УДК 004.056.53

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СУЩЕСТВУЮЩИХ МЕТОДОВ ОБНАРУЖЕНИЯ BRUTE-FORCE АТАК В СИСТЕМАХ АУТЕНТИФИКАЦИИ

Т.А. Мельникова, В.В. Васькевич
Учреждение образования «Гомельский Государственный университет имени Франциска Скорины», г. Гомель, Республика Беларусь

Аннотация. В статье рассматриваются основные подходы к обнаружению атак методом полного перебора в системах аутентификации. Проводится сравнительный анализ пороговых, статистических методов, методов на основе машинного обучения, поведенческого анализа и гибридных подходов. Для каждого метода определены преимущества и недостатки. Сформулированы рекомендации по выбору метода в зависимости от архитектуры системы и модели угроз.
Ключевые слова: техническая средства защиты информации; brute-force атака; обнаружение атак; угроза; уязвимости; система аутентификации; механизмы защиты; информационная безопасность; машинное обучение; системы обнаружения вторжений.

COMPARATIVE ANALYSIS OF EXISTING METHODS FOR DETECTING BRUTE-FORCE ATTACKS IN AUTHENTICATION SYSTEMS

T.A. Melnikova, V.V. Vaskevich
Educational Institution "Francysk Skaryna Gomel State University", Gomel, Republic of Belarus

Abstract. The article discusses the main approaches to detecting brute-force attacks in authentication systems. A comparative analysis of threshold methods, statistical methods, machine learning-based methods, behavioral analysis and hybrid approaches is carried out. Advantages and disadvantages are defined for each method. Recommendations on the choice of the method are formulated depending on the architecture of the system and the threat model.
Keywords: technical means of information protection; brute-force attack; attack detection; threat; vulnerabilities; authentication system; protection mechanisms; information security; machine learning; intrusion detection systems.

Введение

Атаки методом полного перебора остаются одной из наиболее распространенных угроз для систем аутентификации. Несмотря

на кажущуюся примитивность, они продолжают эволюционировать. Классические механизмы защиты все чаще оказываются недостаточными – они либо создают вектор для denial-of-service атак на легитимных пользователей, либо пропускают распределенные атаки, в которых количество попыток с одного IP-адреса удерживается ниже порога.

Основная часть

Для предотвращения brute-force атак применяются пороговые, статические, методы на основе машинного обучения, поведенческий анализ, методы на основе CAPTCHA и proof-of-work, методы на основе анализа графов и репутации.

Пороговые методы основаны на подсчете неудачных попыток аутентификации за заданное время и сравнении с установленным порогом. При его достижении происходит блокировка учетной записи либо ограничение числа запросов с одного IP-адреса. Метод прост в реализации, требует минимальных вычислительных ресурсов и эффективен против нераспределенных атак. Однако он уязвим к распределенным атакам и password spraying, при которых ни один IP-адрес или учетная запись не набирает достаточного числа неудачных попыток. Выбор порога неоднозначен: низкое значение ведет к блокировке легитимных пользователей, высокое – к пропуску атак.

Статистические методы анализируют отклонения паттернов аутентификации от модели нормального поведения, учитывая не только количество неудачных попыток, но и характеристики распределения запросов. К основным подходам относятся: анализ на основе распределения запросов (например, пуассоновского), метод кумулятивных сумм для обнаружения изменений в потоке событий, анализ энтропии целевых учетных записей и IP-адресов, а также последовательный анализ Вальда с контролируемым уровнем ошибок. Эти методы обладают более высокой точностью, способны обнаруживать медленные атаки и password spraying. Вместе с тем они требуют периода обучения, чувствительны к изменениям легитимного поведения и сложнее в настройке [1].

Методы на основе машинного обучения автоматически строят модели классификации или обнаружения аномалий, выявляя сложные нелинейные зависимости в данных. Обучение с учителем использует размеченные наборы данных с примерами атак, обучение без учителя обнаруживает аномалии как отклонения от нормального кластера. Учитываемые признаки включают число и соотношение неудачных попыток, интервалы между ними, число уникальных целевых записей с одного IP, географию источников, характеристики User-Agent и другие. Методы ML обеспечивают высокую точность обнаружения распределенных

и адаптивных атак, однако зависят от качества обучающих данных, требуют значительных вычислительных ресурсов, подвержены переобучению и снижению точности при изменении стратегий атакующих.

Поведенческий анализ строит профиль нормального поведения каждого пользователя и обнаруживает отклонения от него, учитывая временные и географические паттерны, характеристики устройств, ритм набора пароля и сетевые параметры. Метод эффективен при обнаружении credential stuffing и password spraying, устойчив к адаптации атакующего и минимизирует ложноположительные срабатывания. К недостаткам относятся высокие требования к хранению данных, проблемы конфиденциальности и снижение точности при изменении привычек пользователя [2].

CAPTCHA требует решения задачи, трудной для автоматизации, reCAPTCHA v3 присваивает оценку риска без явного взаимодействия с пользователем, proof-of-work требует выполнения вычислительно затратной операции. Эти методы увеличивают стоимость атаки, но не обнаруживают ее – они лишь замедляют перебор. При этом классические CAPTCHA ухудшают процесс погружения пользователя в процесс, а существующие сервисы и ML-алгоритмы позволяют обходить многие их виды.

Методы на основе анализа графов и репутации моделируют взаимосвязи между IP-адресами, учетными записями и устройствами в виде графа, выявляя аномальные структуры. IP-репутация использует внешние базы для оценки риска источника, а коллективная разведка угроз (Threat Intelligence) обеспечивает обмен индикаторами компрометации. Методы эффективны при обнаружении координированных распределенных атак и ботнетов, однако зависят от актуальности репутационных баз и дают ложные срабатывания при использовании VPN легитимными пользователями.

Гибридные методы объединяют несколько подходов для компенсации индивидуальных недостатков – например, пороговый метод отсеивает очевидные атаки, а ML-модель анализирует оставшийся трафик. Такой подход обеспечивает наивысшую точность и устойчивость к обходу, позволяет адаптировать архитектуру под конкретную модель угроз и поэтапно внедрять новые компоненты. Основные ограничения – сложность внедрения и сопровождения, увеличение задержки обработки запросов и высокая стоимость разработки и эксплуатации.

Заключение

Проведенный сравнительный анализ показывает, что ни один метод не является универсальным. Пороговые методы достаточны для простых

атак, но неэффективны против распределенных и адаптивных угроз. Методы машинного обучения демонстрируют наивысшую точность, однако ограничены проблемами качества данных и вычислительными затратами. Поведенческий анализ наиболее устойчив к адаптации атакующего, но требует значительных инвестиций. Оптимальным решением для большинства систем является гибридный подход, комбинирующий методы различных категорий, однако при этом стоимость защиты должна быть соизмерима стоимости защищаемых активов и ожидаемому ущербу от успешной атаки.

Список использованных источников

1. Марков А. С., Цирлов В. Л. (2020) Выявление аномалий в сетевом трафике с использованием статистических методов и кумулятивных сумм. Безопасность информационных технологий. 27(2), 34–45.

2. Ольков С. А. (2021) Поведенческий анализ пользователей в системах непрерывной аутентификации. Проблемы информационной безопасности. Компьютерные системы. (1), 60–68.

References

1. Markov A. S., Tsirlov V. L. (2020) Detection of anomalies in network traffic using statistical methods and cumulative sums. Information Technology Security. 27(2), 34–45 (in Russian).

2. Olek S. A. (2021) Behavioral analysis of users in continuous authentication systems. Problems of information security. Computer systems. (1), 60–68 (in Russian).

Сведения об авторах

Мельникова Т.А., студентка 4 курса факультета физики и информационных технологий специальности «Компьютерная безопасность», учреждение образования «Гомельский Государственный университет имени Франциска Скорины», mva_tanya@mail.ru.

Васькевич В.В., старший преподаватель кафедры радиофизики и электроники, учреждение образования «Гомельский Государственный университет имени Франциска Скорины», vaskevich@gsu.by.

Information about the authors

Melnikova T., 4nd year student of the Faculty of Physics and Information Technology specialty "Computer security", Francysk Skaryna Gomel State University, mva_tanya@mail.ru.

Vaskevich V., Senior Lecturer at the Department of Radiophysics and Electronics, Francysk Skaryna Gomel State University, vaskevich@gsu.by.