Заплахи за сигурността на системи за автоматизирано планиране

Мариян Апостолов, Борис Стойков, Симеон Арнаудов

Threads to the security of automated planning systems

Mariyan Apostolov, Boris Stoykov, Simeon Arnaudov

Abstract:
Automated planning systems assist in many businesses. Educational planning is one direction that automates the resources data. To be accessible from the public network the system must be hosted at a server. The process of planning the hosting includes as many options as possible to keep data safe and not exposed to a wide spectrum of cyber-attacks. Data information must be kept secure from not granted access and complete extraction from not approved clients or external API requests. This article analyzes security as important sub-module to keep the automated system's data secure. They include protection against cross-site request forgery (CSRF), cross-origin resource sharing (CORS) misconfigurations, cross-site scripting (XSS) adding violation scripts, and SQL Injection to access not authorized data from the database. Moreover, DoS/DDoS attacks for slowing or shutting access to servers, and automated attacks from programs or bots are analyzed and stated in the research. Research with security threads is stated to plan and reduce the risk of successful attacks. Practices for secure application building are reviewed and evaluated.
Keywords: security, threads, automated planning systems

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

1. ВЪВЕДЕНИЕ

Системите за автоматизирано планиране са ключов елемент в съвременните интелигентните решения на университет. Надеждността на тяхното функциониране е тясно свързана с включения модул за сигурността на използваните публични софтуерни приложения, които се използват за извършване научни изследвания в областта на авиацията, като един от секторите в които има голям брой иновации, симулации, обработка на данни и инженерни изследвания. Пример за такива изследвания са въздействие на авиационното гориво върху околната среда [1], мениджмънт на въздушния транспорт [2], обслужване на авиационна техника, [3], валидиране и верифициране на компютърни симулации [4], безпилотни летателни апарати [5], метеорологични събития [6], оценяване на обучението [7, 8] и други.

Тези приложения, тук се използва дефиницията за дистанционни образователни технологии (ДОТ), целта им е да създават желани предимства като висока производителност, асинхронност на академичното управление, така и предотвратяване на кибер заплахи.

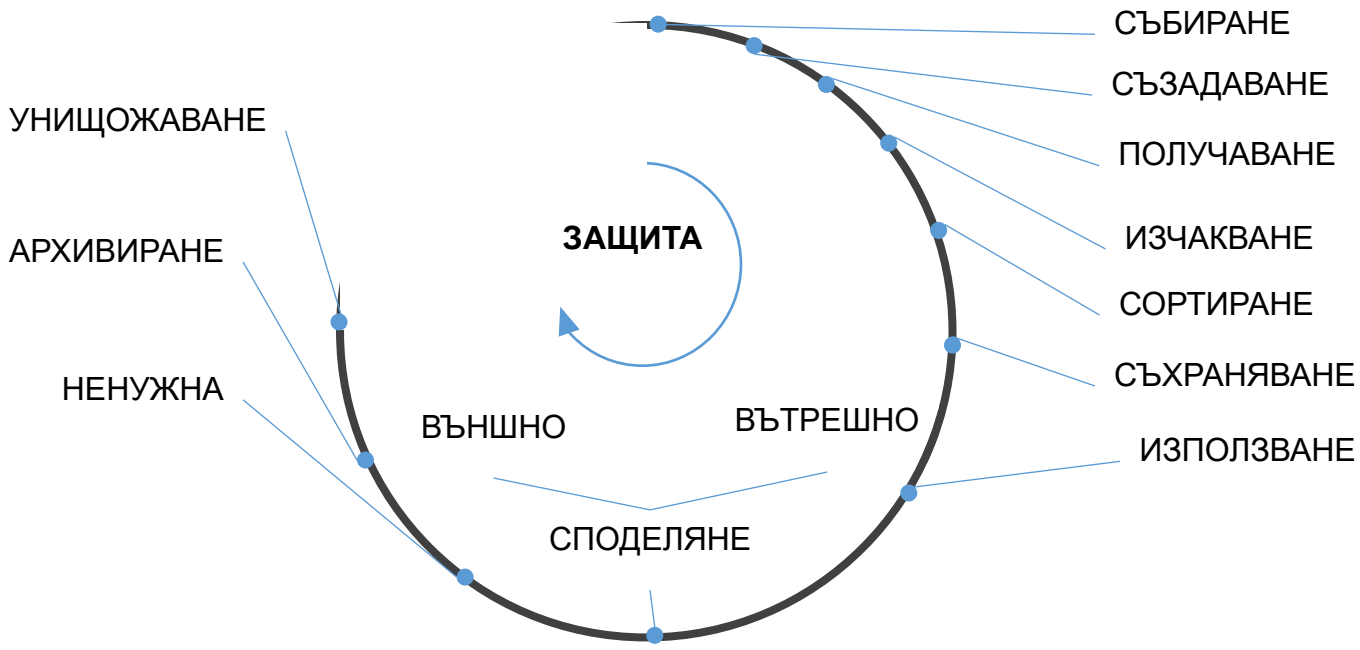
Например уязвимости в протоколите за създаване, записване и съхраняване на информация, което е предпоставка за злонамерени заявки и автоматизирани атаки за нерегламентиран достъп до съхраняваната информация в ДОТ.

Основната цел на настоящата статия е да се акумулират знания за ключови заплахи, и това знание да бъде използвано за да се подобри сигурността на системи за автоматизирано планиране. За целта ще бъде преброени научни статии разглеждащи заплахите за функционирането на автоматизирани системи за планиране, и ще бъдат описани най-често срещаните такива.

2. ЛИТЕРАТУРЕН ОБЗОР

Управлението на генерираната информацията покрива широк обхват от дейности, и е трудно да се адресират всичките области на управление на информацията, в едно и също време при това на непрекъсната основа.

Създаването на знания, тоест на списък със съвременни заплахи за приложенията от модела на автоматизирано планиране ще помогне да се определят приоритети и подобряване на управлението на създадената и съхранявана информация, изследвания, лекции, бизнес данни, тоест въобще цялата съвкупност от база данни на университета. Това е важно за поддръжка на нормални електронни услуги на университета (Фиг. 1). Събирането, съхраняването, сортирането, архивиране на базите данни на университета било те академични или административни трябва да бъдат защитени от непотвърдени клиенти при споделяне на този огромен масив от данни. Не е желателно все още непубликувани научни изследвания да бъдат достъпни за нежелани клиенти на вътрешната или публичната мрежа на университета.



Фиг.1. Жизнен цикъл на информацията при управление на административни и академични база данни в университет.

Създаването на система за ползване в определен бранш изисква анализ на достъпващият брой и тип клиенти, анализ на очаквания трафик и мрежа за достъп, преглед на задължителни и очаквани рискове за атака към системата, планиране на отделни мерки за подобряване и осъществяване на всеки процес, проверка на предложената и реализирана защита.

Заплахите за сигурността на системата изискват изпълнение на всяка една от описаните стъпки. Липсата увеличава възможността, както за трудно или невъзможно достъпване на данни, така и за получаване на ценна информация от непотвърден клиент.

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. [9] Основните заплахи за сигурността включват:

CSRF (Cross-Site Request Forgery) – Принуждаване на потребителя да изпрати заявка без негово знание. Един от най-известните уеб уязвимости е Cross-Site Request Forgery (CSRF), при който неупълномощени команди се предават от потребител, на когото уеб приложението доверява. CSRF атаките, в зависимост от техния тип, могат да доведат до нарушения на данните, неразрешени транзакции и ерозия на доверието от крайните потребители. [10]

CORS (Cross-Origin Resource Sharing) – Неправилна конфигурация може да позволи кражба на чувствителни данни. CORS се базира на два HTTP хедъра, получени в отговор на крос-сайт заявки: „Access-Control-Allow-Origin“ (ACAO), който указва дали тялото на заявката е достоверно, и „Access-Control-Allow-Credentials“ (ACAC), който инструктира сървъра дали удостоверителните бисквитки и всякакви упълномощаващи хедъри могат да бъдат прикачени към заявката в браузъра. [11, 12]

XSS (Cross-Site Scripting) – Вмъкване на злонамерен код в интерфейса. Предвид възможността за фалшифициране на тялото на заявката и контрол на уеб страницата на клиентска страна, XSS е пример за атака. Нападател може да добави таг в тялото на отговора, за да накара браузъра да изпълни произволен JavaScript в уебсайта на жертвата. Такава експлоатация може да открадне бисквитки на потребителя и да инициира нежелан трансфер към нападателя. [13]

SQL/NoSQL Injection – Манипулация на входните данни в заявка. Атаките SQL Injection се превърнаха в една от най-широко експлоатираните уязвимости в уеб приложенията, насочени към бази от данни. Тези атаки се основават на манипулиране на SQL заявка за изпълнение на произволни команди в база данни, което често води до компрометиране на чувствителни данни и даване на неупълномощен достъп. [14]

DoS/DDoS атаки – Претоварване на сървъра. В постоянно развиващата се дигитална ера, мрежовата сигурност стана решаваща за защита на информационните технологични инфраструктури от киберзаплахи, по-специално от атаки от тип „Distributed Denial of Service“ (DDoS). DDoS атаките имат за цел да напълнят мрежа или целева система с изключително висок и прекомерен трафик, правейки услугите недостъпни за потребители на системата или дори да причинят пълна системна повреда. [15]

Автоматизирани атаки и ботове – Понякога злонамерен автоматизиран софтуер атакува уебсайтове, за да забави скоростта за обработка на изпратени заявки към сървърите. Тези автоматизирани инструменти изпращат голям обем фалшива информация от несъществуващи потребители, което може да забави или спре получаването на отговори от сървърите. Тези атаки, обикновено се изпълняват с помощта на компютърни програми [16], които могат да нарушат предлаганите услуги от системата. [17]

3. ЗАКЛЮЧЕНИЕ

Сигурността на системите за автоматизирано планиране обединява технически и организационни дейности. Това са стъпки за подготовка на сървъра, който ще съхранява и пази вътрешната информация. В научния доклад са

представени заплахи за сигурността на системи, които могат да бъдат осъществени при провеждането на атаки за увеличаване на необходимото време за получаване на отговор при изпратен въпрос, за достъп до сървър или към информацията от данни, за срив на сървъра.

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

ЛИТЕРАТУРА

1. 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.

2. 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.

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

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

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

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

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

8. 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,

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

10. Teja, P. K., Aryan, B., Nithesh, C., Kumar, M. G. S., Prasad D. M. Secureweb: A Novel Machine Learning Methodology for Identifying CSRF Vulnerabilities. International Journal of Engineering Science and Advanced Technology, June 2025, 425-430.

11. Golinelli, M., Arshad, E., Kashchuk, D., Crispo, B. Mind the CORS. 2023 IEEE 5th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications, 2023, 213-221.

12. https://github.com/whatwg/fetch/issues/382 (01 September 2025).

13. Chen, P., Chen, J., Zhang, M., Wang, Q., Zhang, Y., Xu, M., Duan, H. Cross-Origin Web Attacks via HTTP/2 Server Push and Signed HTTP Exchange. Network and Distributed System Security (NDSS) Symposium, San Diego, CA, USA, 24-28 February 2025.

14. Yarashov, I., Akbarov, M. Evaluating the Security Risks and Protection Strategies for SQL Insert Queries Against Injection Attacks. Science and Innovation in the Education System, International Scientific-Online Conference, 2025.

15. Tobing, E., Septya, R., Servanda, Y. Comparative Analysis of Network Security: Firewall, IDS, and AI-Based Defense Against DDoS Attacks. Journal of Artificial Intelligence and Engineering Applications, 15th June 2025, vol. 4, no. 3, 1818-1822.

16. Ahn, L., Blum, M., Langford, J. Telling humans and computers apart automatically. Communications of the ACM, 2004, vol. 47, no. 2, 56–60.

17. Bora, N., Bora, P., Tidake, V., Dhomse, G., Pawar, P. AI-driven biometric CAPTCHA: defending against automated threats in web security. International Journal of Basic and Applied Sciences, 2025, vol. 14, no. 1, 32-39.