Техника аутентификации. Введение

Тарас Злонов, CIO-World, 20 февраля 2009 года

«Многие вещи нам непонятны не потому, что наши понятия слабы, но потому, что сии вещи не входят в круг наших понятий».
Козьма Прутков

Данная статья открывает цикл материалов посвящённых вопросам аутентификации, в рамках которого будут рассмотрены современные методы и технические средства аутентификации.

Зачем нужна аутентификация?

Современные компьютерные и сетевые технологии всё больше объединяют людей, предоставляя возможность общаться с коллегами и друзьями в других городах и странах, оставаться на связи в любом уголке земного шара и иметь доступ к огромным по объёму базам знаниям. В противоположность этому, новые возможности с не меньшим успехом и разъединяют людей: мы пишем электронные письма коллегам, находящимся в соседней комнате, общаемся с одноклассниками на сайтах, а не на встречах выпускников и поздравляем друзей с днём рождения SMS-сообщениями.

Среднее расстояние между собеседниками продолжает увеличиваться, но желание сохранять содержание разговора в тайне от других остаётся. Действительно, если бы вся информация была общедоступна и свободна, нам не были бы нужны ни пароли, ни электронные USB-ключи, ни биометрия. К сожалению ли, к счастью ли, но в нашем мире информация стоит денег, и стоит тем больше, чем меньше людей ею владеет. В связи с этим, желание обеспечить конфиденциальность данных, т.е. скрыть их от посторонних, вполне объяснимо, и разработчиками современных ИТ решений и продуктов именной этой задаче уделяется немало внимания.

На практике с помощью сетевых коммуникаций человек взаимодействует не только с другими людьми, но и с оборудованием, сервисами, службами и программным обеспечением и во всех этих случаях требуется гарантия подтверждения личности субъекта, вступающего в информационный обмен. Такая гарантия обеспечивается в процессе регистрации пользователя в той или иной системе. Сам процесс состоит из трёх взаимосвязанных процедур: идентификации, аутентификации и авторизации. Дадим определения этим понятиям.

Терминология

Общее представление об упомянутых выше процедурах имеет любой современный пользователь, поэтому мы постараемся разобраться в тонкостях этих процессов.

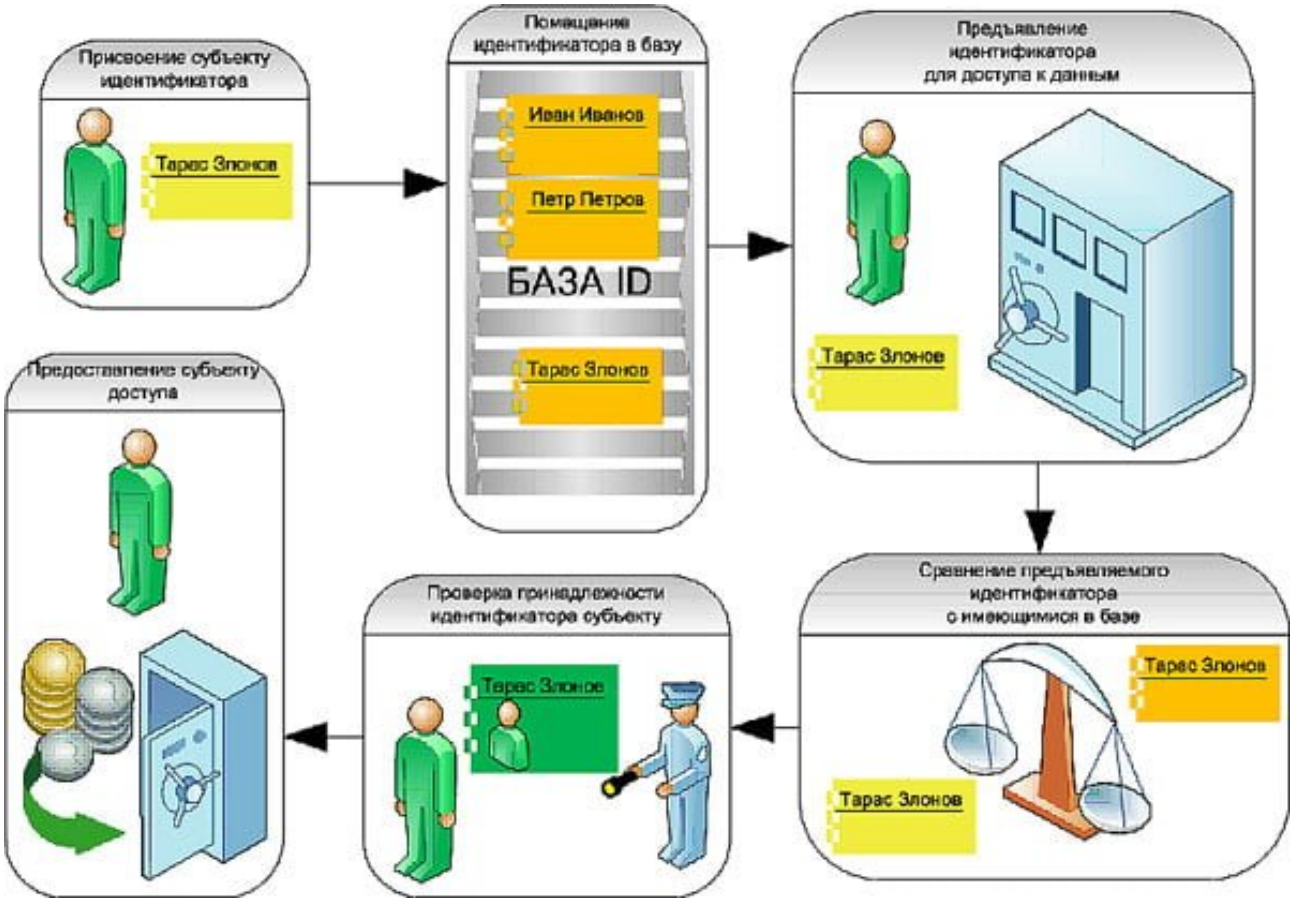

Схема процесса аутентификации

Информационные системы в нашей стране, а тем более в государственных органах, строятся исходя из принципов, изложенных в соответствующих специальных нормативных и методических документах. В частности, в соответствии с руководящими документами Федеральной службу по техническому и экспортному контролю (РД ФСТЭК). В одном из них, а именно в РД «Защита от несанкционированного доступа к информации. Термины и определения» введены следующие определения.

Идентификатор доступа (Access identifier) — уникальный признак субъекта или объекта доступа.

Идентификация (Identification) — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Аутентификация (Authentication) — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Термин «авторизация» опосредованно определён только в РД «Руководство по разработке профилей защиты и заданий по безопасности», где под авторизацией понимается подтверждение прав пользователя.

Рассмотрим в обобщённом виде процесс регистрации пользователя в системе и конкретный пример прохода посетителя на охраняемую территорию, например, банка.

Из приведённого примера видно, что необходимы дополнительные процедуры для обеспечения управления и контроля над процессами идентификации, аутентификации и авторизации. Такими процедурами являются администрирование и аудит.

№	Пояснение к схеме	Пример
1	Субъекту для дальнейшего взаимодействия с системой присваивается некий идентификатор	Для прохода в охраняемое здание посетитель сообщает службе собственной безопасности свои фамилию, имя и отчество (ФИО), которые теперь будут его идентификатором
2	Идентификатор субъекта заносится в базу идентификаторов	ФИО посетителя вписываются в список и отдаются охраннику на проходной
3	При обращении к данным субъект предъявляет свой идентификатор	Посетитель, придя на проходную, сообщает охраннику свои ФИО
4	Осуществляется поиск предъявленного идентификатора в базе, т.е. его идентификация	Охранник проверяет наличие в списке данного посетителя
5	После успешной идентификации осуществляется проверка подлинности субъекта, т.е. проверяется принадлежность ему идентификатора — аутентификация	Для подтверждения подлинности личности посетитель предъявляет охраннику паспорт с фотографией
6	Субъекту предоставляются права доступа, т.е. он авторизуется	Охранник пропускает посетителя на территорию предприятия

Пояснения к схеме процесса аутентификации

В рамках администрирования осуществляется процесс управления доступом субъектов к ресурсам системы: создание идентификатора субъекта, управление данными субъекта, используемыми для его аутентификации и управление правами доступа субъекта к ресурсам системы.

В нашем примере служба собственной безопасности выбирает идентификатор посетителя, вносит его в список и тем самым определяет его права доступа, разрешая проход в определённые помещения и строго отведённое время, а так же разрешает или запрещает тот или иной метод аутентификации: проход только по предъявлению паспорта, проход с паспортом или водительским удостоверением либо проход с любым документом с фотографией.

Аудит предполагает отслеживание происходящих в системе событий и их запись с указанием времени для последующей возможной проверки последовательности событий и/или изменений в последовательности событий. Это необходимо для подтверждения безопасности функционирования системы и проверки подозрений о нарушениях политики безопасности.

Для обеспечения аудита на проходной банка можно поручить охраннику вносить сведения о посетителях в специальный журнал, делать отметки в выдаваемых одноразовых пропусках либо установить камеру видеонаблюдения.

AAA, AAAA, IAAAA — 3A, 4A, I4A

С лёгкой руки компании IDC в терминологию специалистов по информационной безопасности вошло сокращение AAA (3A или Triple A) — Authentication, Authorization, Administration — аутентификация, авторизация, администрирование. Вместе с тем в документах RFC (Request for Comments) Специальной комиссии интернет разработок (Internet Engineering Task Force — IETF) аббревиатура AAA расшифровывается как Authentication, Authorization, Accounting. Последнее слово можно перевести как учёт сетевых [системных] ресурсов. В российских изданиях, посвящённых информационной безопасности, первые две буквы сокращения AAA прочно закрепились за аутентификацией и авторизацией, а третья трактуется попеременно то как аудит, то как администрирование. Можно найти так же упоминание о 4A — аутентификация, авторизация, администрирование и аудит.

В свете рассмотренного подхода к реализации безопасного доступа субъекта к информации и во избежание дальнейших недоразумений, предлагается ввести обобщающий термин I4A (IAAAA) — Identification, Authentication, Authorization, Administration & Audit. Данная аббревиатура максимально информативна и состоит из названий пяти основных процедур комплексного процесса предоставления доступа к информации. Все они тесно связаны между собой и только при соответствующей реализации и корректной работе всех их достигается приемлемый уровень безопасности.