Механизми за защита на сигурността на системи за автоматизирано планиране

Мариян Апостолов, Борис Стойков, Симеон Арнаудов

Security defense mechanisms for automated planning systems

Mariyan Apostolov, Boris Stoykov, Simeon Arnaudov

Abstract:
Automated planning systems manage data with different levels of accessibility depending on their content. Public data may represent information obtained from scientific journals, government institutions, or social groups. This data is accessed internally within the organization or institution that uses the system, and it is also possible for external groups to show interest in gaining access to this information. Therefore, security planning is a mandatory stage in project management and maintenance. The information within an automated planning system must be protected from external clients, such as bots, that have not been granted access. This article analyzes and proposes mechanisms for securing data in automated systems. In addition, advanced techniques such as JSON Web Token (JWT), request rate limiting, brute-force attack protection, and input validation are analyzed and discussed. The research examines multi-layered security approaches to reduce the risk of successful attacks. Practices for building secure applications are reviewed and evaluated.
Keywords: security defense mechanisms, automated planning systems

For contacts: ass. prof. eng. Boris Stokov, “Georgi Benkovski” Air Force Academy, Republic of Bulgaria, bstoykov@af-acd.bg

1. ВЪВЕДЕНИЕ

Изграждането, поддържането и надграждането на сигурността са дейности за защита на данните и осигуряват стабилност на системите за автоматизирано планиране. Процесът на ползване на приложението увеличава големината и структурата на запазените данни. Подготвителен етап с избор на подходящ модел защита за информацията, и съхраняването и защитен достъп до информацията в базата данни, както и до списъка с профили на потребители.

След избора на защита, започва етапа на изпълнение с поддръжката на сигурността. Целта на поддръжката е да се добавят нови механизми на защита, след като се появи нов вид атака. Етапа надгражда първоначалната реализирана архитектурна подредба на системата за автоматизирано планиране, което увеличава нейната устойчивост и надеждност.

Основната цел на настоящия научен труд е да се предложат ефективни механизми за защита за повишаване на сигурността на системи за автоматизирано планиране.

2. ЛИТЕРАТУРЕН ОБЗОР

Всеки сървър може да изпълнява голям на брой задачи, поради широкият набор от номера на портове, на които може да се прикачат. За осъществяване на достъп до софтуерна система тя се качва на избрани номера на портове. В настройките за сигурност на сървъра (FireWall) се позволява външен достъп до избраните номера на портове. След изпълнението на тази стъпка данните стават достъпни в интернет мрежата, в която е включен сървъра. Архитектурната постройка на системата включва задължителни и препоръчителни способи за

защита на данните. Механизмите за защита подобряват процесите, който се изпълняват след изпращане на заявка към система.

Навременно прилагане на мерки за защита, като валидиране на входните данни, защита срещу злонамерени атаки и защитни механизми, е от значение за подобрена сигурност на създаден алгоритъм за автоматизирано планиране. [1] Основните механизми за сигурността включват:

Защита на протоколите за комуникация – Реализация на трафик през протоколите HTTPS и TLS. За сигурността на уеб приложенията се използват редица методи и решения, за да се избегне неоторизиран достъп, загуба на данни и проблеми с интернет услугите. В резултат на това, жизненоважни комуникационни протоколи, като HTTPS, който разчита на TLS протокола, вече са от съществено значение. Благодарение на HTTPS, всички данни, предавани между уебсайт и браузър, са криптирани, така че заплахи като Man-in-the-Middle (MITM), подслушване и промяна на данни могат да бъдат предотвратени. [2, 3]

Сигурно управление на сесии – Настройка на уеб приложението да използва атрибутите HttpOnly, Secure и SameSite. HttpOnly е атрибут, който не позволява достъп до бисквитки с JavaScript. Важен е за защита на бисквитки за удостоверяване на профил. Secure е атрибут, който изпраща бисквитка само през криптирана HTTPS връзка, за да не позволи неоторизиран достъп. SameSite е атрибут, който контролира дали бисквитка може да се изпрати при заявки от един и същ или между различни сайтове.

Създаване на уникален ключ при всяка заявка – Ползване на Cross-Site Request Forgery (CSRF) токени. Модулът за защита на CSRF е отговорен за генериране, валидация и управление на CSRF токените за защита от Cross-Site Request Forgery атаки. Модулът се интегрира безпроблемно със система за удостоверяване, за да гарантира, че изпълнените действия са проверени. [4]

Ограничаване на достъп до надеждни домейни – Защита, която настройва Cross-Origin Resource Sharing (CORS) конфигурация за да се ограничат получени заявки само до доверени домейни.

Предпазване от злонамерени ботове и спам – Защита, чрез Google reCAPTCHA. Част от характеристиките включват двуслоен CAPTCHA от Microsoft, който включва както текстови, така и графични текстове , които увеличават защитата срещу агресивни ботове. Това е подход, който се фокусира върху това да направи уеб сайтовете лесни за ползване от хора, като същевременно усложнява ползването им от ботове. [5, 6, 7]

Удостоверяване на профили – JSON Web Token (JWT) е стандарт за сигурно предаване на информация между две страни в JSON формат. Защитава осъществяването на безопасен трафик между клиент и сървър при вход на профил в софтуерна система.

Ограничаване на броя заявки за период – Rate Limiting е механизъм за осъществяване на контрол на изпратените заявки към сървър или мрежа. Този метод ограничава броя на заявки от профил или IP адрес в рамките на определен период от време. Добавяйки тази настройка на сървъра той ще бъде предпазен от възможност за претоварване и да позволи улесненото ползване от профилите в софтуерната система.

Блокиране на многократни опити за достъп до система – Brute-force защита е вид кибератака, при която нападателите се опитват да получат неоторизиран достъп до системата, като прилагат технически начини и ползват комбинации от ключове за криптиране. Тези атаки са значителна заплаха, понеже могат да бъдат полезни при избор на слаби пароли, като често остават незабелязани, докато не причинят значителни щети. [8, 9, 10]

Защита от SQL/NoSQL Injections и XSS атаки – SQL/NoSQL Injections са атаки, при които злонамерен код е вмъкнат в полета за въвеждане, за да манипулира базата данни. При XSS атаките се добавя злонамерен скриптов код в уебсайта, който се изпълнява след извикване на заявка от други профили.

3. ЗАКЛЮЧЕНИЕ

Сигурността на системите за автоматизирано планиране обединява технически и организационни дейности. Добавяне на многослойни механизми за защита гарантират сигурната комуникация между клиент и система. Описаните модели увеличават броя защитни механизми и намаляват вероятността за успешна атака, увеличават устойчивостта на системата и гарантират нейната надеждност. Това е важно за да се ограничи до минимум достъпа на нежелани клиенти до както до университетски бази данни, така и до научни изследвания като оценяване на обучението [11, 12], метеорологични въздействия на околната среда [13], безпилотни летателни апарати [14], верификация на компютърни симулации [15], изследвания върху обслужване на авиационна техника [16], управление на въздушния транспорт [17], въздействие на авиационната индустрия върху околната среда и други.

Представеното изследване подготвя бъдещ анализ на решения, които да бъдат в полза на съществуващи информационни системи.

ЛИТЕРАТУРА

1. Апостолов, М., Камбушев, М. Решения за изпълнение на модул за автоматизирано планиране. Трета Национална Научно-Практическа Конференция - Дигитална Трансформация на Образованието, гр. Русе, 2025, 5 стр.

2. Malanin, V. Comparative Analysis of HTTPS / TLS Implementations for Healthcare Web Applications. International Journal of Scientific Engineering and Research, May 2025, vol. 13, iss. 5, 61-68.

3. Rescorla, E. TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM) RFC 5289. https://www.rfc-editor.org/rfc/rfc5289.html (10 September 2025).

4. Punitha, P., Abinaya, M., Sona Christy, A., Mohandoss, S., Yadlapalli, M. Building A Secure Plug-And-Play User Management System. Journal of Advance and Future Research, April 2025, vol. 3 iss. 4, 33-35.

5. Fitz-Inteseful, T., Sunkwa, J., Asiedu, W. A Comparative Analysis of the Effectiveness of Recaptcha V3 against Recaptcha V2, Hidden Fields, and Other AntiSpam Techniques. International Journal of Information Technology and Computer Engineering, December 2024-January 2025, vol: 05, no. 01, 14 стр.

6. Chow, Yang-Wai, Willy Susilo, and Pairat Thorncharoensri. "CAPTCHA design and security issues." *Advances in Cyber Security: Principles, Techniques, and Applications*. Singapore: Springer Singapore, 2018. 69-92.

7. Pujeri, U., Kulkarni, S., Ramachandra, P. Smart Captcha to Provide High Security against Bots. Lecture Notes in Engineering and Computer Science, Newswood Limited, 2019, vol. 2240, 144-149.

8. Akwaronwu, B., Akwaronwu, I., Adeniyi, O. Brute Force Attack Detection in Network Traffic Using Convolutional Neural Networks. Asian Journal of Research in Computer Science, 2025, vol. 18, iss. 5, 387-402.

9. Sulochana, V. Implementation of chunks of image password in cloud computing system. Asian Journal of Computer Science and Technology, 2019, vol. 8 iss. S1, 54-57

10. Vijayan, P. M., & Sundar, S. IoT intrusion detection system using ensemble classifier and hyperparameter optimization using tuna search algorithm. Journal of Autonomous Intelligence, 2024, vol 7, iss. 2, 14 стр.

11. Цонев, П., 2022. Някои изводи върху резултатите от националното външно оценяване по математика за VII клас, Математика и информатика, 65(6), 587-601.

12. Цонев, П., Избор на подходящ модел за изследване на задачите от НВО по математика след VII клас според методите на IRT. Математика и информатика, 66(4), 2023, ст. 491-505,

13. Кацаров, Й., „Градушката в София 2014“, Годишна Международна Научна Конференция на ВВВУ „Георги Бенковски“ сборник доклади 07.10.2022 г. ст. 63-69

14. Илиева, Д., К. Камбушев. "„Моделиране на турбулентност при полет на безпилотен летателен апарат “." *XXXII МНТК „АДП-2023”, Созопол* (2023): 96-100.

15. Georgiev, Yoto Georgiev. "Validation and verification in scientific computer simulation." *Aeronautical* (2024): 49.

16. Kanchev, Nikolay. "Extended reality technologies for aircraft maintenance training." *Aeronautical* (2025): 38.

17. Найденов, Н. Глобалните съюзи на традиционни авиопревозвачи като стратегически отговор на конкуренцията от нискотарифните компании (НТАК), Сборник с доклади на Годишна Международна Научна Конференция на ВВВУ „Георги Бенковски“, 2024, ст. 17-18.

18. Benkov, Ivan Russanov. "Aspects of the Impact of Aircraft Emissions on the Environment and the Future of Alternative Aviation Fuels." *Journal of Philology and Intercultural Communication* 8.2 (2024): 105-116.