Техника аутентификации. Идентификатор доступа

Тарас Злонов, CIO-World, 27 февраля 2009 года

— Почему ты каждому из них говоришь: «Ты прав, а твой брат ошибается»? Это же ерунда!
— Не сердись, о жена моя. Ты права, а я ошибаюсь.
Притча о Ходже Насреддине

В рамках цикла статей, посвящённых современным вопросам аутентификации рассмотрим более подробно понятие идентификатор доступа (далее идентификатор). Приведём определения, рассмотренные ранее.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.

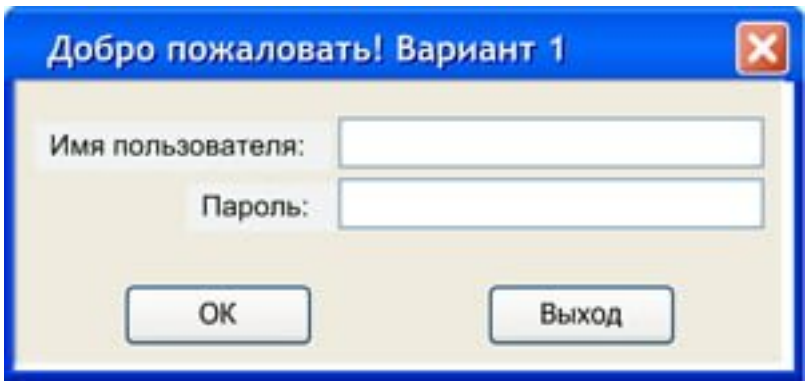
Аутентификация (Authentication) — проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Примечательно, что во многих современных работах по проблемам аутентификации и идентификации эти два процесса чуть ли не противопоставляются друг другу. Приводятся рассуждения о том, что идентификация сегодня морально устарела и только аутентификация решит все проблемы безопасного доступа. Главным недостатком идентификации принято считать тот факт, что в её процессе производится проверка не подлинности субъекта, а только наличия идентификатора в базе данных идентификаторов. Идентификаторами доступа чаще всего называют: логин (имя пользователя), штрих-код, карту с магнитной полосой, RFID-метки и т.п. Отдельные авторы в этот же ряд ставят

биометрические характеристики, показывая тем самым, что биометрия не может использоваться для аутентификации, т.е. для достоверного определения личности пользователя. Вполне естественно, что у других специалистов такая постановка вопроса вызывает сугубо негативную оценку и с их точки зрения биометрия чуть ли не единственное средство, обеспечивающее неотказуемость. По их мнению, пароль можно подсмотреть, аппаратный токен — украсть, а вот палец или сетчатка глаза всегда буду с человеком. Развивая идею противопоставления аутентификации и идентификации, авторы вплотную подходят (а порой и просто используют) термин «аутентификатор», понимая под ним средство аутентификации, представляющее отличительный признак пользователя. Вместе с тем, такого термина нет ни в одном словаре и попытка назвать «аутентификатором», например, электронный USB-ключ выглядит весьма забавно.

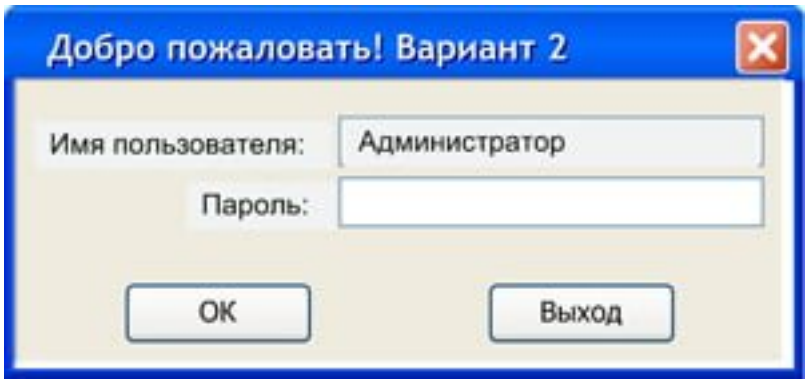
В свете вышеизложенного интересно взглянуть на определение пароля, предложенное в РД «Защита от несанкционированного доступа к информации. Термины и определения».

Пароль (Password) — идентификатор субъекта доступа, который является его (субъекта) секретом. Итак, по терминологии вышеупомянутых специалистов пароль должно было бы назвать «аутентификатором», вместе с тем, пароль — это точно такой же уникальный признак субъекта доступа, как и его логин, но сохраняемый в тайне. Чтобы понять данный вопрос более глубоко можно рассмотреть простой пример.



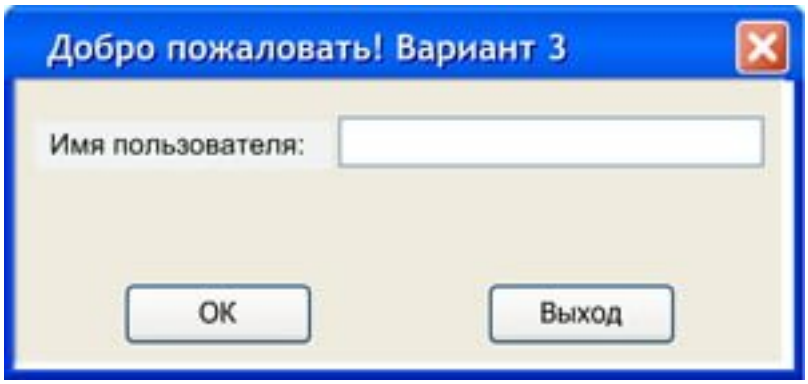
Вход. Вариант 1

При запуске приложения для ограничения несанкционированного доступа к нему, чаще всего у пользователя запрашивается у его логин и пароль. Принято считать логин несекретным идентификатором, в частности, многие системы имеют встроенные учётные записи (root, Administrator и т.д.). Пароль — это то, что пользователь хранит в секрете.



Вход. Вариант 2

В некоторых системах нет многопользовательского режима, т.е. фактически работа всегда ведётся от имени одной и той же учётной записи. На приведённом рисунке имя пользователя условно всегда «Администратор». Это, однако не значит, что пользователь не имеет идентификатора. Идентификатором в данном случае будет пароль, знание (незнание) которого разделит всех пользователей на две группы.



Вход. Вариант 3

И, наконец, система может требовать введение имени пользователя и не запрашивать пароль. Может показаться, что третий вариант самый небезопасный. Казалось бы,

никакой аутентификации пользователя не производится — только идентификация. На самом деле третий вариант практически ничем не отличается от второго. Только теперь в тайне нужно хранить не пароль, а логин. Если к тому же эти логины не хранятся в открытом виде в текстовом файле на жёстком диске в папке с установленным приложением, а надёжно защищены, например, с помощью функции хеширования, то безопасность такой системы будет на порядок выше тех, где используется пара логин-пароль, но не приняты соответствующие меры к защите паролей.

В действительности, разделение на логин и пароль весьма условны. Обычно принято считать паролем то, что держится в секрете, но точно так же и никому не известный логин может оказаться в каком-то смысле паролем. Допустим, злоумышленнику стал известен пароль от одного из почтовых ящиков пользователя на mail.ru: P@$$w0rd, но без знания логина пользователя прочесть его почту не получится.

Таким образом, пароль пользователя, сертификат, закрытый ключ, биометрические характеристики, аппаратный USB-ключ, его местонахождение и т.д. — являются идентификаторами, т.е. некими уникальными признаками, позволяющие идентифицировать пользователя. Для того, чтобы была возможна процедура аутентификации (проверки подлинности) необходимо построить систему так, чтобы часть этих идентификаторов были не известны и не доступны посторонним.

Процедура идентификации (в смысле сравнения предъявленного идентификатора с перечнем имеющихся) при предъявлении пользователем секретного идентификатора имеет некоторые особенности. Так как секретные идентификаторы, как правило, не хранятся в базе данных учётных записей в открытом виде (во избежание их компрометации), для них используют специальные процедуры проверки с использованием, в частности, функций хеширования и других математических преобразований. Более того, отдельные виды секретных идентификаторов пользователь никогда не предъявляет системе, а лишь только

опосредованно доказывает их у него наличие. Например, закрытый ключ пользователя в криптографии с открытым ключом всегда хранится им в секрете, а факт обладания этим закрытым ключом проверяется с использованием специального алгоритма. Всё многообразие таких процедур, в рамках которых явно (или опосредованно) проверяется наличие у субъекта секретного идентификатора доступа и является аутентификацией.

Архивная копия