Тема 5. Идентификация и аутентификация

5.1. Общие сведения

Первые шаги процесса обеспечения безопасности, известны как идентификация и аутентификация **(identification and authentication – I&A)**.

I&A является необходимым шагом, от которого зависит вся безопасность базы данных. Следовательно, проектные решения I&A очень важны.

В сегодняшнем мире большая часть мер по идентификации и аутентификации выполняется на сервере приложений или в самом приложении.

Процесс **I&A** можно свести к следующим трем шагам:

1. Пользователь предоставляет базе данных свои идентификационные данные. Например, он может ввести свое имя пользователя.

2. Пользователь доказывает подлинность предоставленных им идентификационных данных. К примеру, он может предложить значение пароля. Этот пароль будет проверен базой данных для определения того, является ли он подлинным для представленного имени пользователя.

3. Если пароль правильный, база данных принимает решение, что предоставленным идентификационным данным можно доверять. После этого, опираясь на предъявленные идентификаци-онные данные, база данных определяет, какие привилегии и авторизации имеет этот пользователь.

Как правило, люди тратят большую часть своего времени и усилий по созданию защиты на реализацию процессов, относящихся к третьему шагу.

Первые два шага важны, потому что они образуют фундамент безопасности; без них невозможно сделать третий шаг.

Первый шаг принято называть идентификацией.

Второй шаг — это аутентификация.

При проектировании и реализации решений защиты часто упускают из виду один факт: **защита не может базироваться на анонимности.**

Сначала нужно идентифицировать себя. Чтобы без риска проделать эту операцию, требуется аутентифицироваться, т.е. доказать, что ты на самом деле тот, за кого себя выдаешь.

Если база данных или приложение не знает, с кем приходится иметь дело, оно не может выдать соответствующую авторизацию, применить соответствующие привилегиям методы контроля доступа и провести аудит действий пользователя.

Это кажется очевидным, но в бесчисленном множестве проектов приложений об этом моменте забывают.

Большая часть, если не все, меры безопасности основываются на знании того, кем является пользователь.

В качестве подтверждения этого принципа рассмотрим приложение, которое реализует электронную почту, и все письма хранятся в одной базе данных.

Политика безопасности для такой электронной почты заключается в том, что пользователь может получить доступ только к собственному почтовому ящику.

Как можно реализовать меры защиты, если неизвестно, кто такой текущий пользователь?

Это просто невозможно.

Ясно, что необходимо выполнить идентификацию пользователя.

Затем должна быть проведена аутентификация для гарантии того, что пользователь не пытается играть чужую роль, выдавая себя за другого пользователя.

Если аутентификация не обеспечена или обеспечена плохо, все процессы защиты приложения и базы данных окажутся бессмысленными.

Приложения и база данных не смогут запретить выполнение нечестным пользователем своих действий (в нашем случае, получение доступа к чужой почте), так как приложение и база данных будут считать, что это авторизованный пользователь.

5.1. Методы идентификации

Идентификацией называется процесс как можно более точного и бесспорного опознания индивидуума.

Идентификация является частью повседневной жизни.

Приходится идентифицировать себя:

- на работе,
- при разговоре по телефону,
- в письмах по электронной почте;

мы так часто идентифицируем себя, что иногда уже, вероятно, сами не замечаем, как делаем это.

Имеется множество форм идентификации:

- мы сами,
- наши фотографии,
- отпечатки пальцев,
- индивидуальный номер служащего,
- номер банковского счета или номера кредитных карточек,
- номер постоянного пассажира авиакомпании,
- номер карты социального обеспечения
- и, конечно, имя пользователя.

Все перечисленные выше реквизиты могут представлять пользователя в процессе идентификации.

Сегодня имеется множество форм идентификации и много способов идентифицировать себя.

Знание того, для чего необходимо идентифицировать себя и что (или кого) вы идентифицируете, помогает выбрать метод идентификации.

Методы идентификации делятся на две категории:

- **поставляемые пользователем идентификационные данные;**
- и **технологическая идентификация.**

5.1.1. Поставляемые пользователем идентификационные данные

Обращение к пользователям с просьбой предоставить свои идентификационные данные сегодня является наиболее распространенным методом идентификации.

В большинстве компьютерных приложений идентификация базируется на имени пользователя.

Банк, вероятно, предпочитает идентифициро-вать пользователя по номеру (номерам) его счета (счетов), а излюбленная авиакомпания преобразовала вас в последовательность алфавитно-цифровых символов.

Все эти имена, названия и номера служат одной-единственной цели — **определить, кто вы такой.**

В любом случае ответственность за предоставление точной информации несет пользователь.

Это важно, потому что знание верных идентификационных данных обеспечивает некоторую защищенность.

Например, нельзя снять деньги с несуществующего банковского счета

Маловероятно, что кому-то удастся войти в базу данных, не предоставив ей допустимого имени пользователя.

Для пытающихся проникнуть в систему хакеров хорошим началом могло бы стать получение списков допустимых пользователей системы.

Довольно полезным может оказаться сокрытие имени пользователя или выбор таких идентификаторов, которые не служат указанием на привилегии пользующегося ими лица.

Имя пользователя «Administrator» (администратор) невольно ассоциируется с высокими привилегиями и, следовательно, является более ценной мишенью для атаки хакера, чем нейтральное имя «User 125» (пользователь 125).

Однако проектирование реализации обеспечения безопасности, основанной исключительно на знании какого-то идентификатора — скажем, имени пользователя или номера счета, — является довольно рискованным делом, поскольку может оказаться несложным угадать, предсказать или получить правильные идентификационные данные из другого источника.

Широко распространенной технологией аутентификации является использование паролей. Естественно ожидать, что технология подбора паролей также находится на достаточно высоком уровне развития.

Можно выделить следующие методы подбора паролей пользователей.

1. Тотальный перебор. В этом случае злоумышленник последовательно опробует все возможные варианты пароля.

Для паролей длиннее **шести** символов во многих случаях данный метод может быть признан **неэффективным.**

2. Тотальный перебор, оптимизированный по статистике встречаемости символов.

Разные символы встречаются в паролях пользователей с разной вероятностью.

Например, вероятность того, что в пароле пользователя встретится буква **«а»,** гораздо выше вероятности того, что в пароле присутствует символ **«л».**

Согласно различным исследованиям, статистика встречаемости символов в алфавите паролей близка к статистике встречаемости символов в естественном языке.

При практическом применении данного метода злоумышленник вначале опробует пароли, состоящие из наиболее часто встречающихся символов, за счет чего время перебора существенно сокращается.

Иногда при подборе паролей используется не только статистика встречаемости символов, но и статистика встречаемости ***биграмм*** и ***триграмм*** — комбинаций двух и трех последовательных символов соответственно.

Для подбора паролей по данному методу в разное время было написано множество программ, в основном ориентированных на взлом операционных систем.

Можно выделить две базовые технологии:

- явное опробование последовательно генерируемых паролей подачей их на вход подсистемы аутентификации;
- расчет значения хэш-функции и ее последующего сравнения с известным образом пароля.

Особенность второго варианта состоит в том, что *при известном образе пароля* задача эффективно распараллеливается и может решаться без активного взаимодействия с атакуемой системой.

3. Тотальный перебор, оптимизирован-ный с помощью словарей

В большинстве случаев пароли пользователей представляют собой слова английского или русского языка.

Поскольку пользователю гораздо легче запомнить осмысленное слово, чем бессмысленную последовательность символов, пользователи предпочитают применять в качестве паролей осмысленные слова. При этом количество возможных вариантов пароля резко сокращается.

Словарь С. И. Ожегова содержит около 60000 слов, объем словаря среднестатистического пользователя заметно меньше.

При использовании данного метода подбора паролей злоумышленник вначале опробует в качестве паролей все слова из словаря, содержащего наиболее вероятные пароли.

В сети Интернет представлено множество подобных словарей, адаптированных для различных стран и групп пользователей.

Если подбираемый пароль отсутствует в словаре, злоумышленник, как правило, может опробовать всевозможные комбинации слов из словаря, слова из словаря с добавленными к началу или к концу одной или несколькими буквами, цифрами и знаками препинания и т. д.

«Хитрости» с написанием слов в обратном порядке в иной раскладке клавиатуры также не являются чем-то новым.

Обычно данный метод используется в комбинации с предыдущим.

4. Подбор пароля с использованием знаний о пользователе. Человек склонен использовать пароли, которые легко запоминаются.

Многие пользователи, чтобы не забыть пароль, выбирают в качестве пароля свое имя, фамилию, дату рождения, имена детей, любимых (в том числе принятые в узком кругу), номера телефонов и автомобилей и т. д.

Часто выбираемые и вскрываемые группы паролей

Тематические группы паролей	Процент частоты выбора	Процент раскрываемости
Имена, фамилии и производные	**22,2**	**54,5**
Интересы (хобби, спорт, музыка)	**9,5**	**29,2**
Даты рождения, знаки зодиака свои и близких, их комбинации	**11,8**	**54,5**
Адрес жительства, место рождения	**4,7**	**55,0**
Последовательность клавиш, повтор символа	**14,1**	**72,3**
Номера телефонов	**3,5**	**66,6**
Номера документов (паспорт, пропуск, удостоверение)	**3,5**	**100**

аутентификации

Хорошо известно, что некоторая категория мужчин склонна использовать в качестве (не отображаемого на дисплей) пароля ненормативную лексику, а определенная категория женщин часто использует уменьшительно-ласкательные имена домашних животных.

В этом случае, если злоумышленник хорошо изучил пользователя, ему, как правило, достаточно провести меньше сотни опробований.

Уязвимость паролей

60% респондентов готовы обменять данные о пароле на подарочный купон стоимостью **5 фунтов**

45% для доступа к электронной почте, социальным сетям и даже финансовым сайтам используют пароли, состоящие из:

- **даты рождения**
- **девичьей фамилии матери**
- **клички любимого животного**

исследование Symantec и moneysupermarket.com

аутентификации

Преимущество поставляемой пользователем идентификации состоит в том, что идентификатор (в нашем случае, имя пользователя) является достаточно гибким.

Это позволяет администраторам создавать интуитивно понятные идентификаторы, которые пользователи могут легко запомнить.

Например, можно создать имя пользователя по первой букве его имени и фамилии (для меня — автора этой книги — получится dknox).

Но **оборотной стороной** преимущества является его слабость.

Идентификаторы, которые легко угадать или предсказать, могут ослабить систему защиты.

Уязвимость паролей

исследование британской сети Comet

30% опрошенных сообщают свои пароли коллегам по работе

11% используют в качестве пароля слово password

Неэффективность паролей

- до 50% обращений в службу поддержки вызваны проблемами с паролями

  источник: Lenovo

- $25-50 – стоимость исполнения одного обращения в службу поддержки

  источник: Compulenta

5.1.2. Технологическая идентификация

Технология также вносит свой вклад в выбор способов идентификации. Мы рассмотрим:

- а) биометрические,
- б) компьютерные и
- в) цифровые идентификационные данные.

а) Биометрические идентификационные данные

Термином ***«биометрические»*** принято называть биологические характеристики людей, которые можно измерять для учета и определения различий между ними.

Мы часто применяем биометрику для идентификации людей.

Наш мозг использует распознавание по лицу, когда мы встречаем знакомых людей, и по голосу, когда мы отвечаем на телефонные звонки.

В настоящее время множество компаний пытаются довести до нужной степени зрелости разнообразные биометрические технологии.

Распознавание по лицу, сканирование радужной оболочки глаза, геометрия руки и считывание отпечатков пальцев — эти технологии входят в число наиболее популярных.

Биометрика во многих отношениях является просто идеальной.

Пользователи не могут забыть свои показатели, и их практически невозможно подделать.

Кража биометрических значений также маловероятна, хотя существует риск, связанный с хищением цифрового представления биометрических данных.

Если такое произойдет, имеется шанс, что кто-то сможет выдать себя за другого, скопировав и воспроизведя биометрическую подпись, или как-то изменить метаданные, указывающие, чья это биометрика.

Часто возникает путаница относительно применения биометрики.

Это связано с тем, что биометрические данные могут быть использованы как в процессе идентификации, так и в процессе аутентификации.

При биометрической идентификации биометрическая информация считается уникальной и может быть использована для точной идентификации лица, представившего эти данные.

Это отличается от предоставляемой пользо-вателем информации, так как пользователи не говорят системе о том, кто они такие; система идентифицирует их автоматически.

Заметьте, что это не аутентификация, а всего лишь идентификация.

Биометрическая аутентификация предпола-гает сравнение биометрической подписи с ее образцом для доказательства (или опровер-жения) их идентичности (это значит, что идентификационные данные уже известны).

б) Компьютерные идентификационные данные

В компьютерных средах идентификационные данные могут базироваться на различных нестандартных элементах, например на имени компьютера, физическом сетевом адресе (так называемый MAC-адрес — уникальный идентификатор сетевой карты компьютера), логическом сетевом адресе (IP-адрес) или на отличительном признаке какого-либо другого прибора, который можно присоединить к компьютеру.

Адреса и домены IP часто используются в архитектурах защиты.

Доступ к адресу или домену либо разрешается, либо запрещается.

Межсетевые экраны и различные технологии сетевой маршрутизации довольно сильно зависят от MAC-адресов и IP-адресов.

Серверы приложений и защита базы данных также применяют IP-адреса для обеспечения дополнительных уровней защиты.

в) Цифровые идентификационные данные

Другой превалирующей формой идентификации является идентификация посредством цифрового представления или цифровых идентификационных данных.

Например, сегодня можно встретить цифровые сертификаты, используемые как часть инфраструктуры открытых ключей (Public Key Infrastructure, PKI).

Эта инфраструктура предлагает для защиты много возможностей, в том числе идентификацию, аутентификацию, шифрование и строгое выполнение обязательств.

Цифровые сертификаты популярны не только потому, что они построены на стандартах, но и потому, что в них содержится дополнительная информация, которую можно использовать для управления безопасностью.

К примеру, доступ пользователя к данным может быть основан на сочетании имени пользователя и названии организации и ее адреса.

Для идентификации пользователей цифровые сертификаты обычно устанавливаются в web-браузерах пользователей.

Кроме того, они могут быть встроены в такие устройства, как смарт-карты.

Для защиты цифровых идентификационных данных пользователю может быть предложено ввести PIN или пароль для разблокирования сертификата.

5.2.Кризис идентификационных данных

Одной из проблем, возникающих при реализации эффективной защиты, является организация защиты идентификационных данных.

Если защита опирается на надлежащую идентификацию, естественно предположить, что она является центральным моментом процесса защиты в областях высокого риска.

Скомпрометируйте процесс установления тождественности, и у вас будет скомпрометирована целостность защиты приложения или базы данных, или и того и другого вместе.

5.2.1. Получение доступа путем обмана

Одним из наиболее успешных способов сокрушить систему защиты является «игра на стороне защиты».

Вместо того чтобы пытаться преодолеть средства контроля доступа и обойти используемые меры аудита, можно заявить, что вы являетесь кем-то другим.

Маскировка под легального пользователя, или ***спуфинг*** (от английского слова **spoofing**, означающего получение доступа путем обмана), является цифровым эквивалентом кражи идентификационных данных.

«Кто-то еще» может стать либо привилегированным пользователем, либо даже обычным пользователем.

В обоих случаях спуфинг способен привести к катастрофическим результатам.

Существует бесчисленное количество способов замаскироваться под кого-то другого, но главным моментом здесь является то, что идентификационные данные пользователя оказываются критичными для процесса защиты.

Уверенность в том, что идентификационные данные защищены надлежащей аутентификацией, реализацией и мониторингом, имеет огромное значение для обеспечения эффективной защиты в целом.

5.2.2. Кража идентификационных данных

Кража идентификационных данных является все усиливающейся проблемой, свирепствующей в наши дни.

Этот термин описывает злоупотребление и искажение информации, связанной с одним лицом, для предоставления преимуществ другому лицу.

По многим причинам это чрезвычайно разрослось в последние годы.

Наша задача состоит в том, чтобы не умножать эту проблему.

Защита идентификационных данных пользователей может быть такой же важной задачей, как и защита тех данных, к которым можно получить доступ с их помощью.

Зная о человеке такую малость, как номер его карты социального обеспечения и дата рождения, кто-то может оказаться в состоянии украсть его идентификационные данные и с их помощью открыть новый счет в банке, подать заявление о ссуде, покупать дорогие вещи и делать множество других противозаконных действий — и все это под маской другого лица.

К чему весь этот разговор?

Да к тому, что из баз данных и плохо спроектированных приложений вытекает много информации, которую можно использовать для создания фальшивых идентификационных данных.

Неправильно выбранный идентификатор может оказаться катализатором для похищения идентификационных данных.

Необходимо тщательно выбирать идентификаторы.

Конфиденциальная и имеющая отношение к личной жизни информация не должна использоваться для представления идентификационных данных пользователей.

5.3. Аутентификация

Технически все, что требуется для того, чтобы система применила авторизацию, принудительно выполнила контроль доступа и аудит, — это предоставить ей свои идентификационные данные.

Но, к сожалению, мир состоит не только из честных людей. Поэтому идентификационные данные должны сопровождаться чем-то еще, что подтверждает их легитимность.

Чтобы идентификация работала успешно, должен иметься процесс, доказывающий, что идентифицирующее себя лицо является именно тем, кем оно себя объявило.

Этот процесс и называется аутентификацией.

5.3.1. Методы

Методы аутентификации относятся к одной из следующих трех категорий:

Что-то такое, что вы знаете, например пароль или персональный идентификационный номер (PIN). Для компьютерных систем пароли являются наиболее часто используемым методом аутентификации, потому что они просты (и дешевы) в реализации и их легко сопровождать.

Что-то такое, чем вы обладаете, скажем, карта с электронным ключом, сертификат X.509, смарт-карта, кредитная карта или лицензионный ключ программного обеспечения. Эти средства обладают разными возможностями в поддержке идентификационных данных пользователей.

Иногда аутентификация используется только для того, чтобы показать, что вы являетесь легитимным (законным) объектом.

Например, карточка для прохода в здание подтверждает, что вы являетесь служащим компании, а лицензионный ключ показывает, что вы являетесь платежеспособным подписчиком программного обеспечения.

Что-то из того, чем вы являетесь, или биометрические данные. Отпечатки пальцев, распознавание по лицу, сканирование радужной оболочки глаза, а со временем, может быть, и анализ ДНК — все эти методы могут быть использованы компьютерными приложениями для аутентификации пользователей.

Методы ***«что-то, чем вы обладаете»*** и ***«что-то, чем вы являетесь»*** считаются более сильными формами аутентификации, чем методы типа «что-то, что вы знаете».

Пароли можно угадать, и поэтому они считаются слабым методом аутентификации.

Сфальсифицировать сертификат X.509 (что-то, чем вы обладаете) или продублировать биометрические показатели (что-то, чем вы являетесь) далеко не так просто.

Следовательно, аутентификация с помощью цифровых сертификатов, электронных ключей и биометрики считается сильной.

Сильная и слабая аутентификация

Обычно термин «сильная аутентификация» подразумевает, что аутентифицирующий признак нельзя с легкостью фальсифицировать, подделать или догадаться о его значении.

У технологий аутентификации имеются различные возможности в выполнении своих задач.

Одной из метрик для определения силы метода аутентификации является то, насколько трудно его сфальсифицировать.

Из сказанного выше вовсе не следует, что нельзя использовать для аутентификации пароли.

Существуют сильные и слабые пароли.

Сильные пароли состоят из большого количества символов, поэтому их сложно разгадать; слабые пароли легко угадать или предсказать — например, в случае применения в качестве пароля имени пользователя или хорошо известных строк типа «password».

Слабые пароли не должны использоваться.

Многофакторная аутентификация

Объединение нескольких методов аутентификации может дать аналогичный эффект и рассматривается как очень удачное решение.

Например, сильным методом аутентификации считается обладание объектом в сочетании со знанием пароля или PIN.

Для того чтобы владельцы банковского счета могли снять с него наличные деньги, они должны иметь кредитную карту и знать связанный с ней PIN.

В этом примере карта играет две роли:

во-первых, она используется для идентификации (ведь на ней записан номер вашего счета в банке),

и, **во-вторых**, она является одним из факторов аутентификации.

Простого владения картой еще недостаточно, так как карта может быть потеряна или украдена.

Вообще говоря, чем больше методов используется для аутентификации, тем больше гарантий ее надежности.

Две формы (или ***двухфакторная аутентификация)*** лучше, чем одна, а три формы (или ***многофакторная аутентификация)*** лучше, чем две, и так далее.

5.3.2. Лучшие методы аутентификации

Важно надежно защищать не только конфиденциальные идентификационные данные пользователя, но и конфиденциальные данные для аутентификации пользователя.

Защита аутентификации означает не только защиту того места, где хранится аутентификатор (т. е. тот объект, с помощью которого производится аутентификация), но и организацию защиты аутентификатора при его пересылках.

Можно применить сильную аутентификацию и проиграть битву с хакером, потому что используемый вами канал аутентификации или способ хранения полномочий аутентификации (**credentials** — учетная запись пользователя с параметрами доступа, сформированными после его успешной аутентификации) не является достаточно защищенным.

Так, биометрическая аутентификация считается надежной и сильной; однако для компрометации биометрической аутентификации можно и не делать пластическую операцию, достаточно скопировать, а затем воспроизвести биометрическую подпись или изменить метаданные, указывающие, кому именно принадлежат те или иные биометрические данные.

Шифрованные аутентификаторы

Шифрование является важным средством защиты аутентификаторов.

Предположим, что пользователь аутентифицируется с помощью отпечатков пальцев.

Если эталонные отпечатки пальцев пересылаются по сетевому каналу в незашифрованном виде, хакер, использующий сетевой анализатор пакетов, может записать и идентификационные данные, и оцифрованные отпечатки пальцев пользователя.

Позже хакер может воспроизвести или передать перехваченные идентификационные данные и отпечатки пальцев, тем самым успешно сымитировав настоящего пользователя.

При шифровании сети для каждого коммуникационного сеанса применяется новый ключ.

Тот ключ, который был использован в первом (перехваченном) сеансе, никогда не будет повторно применен впоследствии.

Поэтому воспроизведение перехваченных зашифрованных биометрических данных не сработает, если используются стандартные протоколы шифрования типа SSL.

Аутентификаторы подвергаются большому риску, потому что они часто пересылаются по компьютерным сетям.

Шифрование сетевого трафика является хорошей защитной мерой против копирования и воспроизведения аутентификаторов.

Оптимальная безопасность достигается путем шифрования всего сетевого потока.

Шифрование защищает не только аутентификаторы, но и идентификационные данные пользователей, размещаемые ими запросы и возвращаемые результаты.

Точно так же необходимо обеспечить безопасное хранение аутентификаторов.

Часто аутентификаторы хранятся в зашифрованном формате для поддержания их конфиденциальности

Хешированные аутентификаторы

Если для аутентификации используются пароли, они не должны храниться в незашифрованном виде.

Естественным решением представляется шифрование, но оно не годится.

Шифрование, которое является процессом преобразования незашифрованного текста в не поддающиеся расшифровке данные, подразумевает наличие ***дешифрования*** — процесса преобразования зашифрованного текста обратно в незашифрованный текст.

Золотое правило паролей гласит, что они не должны разглашаться — **никогда и никому**.

Шифрование паролей, которое потенциально допускает их расшифровку, может привести к тому, что разглашение все-таки произойдет.

Для решения этой проблемы используется технология, называемая хешированием.

Хеширование принимает незашифрованный текст и конвертирует его в не поддающийся расшифровке текст.

Однако, в отличие от шифрования, не существует способа определить по хешированному значению, из чего оно было получено.

Из-за этого свойства хеширование называют ***однонаправленной функцией.*** Еще одним важным свойством хеширования является то, что при одинаковых входных данных всегда будут получаться одинаковые выходные данные.

5.4. Ассоциирование пользователей со схемами базы данных

Изучив различные методики I&A, мы должны принять решение, как представлять базе данных наших конечных пользователей (или пользователей приложения). От этого зависит общая безопасность приложения и тех данных, с которыми оно имеет дело.

Когда речь заходит о построении приложения, следует учитывать, что всего три модели могут быть применены для отображения реальных конечных пользователей на учетные записи базы данных. Каждой из этих моделей присущи свои преимущества и риски. Нередко модели ограничивают, что и как можно сделать в их рамках.

:1. Отображение «один к одному» встречается преимущественно в программах типа клиент/сервер. Это означает, что у каждого конечного пользователя имеется своя учетная запись базы данных, или схема.

:M. Отображение «все на несколько» чаще всего имеет место в web-приложениях. Оно означает, что все конечные пользователи отображаются на несколько различных схем. Каждая учетная запись создается на основании совместно применяемых конечными пользователями привилегий. Все пользователи с одним и тем же набором привилегия подключаются к одной и той же схеме.

:1. Отображение типа «все к одному» является типичным для web-приложений. Приложение подключает всех пользователей к одной и той же схеме. Схема содержит объединение всех привилегий всех подключенных к ней пользователей.

5.4.1. Пользовательские привилегии для уникальных учетных записей базы данных

В зависимости от того, как организован доступ к базе данных и какую роль играет приложение (приложения), в базе данных может иметься либо всего одна учетная запись, либо много учетных записей конечных пользователей, что соответствует модели отображения 1:1.

Выбор этой модели характерен для приложений клиент/сервер и гораздо реже встречается в web-приложениях.

Отображение 1:1 может осуществляться несколькими способами, но основным моментом является то, что здесь имеется прямое отображение каждого пользователя на его индивидуальные свойства (чаще их называют учетной записью) в базе данных.

В простейшем случае пользователь предлагает имя и пароль, которые являются именем пользователя и паролем реальной учетной записи пользователя базы данных.

Альтернативно, приложение может предлагать собственное отображение.

Дело здесь не в том, ***как*** это делается, а в том, ***что*** именно делается.

При создании учетных записей базы данных в режиме 1:1 важно соблюдать принцип минимальных привилегий.

Это значит, что нужно создавать пользователей без каких бы то ни было привилегий, а затем селективно предоставлять им привилегии, требующиеся для выполнения порученной работы.

Отображение 1:1 является особенно критичным для администраторов баз данных и привилегированных пользователей.

Совместное применение привилегирован-ной учетной записи группой пользователей является плохим решением.

Во многих организациях имеется специальная политика, запрещающая совместное использование привилегированных учетных записей, но, тем не менее, подобное практикуется довольно часто. В таких случаях отсутствует подотчетность пользователей.

Отображение 1:1 упрощает задачу обеспечения безопасности базы данных, потому что отличительные свойства пользователя всегда доступны для базы данных; следовательно, пользователь подотчетен базе данных.

Кроме того, многие из средств защиты базы данных оперируют на уровне индивидуальных схем.

Если у каждого пользователя имеется уникальная схема, то база данных может с легкостью применить индивидуальную защиту к соответствующим пользователям на основании их схем.

База данных может с высокой степенью гарантии распознавать конечных пользователей и при этом применять все доступные средства защиты.

5.4.2. Совместно используемые учетные записи базы данных

Принцип минимальных привилегий важен даже в тех случаях, когда пользователи не подключаются непосредственно к базе данных.

Наиболее типичным решением является следующее: пользователь имеет уникальную учетную запись в приложении, которая совместно с другими такими же записями использует одну схему базы данных.

В таком случае существуют два отображения.

Первое отображение, N:M, делит пользователей по разным схемам. Это, как правило, осуществляется с помощью ролей — все пользователи, имеющие одну и ту же роль, будут отнесены к одной и той же схеме.

Важный момент — соблюдение принципа минимальных привилегий.

Это довольно легко сделать, если все пользователи, подключенные к одной схеме базы данных, имеют одинаковые наборы привилегий базы данных, т.е. с точки зрения привилегий все пользователи являются гомогенными.

В таком проекте важной оказывается передача индивидуальных данных пользователей, так как база данных может оказаться не в состоянии провести различия между пользователями, подключенными к одной и той же схеме.

Второе отображение, N:1, подключает всех конечных пользователей к одной схеме базы данных.

Такое отображение весьма сомнительно с точки зрения защиты.

Проблема в том, что базе данных трудно отличать привилегии доступа различных пользователей, так как все они подключены к одной и той же схеме базы данных.

Проверка того, что пользователю доступны только действительно необходимые привилегии, по большей части ложится на приложение.

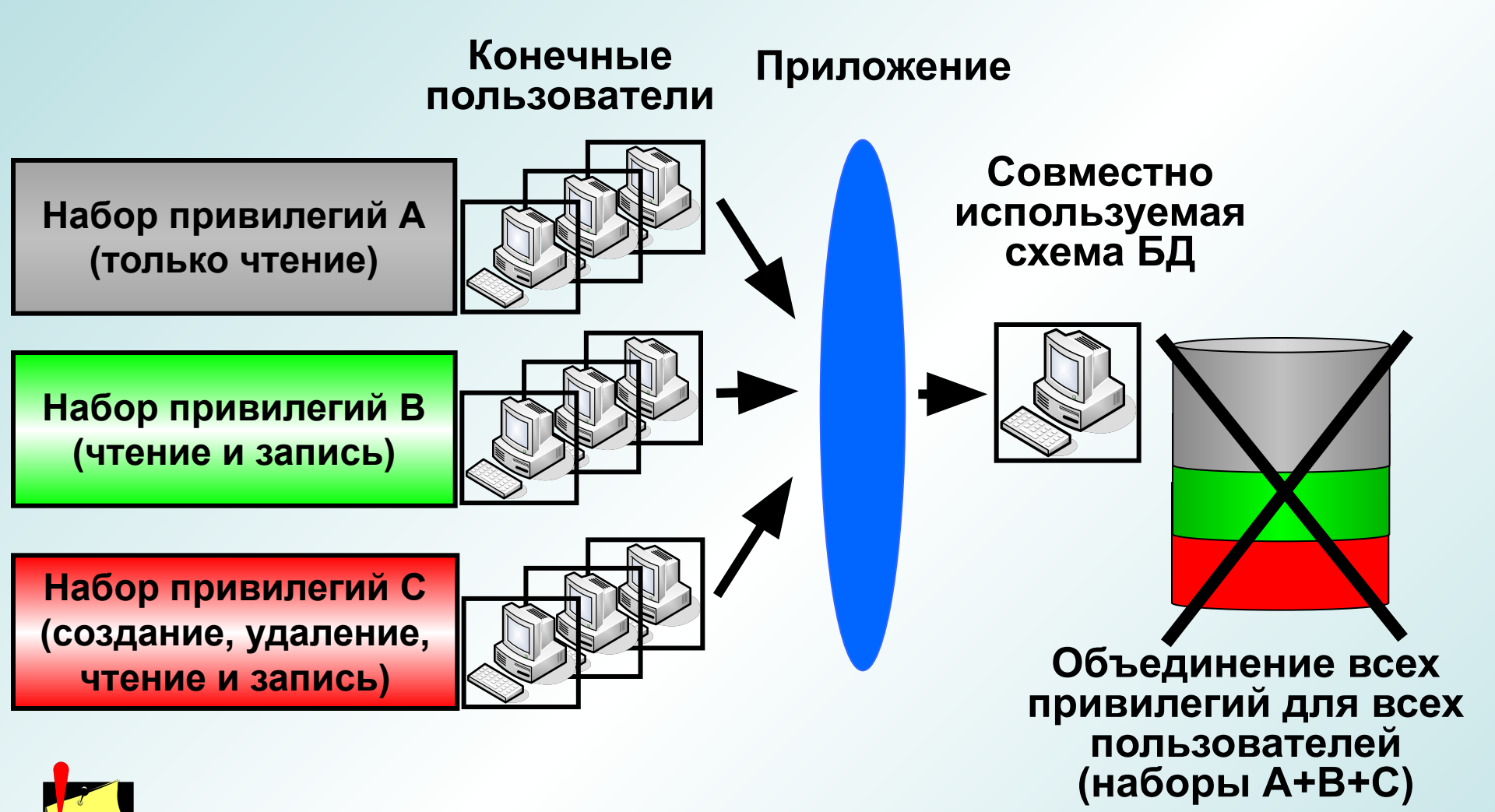
С точки зрения аудита, идентификационные данные пользователей не смогут естественным образом поддерживаться в этом проекте, так что их индивидуальные действия могут быть неотслеживаемыми и нерегулируемыми.

Рассмотрим сценарий, в котором пользова-телям необходимы различные привилегии в рамках одной и той же схемы базы данных.

Предположим, что имеются три группы пользователей:

- одна с доступом только по чтению,
- вторая — с доступом по чтению и записи
- и третья — группа администраторов, которые могут создавать и удалять объекты и, конечно, имеют доступ по чтению и записи.

Если все три эти группы отображаются на одну учетную запись (схему) базы данных, приложение ***обязано*** регулировать, какие привилегии должны быть активизированы, а какие заблокированы, на основании того, что известно о пользователях.



Конечные пользователи с различными наборами привилегий не должны отражаться на одну схему, имеющую полный набор привилегий для всех пользователей

аутентификация

С точки зрения базы данных, у всех пользователей имеются одинаковые привилегии.

Это является нарушением принципов минимальных привилегий и защиты в глубину.

Если защита приложения «проваливается» либо пользователь каким-то образом обходит приложение (т.е. получает непосредственный доступ к данным, минуя приложение), то безопасность может быть нарушена.

При проектировании и построении приложения требуется соблюдение принципа минимальных привилегий.

Одним из способов является изоляция схем для объединения пользователей, обладающих одним набором привилегий.

5.5. Разделение пользователей и данных

Критичным для приложения является гарантированное разделение учетных записей пользователей базы данных и учетных записей данных/приложений.

Владелец данных имеет все привилегии на эти данные.

Если даже пользователи подключаются к этой схеме через приложение, остается высокий риск инцидентов в сфере безопасности.

Другими словами, если пользователь сможет взломать приложение или приложение способно к «самовзлому», пользователь получит полный контроль над каждым элементом данных.

Это относится не только к доступу, но и к таким разрушительным возможностям, как усечение таблиц и удаление объектов.

По этой причине для обеспечения безопасности нужна гарантия того, что пользователь приложения не может подключиться непосредственно к учетной записи данных.

Следует также рассмотреть блокирование всех способов присоединения пользователей к схеме данных.

Для этого можно применить одну из таких методик, как блокировка учетной записи, отзыв привилегий на подключение и создание невозможного пароля

Защищенным можно считать проект приложения, где имеется одна схема, содержащая данные, одна схема, где хранятся все программы на PL/SQL, работающие с данными из первой схемы, и хотя бы одна схема, к которой подключаются пользователи.

Никогда не давайте конечным пользователям возможности подключаться к схемам данных.

5.6. Определение подходящего уровня I&A

После того как вы изучите все возможные способы проведения I&A, у вас может появиться чувство легкого «головокружения от успехов».

Не поддавайтесь ему. Пользуйтесь практичным и разумным подходом при рассмотрении того, какие тактики и методы следует применить.

При выборе методов I&A нужно определить чувствительность данных, привилегии и права доступа, а также уравнять прочие конкурирующие факторы.

Первая руководящая директива основыва-ется на том, что именно защищается.

Обычно по мере повышения чувствительности и конфиденциальности данных требуются более мощные средства I&A.

Если приложение разрешает пользователю обращаться к своему излюбленному списку акций, достаточно простого пароля без каких-либо ограничений.

Если предоставляемый пользователю доступ позволяет ему получать коды запуска ракет с ядерными боеголовками, то, как правило, оптимальным выбором является сильная аутентификация, возможно, даже многофакторная аутентификация.

Вторая директива по определению подходящей I&A **базируется на том, что может видеть и делать пользователь.**

Чем полнее привилегии и шире доступ, тем сильнее должна быть аутентификация.

Для обычных пользователей, чей доступ контролируется, обычно подходят сильные пароли.

Для пользователей с более широким кругом полномочий, например, для АБД, желательно применять более сильную аутентификацию.

Может возникнуть вопрос: **«А почему бы <u>всегда</u> не использовать сильную аутенти-фикацию?»**

Прежде чем сделать ставку на этот подход, необходимо вспомнить, что в реальности приходится учитывать и другие аспекты.

На практике защита должна быть сбалансирована с практичностью, производительностью, стоимостью реализации и администрированием.

Как правило, слабая аутентификация, например, с помощью паролей, недорога в реализации, ее легко поддерживать и управлять ею.

Методы сильной аутентификации, например биометрика и смарт-карты, связаны с более высокими первоначальными и эксплуатационными расходами.

Вдобавок простота использования или агрессивная природа аутентификации может стать барьером для ее эффективности.

Следовательно, правильный метод аутентификации должен учитывать все аспекты, а не только обеспечение безопасности.

Это вовсе не означает, что сильная аутентификация — это обязательно плохо; необходимо проанализировать затраты и результаты и сравнить затраты на реализацию с последствиями возникновения бреши в системе защиты.

Итоги

Идентификация и аутентификация служат фундаментом процессов обеспечения безопасности.

Они должны быть реализованы в самом начале, и они должны быть реализованы правильно.

Не имеет значения, насколько хитры и изощренны методы контроля доступа и аудита, если пользователь совсем не тот, за кого себя выдает.

В подобных случаях все остальные меры защиты будут пустой тратой времени, ресурсов компьютера и усилий на программирование.

Прочие проектные решения, имеющие отношение к I&A, также влияют на безопасность системы.

Хранение идентификационных данных пользователей в базе данных позволяет применять к ним средства организации защиты самой базы данных, что хорошо согласуется с принципом обороны в глубину.

Необходимо заложить эту защиту в проектируемое приложение заблаговременно.

Моделирование отношения пользователь-база данных весьма важно для предсказания того, какие средства базы данных можно будет задействовать.

По меньшей мере, необходимо отделить схему с данными от схем для пользователей.

Администраторы не должны применять общие учетные записи.

Совместное использование схем допустимо только в тех случаях, когда идентификационные данные пользователей могут быть надежно сохранены и привилегии базы данных одинаковы для всех пользователей, подключаемых к этой схеме.

Понимание общей картины идентификации и аутентификации очень важно для выбора способа построения политики безопасности.

Необходимо тщательно соблюдать баланс

- между требованиями безопасности — значимость и чувствительность данных — и простотой использования,
- администрированием и расходами, связанными с применением различных технологий аутентификации.