РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ДОКЛАД

на тему «Идентификация и аутентификация. Управление доступом.»

дисциплина: Информационная безопасность

Студентка: Пономарева Л. М.

Группа: НПИбд-02-19

МОСКВА

2022 г.

Содержание

Введение

На современном этапе развития общества информация выступает как форма собственности, и следовательно, имеет определенную ценность. Чтобы подчеркнуть роль информации в обществе, говорят об «информационном обществе». В связи с этим, вопрос информационной безопасности в современном обществе стоит весьма остро.

В информационных системах рассматривают три основных вида угроз [1]:

1) Угроза нарушения конфиденциальности реализуется в том случае, если информация становится известной лицу, не располагающему полномочиями доступа к ней.
2) Угроза нарушения целостности реализуется при несанкционированном изменении информации, хранящейся в информационной системе или передаваемой из одной системы в другую.
3) Угроза нарушения доступности (отказа служб) реализуется, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы.

Одним из видов угроз нарушения конфиденциальности является несанкционированный доступ к информации [2]. Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности: организационные, технологические (или инженерно-технические), правовые, финансовые, морально-этические (или социально-психологические).

Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации, о которых далее и пойдет речь.

Идентификация и аутентификация

Одной из важных задач обеспечения защиты от НСД является использование методов и средств, позволяющих одной (проверяющей) стороне убедиться в подлинности другой (проверяемой) стороны.

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности. Идентификация и аутентификация — это первая линия обороны информационного пространства организации [3].

С каждым зарегистрированным в компьютерной системе субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов. Эту информацию называют идентификатором субъекта. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным. Прежде чем получить доступ к ресурсам компьютерной системы, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию и аутентификацию.

Определения

Идентификация — это процедура распознавания пользователя по его идентификатору (имени). Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация — процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией.

Методы аутентификации

I. Парольная аутентификация

Главное достоинство парольной аутентификации - простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности [3].

Рассмотрим причины.

Чтобы пароль был запоминающимся, пользователи его зачастую делают простым. Однако простой пароль нетрудно угадать, особенно если знать пристрастия пользователя.

Иногда пароли с самого начала не хранятся в тайне, так как имеют стандартные значения, указанные в документации, и далеко не всегда после установки системы производится их смена.

Ввод пароля можно подсмотреть.

Пароль можно угадать "методом грубой силы", используя, скажем, словарь. Если файл паролей зашифрован, но доступен для чтения, его можно скачать к себе на компьютер и попытаться подобрать пароль, запрограммировав полный перебор.

Тем не менее, следующие меры позволяют значительно повысить надежность парольной защиты:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

II. Аутентификация с помощью биометрических данных

Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик. К числу физиологических характеристик принадлежат особенности отпечатков пальцев, сетчатки и роговицы глаз, геометрия руки и лица и т.п. К поведенческим характеристикам относятся динамика подписи (ручной), стиль работы с клавиатурой. На стыке физиологии и поведения находятся анализ особенностей голоса и распознавание речи [3].

Биометрией во всем мире занимаются очень давно, однако долгое время все, что было связано с ней, отличалось сложностью и дороговизной. В последнее время спрос на биометрические продукты, в первую очередь в связи с развитием электронной коммерции, постоянно и весьма интенсивно растет. Это понятно, поскольку с точки зрения пользователя гораздо удобнее предъявить себя самого, чем что-то запоминать. Спрос рождает предложение, и на рынке появились относительно недорогие аппаратно-программные продукты, ориентированные в основном на распознавание отпечатков пальцев.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (называемый биометрическим шаблоном) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных.

К достоинствам данного метода аутентификации можно отнести его удобство для пользователя. Но говоря о недостатках нельзя забыть о его опасности, любая "пробоина" для биометрии оказывается фатальной. Пароли, при всей их ненадежности, в крайнем случае можно сменить. Утерянную аутентификационную карту можно аннулировать и завести новую. Палец же, глаз или голос сменить нельзя. Если биометрические данные окажутся скомпрометированы, придется как минимум производить существенную модернизацию всей системы.

III. Аутентификация с помощью физических носителей.

Является более защищенным, чем предыдущий подход.

Чтобы установить пользователя, требуется просто вставить в устройство тот или иной физический носитель.

Авторизация с помощью токена происходит следующим образом. Сначала человек запрашивает доступ к серверу или защищенному ресурсу. Запрос обычно включает в себя ввод логина и пароля. Затем сервер определяет, может ли пользователь получить доступ. После этого сервер взаимодействует с устройством: ключ, телефон, USB или что-то ещё. После проверки сервер выдает токен и отправляет пользователю. Токен находится в браузере, пока работа продолжается.

Управление доступом

С традиционной точки зрения средства управления доступом позволяют специфицировать и контролировать действия, которые субъекты (пользователи и процессы) могут выполнять над объектами (информацией и другими компьютерными ресурсами).

Управление доступом можно разделить на физическое и логическое УД.

1) Физическое управление доступом.

Контроль и управление доступом на физические объекты в общем случае рассматриваются как комплекс мероприятий, направленных на ограничение и санкционированное перемещение людей, предметов, транспорта в помещениях, зданиях, сооружениях и по территории объектов.

2) Логическое управление доступом.

Цель управления доступом – это ограничение операций, которые может проводить легитимный пользователь (зарегистрировавшийся в системе). Управление доступом указывает что конкретно пользователь имеет право делать в системе, а также какие операции разрешены для выполнения приложениями, выступающими от имени пользователя [3].

Таким образом управление доступом предназначено для предотвращения действий пользователя, которые могут нанести вред системе.

Модели управления доступом [4]:

- Дискреционное управление доступом
- Мандатное управление доступом
- Ролевое управление доступом

I. Дискреционное управление доступом.

Избирательное управление доступом (англ. discretionary access control, DAC) — управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

Эта модель называется дискреционной (избирательной), т.к. управление доступом основано на решениях владельца. Часто руководители подразделений являются владельцами данных в рамках своих подразделений. Будучи владельцами,

они могут решать, кому следует, а кому не следует иметь доступ к этим данным.

Рассмотрим формальную постановку задачи управления доступом в традиционной трактовке. Имеется совокупность субъектов и набор объектов. Задача логического управления доступом состоит в том, чтобы для каждой пары "субъект-объект" определить множество допустимых операций и контролировать выполнение установленного порядка.

Отношение "субъекты-объекты" можно представить в виде матрицы доступа, в строках которой перечислены субъекты, в столбцах - объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия и разрешенные виды доступа (Таблица 1).

Таблица 1 Матрица доступа

	OS	Accounting Program	Accounting Data	Insurance Data	Payroll Data
Alice	rx	rx	r	-	-
Bob	rx	rx	r	rw	rw
Sam	rwx	rwx	rw	rw	rw

Матрицу доступа, ввиду ее разреженности (большинство клеток - пустые), неразумно хранить в виде двухмерного массива. Обычно ее хранят по столбцам, то есть для каждого объекта поддерживается список "допущенных" субъектов вместе с их правами. Некоторые проблемы возникают только при удалении субъекта, когда приходится удалять его имя из всех списков доступа; впрочем, эта операция производится нечасто.

При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

II. Мандатное управление доступом

Мандатное управление доступом (англ. Mandatory access control, MAC) — разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации такого уровня конфиденциальности.

Все субъекты и объекты системы должны быть однозначно идентифицированы;

Каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации. Чем важнее объект или субъект, тем выше его метка критичности. Поэтому наиболее защищенными оказываются объекты с наиболее высокими значениями метки критичности;

Каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

В том случае, когда совокупность меток имеет одинаковые значения, говорят, что они принадлежат к одному уровню безопасности.

Основное назначение полномочной политики безопасности - регулирование доступа субъектов системы к объектам с различным уровнем критичности и предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

III. Ролевое управление доступом

Управление доступом на основе ролей (англ. Role Based Access Control, RBAC) — развитие политики избирательного управления доступом, в котором права доступа субъектов системы на объекты группируются с учётом специфики их применения, образуя роли.

Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли (Рис. 1). Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

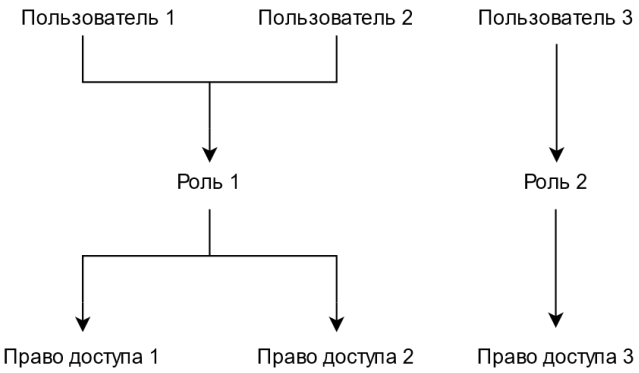

Рис. 1 Ролевое управление доступом

Между ролями может быть определено отношение частичного порядка, называемое наследованием. Если роль r1 является наследницей r2, то все права r2 приписываются r1, а все пользователи r1 приписываются r2.

Отношение наследования является иерархическим. В общем случае наследование является множественным, то есть у одной роли может быть несколько предшественниц.

Ролевой доступ можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов.

Заключение

С развитием технологий совершенствуются как методы защиты нашей информации, так и способы эту информацию скомпрометировать, поэтому единого ответа на вопрос, как защитить себя от информационных атак, не существует. Есть множество методов защиты информации и на примере тем аутентификации и идентификации, и управления доступом мы убедились в этом.

Так, среди множества средств аутентификации мы выделили парольную, которая охарактеризована как привычная и довольно удобная, но слабая, если не соблюдать правила безопасности, и наоборот неудобная и довольно защищённая, если эти правила соблюдать; аутентификацию с физическими носителями - надежную и не совсем удобную; аутентификацию с помощью биометрических данных - самую удобную для пользователей, но при этом сопряженная с большим риском. Так что выбор средства аутентификации полностью зависит от тех характеристик, которые важны в конкретной системе.

Методы управления доступом разделены по степени гибкости метода. Так, дискреционное управление доступом позволяет легко выполнить требование о гранулярности прав с точностью до пользователя. Безусловно, списки являются лучшим средством произвольного управления доступом. Но при большом количестве пользователей ролевое управление доступом становится крайне сложными для администрирования. Число связей в ней пропорционально произведению количества пользователей на количество объектов. Тогда на помощь приходят мандатное и ролевое управление, которые группируют пользователей по уровню доступа или по ролям.

Литература

1. Вострецова Е. В. Основы информационной безопасности — Екатеринбург: Изд-во Уральского ун-та, 2019.— 208 с. – URL: https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf (дата обращения: 17.10.2022).
2. Девянин П.Н. Теоретические основы компьютерной безопасности — Москва: Радио и связь, 2000.— 192 с.
3. Галатенко, В. А. Основы информационной безопасности: учебное пособие / В. А. Галатенко. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 266 с. — ISBN 978-5-4497-0675-1. — URL: https://profspo.ru/books/97562 (дата обращения: 16.10.2022).
4. Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем: учебное пособие / Щеглов А.Ю. — Санкт-Петербург: Университет ИТМО, 2014. – URL: https://books.ifmo.ru/file/pdf/1764.pdf (дата обращения: 16.10.2022).