Актуальные уязвимости в системах контроля доступа

Миланович Евгений Александрович, студент магистратуры
Белорусский государственный университет информатики и радиоэлектроники (г. Минск)

Контроль доступа предотвращает несанкционированный доступ к объектам, которые включают доступ к информационным системам, таким как линии связи, сети, компьютеры, услуги и конфиденциальные данные. Методы защиты информации в сочетании с контролем доступа обеспечивают защиту от несанкционированного раскрытия и изменения информации.

С другой стороны, нарушение контроля доступа продолжает оставаться самой распространенной уязвимостью веб-приложений. Эта уязвимость концептуально проста — приложение позволяет пользователю делать то, на что у него нет разрешений. Несколько атак могут быть успешны, просто используя эту уязвимость. В этой статье будут рассмотрены самые актуальные и распространенные атаки нарушения контроля доступа, которые пытаются обойти методы управления доступом.

Переполнение буфера или стека

На сегодняшний день это открывает двери для наиболее распространенных и успешных системных атак. Хотя оно часто сопровождается атаками DoS, что, в свою очередь, делает ресурс недоступным, переполнение стека в приложении или системе может помочь злоумышленнику получить несанкционированный доступ к каталогу или системе. Как правило, переполнение происходит, когда протокол или приложение пытается сохранить информацию за пределами своих выделенных ресурсов. Это может привести к повреждению данных, находящихся в стеке, или к аварийному завершению приложения, или к другому ошибочному или неожиданному поведению. Например, Teardrop Attack — тип атаки переполнения стека, использует уязвимости протокола IP.

Агрегированные атаки доступа

Атаки на регулирование доступа обычно крадут учетные данные пользователя и подражают ему для создания некоторых предварительных пассивных атак. Одной из таких атак является агрегация доступа, которая объединяет несколько нечувствительных данных для получения конфиденциальных данных. Например, данные о рождении, в совокупности с именем, могут быть паролем пользователя.

Разведывательные атаки — это атаки агрегации доступа, которые объединяют несколько инструментов для сбора системных показателей, таких как баннер сервера, IP-адрес, открытые порты и операционная система, для запуска атаки.

Атака на пароли

Поскольку пароли являются самой слабой формой аутентификации, злоумышленники могут легко преуспеть в этой атаке и получить доступ к ресурсам, которые доступны для взломанной учетной записи. Если злоумышленник обошел пароль администратора или root, он может получить доступ к любой другой учетной записи, а также к ее ресурсам. В худшем случае злоумышленник создает другие учетные записи в качестве бэкдора для последующего доступа к приложению.

Злоумышленники выполняют атаки на пароли, используя несколько методов, таких как:

- **Атака по словарю**

Под атакой по словарю понимается попытка найти пароль путем применения каждого возможного пароля в списке ожидаемого пароля или предопределенной базы данных. База данных атаки по словарю обычно включает символы, которые обычно не встречаются в общем словаре, но часто используются в качестве паролей.

- **Атака перебором (Brute-Force)**

Brute-Force включает в себя перебор каждой возможной комбинации цифр, букв, а также символов для обнаружения пароля. Вместо ручного перебора злоумышленники используют программы, с помощью которых проверяют все комбинации автоматически. Они также могут усиливать гибридные атаки, выполняя атаку методом перебора после атак по словарю. В настоящее время, в качестве улучшенной защиты, пароли не хранятся и не передаются в виде открытого текста, а в хешированном виде. Однако некоторые инструменты для атаки на пароли теперь достаточно компетентны для поиска паролей с таким

же значением хеш-функции, что и в базе данных учетных записей. Следовательно, злоумышленникам не нужно находить действительный пароль, вместо этого они могут использовать пароль, который дает такое же значение хеш-функции.

• **Атака по радужным таблицам** (Rainbow Table Attack)

Такие процессы, как угадывание пароля, его хеширование и сравнение с целевым паролем занимают очень много времени. Однако злоумышленники сократили время с помощью радужной таблицы, в которой можно найти предварительно вычисленные значения хеш-функции для угаданных паролей. Взломщик может сравнивать каждое хеш-значение в радужной таблице в противовес хеш-значениям в захваченном файле базы данных. Вместо того, чтобы тратить время на угадывание паролей и вычисление хэшей, здесь они сравнивают только хэши, чтобы взломать пароль.

• **Прослушивание сети** (Sniffer Attacks)

Он также известен как сниффинг, анализатор пакетов или анализатор протоколов. Он использует анализаторы для мониторинга трафика и собирает информацию, передаваемую по сети. С помощью сниффера злоумышленник может получить любую информацию, включая общие ключи, имена пользователей и пароли, переданные в виде открытого текста.

Атаки подмены

Она также известна как маскирующая атака, которая включает в себя доступ к ИТ-системе с использованием чужих учетных данных. Существуют различные типы атак подмены, такие как:

• **Подмена IP-адреса**: злоумышленник заменяет исходный IP-адрес поддельным, чтобы выдать себя за систему или скрыть свою личность;

• **Подмена электронной почты**: злоумышленник заменяет поле «от кого» в электронной почте, чтобы создать впечатление, что это электронное письмо отправлено надежным источником;

• **Подмена номера телефона**: злоумышленник подделывает номер телефона с помощью идентификатора вызывающего абонента. Этот метод обычно используется в системах VoIP (Voice Over Internet Protocol).

Атаки социальной инженерии

Атака социальной инженерии заставляет жертву выполнить действие, которое он обычно не выполняет, или раскрыть информацию, которой она обычно не делится. В этот тип атаки вовлечен широкий спектр техник, таких как:

• **Плечевой серфинг**: социальные инженеры пытаются прочитать информацию на экране через плечо жертвы.

• **Фишинг**: это вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей [3] в результате нажатия на ссылку или открытия вложения. Кроме того, эта атака также намеревается установить вредоносную программу.

• **Квид про кво** (услуга за услугу): данный вид атаки подразумевает обращение злоумышленника в компанию по корпоративному телефону (используя актёрское мастерство [1]) или электронной почте. Зачастую злоумышленник представляется сотрудником технической поддержки, который сообщает о возникновении технических проблем на рабочем месте сотрудника и предлагает помощь в их устранении. В процессе «решения» технических проблем злоумышленник вынуждает цель атаки совершать действия, позволяющие атакующему запускать команды или устанавливать различное программное обеспечение на компьютере жертвы. [2]

• **Телефонный фишинг**: эта атака делает автоматический звонок жертве, объясняющей проблему с их банковским счетом или другим важным счетом. Это подталкивает пользователя к вводу конфиденциальных данных, таких как номер кредитной карты или код безопасности, для проверки информации. Эта атака происходит путем подмены номера телефона для маскировки действующего банка или другого финансового учреждения.

Атаки с помощью смарт-карт

Хотя смарт-карта обеспечивает лучший контроль аутентификации, чем пароль, она также может быть подвержена атакам контроля доступа. Атака по побочному каналу, разновидность атаки с использованием смарт-карт, направлена на наблюдение за функционированием устройства. Успешная атака может заставить злоумышленника наблюдать ценную информацию, присутствующую на смарт-карте, например, ключ шифрования. Эта атака обнаруживает информацию, анализируя детали, передаваемые считывателю, или измеряя энергопотребление с помощью атаки мониторинга мощности.

Атаки отказа в обслуживании

Отказ в обслуживании или DoS блокирует систему от обработки или ответа на любые запросы или доступ к ресурсам. При сбое управления доступом злоумышленники берут на себя управление системой и вынуждают зараженную систему перезагружаться или иногда потребляют ее ресурсы. Следовательно, он больше не может продолжать свою работу.

Различные атаки могут быть успешными за счет использования уязвимостей взлома контроля доступа. Организация должна предпринять серьезные усилия для укрепления системы контроля доступа для предотвращения этих атак.

Литература:

1. Социальная инженерия [электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Социальная_инженерия

2. Никишова, А. В., Чурилина А. Е. Программный комплекс обнаружения атак на основе анализа данных реестра// Вестник ВолГУ. Серия 10. Инновационная деятельность. Выпуск 6. 2012 г. В.: Изд-во ВолГУ, 2012, стр. 152—155
3. Федеральная торговая комиссия [электронный ресурс]. Режим доступа: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams