УДК 004.056.5

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРЗАХИЩЕНОСТІ СИСТЕМ ЦЕНТРАЛЬНОГО ВХОДУ У БАГАТОСАЙТОВИХ ОСВІТНІХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Малініч П. П., *інженер ІнтерЦЕК, Вінницький національний технічний університет, м. Вінниця*
Коваленко О. О., *канд. техн. наук, доцент, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця*
Малініч І. П., *асистент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця*

Використання систем централізованого входу SSO в значній мірі підвищує захищеність багатосайтових інформаційних систем в цілому, однак не є гарантованим вирішенням всіх проблем із кібербезпекою. Серед переваг використання подібних систем є централізований контроль над користувачами та можливість застосування мультифакторної автентифікації [1]. Автоматизація централізованого контролю над базою користувачів організацій дозволяє виявляти спроби взлому акаунтів користувачів за допомогою засобів штучного інтелекту [2, 3], додавати нових співробітників та клієнтів, а також деактивувати співробітників, які звільнені. Подібні рішення є затребуваними і в сфері освіти.

Як і у будь-яких інших технологіях захисту від несанкціонованого доступу, в систем централізованого входу також існує проблема змагання "замка та відмички". Ця проблема полягає у тому що по мірі вдосконалення технологій захисту від несанкціонованого доступу вдосконалюються і методи та засоби для їх подолання, що в свою чергу знову призводить до продовження розвитку перших. У системах автентифікації та авторизації вона виявляється у спробах заволодіти акаунтами користувачів, які можуть мати доступ до даних, що складають комерційну таємницю, чи до менш захищених систем, які легше взломати.

На даний момент існують наступні перспективи кіберзагроз для систем централізованого входу SSO:

1. Використання менш захищених мережевих протоколів. Поряд із добре захищеною системою SSO із застосуванням мультифакторної автентифікації можуть застосовуватись менш захищені протоколи, наприклад FTP, POP3,

IMAP, LDAP та SMB. Ці протоколи зазвичай обмежуються або підтримують лише однофакторну автентифікацією з вводом логіну та паролю, що може бути використане зловмисниками для обходу центрального входу. Протоколи AAA – RADIUS та TACACS+ мають підтримку двофакторної автентифікації [4], однак зазвичай їх складно інтегрувати з системою SSO. Саме через проблеми менш захищених протоколів компанія Google вирішила відмовитись від класичних протоколів POP3 та IMAP у своєму поштовому сервісі Gmail.

2. Використання слабкого шифрування, що є вразливим до розшифрування квантовими обчисленнями. Багато сучасних алгоритмів шифрування можуть бути розшифровані з використанням методів квантових обчислень. Це може робити процеси автентифікації та авторизації більш вразливими до розшифрування зловмисниками. Однак проблема активно вирішується завдяки розробці пост-квантових алгоритмів шифрування. Сучасні браузери регулярно оновлюються та видають сповіщення при спробі підключитись до менш захищених сайтів. Проте нестійке до квантового розшифрування шифрування може бути не лише між браузером та сервером, але й між сервером IdP та сервером сервіс-провайдеру системи SSO. Через те, що подібні системи можуть використовувати різні програмні компоненти із досить складним процесом налаштування, поверхневий аудит може не виявити використання слабкого шифрування.

3. Аналіз вразливостей за допомогою інструментів штучного інтелекту. У згаданому змаганні "замка та відмички" відбувається боротьба між засобами захисту та взлому. Застосування інструментів штучного інтелекту для виявлення вразливостей має дві сторони медалі: це дозволить з однієї сторони прискорити пошук вразливостей у своїх продуктах компаніям-розробникам і таким чином підвищити захищеність програмного забезпечення, а з іншої сторони це збільшить можливості зловмисників направлених проти людей та організацій, що використовують програмні рішення без регулярних оновлень безпеки [2]. Найбільш вразливими в даному випадку можуть виявитись користувачі програм (або компонентів цих програм), регулярні оновлення безпеки до яких більше не випускаються.

4. Розвиток ботів, керованих штучним інтелектом, що здатні імітувати діяльність користувача у браузері. Більш складні системи автентифікації здатні визначати характерність дій користувача людині [3]. На противагу їм, продовжують розвиватись боти, що здатні орієнтуватись у інтерфейсі веб-додатків та вирішувати слабкі різновиди технології CAPTCHA. Для цього виявились дуже корисними такі QA-інструменти як Selenium. Крім аналізу DOM-структури сторінок для створення таких ботів може бути також задіяне комп’ютерне бачення [5].

5. Соціальна інженерія залишається не менш дієвим засобом для заволодіння акаунтами користувачів, зокрема тих, які захищені мультифакторною автентифікацією. Найбільш часто використовуваний у ній підхід підміни веб-сторінок з використанням проксі-технологій здатен обходити як мультифакторну автентифікацію, так і прості різновиди CAPTCHA-тесту.

Серед рішень останніх двох проблем є використання інтелектуальних систем тесту Тюринга, на зразок Cloudflare Turnstile, яка крім вирішення завдань з вибором зображень здатна аналізувати поведінку користувача на веб-ресурсі на її характерність людській. На момент написання даного матеріалу подібні технології продовжують розвиватись і витісняти традиційні CAPTCHA-тести [6].

Висновок. Всі описані проблеми є актуальними як для систем SSO у освітній сфері, так і у інших. Однак серед українських ЗВО крім хмарних рішень часто використовуються SSO-рішення з відкритим вихідним кодом [1], встановлені у вигляді Self-hosted розгортань. На відміну від хмарних рішень, подібні розгортання потребують кваліфікованого супроводу, який включає в себе регулярний аудит безпеки та регулярні безпекові оновлення програмного забезпечення. Розглянуті проблеми 4 та 5 у подібних розгортаннях можливо вирішити завдяки інтеграції з такими технологіями як Managed Challenge [6].

Технологія тесту Тюринга на основі відслідковування подій у веб-браузері JavaScript Challenge продовжує успішно розвиватись і витісняти традиційний CAPTCHA, однак технології подібного тесту все ще недостатньо, щоб повністю переконатись чи є користувач людиною, тому все ж є сенс у розробці покращених методів тестування Тюринга, основаних на вирішенні завдань.

Список використаних джерел

1. Малініч П. П., Коваленко О. О., Малініч І. П. Впровадження технологій централізованої ідентифікації, автентифікації та авторизації користувачів у освітніх інформаційних системах. *Інформаційні технології та автоматизація – 2023* : матеріали Міжнар. наук. конф., м. Одеса, 19–20 жовт. 2023 р. URL: https://ir.lib.vntu.edu.ua/handle/123456789/37994 (дата звернення: 24.10.2023).

2. Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., ... & Li, K. Artificial intelligence security: Threats and countermeasures. *ACM Computing Surveys (CSUR)*. 2021. 55(1), p. 1-36.

3. Sonthi, V. K., Nagarajan, S., Murali Krishna M, M. V. B., Giridhar, K., Lalitha, V. L., & Mohan, V. M. Imminent threat with authentication methods for AI data using blockchain security. *Blockchain Security in Cloud Computing*. 2022. 283-303.

4. Малініч П. П., Малініч І. П., Коваленко О. О. Негативні безпекові чинники у локальних Ethernet-мережах та абонентських мереж останньої милі. LI *Науково-технічна конференція підрозділів Вінницького національного технічного університету (НТКП ВНТУ–2022)* : матеріали Науково-технічної конференції. м. Вінниця, 31 травня 2022 р. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2022/paper/view/15614 (дата звернення: 24.10.2023).

5. Chen, J., Xie, M., Xing, Z., Chen, C., Xu, X., Zhu, L., & Li, G. Object detection for graphical user interface: Old fashioned or deep learning or a combination? *Proceedings of the 28th ACM joint meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2020. pp. 1202-1214.

6. The end of the road for Cloudflare CAPTCHAs. *The Cloudflare Blog* : website. URL: https://blog.cloudflare.com/end-cloudflare-captcha.