Смирнов А.М., Исхаков А.Ю.

Алгоритм двухфакторной аутентификации как инструмент снижения FRR для проактивного фильтра выявления атак

Аннотация: В исследовании предлагается подход к снижению ложноотрицательных заключений проактивного фильтра веб-ориентированной платформы за счет применения двухфакторной аутентификации. Предлагаемый алгоритм в случае подозрения на инцидент информационной безопасности осуществляет дополнительные проверки субъекта доступа, тем самым позволяя избежать блокировки легитимных посетителей. Данная проблема особенно актуальна для сложных систем, характеризующихся динамичностью параметров окружения профилей субъектов доступа.

Ключевые слова: информационная безопасность, аутентификация субъектов доступа, фактор аутентификации, система управления контентом машинное обучение

Введение

Задача разработки адаптивных или риск-ориентированных алгоритмов аутентификации неразрывно связана с применением интеллектуального анализа данных. Современные возможности злоумышленников – подходы и программные средства для автоматизации – зачастую с легкостью позволяют обходить статичные алгоритмы проверки легитимности и механизмы защиты от брутфорс-атак.

В данном исследовании рассматривается алгоритм двухфакторной аутентификации, основанный на дополнительной проверке параметров веб-окружения, фиксируемых системой управления контентом.

Состояние исследований

Разработка эффективного алгоритма двухфакторной аутентификации для веб-ориентированных платформ является актуальной научно-технической задачей, сочетающей комплекс взаимосвязанных работ по применению методов машинного обучения с учетом совокупности структур данных, программно-

аппаратной инфраструктуры, архитектуры фреймворков, протоколов прикладного уровня и т.д. При этом, в литературе достаточно полно рассматриваются аспекты применения различных методов интеллектуального анализа данных в задаче адаптивной аутентификации. Так, согласно [1,2], одним из эффективных механизмов является Байесовская сеть. Кроме того, метод Байесовской сети может быть применен для автоматической генерации правил корреляции при анализе ранее наблюдаемых предупреждений, что позволяет применять подобные сети и для изучения стратегий вторжения. В работах [3-5] отражены исследования различных алгоритмов выявления аномалий и взаимосвязанных процедур идентификации и аутентификации пользователей.

В работе [6] с целью повышения надежности механизма аутентификации пользователей рассматривается технология, сочетающая в себе проверку пароля, биометрических данных и OTP. Стремление специалистов по информационной безопасности сделать многофакторные технологии проверки более доступными и массовыми также находит свое подтверждение в виде научных работ. В частности, в статье [7] рассматриваются результаты проекта по внедрению многофакторной аутентификации с использованием карты «My Number Card», предоставляемой публичной службой идентификации личности, и WebUSB (находится в стадии стандартизации)

Постановка задачи

В качестве исходного объекта был использован действующий веб-портал, построенный на базе популярной сертифицированной ФСТЭК системы управления контентом (CMS). С целью повышения эффективности работы встроенного проактивного фильтра было принято решение разработать алгоритм двухфакторной аутентификации, позволяющий в случае детектирования подозрения на инцидент информационной безопасности осуществлять адаптивный подбор транспортного механизма для отправки одноразовых верификационных кодов в зависимости от источника атаки. В таблице 1 представлен пример запросов, помеченных проактивным фильтром как вредоносные.

Пример регистрации событий, отмеченных как инцидент информационной безопасности приведен в таблице 1.

Таблица 1 – Примеры детектирования инцидентов

Объект	Событие	IP	User Agent	URL	Комментарий
$_SERVER["REQUEST_URI"]	Попытка внедрения PHP	XXX.40.250.124	python-requests/2.26.0	/remote/fgt_lang?lang=/../../../..////////dev/cmdb/sslvpn_websession/../../../..////////dev/cmdb/sslvpn_websession	Корректное определение вредоносной сигнатуры запроса
$_POST['FEEDBACK_TEXT_FID1']	Попытка внедрения SQL	XXX.92.178.86	Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.72 Safari/537.36	/support/	Корректное определение вредоносной сигнатуры запроса
123751	Попытка авторизации	XXX.211.197.12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.71 Safari/537.36	/auth/	Ошибочное определение в связи с нехарактерной геопозицией субъекта

Представленные данные свидетельствуют о наличии ошибок 1 рода, связанных с преобладанием сигнатурных методов выявления атак и статических моделей субъектов доступа.

Предложенный алгоритм

На рисунке 1 представлена блок-схема предложенного алгоритма двухфакторной аутентификации, позволяющей снизить количество ошибок работы встроенного проактивного фильтра веб-ориентированной платформы, при этом обеспчивая надлежащий уровень доверия к процедурам проверки легитимности за счет применения дополнительного фактора аутентификации.

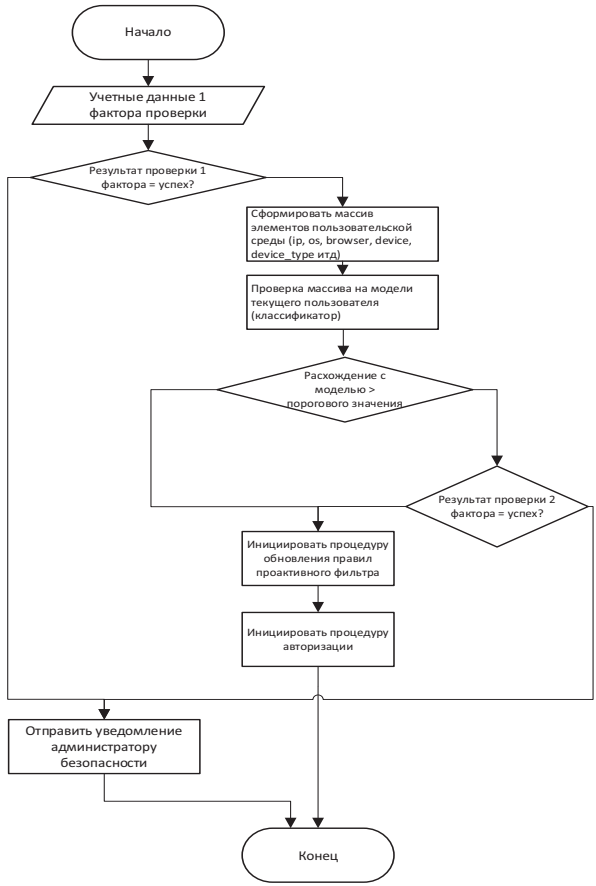

Рисунок 1 – Блок-схема работы алгоритма адаптивной аутентификации

Эксперимент

Реализация классификатора субъектов доступа осуществлена на языке программирования Python. Выходным признаком был выбран параметр event из журнала аудита CMS. Для обучения классификаторов использовался стандартные журналы аудита объемом 20000 записей. Программная реализация классификации данных была внедрена в обработчик процесса аутентификации и синхронизирована с проактивным фильтром обнаружения атак. Оценка алгоритмов осуществлялась с применением метода K-Fold Cross-validation с параметром K = 8. В результате проведения EDA анализ и последующей оценки информативности входных признаков, наибольшее влияние на результат оказывают IP-адрес и отдельные компоненты UserAgent.

Результаты апробирования алгоритмов представлены в таблице 2.

Таблица 2 – Результаты внедрения алгоритма

Механизм	FRR
Однофакторная аутентификация, проактивный фильтр CMS	0,0045%
Двухфакторная аутентификация, проверка окружения с помощью алгоритма KNN (Евклидово расстояние)	0,0031%
Двухфакторная аутентификация, проверка окружения с помощью алгоритма KNN (Косинусная метрика)	0,0033%
Двухфакторная аутентификация, проверка окружения с помощью алгоритма SVM (Линейная разделяющая функция)	0,0034%
Двухфакторная аутентификация, проверка окружения с помощью алгоритма SVM (Радиальная базисная функция)	0,0023%

Экспериментальная проверка доказывает эффективность предложенного алгоритма с использованием классификатора набора данных по входным признакам. Наилучший результат классификации показало применение алгоритма двухфакторной

аутентификации, с применением проверки окружения с помощью алгоритма SVM с радиальной базисной функцией.

Исследование выполнено при частичной финансовой поддержке гранта Президента Российской Федерации в рамках научного проекта № МК-2421.2020.9

Литература:

1. *Chantan C., Sinthupinyo S., Rungkasiri T.* Improving Accuracy of Authentication Process via Short Free Text using Bayesian Network // International Journal of Computer Science Issues. – 2012. – Vol. 9. Issue 2, № 3. – P. 10-16.

2. *Kavousi F., Akbari B.* A Bayesian network-based approach for learning attack strategies from intrusion alerts // Security Comm. Networks. – 2014. – Vol. 7. – P. 833-853.

3. *Srilakshmi V., Dhamodharan P.* Improved Privacy over Authentication of K-Nearest Neighbor Query on Spatial Network. IJSRM. – 2015. – Vol. 3. Issue 2. – P. 2196-2203.

4. *Калинин М.О., Штеренберг С.И.* Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения // Интеллектуальные технологии на транспорте. – 2018. – №3 (15). – С. 47-54.

5. *Попова И.А.* Обнаружение аномалий в наборе данных с помощью алгоритмов машинного обучения без учителя Isolation Forest и Local Outlier Factor // StudNet. – 2020. – Т.3. № 12. – С. 1460-1470.

6. *Hassan M.A., Shukur Z.* A Secure Multi Factor User Authentication Framework for Electronic Payment System / 3rd International Cyber Resilience Conference (CRC) (29-31 Jan. 2021 Langkawi Island, Malaysia). – URL: https://ieeexplore.ieee.org/document/9392564 (дата обращения 10.10.2021).

7. *Fujita Y., Inomata A., Kashiwazaki H.* Implementation and Evaluation of a Multi-Factor Web Authentication System with Individual Number Card and WebUSB / 20th Asia-Pacific Network Operations and Management Symposium (APNOMS) (18-20 Sept. 2019 Matsue, Japan). – Matsue, 2019. – P. 1-4. – URL: https://ieeexplore.ieee.org/document/8893134 (дата обращения 10.10.2021).