Идентификация и аутентификация с использованием паролей

Основные понятия

Идентификацию и *аутентификацию* можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. *Идентификация* и *аутентификация* – это первая линия обороны, "проходная" информационного

Основные понятия

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством ***аутентификации*** вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "*аутентификация*" иногда исполь проверка подлинности".

Основные понятия

Аутентификация бывает ***односторонней*** (обычно клиент доказывает свою подлинность серверу) и ***двусторонней*** (***взаимной***). Пример *односторонней аутентификации* – процедура входа пользователя в систему.

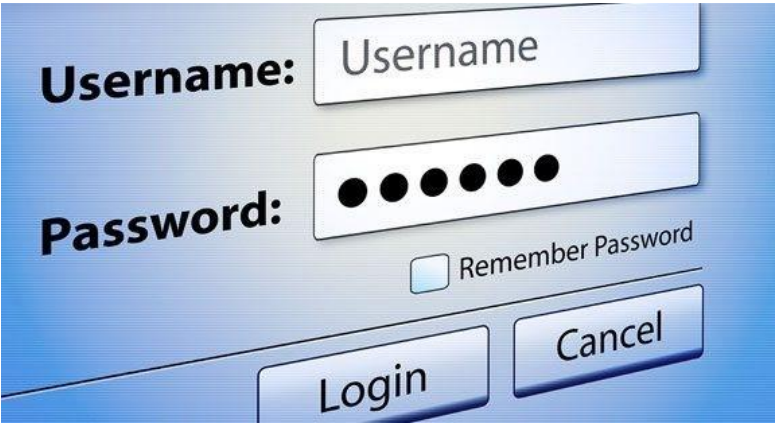
В сетевой среде, когда стороны *идентификации/аутентификации* территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

- что служит ***аутентификатором*** (то есть используется для подтверждения подлинности субъекта);
- как организован (и защищен) обмен данными *идентификации/аутентификации*.

Основные понятия

Субъект может подтвердить свою подлинность, предъявив по крайней мере одну из следующих сущностей:

- нечто, что он знает (пароль, личный *идентификационный* номер, криптографический ключ и т.п.);
- нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);
- нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).



Основные понятия

В открытой сетевой среде между сторонами *идентификации/аутентификации* не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от ***перехвата***, ***изменения*** и/или ***воспроизведения*** данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от *воспроизведения*. Нужны более сложные протоколы *аутентификации*.

Основные понятия

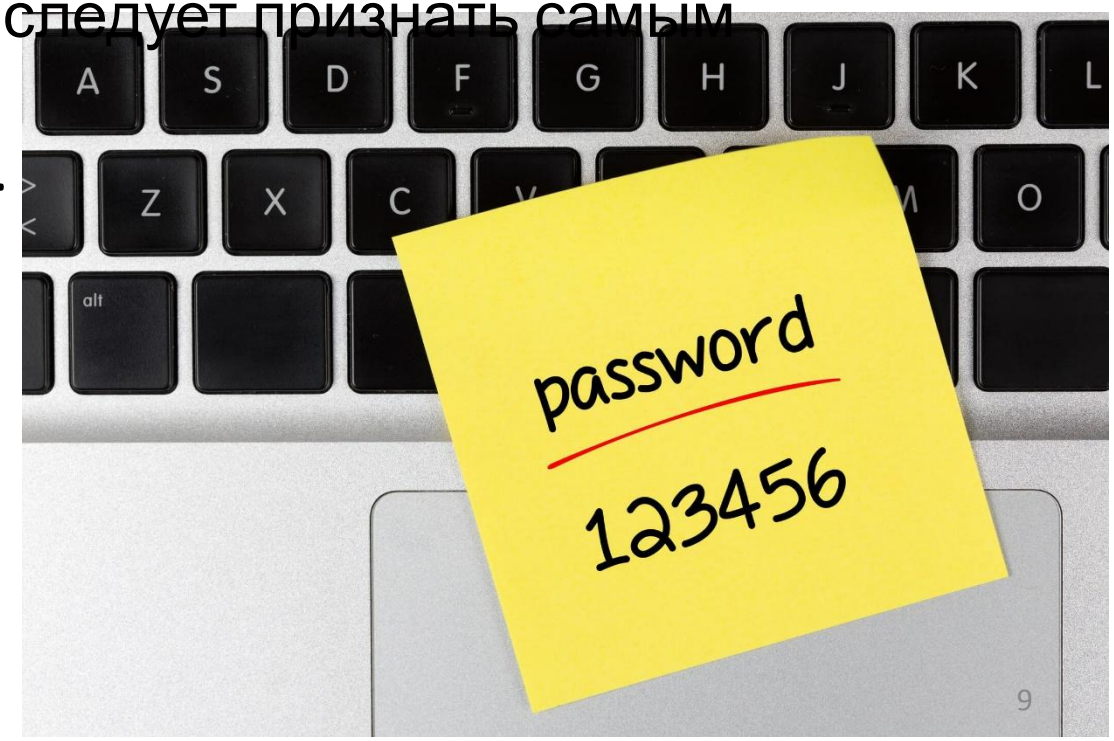
Надежная *идентификация* и затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все *аутентификационные* сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью *аутентификации*, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить *аутентификационную* информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Основные понятия

Современные средства *идентификации/аутентификации* должны поддерживать концепцию *единого входа в сеть*. *Единый вход в сеть* – это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная *идентификация/аутентификация* становится слишком обременительной. К сожалению, пока нельзя сказать, что *единый вход в сеть* стал нормой, доминирующие решения пока не сформировались.

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.



Парольная аутентификация

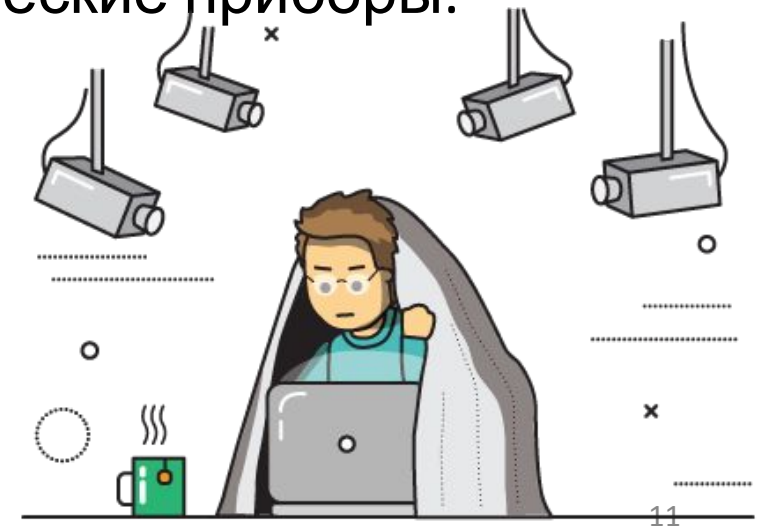
Чтобы пароль был запоминающимся, его зачастую делают простым (имя подруги, название спортивной команды и т. п.). Однако простой пароль нетрудно угадать, особенно если знать пристрастия данного пользователя. Известна классическая история про советского разведчика Рихарда Зорге, объект внимания которого через слово говорил "карамба"; разумеется, этим же словом открывался сверхсекретный сейф.

Плохие пароли	Хорошие пароли
123456789	D)dzq4Smo@
password	4j~8GvG{qB
qwerty	Re18ZEVH1#
master	Hx4@5g8DoJ
login1	%FfZMv4vDu
1a2s3d4f5g	pWjtbQ$g6B

Парольная аутентификация

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. Иногда для подглядывания используются даже оптические приборы.



Парольная аутентификация

Пароли нередко сообщают коллегам, чтобы те могли, например, подменить на некоторое время владельца пароля. Теоретически в подобных случаях более правильно задействовать средства управления доступом, но на практике так никто не поступает; а тайна, которую знают двое, это уже не тайна.

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 (предполагается, что алгоритм шифрования известен).

Парольная аутентификация

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");

Парольная аутентификация

- 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.

Одноразовые пароли

Рассмотренные выше **пароли можно назвать многоразовыми**;

их раскрытие позволяет злоумышленнику действовать от имени легального пользователя. Гораздо более сильным средством, устойчивым к пассивному прослушиванию сети, являются **одноразовые пароли**.

ЧЕК
ОДНОРАЗОВЫЕ ПАРОЛИ

15/03/10 16:31:56
НОМЕР ОПЕРАЦИИ: 0177
ТЕРМИНАЛ: 835239

КАРТА: XXXXXXXXXXXXXX0521 D
НОМЕР ЧЕКА: 007463427529
СПИСОК ПАРОЛЕЙ:

1.ZNFR5NH4	11.D7NNW62R
2.S9HZD7DL	12.4451SDRZ
3.Z8GR62WN	13.ZH1WMR6I
4.5458H4HL	14.6MF7GZD6
5.FRM4SRDS	15.IHVN2M29
6.G44LRF36	16.16328G9W
7.G6V8865Z	17.FFFW9H49
8.VHFMLNV9	18.2N31SFFH
9.HH81WM9I	19.9R19LNWF
10.GF877S35	20.7582GW65

ХРАНИТЕ ЧЕК ОТДЕЛЬНО ОТ КАРТЫ!
ПРИ УТРАТЕ ЧЕКА ИЛИ КОМПРОМЕТАЦИИ
ИНФОРМАЦИИ, УКАЗАННОЙ НА НЕМ,
НЕЗАМЕДЛИТЕЛЬНО ПОЛУЧИТЕ НОВЫЙ

Одноразовые пароли

Наиболее известным программным *генератором одноразовых паролей* является система **S/KEY** компании Bellcore. Идея этой системы состоит в следующем. Пусть имеется **односторонняя функция** f (то есть функция, вычислить обратную которой за приемлемое время не представляется возможным). Эта функция известна и пользователю, и **серверу аутентификации**. Пусть, далее, имеется **секретный ключ** K, известный только пользователю.

Одноразовые пароли

На этапе начального администрирования пользователя функция f применяется к ключу K n раз, после чего результат сохраняется на сервере. После этого процедура проверки подлинности пользователя выглядит следующим образом:

- сервер присылает на пользовательскую систему число (n-1);
- пользователь применяет функцию f к секретному ключу K (n-1) раз и отправляет результат по сети на сервер аутентификации;

Одноразовые пароли

- сервер применяет функцию f к полученному от пользователя значению и сравнивает результат с ранее сохраненной величиной. В случае совпадения подлинность пользователя считается установленной, сервер запоминает новое значение (присланное пользователем) и уменьшает на единицу счетчик (n).

Одноразовые пароли

На самом деле реализация устроена чуть сложнее (кроме счетчика, сервер посылает затравочное значение, используемое функцией f), но для нас сейчас это не важно. Поскольку функция f необратима, *перехват* пароля, равно как и получение доступа к серверу *аутентификации*, не позволяют узнать секретный ключ K и предсказать следующий одноразовый пароль.

Система S/KEY имеет статус Internet-стандарта (RFC 1938).

Одноразовые пароли

Другой подход к надежной *аутентификации* состоит в *генерации нового пароля* через небольшой промежуток времени (например, каждые 60 секунд), для чего могут использоваться программы или специальные интеллектуальные карты (с практической точки зрения такие пароли можно считать одноразовыми). Серверу *аутентификации* должен быть известен алгоритм *генерации паролей* и ассоциированные с ним параметры; кроме того, часы клиента и сервера должны быть синхронизированы.

Аутентификация на основе открытого пароля

Самым старым и простым методом парольной аутентификации является аутентификация на основе открытого пароля (рис. 1).

Рис. 1 – Аутентификация на основе открытого пароля

Пример прохождения пользователем процедуры аутентификации на основе открытого пароля:

1. Пользователь (Андрей) вводит свои имя пользователя и пароль (Qwe12Ty) на рабочей станции.
2. Имя пользователя и пароль передаются по сети в открытом виде.
3. Сервер аутентификации находит учётную запись Андрея в базе данных аутентификации и сравнивает введённые данные с её содержимым.

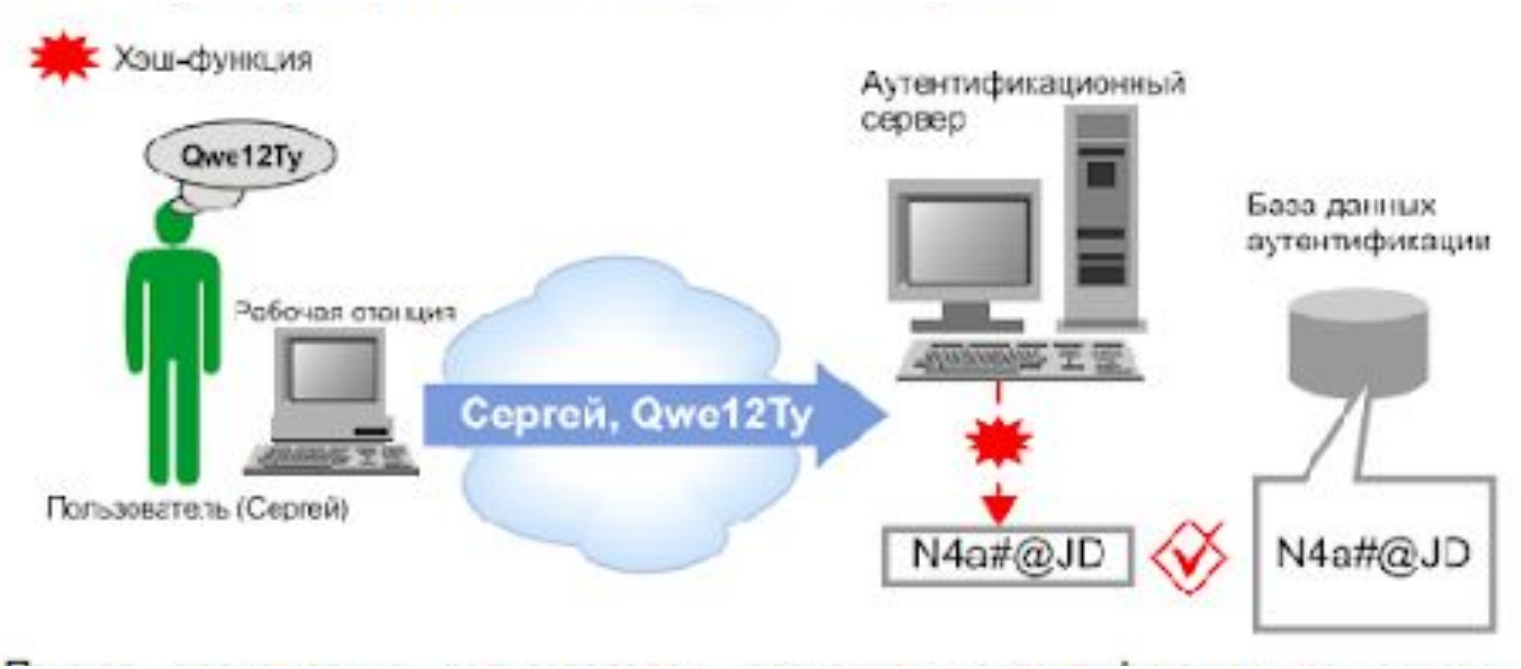


Рис. 2 – Аутентификация на основе хэшированного пароля

Пример прохождения пользователем процедуры аутентификации на основе хэшированного пароля (рис. 2):

1. Пользователь (Сергей) вводит свои имя пользователя и пароль (Qwe12Ty) на рабочей станции.
2. Имя пользователя и пароль передаются по сети в открытом виде.
3. Сервер аутентификации хэширует введённый пароль и находит учётную запись Антона в базе данных аутентификации. Далее сравнивает результат хэширования введенного пользователем пароля (N4a#@JD) с хэшированным паролем пользователя, хранящимся в его учетной записи (N4a#@JD).

Таким образом, если злоумышленник получит доступ к базе данных аутентификации, это ему ничего не даст, так как он не сможет восстановить пароль пользователя из хранящегося в базе хэш-значения.

Достоинства паролей

Все простейшие системы аутентификации используют именно парольный принцип. При этом пользователю достаточно просто знать пароль и правильно ввести его, чтобы получить беспрепятственный доступ к ресурсу, который ему нужен. Поэтому парольная аутентификация является наиболее часто используемой.

Единственным достоинством этого метода является его простота. Этот фактор и то, что метод пароля используется очень давно, появившись раньше, чем все прочие методы, позволяет применять его в большом количестве разнообразных компьютерных программ.

Недостатки

- Пользователи, благодаря собственной неискушенности, часто применяют пароли, которые можно легко и просто угадать. Чаще всего используется пароль в виде производной от идентификатора клиента. Иногда это и сам идентификатор, что очень предсказуемо. Пользователи берут в качестве пароля кличку своей собаки, имя собственного созданного сайта, название хоккейной команды, за которую болеют, фразу, которая является часто употребляемой. Вскрыть подобный пароль умелому злоумышленнику не составляет труда. Есть список общеупотребимых фраз, слов и словосочетаний. Такие списки публикуются в общедоступной литературе, которую читают не только законопослушные граждане. Слишком короткие пароли легко подобрать.
- Пароль может быть попросту перехвачен или подсмотрен в процессе его ввода.
- Пароль можно просто выбить из владельца. Ведь иногда для получения доступа к важным сведениям могут применить и насилие.
- Самый простой способ узнать у пользователя его пароль – это притвориться администратором системы и связаться с пользователем. Тот сам легко и непринужденно откроет лже-администратору все свои секреты. Фишинг – последнее достижение лиходеев на этом поприще. Пользователь обманным путём завлекается на веб-страницу, которая является полной имитацией известной ему страницы разработанного сайта его банка, например. На этой странице он сам вводит все данные своей кредитной карты, чем и открывает мошенникам полный доступ к финансовым средствами, которые на ней находятся. Кстати, для предотвращения неприятностей такого рода и существует взаимная аутентификация, когда не только сервер убеждается в подлинности пользователя, который хочет получить доступ, но и пользователь имеет возможность удостовериться в том, что сервер, на который он попал, является именно тем, куда он и хотел отправиться.

Выводы

Технический прогресс не остановился и в отношении парольной аутентификации. Простота и удобство применения пароля – факторы, которые играют заметную роль, и их наличие хотелось бы сохранить. Поэтому попытки организовать на основе пароля сильную аутентификацию и по сей день не прекращаются.

Разработаны пароли, которые генерируются при помощи специальных программ и аппаратуры. Она неуязвимы для таких вариантов подбора, как словарные атаки. В результате этих усилий возникают очень сложные пароли, которые невозможно разгадать и… запомнить. Пользователи попросту записывают их на бумажку, которую прикрепляет на монитор. О какой секретности может идти речь?

Есть специальные системы, которые обладают особым порядком включения пароля, если пользователь вводит его под принуждением. При этом пользователь применяет определенный пароль, если входит в систему не под давлением. Если же он вынужден войти в систему в силу ряда внешних обстоятельств, он вводит другой пароль, который ему выдается именно на такой случай. Модуль аутентификации получает сигнал о том, что пользователя принуждают к доступу в систему. Существуют специальные программы прозрачного шифрования, которые в этом случае показывают пользователю дезинформацию, которую он сам для такого случая сформировал.

Такая система делает работу под паролем безопаснее, но лишает её единственного преимущества – простоты и доступности.