Швейкин Владислав Витальевич
студент
ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»
г. Самара, Самарская область

АТАКИ НА БАЗЫ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ПОДБОРА ПАРОЛЕЙ

Аннотация: *в данной статье рассматриваются основные методы реализации несанкционированных прав с использованием манипуляций паролями. Автором представлены базовые технологии подбора паролей.*

Ключевые слова: *пароль, подбор, угроза, информационная безопасность, базы данных.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. СУБД (система управления базами данных) – программно-аппаратный комплекс, позволяющий управлять и манипулировать базами данных.

Определение 2. Информационная система – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

Введение

Каждая многопользовательская система обработки данных предусматривает процедуры идентификации и аутентификации пользователей и процессов как обязательное предусловие предоставления прав доступа к ресурсам системы. На сегодняшний день широко распространена технология аутентификации с использованием паролей. В связи с эти технология подбора паролей так же находится на достаточно высоком уровне развития.

Можно выделить некоторые методы подбора паролей пользователей:

1. Полный перебор. Используя этот метод, злоумышленник последовательно проверяет все возможные варианты пароля. Сложность полного перебора зависит от количества возможных решений задачи. Таким образом, при достаточной длине пароля метод может быть признан эффективным.

2. Полный перебор, оптимизированный по статистике встречаемости символов. Символы, встречающиеся в паролях пользователей, имеют разную вероятность. Различные исследования показывают, что статистика встречаемости символов в алфавите паролей близка к статистике встречаемости символов в естественном языке. На практике злоумышленник начнёт перебор паролей, состоящих из наиболее встречающихся символов, за счёт чего время перебора сокращается. В некоторых случаях для подбора паролей используется не только статистика встречаемости одного символа, но и статистика встречаемости комбинаций из двух и трёх последовательных символов – биграмм и триграмм соответственно.

Существует две базовых технологии подбора паролей:

1) последовательная генерация паролей и подача их на вход подсистемы аутентификации;

2) расчёт значения хэш-функции и её сравнения с известным образом пароля. Данный вариант позволяет при известном образе пароля эффективно распараллелить и решить задачу без активного взаимодействия с атакуемой системой.

3. Оптимизированный полный перебор с использованием словарей. Во многих случаях пароли пользователей представляют собой слова английского или русского языка. Используя данный метод, злоумышленник сначала опробует в качестве пароля все слова из словаря, который содержит наиболее вероятные пароли. Как правило, данный метод используется в комбинации с предыдущим методом.

4. Подбор пароля с использованием знаний о пользователе. Некоторые пользователи, чтобы не забыть пароль, выбирают в качестве пароля информацию о себе (имя, фамилию, дату рождения и т. д.). Если злоумышленник достаточно

изучил пользователя, то вероятность получить пароль методом подбора пароля увеличивается.

В заключении следует отметить, что в большинстве информационных систем базовые процедуры аутентификации на основе паролей построены на сравнении вычисляемой значения хэш-функции от вводимого пароля с хранимым образом пароля, который приписан для каждого пользователя.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.

2. Дейт К.Дж. Введение в системы баз данных. – 8-е изд. – М.: Вильямс, 2005. – 1328 с.