

SECTION 13

TECHNICAL SCIENCES, PRODUCTION AND TECHNOLOGY

УДК 004.056.5

Куцак Д. С.

студент факультету інтелектуальних інформаційних технологій

Арсенюк І. Р.

к. т. н., доцент, доцент кафедри комп'ютерних наук,
Вінницький національний технічний університет

ВИЯВЛЕННЯ ПІДОЗРІЛОЇ АКТИВНОСТІ В СИСТЕМАХ ЄДИНОГО ВХОДУ З УРАХУВАННЯМ РЕЖИМУ СПІЛЬНОГО ДОСТУПУ

Системи єдиного входу (Single Sign-On, SSO) використовуються у банківських, корпоративних, державних та інших середовищах. Ці системи надають можливість користувачам автентифікуватися лише раз та отримати доступ до веб додатків та систем, що спрощує контроль доступу користувачів до додатків, підвищує зручність отримання доступу та зменшує кількість паролів, які потрібно пам'ятати користувачеві. Проте єдиний вхід користувача створює ризики безпеки. Компрометація облікового запису користувача призводить до втрати доступу цим користувачем до всіх додатків та систем [1 – 3].

Питання виявлення підозрілої активності є актуальним, оскільки постійно розвиваються кіберзагрози та збільшується кількість цільових атак. Існуючі моделі захисту покладаються на багатофакторну автентифікацію та поведінковий аналіз. Проте більшість із готових рішень розроблені для персоналізованого використання пристроїв та не враховують аутентифікацію декількох користувачів на одному пристрої. В багатьох галузях, таких як підприємства та навчальні лабораторії, є поширеним використання спільних пристроїв (Kiosk mode), тобто коли декілька користувачів автентифікуються послідовно на одному пристрої для отримання доступу до ресурсів чи систем.

Для таких пристроїв стандартні методи виявлення підозрілої активності, а саме автентифікації, є неточними та часто призводять до хибних спрацювань. Параметри, які використовуються для аналізу (такі як назва та версія браузера, час автентифікації, адреса) стають однаковими або подібними для різних користувачів. Це призводить до неможливості відрізнити підозрілу активність від звичайної та викликає незручність у користуванні [4, с. 55-63].

З метою подолання цих обмежень інформаційна технологія оцінювання рівня довіри користувача повинна врахувати контекст спільного використання пристроїв, а також послідовність змін між користувачами в межах одного терміналу. Вона має

аналізувати не лише окремі події автентифікації, а й загальну динаміку користування системою – частоту входів, тривалість сесій, циклічність використання облікових записів. Завдяки цьому можна виявляти аномальні сценарії, зокрема підозріло часті входи з одного пристрою, повторні спроби під різними обліковими записами чи надмірно короткі інтервали між автентифікаціями.

У роботі запропоновано підхід до метричної оцінки рівня довіри користувача (Trust Score), який кількісно визначає ризик кожної автентифікаційної події. Індекс довіри формується на основі поєднання часових, технічних і поведінкових параметрів, зокрема:

- часових відхилень між входами користувачів;
- зміни пристроїв або браузерів;
- частоти невдалих спроб входу;
- географічної відстані між точками доступу;
- черговості користувачів на одному пристрої.

Рівень довіри можна виразити у вигляді функції:

$$T(u, d) = 1 - \frac{\sum_{i=1}^n w_i * R_i(u, d)}{\sum_{i=1}^n w_i}, \quad (1)$$

де $T(u, d)$ – індекс довіри користувача u на пристрої d ;

$R_i(u, d)$ – нормалізоване значення ризику за певним параметром;

w_i – ваговий коефіцієнт його важливості.

Чим нижчим є значення $T(u, d)$, тим більша ймовірність того, що подія має аномальний характер.

Такий підхід дозволяє не лише виявляти підозрілі події, а й оцінювати накопичувальний ризик пристрою, тобто ступінь довіри до середовища, в якому здійснюється автентифікація. Це дає змогу враховувати контекст поведінки не лише конкретного користувача, а й усіх, хто працює з даним пристроєм. Подібна ідея узгоджується з сучасними тенденціями ризик-орієнтованої безпеки та рекомендаціями з оцінювання кіберризиків [5, с. 18-25].

Важливою перевагою запропонованого підходу є його адаптивність – порогові значення ризику змінюються залежно від поточної поведінкової ситуації. Це дає змогу мінімізувати кількість хибних спрацьовувань і підвищити точність визначення реальних загроз. Запропонована модель може бути інтегрована в сучасні системи автентифікації (наприклад, Keycloak або IdentityServer) без суттєвих змін у їхній архітектурі, виступаючи додатковим рівнем поведінкового моніторингу.

Результати експериментальних перевірок показали, що застосування метричної оцінки довіри дозволяє знизити кількість помилкових спрацьовувань у середовищах із багатокористувацьким доступом до 30% та підвищити точність виявлення реальних інцидентів безпеки. Такі результати свідчать про ефективність використання контекстного аналізу в системах єдиного входу.

Розроблений підхід має практичне значення для українських установ, які впроваджують електронне урядування, цифрові кабінети громадян і корпоративні системи доступу. Його використання дає можливість створювати інтелектуальні

механізми моніторингу поведінки користувачів, що підвищують рівень кіберзахисту відповідно до вимог Закону України “Про захист інформації в інформаційно-комунікаційних системах” [1].

Таким чином, удосконалення технологій виявлення підозрілої активності в системах єдиного входу з урахуванням спільного використання пристроїв є важливим кроком у розвитку національної системи кібербезпеки. Використання метричної оцінки довіри користувача забезпечує підвищення стійкості систем до внутрішніх загроз, а також зменшує ризик несанкціонованого доступу до конфіденційних даних у публічних або корпоративних середовищах.

Ключові слова: Single Sign-On, інформаційна безпека, підозріла активність, Trust Score, поведінковий аналіз, Kiosk mode, автентифікація.

Список літератури

1. Закон України “Про захист інформації в інформаційно-комунікаційних системах” від 05.07.1994 № 80/94-ВР. – [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/go/80/94-вр>.
2. Гончарук Б. І., Арсенюк І. Р. Моделювання процедури захисту веб-ресурсів та веб-сервісів // Матеріали XII Міжнародної науково-практичної конференції “Інтернет-Освіта-Наука” (ІОН-2020). – Вінниця: ВНТУ, 2020. – С. 84 – 87.
3. Гончарук Б. І., Арсенюк І. Р. Захист веб-додатків та веб-служб за допомогою багатоетапної верифікації з використанням потоку авторизації через веб-сервер // Тези доповідей XLIX науково-технічної конференції факультету інформаційних технологій та комп'ютерної інженерії. – Вінниця: ВНТУ, 2020. – [Електронний ресурс]. – режим доступу <https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2020/paper/view/8992/7757>)
4. Здолбіцька Н. І. Сучасні способи автентифікації та захист на веб-додатках // Актуальні проблеми комп'ютерних систем, системного та програмного інжинірингу. – 2024. – Вип. 2. – с. 55 – 63.
5. Жеребець О. М. Правове забезпечення методики ідентифікації та оцінки ризиків кібербезпеки // Інформаційне право України. – 2025. – № 1. – с. 18 – 25.