ДОВЕРЕННАЯ СРЕДА

УДК 004.089

Бесфакторная классификация аутентифицирующих данных

С. В. Конявская, канд. филол. наук
ЗАО "ОКБ САПР", Москва, Россия
Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

Проведен анализ существующей классификации аутентификационных данных, и предложено ее усовершенствование. Показано, что классификация данных с помощью перечня "факторов аутентификации" не соответствует требованиям к классификациям, а также современному состоянию науки и техники. Предложенная альтернативная классификация строится с учетом полученного опыта и требований, предъявляемых к научным классификациям.

Ключевые слова: аутентификационные данные, аутентификация, фактор аутентификации.

"Факторы" аутентификации сыграли положительную роль в популяризации вопросов аутентификации за счет своей наглядности. Однако в настоящее время они используются как фундамент системы представлений об этом феномене [1], что представляется неприемлемым.

"Общим местом" является список из трех факторов: знание, владение, биометрия (обладание некоторой биологической особенностью). Согласно NIST [2] биометрический фактор является дополнительным, способным подтвердить обладание субъекта тем предметом, который для него воплощает фактор "владения" (например, биометрическое подтверждение того, что данная смарт-карта этого человека): "Биометрия ДОЛЖНА использоваться только как часть многофакторной аутентификации с физическим аутентификатором (*то, что у вас есть*)" [2, раздел 5.2.3]*. Таким образом, в многофакторной аутентификации этот "фактор" может быть только третьим. Если *заменить* ввод пароля к смарт-карте предъявлением отпечатка пальца, то аутентификация перестанет считаться многофакторной. Допустимо только *добавить* предъявление биометрического признака**.

Иногда к факторам также относят расположение в определенном месте [3, с. 13], но, согласно ISO это не фактор, а только свидетельство т. е. данные, которые могут дополнительно привлекаться для усиления уверенности в положительном результате аутентификации или при первичной идентификации. В то же время согласно ISO/IEC 29003 факторов все-таки четыре, но 4-й — это не расположение в пространстве, а то, что субъект "обычно делает" (например, какие-то поведенческие паттерны) [4, раздел 3.6].

Использовать инструмент популяризации в целях классификации и кодификации неверно, однако это происходит [2, 4—6], что порождает коллизии, которые приходится снимать, вводя большое количество разных оговорок относительно того, как и что понимать в каком контексте.

В данной работе продемонстрировано, почему использование системы понятий, сформировавшейся вокруг идиоматического выражения "факторы аутентификации", на современном этапе развития науки и техники вредно и должно быть прекращено. Предлагается альтернативный подход к классификации аутентифицирующих данных.

Конявская Светлана Валерьевна, заместитель генерального директора, преподаватель кафедры "Защита информации".
E-mail: cd@okbsapr.ru

Статья поступила в редакцию 19 июля 2019 г.

* В п. 4.2.1 есть примечание: "Если биометрическая аутентификация соответствует требованиям, изложенным в разделе 5.2.3, устройство должно быть аутентифицировано в дополнение к биометрической — биометрия признается как фактор, но сама по себе не распознается как аутентификатор. Поэтому при проведении аутентификации с использованием биометрии нет необходимости использовать два аутентификатора, поскольку связанное устройство служит "чем-то, что у вас есть", в то время как биометрия служит “тем, чем вы являетесь”".

** Благодарю за это данное в личной беседе уточнение А. Г. Сабанова.

Материалы и методы

В отношении классификаций в научном исследовании возможна постановка нескольких принципиальных вопросов.

- Является ли рассматриваемое классификацией или имеет место результат какой-то другой операции над предметом изучения (именно к классификации применимы требования быть исчерпывающей, построенной на одном основании, причем на основании значимого для всего классифицируемого множества признака, и т. д.).
- Корректна ли классификация, т. е. соответствует ли она действительному наблюдаемому положению вещей.
- Целесообразна ли классификация, т. е. продуктивна ли она, позволяет ли решить какие-либо задачи (прогнозирование, объяснение причин и т. д.), устанавливаются ли соответствие или связи иного рода между нею и другими фрагментами научного описания того же сегмента действительности.

Всегда желательно минимизировать изменения в устоявшейся практике, поэтому если выявлено, что классификация построена с нарушениями, но при этом она целесообразна, имеет смысл постараться ее сохранить, устранив недостатки, а не создавать новую классификацию на других основаниях.

Материалом исследования является классификация аутентифицирующих данных, в научном обороте представленная перечнем "факторов аутентификации". Основными методами в связи с особенностями объекта рассмотрения являются системный и текстологический анализ литературы, а также наблюдение и классические методы теоретического исследования — дедукция и индукция.

Обзор литературы

Определение "факторов". Понятие, лежащее в основе классификации, очевидно, должно быть определено, так как этим определением задаются границы класса.

Определение фактора аутентификации дано в проекте ГОСТ Р Идентификация и аутентификация. Общие положения [5, с. 14]: "фактор аутентификации: Вид (форма) существования аутентификационной информации, предъявляемой субъектом доступа или объектом доступа при аутентификации".

Похожее определение есть в [3, с. 13] и других работах. Определение из проекта ГОСТа предлагается к рассмотрению потому, что он разработан теми же авторами и является последним по хронологии, т. е. аккумулирует результаты развития их взглядов на предмет.

Однако все, что можно почерпнуть из этого определения, — это то, что понятие "фактор" *каким-то образом связано* с аутентифицирующими данными (так как "предоставляемые при аутентификации" и "аутентифицирующие" — в общем случае синонимичные выражения). Как именно связано, напрямую установить невозможно, так как выражение "вид существования информации" (или "форма существования информации") неясно.

Надо отметить, что "форма существования" — это формула, естественная для научного дискурса вообще, и к понятию информации она применяется достаточно часто. По системе определений, сформулированной А. А. Стрельцовым [7, с. 10—33], информация существует в форме сведений и сообщений, при этом обе формы существования информации определены и четко отделены одна от другой. По системе определений В. А. Конявского [8, с. 179—191], в цифровой среде следует говорить не об информации как таковой, а о ее отображении (если провести параллель с системой определений Стрельцова, то в ней сведения отображаются в сообщениях). Отображается информация или в статической форме — в форме данных (чисел, представляющих собой упорядоченное множество символов), или в форме процессов — динамической форме. В обеих системах дефиниций понятна природа определяемых феноменов, понятны их взаимосвязи и следствия из них: "форма существования" информации в виде сведений и сообщений позволяет выделить и определить предмет правоотношений, форма существования в виде данных и процессов — построить модель электронного документа и его защиты.

Что позволяет прояснить существование аутентифицирующей информации в форме факторов аутентификации?

Поскольку определение должно анализироваться не изолированно, а в совокупности с введенным в научный оборот закрытым перечнем "факторов аутентификации", можно сделать вывод о том, что "вид" и "форма" здесь характеризуют парадоксальным образом как раз не форму, а содержание. Целесообразность такого оксюморона в научном определении представляется неочевидной. Речь ведется о разделении всех возможных для применения в процессе аутентификации данных на типы по их содержанию (по тому, какова их диктумная предметность, *чем* в реальном физическом мире является их источник — знанием, характеристикой какого-то предмета, физиологической особен-

ностью, местом, образом действия). "Расположение в пространстве" — это не форма и не вид существования геолокационных данных, такое высказывание может пониматься только метафорически. Метафоры, так же как оксюмороны или любые другие тропы, желательно исключить при построении основ системы.

Содержание понятий раскрывает помимо определений и прямых классификаций контекст их применения. В проекте ГОСТ [6, с. 21] упоминается еще один процесс (кроме предъявления при аутентификации), в котором участвуют аутентифицирующие данные и факторы аутентификации: "…для достоверного установления соответствия необходимо осуществить привязку идентификационных данных к субъекту (объекту) доступа. При этом должны использоваться механизмы привязки с использованием следующих факторов…". Здесь снова, казалось бы, создается некоторый интуитивно понятный образ: данные каким-то образом привязываются к субъекту, который будет затем их предъявлять. Но совершенно непонятно, что именно за этим стоит, если пытаться рассмотреть какой-то конкретный пример. Например, отпечаток пальца — идентификационные данные человека. Он *привязывается* к субъекту *с использованием биометрического фактора*? Что это может означать? Как можно привязать информацию к чему-либо с помощью формы ее же существования?

Классификация "факторов". Есть основания считать, что перечень факторов аутентификации позиционируется как классификация. Перечень всегда представляется как закрытый, несмотря на то что факторов в нем от 2 до 4 (при этом самих пунктов 5: знать, владеть, биометрия, расположение, поведение, но все пять одновременно в одном перечне никогда не встречаются; более того, в построениях, в которых факторы используются вне перечней, эксперты ISO склонны сужать перечень факторов "в чистом виде" до 2, а остальные называть дополнительным, свидетельством и т. д.).

Однако в классификации должен быть ясно выраженный классификационный признак, все группы должны быть выделены на одном основании и, наконец, классификация должна быть исчерпывающей и желательно постоянной в своем составе (или по крайней мере разные представления о составе классификации должны быть соотнесены между собой в какой-то дискуссии, а не существовать просто параллельно).

Классификационный признак. Классификационный признак должен быть связан с целью, для которой проводится классификация, он должен быть объясним.

Не удается обнаружить явных причин, которые могут объяснить тот факт, что классифицировать аутентифицирующие данные целесообразно именно *по содержанию*. Более того, при *использовании* "факторов" аутентификации в построении дальнейших рассуждений в дело идут не содержательные характеристики данных, а признаки, характеризующие степень их связанности с субъектом (чаще всего, *насколько необходимо* вступать в *насколько тесный* контакт с субъектом, чтобы завладеть этими данными). Таким образом, разделяются феномены на группы по одному признаку, а далее используются другие признаки, свойственные этим же группам.

Единое основание. О едином основании в перечислении "знать, владеть, биометрия" говорить невозможно. Если отклонить биометрию, как дополнительный фактор, все равно ясно формулируемое основание, более узкое, чем "признак", выделить невозможно.

Полнота классификации.

1. Охвачены не все типы субъектов. Первое, что необходимо отметить в связи с полнотой классификации, это то, что классификация "знать, владеть, биометрия" оставляет полностью не закрытым один из двух типов субъектов аутентификации.

Неуниверсальность подхода становится очевидной при попытке применения "факторов" для создания общего описания процессов идентификации и аутентификации *любых субъектов*, не только пользователей-людей, но и сущностей цифровой природы. Именно это наблюдаем в разрабатываемом ГОСТе [6, с. 21], в частично уже приведенном фрагменте: "Для достоверного установления соответствия необходимо осуществить привязку идентификационных данных к субъекту (объекту) доступа. При этом должны использоваться механизмы привязки с использованием следующих факторов*:

- фактор знания. Привязка устанавливается с использованием информации, которая известна субъекту (объекту) доступа;
- фактор владения. Привязка устанавливается с использованием идентификационных данных, которые имеет (обладает) субъект (объект) доступа. При этом идентификационные данные свойственны (присущи) субъекту (объекту) доступа или содержатся в его свидетельствах, представляющих собой документальное подтверждение. Субъект (объект) доступа должен правомочно обладать данными свидетельствами;

---

* Общая характеристика факторов по ГОСТ Р Идентификация и аутентификация. Общие положения.

- фактор биометрический. Привязка устанавливается по результатам верификации биометрических характеристик, которые свойственны субъекту доступа. При этом принимается, что эталонные характеристики субъекта доступа действительно принадлежат ему.

Примечания

- Условно считается, что при привязке для субъектов доступа и объектов доступа, которые являются информационными и вычислительными ресурсами (средствами вычислительной техники, автоматизированными (информационными) системами и т. п.), может использоваться один фактор — фактор владения.
- Привязка с использованием биометрического фактора применяется для субъектов доступа, ассоциированных с физическими лицами. Порядок и правила применения фактора биометрического определяются соответствующими действующими нормативными правовыми документами и документами по стандартизации".

Отдельно надо заметить, что второе примечание избыточно, так как в первом примечании уже указано, что применяться может только один фактор. Следовательно, отдельно оговаривать невозможность применения одного из оставшихся факторов не имеет смысла. Однако это лишь проект стандарта и его редактирование еще продолжается.

Очевидно, что не просто "не все", а ни один из "факторов" (кроме относительно нового и не совсем фактора, который коротко назовем "расположение") не может быть без оговорок отнесен ни к процессу, ни к техническому или программному средству, ни к информационной системе в целом (ничто из перечисленного не может ни знать, ни владеть, ни иметь биологические особенности).

Представляется, что связанность информационных и вычислительных ресурсов скорее соотносится с биометрическими признаками человека, чем с владением, однако на таком метафорическом уровне разговор о технических параметрах в любом случае не вполне уместен.

Оговорки позволяют некоторым образом снять самые очевидные противоречия, однако терминологическая система, подходящая без оговорок только одной из двух глобальных групп субъектов, очевидно, несовершенна.

2. Охвачены не все фактически применяемые для аутентификации виды данных. Эмпирически из словоупотребления в стандарте и дискуссиях вокруг него выявляется, что "формы существования" аутентифицирующих данных, которые без оговорок не укладываются в "знать" и "владеть", зачастую называются "свидетельствами". Например, паспорт — это официальное свидетельство. Действительно, в парадигме "знать, владеть, биометрия" классификация паспорта как того, с помощью чего человек аутентифицируется, затруднительна хотя бы потому, что некоторые из паспортов — биометрические, а некоторые — нет. А главное, в отношении паспорта сомнительным представляется установление связи "владение". Вместе с тем, кроме этого затруднения, нет никаких причин отказывать паспорту в том, что он является носителем аутентифицирующих данных.

Однако свидетельства в парадигме понятий ГОСТов [5, 6] могут применяться только в процессах идентификации, а не аутентификации, а значит, паспорт не может применяться для аутентификации, а может применяться только для идентификации*, хотя наблюдение над практикой аутентификации показывает обратное.

Бесспорно не охвачены классификацией те виды данных, которые предъявляются субъектами цифровой природы (контрольные суммы, серийные номера, UID'ы и т. д.).

Получается разрыв между кодифицируемой аксиоматикой и практикой уже на этапе разработки первой, а это значит, что в дальнейшем он будет только увеличиваться.

Результаты

В то же время представляется вполне возможным устранить указанные недостатки системного описания аутентифицирующих данных таким образом, чтобы его можно было распространить на всю область определения субъектов аутентификации, причем без коренного разрушения привычной понятийной системы.

Коренные изменения нецелесообразны в первую очередь потому, что сама предметная область характеризуется высокой степенью стабильности: если что-то начинает использоваться для аутентификации, то остается в этом качестве надолго, несмотря на все недостатки способов аутентификации с помощью данных этого типа, как происходит, например, с паролями.

Если достаточно стабилен сам перечень возможных данных и нет оснований считать, что он должен быть радикально изменен, то задача сводится к изменению *описания* сегмента действительности как есть.

---

* Этот вывод не сделан автором, он получен от А. Г. Сабанова в личной беседе о том, к какому фактору аутентификации относить паспорт.

Классификация может быть принята к рассмотрению, если она будет полной, на едином основании, целесообразной и совместимой с другими объектами этого же семантического поля, например будет без противоречий накладываться на перечень способов аутентификации, фактически применяемых на практике, а желательно позволять спрогнозировать возможные, но до сих пор не используемые способы или механизмы.

Предмет классификации. В первую очередь необходимо зафиксировать, что в информационную систему мы в любом случае представляем только *данные*, а не знания, не собственность или что-то еще из аналогового или духовного мира. Поэтому речь должна идти о *данных*, характеризуемых какими-то *признаками* или наборами признаков.

Таким образом, предмет классификации — аутентифицирующие данные.

Способы аутентификации и *аутентифицирующие данные,* безусловно, связаны, хотя и не должны смешиваться. Является общим тот факт, что значение имеет не только и не столько то, какие данные используются для аутентификации, сколько то, каким образом реализован механизм аутентификации в системе (так, реализация парольной защиты может быть признана слабой, если она не включает в себя проверку на слабые пароли или какие-то механизмы блокировки угроз, связанных с возможным применением слабого пароля, но также может быть признана слабой и в случае, если слабые пароли в ней исключены, но сильные хорошие пароли хранятся и передаются в открытом виде и в форме, делающей их доступными для нелегального применения; так или иначе слабость пароля и слабость реализации — это две разные слабости).

В данном случае речь пойдет не о способах и не о механизмах аутентификации, а именно об аутентифицирующих данных и их признаках. Следствия из полученной классификации, имеющие значение для выводов о механизмах или способах аутентификации, вероятно, станут развитием этого рассуждения.

Классификационные признаки. Значение имеет не только то, какую особенность сегмента действительности взять за основу, но и то, каким признаком ее описать.

Особенностей у аутентифицирующих данных можно выделять множество, и значительная часть описывающих эти особенности признаков будет важна с точки зрения защиты информации. Например, данные могут быть инвариантны или вариативны (сравнение может требовать точного совпадения или совпадения в рамках некоторого диапазона; пример первого — пароль, второго — биометрический эталон), могут быть постоянными/временными/однократными (постоянные — статические биометрические данные (никогда не меняются), временные — пароль, ключи в токене (могут меняться, и если не меняются — это все равно *время действия*), однократные — одноразовый пароль, динамические биометрические данные (каждый раз разные)) и т. д.

Это все важные параметры. Они характеризуют именно те *особенности* аутентифицирующих данных, которые определяют их принципиальную применимость и конкретные способы их применения в механизмах аутентификации. Однако для классификации нужны такие признаки, которые характеризуют одновременно *все* возможные данные, причем характеризуют информативно, а не формально (так, наличие частоты не дает оснований классифицировать звук и цвет по длине волны в одну сплошную классификацию).

Признаки, по которым данные будут классифицированы, должны позволять строить на основе этой классификации рассуждения о защищенности механизмов аутентификации, использующих эти признаки аутентифицирующих данных. Значит, они должны быть связаны с ключевыми элементами системы аутентификации — аутентифицирующимися сторонами (назовем их субъектом и объектом аутентификации, так как даже при *взаимной* аутентификации все равно целесообразно ассоциировать аутентификацию с доступом, относительно которого так или иначе всегда выделяют *субъект* и *объект*), а также *носителем* аутентифицирующих данных.

Отдельно необходимо оговорить, что *объектом доступа* может быть некоторый целевой ресурс, а не информационная система в целом, или даже СВТ. Предположим, аутентификацию в идентификации/аутентификации банкомата клиент банка проходит для того, чтобы получить доступ к своему счету, а не к банкомату. *Объектом аутентификации* будет банкомат как информационно-вычислительный ресурс, предоставляющий доступ к целевому *объекту доступа*.

Канал передачи данных от субъекта в подсистему аутентификации объекта, с одной стороны, зачастую детерминирован носителем данных (USB-токен не передаст данные через сканер отпечатка пальца, и наоборот), а с другой стороны, сами данные как раз с каналом их передачи практически не связаны, поэтому отдельно выделять его не представляется целесообразным.

"Связанность" чего-либо может быть разной степени (например, по возрастанию: соотнесенность, зависимость, неотчуждаемость), и связан-

ность аутентифицирующих данных с каналом их передачи, безусловно, вполне реально установить, но это будет не более чем ***соотнесенность***. Признак связанности такой степени непродуктивен, поэтому не будет браться в расчет.

Неотчуждаемость также представляется непродуктивным для классификации признаком, так как этот признак может характеризовать только те данные, которые *в непреобразованном виде* в систему (и подсистему аутентификации, в частности) передаваться *не могут*. От чего бы неотчуждаемыми ни были эти данные, они неотчуждаемы от чего-то, что находится за *рамками* системы. Значит, в систему они *никогда не попадают*. Таким образом, признак неотчуждаемости от чего бы то ни было, фактически, делит аутентифицирующие данные на два вида: передаваемые и не передаваемые в систему. Больше из этого признака невозможно извлечь никакой полезной информации.

Признак ***зависимости*** позволяет описать в том числе и те случаи, когда данные от чего-либо неотчуждаемы. Такие данные в систему не передаются, но что-то другое передается, иначе не состоится аутентификация. Передаются данные, которые от них тем или иным образом *производны*, т. е. *зависимы* от того элемента, от которого первые данные неотчуждаемы.

В связи с этим нужно иметь в виду, что в части случаев аутентифицирующие данные представляют собой *цепочку данных*. Возможно, для каких-то задач этот факт может оказаться значимым, поскольку хотя все процессы жизненного цикла "первичных" неотчуждаемых данных протекают вне подсистемы аутентификации, процедура *создания передаваемых в систему данных* из "первичных" неотчуждаемых данных находится в границах этой подсистемы.

Однако непосредственно для классификации аутентифицирующих данных это представляется избыточным.

Еще одним дискуссионным вопросом является самостоятельность третьего выделенного элемента — носителя аутентифицирующих данных. В рамках процесса аутентификации он всегда находится на стороне субъекта аутентификации и предъявляется объекту. Видится целесообразным представлять зависимость от носителя видом зависимости от субъекта.

Характеристики по классификационным признакам. Зависимость — это понятие с крайне размытой областью определения, поэтому в качестве характеристики нецелесообразно брать "наличие" и "отсутствие" зависимости. В то же время вполне реально формализовать *характер* зависимости как от системы, так и от субъекта.

Таким образом, данные, используемые для аутентификации, могут характеризоваться по тому, *как* они зависят от субъекта аутентификации и от объекта классификации.

Например, они могут быть *назначены* субъекту, могут быть с ним *ассоциированы*, а могут быть ему *имманентны*.

Не зависеть от объекта совсем аутентифицирующие данные не могут, так как иначе они не смогут сыграть целевую для них роль доказательства. Объект должен располагать какими-то данными для того, чтобы принять решение о корректности представленного подтверждения. Эти данные могут быть *именно теми*, которые субъект будет предъявлять, или какими-то *косвенными данными*, позволяющими определить корректность данных, не располагая ими напрямую. Например, так производится проверка закрытого ключа сертификата: закрытым ключом субъета объект не располагает, но располагает возможностью его проверить.

Возникает сомнение, имеет ли значение, порождаются данные системой или записываются в нее. На текущем этапе работы над классификацией не обнаружено доводов в пользу того, что это разделение может быть для чего-то полезным.

Если проводить параллель между субъектом и объектом (т. е. сравнивать порожденные системой и записанные в нее данные с назначенными и ассоциированными с субъектом данными), то разница между назначенными и ассоциированными данными состоит в том, что ассоциированные данные не тиражируются (одновременно носитель может находиться только у одного пользователя, если считать носитель условно некопируемым, так как мы смотрим в этом случае только на данные, а не на конкретную реализацию). Это значимо с точки зрения защищенности способов аутентификации, использующих одни или вторые данные, поэтому такую разницу целесообразно учитывать.

Не так очевидно, что зависит от того, сам ли объект породил данные для последующей аутентификации субъекта. Не исключено, что это дает возможность при определенных реализациях затруднить мошеннические действия пользователя. Но эти различия лежат, скорее, в области характеристики механизмов, чем данных. Аналогично от реализации системы аутентификации будет зависеть, постоянными или временными будут данные, ассоциированные с субъектом или назначенные ему. Система может:

- использовать заводской номер идентификатора (он постоянен) или вычисление от каких-либо данных, записанное в память идентификатора либо даже им осуществляемое (временные данные);

- требовать или не требовать смены пароля по регламенту;
- предъявлять или не предъявлять требований к его сложности и т. д.

Однако разделение этих данных на "аппаратный идентификатор" и "пароль" все равно справедливо находится на уровень выше, а детали реализации определяют качество (лучше\хуже), а не архитектуру системы.

Суммируя все изложенное, можно сформулировать следующие варианты зависимости аутентифицирующих данных от субъекта и объекта:

- зависимость от объекта аутентификации:

  – прямая (в системе хранятся (или создаются) сами данные, сравнение с ними производится напрямую; в этом смысле не имеет значения, что сравнивается, "пароль с паролем" или "свертка со сверткой", и точное совпадение должно быть или вероятностное; главное, что сравнивается именно непосредственно то, что получается от субъекта при аутентификации);

  – косвенная (в системе хранится "стимул", порождающий данные как ответ, или какие-то признаки, которым данные должны удовлетворять (атрибутный сертификат));
- зависимость от субъекта аутентификации

  – назначены субъекту (строго говоря, зависимости нет: мой пароль никак от меня не зависит, даже если я сама его выдумала);

  – ассоциированы с субъектом (зависимы от чего-то (в случае с человеком — от носителя), что не имманентно субъекту);

  – имманентны субъекту (для человека — это преимущественно биометрические данные, а для информационных и вычислительных ресурсов — это любые присущие им признаки, такие, как серийные и заводские номера, фрагменты кода, контрольные суммы и т. п.).

Классификация. Одновременно данные характеризуются какой-то зависимостью и от субъекта, и от объекта. Таким образом, получается 6 вариантов сочетаний характеристик:

- 0; 0 — прямая зависимость от объекта, назначен субъекту (пароль, в том числе одноразовый пароль (с точки зрения *данных*, а не механизма отличий нет), здесь же контрольные вопросы, талончики на очередь);
- 0; 1 — прямая зависимость от объекта, ассоциированность с субъектом (зависит от носителя) (аппаратный идентификатор (ничего, кроме того, что это обладатель идентификатора (возможно, случайный), мы о субъекте не знаем); аппаратный идентификатор с одноразовым паролем относится к этой же категории, меняется только реализация механизма.
- 0; 2 — прямая зависимость от объекта, имманентность субъекту (биометрические данные, сравниваемые с шаблоном (данные имманентны субъекту и зарегистрированы в объекте), или неотчуждаемые характеристики, например характеристики СВТ, сравниваемые с зарегистрированными в служебном носителе "Секрет");
- 1; 0 — косвенная зависимость от объекта, назначается субъекту (случай довольно экзотичный, но встречающийся; например, такими аутентифицирующими данными являются многие билеты*; именно с этим связаны проблемы с подделкой билетов: назначаемые данные тиражируемы);
- 1; 1 — косвенная зависимость от объекта, ассоциированность с субъектом (сертификат закрытого ключа, "рукопожатие" СВТ с аппаратным идентификатором, какое-то вычисление, например КС (объект передает данные, на основании которых производится какое-то вычисление в устройстве, ассоциированном с субъектом, или самим субъектом, если это программа или система));
- 1; 2 — косвенная зависимость от объекта, имманентность субъекту (интерактивная биометрия стимул—реакция, клавиатурный почерк при наборе фразы по запросу).

Обсуждение

Получается, что любое из пересечений значений признаков дает описание реально применяющихся в жизни аутентифицирующих данных, причем охвачены даже такие *способы* аутентификации, которые еще не реализованы, а только разработаны на уровне концепций (рефлекторная биометрия "стимул—реакция"), а также такие, которые не очевидно ассоциируются именно с аутентификацией (талончики на очередь).

Примера данных, которые не попадают ни в одну из 6 получившихся категорий, пока не обнаружено, что, безусловно, не говорит само по себе о том, что классификация верна, однако усиливает ее правдоподобность.

Необходимо иметь в виду, что билеты могут включать в себя (в тексте на билете, например) какие-либо идентифицирующие данные, которые могут быть проверены (допустим, паспортные данные проверяются путем сличения с паспортом); это будет другой, отдельный процесс аутентификации человека как легального владельца билета (проверяется, что он владеет билетом законно, а не что именно он имеет право посмотреть спектакль); отличаются случаи, когда аутентифицирующими данными являются собственно данные субъекта, а билет является только способом учета (например, при авиаперевозках билеты существуют, однако регистрируют на рейс не по билету, а по паспорту; это будет случай 2 — 0; 1).

Получившиеся типы данных можно расположить по возрастанию сложности получения этих данных в распоряжение:

- прямо сравниваемые данные можно "подложить", перехватив ранее отправленный при аутентификации легального субъекта пакет, а косвенная зависимость требуется для более сложной атаки;
- не связанные с субъектом данные могут быть переданы неограниченно большому кругу лиц, растиражированы (они не могут быть по каким-либо причинам нетиражируемыми);
- устройство теоретически может быть нетиражируемым, в любом случае его тиражирование сложнее;
- неотчуждаемые характеристики теоретически воспроизводимы, но еще сложнее и т. д.

В то же время нельзя не заметить, что так же возрастает и сложность реализации подсистемы идентификации\аутентификации, использующей данные разных типов.

Однако это в некотором смысле компенсируется тем, что снижаются требования к обеспечению доверия тем или иным компонентам системы, которые могут в разных случаях быть легче или сложнее доступны для контроля. Иногда проще сделать доверенным клиентское устройство, а иногда использовать намного более сложную систему аутентификации, но не контролировать клиентские устройства совсем. Эти параметры (контроль какого компонента должен быть усилен, а какого может быть ослаблен) тоже можно получить как следствие из предложенной классификации.

Это означает, что классификация обладает определенной продуктивностью, т. е. целесообразна.

Верна ли она, покажет анализ со стороны широкого круга специалистов.

Заключение

В связи с тем, что ввод в научный оборот новой классификации уже известного и представляющегося изученным феномена требует тщательного обоснования, значительная часть работы посвящена критике принятой классификации. В то же время представляется нежелательной радикальная смена понятийной базы, так как ее негативные последствия могут превысить конструктивные.

Предлагаемая в качестве альтернативы классификация аутентифицирующих данных представляется решающей задачу нетравматичного вывода исчерпавшего эвристический ресурс термина "фактор аутентификации" из системы понятий.

Литература

1. Аутентификация // Википедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/Аутентификация#Факторы_аутентификации (дата обращения: 29.04.2019).
2. NIST Специальная публикация 800-63B. Руководство по цифровой идентификации. Аутентификация и управление жизненным циклом. 2017 [Электронный ресурс]. URL: https://pages.nist.gov/800-63-3/sp800-63b.html (дата обращения: 30.04.2019).
3. *Комаров А.* Современные методы аутентификации: токен и это все о нем…! // T-Comm. 2008. № 6. С. 13—16.
4. ISO/IEC 2nd WD 29003 — Information technology — Security techniques — Identity proofing. 2013 [Электронный ресурс]. URL: https://cabforum.org/pipermail/public/attachments/20130814/f2f4a333/attachment.pdf (дата обращения: 30.04.2019).
5. ГОСТ Р Идентификация и аутентификация. Общие положения. Проект, окончательная редакция.
6. ГОСТ Р Защита информации. Идентификация и аутентификация. Уровни доверия к результатам идентификации. Проект, первая редакция.
7. *Стрельцов А. А.* Обеспечение информационной безопасности России. Теоретические и методологические основы. — М.: МЦНМО, 2002. — 296 с.
8. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. — Минск: Сер. "Библиотека журнала "УЗИ"", 2004. — 327 с.

Factorless Classification of Authenticating Data

S. V. Konyavskaya
Closed Joint Stock Company "OKB SAPR", Moscow, Russia
Moscow Institute of Physics and Technology (State University), Dolgoprudny, Moscow region, Russia

The article is devoted to the analysis of the existing classification of authentication data and the proposal for its improvement. It is shown that the classification of data using a list of "authentication factors" does not meet the requirements for classifications, as well as the current state of science and technology. The alternative classification proposed in the article is based on this experience and the requirements for scientific classifications.

Keywords: authentication data, authentication, authentication factor.

Bibliography — 8 references. *Received July 19, 2019*