *R* удовлетворяется, а результат работы транзакции *A* аннулируется. С другой стороны, запрос из транзакции *B* на совместную блокировку записи *R* будет удовлетворен, т.е. теперь обе транзакции будут удерживать совместную блокировку записи *R*. Сказанное можно резюмировать с помощью матрицы совместимости (табл. 3).

Таблица 3

Матрица совместимости типов блокировки

	Монопольная	Совместная	–
Монопольная	Нет	Нет доступа	Да
Совместная	Монопольная – да, предыдущие транзакции – отменяются	Да	Да
–	Да	Да	Да

Если транзакция содержит хотя бы одно обновление, то ее уровень является конфиденциальным, а все используемые объекты также являются конфиденциальными. Блокировки удерживаются до успешного или неудачного завершения транзакций.

Итак, были рассмотрены существующие модели безопасности и доступности и построена объединенная модель безопасности, которая объединила модели Белла и Лападула, а также Биба. Можно показать, что в модель легко включить контроль доступа, базирующегося на ролях, а также дискреционный доступ [11]. Предложено использование полученной модели в качестве эффективного механизма для поддержки универсальной идентификации объектов.

Литература

1. Мачабели К. Компьютерные мошенничества чрезвычайно разнообразны // На Пресне. Информационный сайт Пресненского района/ http://www.napresne.info/default.aspx?menu=smi&id=2972

2. Мирошников Б.Н. Мы смотрим в закон! // 10-й Всероссийский форум информационной безопасности «Инфофорум-X». 31 января – 1 февраля 2008 г.; / Компьютерра Online/ http://offline.computerra.ru/offline/2007/686/319082/ .

3. Борьба с киберпреступностью по российскому рецепту: Лента.Ру. Издание Rambler Media Group / http://lenta.ru/news/2007/05/18/cyber/.

4. Дейт К. Руководство по реляционной СУБД DB2/ Пер. с англ. и предисл. М.Р. Когаловского. – М.: Финансы и статистика, 1988.– 320 с.

5. Корт С.С. Теоретические основы защиты информации: Учеб. пособие. – М.: Гелиос АРВ, 2004. – 240 с.

6. Теория и практика обеспечения информационной безопасности / Под ред. П.Д. Зегжды – М.: Яхтсмен, 1996. – 192 с.

7. Bell D.E., LaPadula L.J. Secure Computer System: Mathematical Foundation, ESD-TR-73-278. Vol. 1. MITRE Corporation.

8. McLean J. Secure models // In J. Marciniak, editor, Encyclopedia of Software Engineering. – Wiley Press, 1994.

9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учеб. для вузов. – 3-е изд. –СПб.: Питер, 2007. – 960 с.

10. Gardner W.D. Author of Grosch's Law Going Strong At 87: TechWeb Technology News: tech-web.com/wire/ networking / 160701379/

11. Муллер А.А., Кучеров М.М. Проблема доступности в модели информационной безопасности // Современные проблемы информатизации в анализе и синтезе технологических и программно-телекоммуникационных систем: Сб. тр. – Вып. 13 / Под ред. О.Я. Кравца. – Воронеж: Научная книга, 2008. – С. 375–385.

Ларченко Марина Владимировна
Институт космических и информационных технологий Сибирского федерального университета (ИКИТ СФУ)
Магистр техники и технологий по направлению «Информационная безопасность»,
аспирант кафедры «Информационная безопасность».

Кучеров Михаил Михайлович
Институт космических и информационных технологий Сибирского федерального университета (ИКИТ СФУ)
К.ф.-м., доцент, докторант СФУ
Эл. почта: kucherov@akadem.ru.

M.V. Larchenko, M.M. Kutcherov

Universal identification – the important means of struggle with cybercrime

Increasingly, organizations are developing sophisticated computing systems on whose services they need to place great trust. In different circumstances the focus will be on differing properties of such services. Simultaneous consideration of availability and integrity provides a very convenient means of subsuming these various concerns within a single conceptual framework, where necessity of the universal identification system is considered and the possible variant of its support is offered on the basis of various models of access.