А.И. Кучеров, А.В. Воруев
УО «Гомельский государственный университет
имени Франциска Скорины», Гомель, Беларусь

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ ПОДБОРА ПАРОЛЯ ЗЛОУМЫШЛЕННИКОМ В ТЕЧЕНИЕ СРОКА ЕГО ДЕЙСТВИЯ

Введение

В век информационных технологий информация имеет большую ценность и прежде всего в электронном виде, поэтому необходимо защищать вычислительные системы от несанкционированного использования.

Рассмотрим теоретические и практические аспекты по определению вероятности подбора пароля в течении срока его действия.

1. Теоретические сведения

Подсистемы идентификации и аутентификации пользователя играют важную роль в системах защиты информации (рисунок 1).

Стойкость подсистемы идентификации и аутентификации пользователя в системе защиты информации во многом определяет устойчивость к взлому самой системы защиты информации. Данная стойкость определяется гарантией того, что злоумышленник не сможет пройти аутентификацию, присвоив чужой идентификатор или завладев им.

Парольные системы аутентификации являются одними из основных и наиболее распространенных в системах защиты информации методами пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только зарегистрированному пользователю вычислительной системы.

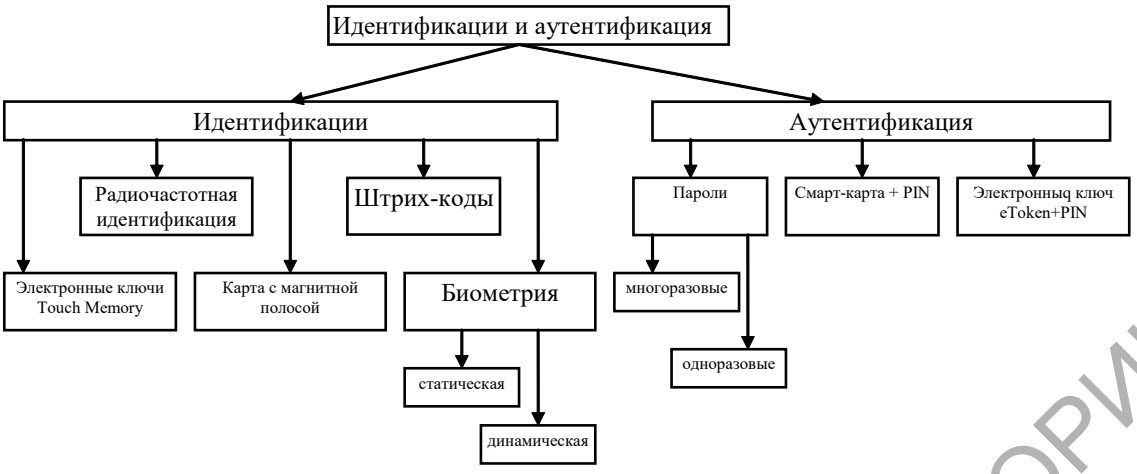

Рисунок 1 – Классификация технологий идентификации и аутентификации

Парольная аутентификация пользователя, как правило, первая ступень обороны системы защиты информации. В связи с этим модуль аутентификации по паролю наиболее часто подвергается атакам со стороны злоумышленника. Целью злоумышленника в этом случае будет подбор аутентифицирующей информации, то есть пароля зарегистрированного пользователя.

Методы парольной аутентификации пользователя наиболее просты и при несоблюдении определенных требований к выбору пароля являются достаточно уязвимыми.

Поэтому во многом от стойкости парольной системы защиты зависит успешность реализации злоумышленником своих замыслов. Существует множество реализаций парольных систем, в структуре которых можно выделить несколько наиболее важных компонентов:

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

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

1. Установление минимальной длины пароля (рекомендуется не менее 8 символов).

2. Использование в пароле различных групп символов (малые и большие латинские буквы, цифры, специальные символы ‘(’, ‘)’, ‘#’ и т. д.).

3. Проверка и отбраковка пароля по словарю (в качестве пароля не должны использоваться реальные слова, имена, фамилии и т. д).

4. Установление максимального срока действия пароля.

5. Ведение журнала истории паролей. Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории.

6. Ограничение числа попыток ввода пароля.

7. Поддержка режима принудительной смены пароля пользователя.

8. Использование задержки при вводе неправильного пароля.

9. Запрет на выбор пароля самими пользователями и автоматическая генерация паролей.

10. Принудительная смена пароля при первой регистрации пользователя в системе.

2. Количественная оценка стойкости парольной защиты

Как правило, для генерирования паролей в системе защиты информации, удовлетворяющих перечисленным требованиям к паролям, используются программы – автоматические генераторы паролей пользователей.

При выполнении перечисленных требований к паролям и к подсистеме па-рольной аутентификации единственно возможным методом взлома данной подсистемы злоумышленником является прямой перебор паролей. В данном случае, оценка стойкости парольной защиты осуществляется следующим образом.

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля. Если пароль состоит только из малых букв английского алфавита, то A = 26. Если, например, пароль состоит из малых и больших букв русского алфавита, то A = 66, и т.д. и т.п.

Пусть L – длина пароля в знаках. Может изменяться для обеспечения заданной стойкости парольной системы.

$S = A^L$ – мощность пространства паролей, т. е. множество всех возможных паролей в системе длины L, которые можно составить из символов алфавита A.

V – скорость подбора пароля (соответственно различают скорость подбора пароля для интерактивного (1-2 паролей / минуту) и неинтерактивного (10 и более паролей / секунду) подбора паролей). T – срок действия (жизни) пароля (обычно задается в днях). P – вероятность подбора пароля в течение срока его действия.

Тогда, вероятность P подбора пароля злоумышленником в течение срока его действия определяется следующим образом:

$$P = \frac{V * T}{S} = \frac{V * T}{A^L}, \quad (1)$$

В конкретной ситуации задают некоторые желательные значения для одних параметров (например, очень маленькое значение вероятности подбора пароля) и высчитывают остальные параметры. Очевидно, что с увеличением длины пароля и/или мощности алфавита паролей вероятность подбора пароля уменьшается. А при увеличении срока жизни пароля, вероятность его подбора увеличивается.

Пример. Задание: определить время перебора всех паролей, состоящих из 8 цифр и вероятность подбора пароля злоумышленником P при сроке действия пароля 30 дней.

Решение: алфавит составляют цифры (A=10). Длина пароля 8 символов (L=8). Таким образом, получаем количество вариантов: $S=A^L=10^8$ (паролей), T=30 дней.

Примем скорость перебора паролей V=1000 паролей/секунду. Получаем время перебора всех паролей

$$t = \frac{S}{V} = \frac{10^8}{1000} = 10^5 секунд \approx 1667 минут \approx 28 часов \approx 1{,}2 дня$$

Примем, что после каждого из m = 3 неправильно введенных паролей идет пауза в τ = 5 секунд. Получаем продолжительность всех пауз при переборе всех паролей

$$t_{пауза} = \frac{S * \tau}{m} = \frac{10^8 * 5}{3} = 166666667 секунд \approx 2777778 минут \approx 46296 часов \approx 1929 дней$$

Время перебора всех паролей $t_{Итог} = t + t_{пауза} = 1{,}2 + 1929 = 1930{,}2 дня$

вероятность подбора пароля $P = \frac{V * T}{S} = \frac{V * T}{A^L} = \frac{1000 * 30}{10^8} = 0{,}0003$

Таким образом, за счет введения пауз при неправильном вводе пароля мы можем существенно увеличить время интерактивного подбора пароля.

Заключение

При соблюдении приведенного ряда требований к выбору и использованию паролей можно добиться эффекта существенной защиты от подбора паролей злоумышленником. Но существуют и другие методы при помощи, которых злоумышленник может получить доступ к вычислительной системе. Для этих целей существуют и другие мето-

ды защиты вычислительной системы от несанкционированного использования (рисунок 2).

Рисунок 2 – Защита вычислительной системы от несанкционированного использования

Литература

1. Кучеров, А.И. Методика повышения надежности вычислительных систем / А.И. Кучеров // Известия Гомельского государственного университета им. Ф.Скорины. – 2012. – № 6 (75). – С. 120–123.

2. Мещеряков, Р.В. Теоретические основы компьютерной безопасности [Текст]: лабораторный практикум для студентов специальности 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем» / Мещеряков Р.В., Праскурин Г.А., Шелупанов А.А.; М-во образования и науки Российской Федерации, Федеральное гос. бюджетное образовательное учреждение высшего профессионального образования, “Томский гос. ун-т систем управления и радиоэлектроники” (ТУСУР), Каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС). – Томск: В-Спектр, 2012. – 63 с.

3. Кучеров, А.И. Получение информации об интенсивности использовании ЭВМ с целью дальнейшего повышения ее надежности / А.И. Кучеров // Известия Гомельского государственного университета им. Ф. Скорины. – 2013. – № 6 (81). – С. 125–129.

4. Кучеров, А.И. Инициализация начального состояния компьютера для реализации экспериментов по надежности узла локальной вычислительной сети / А.И. Кучеров, А.В. Воруев, В.Д. Левчук // Изве-

стия Гомельского государственного университета им. Ф. Скорины. – 2015. – № 6 (93). – С. 64–68.

5. Демиденко, О.М. Сравнительный анализ математических методов повышения надежности информационных и технических систем / О.М. Демиденко, А.И. Кучеров // Проблемы физики, математики, техники. – 2015. – № 1 (22). – С. 92–97.

6. Кучеров, А.И. Архитектура программного инструментария по обеспечению надежности узла ЛВС / А.И. Кучеров, А.В. Воруев, О.М. Демиденко, В.Д. Левчук // Проблемы физики, математики и техники. – 2017. – № 4(33). – С. 100–103.