7. Общие подходы к построению парольных систем и основные угрозы их безопасности

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников.

Эти методы включают следующие разновидности способов аутентификации:

- по хранимой копии пароля или его свёртке;
- по некоторому проверочному значению;
- без непосредственной передачи информации о пароле проверяющей стороне;
- с использованием пароля для получения криптографического ключа.

В первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. **Их слабой стороной является** то, что получение злоумышленником этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь"). Пример системы парольной защиты ("доказательство с нулевым разглашением"), построенной по данному принципу, будет рассмотрен ниже.

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации:

Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств, задействованных в них математических и криптографических преобразований и может быть строго доказана.

Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений:

- **Пароль пользовател**я - некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации.
  Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию.
  Многоразовый пароль может быть использован для проверки подлинности повторно.
- **Учетная запись пользователя** - совокупность его идентификатора и его пароля.
- База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

- Под парольной системой будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей КС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:

- интерфейс пользователя;
- интерфейс администратора;
- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему.

Типы угроз безопасности парольных систем:

1. Разглашение параметров учетной записи через:

- подбор в интерактивном режиме;
- подсматривание;
- преднамеренную передачу пароля его владельцем другому лицу;
- захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
- перехват переданной по сети информации о пароле;
- хранение пароля в доступном месте.

2. Вмешательство в функционирование компонентов парольной системы через:

- внедрение программных закладок;
- обнаружение и использование ошибок, допущенных на стадии разработки;
- выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:

- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
- ввести пароль так, что его смогут увидеть посторонние;
- передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее.

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного (разрушительного) влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей (табл.1).

Требование к выбору пароля	Получаемый эффект
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом "тотального опробования" ***Метод полного (тотального) опробования ключей-*** *Метод анализа криптографического, состоящий в переборе всех возможных ключей криптосистемы с отбраковкой ложных вариантов по некоторому критерию.*
Использование в пароле различных групп символов	Усложняет задачу злоумышленника при попытке подобрать пароль методом "тотального опробования"
Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленника по подбору паролей методом тотального опробования, в том числе без непосредственного обращения к системе защиты (режим off-line)
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию
Ведение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию "
Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником
Запрет на выбор парс-ля самим пользователем и автоматическая генерация паролей	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом "тотального опробования"
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действии системного администратора, имеющего доступ к паролю в момент создания учетной записи

Параметр	Способ определения
Мощность алфавита паролей *A*	Могут варьироваться для обеспечения заданного значения $S(S=A^L)$
Длина пароля L	
Мощность пространства паролей S ′	Вычисляется на основе заданных значений P,T или V
Скорость подбора паролей V: • Для интерактивного режима определяется как скорость обработки одной попытки регистрации проверяющей стороной. • Для режима off-line (на основе свертки пароля) определяется как скорость вычисления значения свертки для одного пробного пароля	• Может быть искусственно увеличена для защиты от данной угрозы. • Задается используемым алгоритмом вычисления свертки. Алгоритм, имеющий медленные реализации, повышает стойкость по отношению к данной угрозе
Срок действия пароля (задает промежуток времени, по истечении которого пароль должен быть обязательно сменен) T	Определяется исходя из заданной вероятности P, или полагается заданным для дальнейшего определения S
Вероятность подбора пароля в течение его срока действия (подбор продолжается непрерывно в течение всего срока действия пароля) P	Выбирается заранее для дальнейшего определения S или T

В качестве иллюстрации рассмотрим задачу определения минимальной мощности пространства паролей (зависящей от параметров A и L) в соответствии с заданной вероятностью подбора пароля в течение его срока действия.

Задано P=10-6. Необходимо найти минимальную длину пароля, которая обеспечит его стойкость в течение одной недели непрерывных попыток подобрать пароль. Пусть скорость интерактивного подбора паролей V=10 паролей/мин.

Тогда в течение недели можно перебрать: $10 \cdot 60 \cdot 24 \cdot 7 = 100800$ паролей.

Далее, учитывая, что параметры S, V, T и P связаны соотношением P $P=V \cdot T/S$, получаем

$S = 100 \cdot 800/10^{-6} = 1{,}008 \cdot 10^{11} \approx 10^{11}$

Полученному значению S соответствуют пары: A=26, L=8 и A=36, L=6.

Другим важным аспектом стойкости парольной системы, является способ хранения паролей в базе данных учетных записей. Возможны следующие варианты хранения паролей:

- в открытом виде;
- в виде свёрток (хеширование);
- зашифрованными на некотором ключе.

Наибольший интерес представляют второй и третий способы, которые имеют ряд особенностей.

Хеширование не обеспечивает защиту от подбора паролей по словарю в случае получения базы данных злоумышленником. При выборе алгоритма хеширования, который будет

использован для вычисления сверток паролей, необходимо гарантировать несовпадение значений сверток, полученных на основе различных паролей пользователей. Кроме того, следует предусмотреть механизм, обеспечивающий уникальность сверток в том случае, если два пользователя выбирают одинаковые пароли. Для этого при вычислении каждой свертки обычно используют некоторое количество "случайной" информации, например, выдаваемой генератором псевдослучайных чисел.

При шифровании паролей особое значение имеет способ генерации и хранения ключа шифрования базы данных учетных записей.

Перечислим некоторые возможные варианты:

- ключ генерируется программно и хранится в системе, обеспечивая возможность ее автоматической перезагрузки;
- ключ генерируется программно и хранится на внешнем носителе, с которого считывается при каждом запуске;
- ключ генерируется на основе выбранного администратором пароля, который вводится в систему при каждом запуске.

Процедура опознавания с использованием простого пароля может быть представлена в виде следующей последовательности действий:

- пользователь посылает запрос на доступ к компьютерной системе и вводит свой идентификатор;
- система запрашивает пароль;
- пользователь вводит пароль;
- система сравнивает полученный пароль с паролем пользователя, хранящимся в базе эталонных данных системы защиты, и разрешает доступ, если пароли совпадают; в противном случае пользователь к ресурсам компьютерной системы не допускается.

Поскольку пользователь может допустить ошибку при вводе пароля, то системой должно быть предусмотрено допустимое количество повторений для ввода пароля.

В базе эталонных данных пароли, как и другую информацию, никогда не следует хранить в явной форме, а только зашифрованными. При этом можно использовать метод как обратимого, так и необратимого шифрования.

Согласно методу обратимого шифрования, эталонный пароль при занесении в базу эталонных данных зашифровывается по ключу, совпадающему с этим эталонным паролем, а введенный после идентификации пароль пользователя для сравнения с эталонным также зашифровывается по ключу, совпадающему с этим введенным паролем.

Таким образом, при сравнении эталонный и введенный пароли находятся в зашифрованном виде и будут совпадать только в том случае, если исходный введенный пароль совпадет с исходным эталонным.

При несовпадении исходного введенного пароля с исходным эталонным исходный введенный пароль будет зашифрован по-другому, так как ключ шифрования отличается от ключа, которым зашифрован эталонный пароль, и после зашифровки не совпадет с зашифрованным эталонным паролем.

Для обеспечения возможности контроля правильности ввода пароля при использовании необратимого шифрования на винчестер записывается таблица преобразованных паролей.

Для их преобразования используется односторонняя криптографическая функция $y= F(x)$, обладающая следующим свойством: для данного аргумента x значение $F(x)$ вычисляется легко, а по данному y вычислительно сложно найти значение аргумента x, соответствующего данному y.

В таблице паролей хранятся значения односторонних функций, для которых пароли берутся в качестве аргументов. При вводе пароля система зашиты легко вычисляет значение функции от пароля текущего пользователя и сравнивает со значением, приведенным в таблице для пользователя с выбранным идентификатором.

Нарушитель, захвативший компьютер, может прочитать таблицу значений функций паролей, однако вычисление пароля практически не реализуемо.

При работе с паролями должна предусматриваться и такая мера, как недопустимость их распечатки или вывода на экраны мониторов. Поэтому система защиты должна обеспечивать ввод пользователями запрошенных у них паролей без отображения этих паролей на мониторах.

Можно выделить следующие основные способы повышения стойкости системы защиты на этапе аутентификации:

- повышение степени нетривиальности пароля;
- увеличение длины последовательности символов пароля;
- увеличение времени задержки между разрешенными попытками повторного ввода неправильно введенного пароля;
- повышение ограничений на минимальное и максимальное время действительности пароля.

Чем нетривиальнее пароль, тем сложнее его запомнить. Плохо запоминаемый пароль может быть записан на листе бумаги, что повышает риск его раскрытия. Выходом здесь является использование определенного числа не записываемых на бумаге пробелов или других символов в начале, внутри, а также в конце последовательности основных символов пароля.

Кроме того, отдельные символы пароля могут набираться на другом регистре (например, вместо строчных быть прописными или наоборот), что также не должно отражаться на листе бумаги. В этом случае незаконно полученный лист бумаги с основными символами пароля не будет достаточным условием раскрытия пароля целиком.

Для исключения необходимости запоминания пользователями длинных и нетривиальных паролей в системе защиты может быть предусмотрена возможность записи паролей в зашифрованном виде на информационные носители, например, флешки, магнитные карты, носители данных в микросхемах и т. д., а также считывания паролей с этих информационных носителей.

Такая возможность позволяет повысить безопасность за счет значительного увеличения длины паролей, записываемых на носители информации. Однако при этом администрации службы безопасности следует приложить максимум усилий для разъяснения пользователям ВС о необходимости тщательной сохранности носителей информации с их паролями.

На степень информационной безопасности при использовании простого парольного метода проверки подлинности пользователей большое влияние оказывают ограничения на минимальное и максимальное время действительности каждого пароля. Чем чаше меняется пароль, тем обеспечивается большая безопасность.

Минимальное время действительности пароля задает время, в течение которого пароль менять нельзя, а максимальное — время, по истечении которого пароль будет недействительным.

Соответственно, пароль должен быть заменен в промежутке между минимальным и максимальным временем его существования. Поэтому понятно, что более частая смена пароля обеспечивается при уменьшении минимального и максимального времени его действительности.

Минимальное и максимальное времена действительности пароля задаются для каждого пользователя администратором службы безопасности, который должен постоянно контролировать своевременность смены паролей пользователей.

При выборе пароля руководствуйтесь следующими инструкциями:

- Не указывайте свой ИД пользователя, а также всевозможные его модификации (в обратном порядке, удвоенный) в качестве пароля.
- Не используйте пароли повторно. Повторное использование паролей может быть запрещено конфигурацией системы.
- Не указывайте в качестве паролей личные имена.
- Не указывайте в качестве пароля слова, хранящиеся в электронных орфографических словарях.
- Длина пароля должна составлять не менее шести символов.

- Не указывайте в качестве паролей ругательства; при угадывании паролей их пробуют прежде всего.
- Выбирайте легко запоминающиеся пароли, чтобы вам не пришлось их записывать.
- Выбирайте пароли, содержащие цифры, а также строчные и прописные буквы.
- Рекомендуется задавать пароли, состоящие из двух слов, разделенных цифрами.
- Выбирайте легко произносимые пароли. Их легче запомнить.
- Не записывайте пароль. Если все же возникает необходимость записать его, поместите запись в надежное место, например, в сейф.