УДК 004

Д. П. Курніцький
О.Ю. Софина

НАЛАШТУВАННЯ ПОРОГІВ ALLOW/STEP-UP/DENY ДЛЯ RBA-ЛОГІНУ ЗА ОБМЕЖЕННЯ НА ATTACK-PASS RATE

Вінницький національний технічний університет

Анотація

У роботі розглянуто задачу налаштування порогів прийняття рішень у ризик-орієнтованій автентифікації під час логіну. Запропоновано підхід, за якого межі дозволу входу, додаткової перевірки та відмови у вході визначаються не лише за загальною точністю моделі, а й за обмеженням на частку пропущених атак. Це дає змогу підвищити стійкість входу до спроб з використанням викраденого пароля та зменшити кількість зайвих перевірок для легітимних користувачів.

Ключові слова: ризик-орієнтована автентифікація, логін, порогова політика, динаміка натискань клавіш, поведінковий фінгерпринт, додаткова перевірка, частка пропущених атак.

Abstract

The paper considers the problem of threshold tuning in risk-based authentication at login time. An approach is proposed in which the thresholds for access approval, additional verification and denial are selected not only according to overall model accuracy, but also under a constraint on the rate of passed attacks. This makes it possible to improve resistance to stolen-password login attempts while reducing the number of unnecessary additional checks for legitimate users.

Keywords: risk-based authentication, login, threshold policy, keystroke dynamics, behavioral fingerprint, additional verification, attack-pass rate.

Мета

Метою дослідження є обґрунтування підходу до налаштування порогів прийняття рішень у RBA-логіні, який забезпечує обмеження на частку пропущених атак і водночас мінімізує кількість зайвих додаткових перевірок для легітимних користувачів.

Вступ

У сучасних інформаційних системах автентифікація користувачів залишається одним із ключових механізмів захисту доступу. Попри поширення додаткових засобів безпеки, пароль і далі є найуживанішим способом входу, а тому атаки з використанням викрадених або скомпрометованих облікових даних залишаються серйозною проблемою. За таких умов постає потреба в таких підходах до автентифікації, які не лише посилюють захист, а й не створюють надмірних труднощів для легітимного користувача під час повсякденного входу до системи.

Одним із таких підходів є ризик-орієнтована автентифікація, у межах якої рішення про дозвіл доступу приймається з урахуванням ознак конкретної спроби входу. До таких ознак можуть належати параметри пристрою, мережевого оточення, місця входу, а також поведінкові характеристики користувача, зокрема динаміка натискань клавіш. На відміну від фіксованих правил перевірки, цей підхід дає змогу більш гнучко реагувати на рівень ризику: безпечні спроби не ускладнюються зайвими діями, тоді як підозрілі можуть вимагати додаткового підтвердження або бути відхилені.

Разом із тим ефективність такого підходу визначається не лише якістю оцінювання ризику, а й тим, як саме система інтерпретує отриманий результат. Якщо пороги між зонами дозволу входу,

додаткової перевірки та відмови визначено невдало, навіть точна модель ризику не забезпечить належного балансу між безпекою та зручністю. Саме тому задача налаштування порогів allow / step-up / deny є важливою складовою побудови практичних систем RBA-логіну і потребує окремого обґрунтування.[1, 2]

Формування порогової політики рішень у RBA-логіні

У ризик-орієнтованій автентифікації кожна спроба входу описується набором контекстних і поведінкових ознак

$$x = (x1, x2, \ldots, xn)$$

де x_i характеризують параметри пристрою, мережевого оточення, часові особливості входу, а також поведінкові характеристики користувача, зокрема динаміку натискань клавіш. На основі цих ознак формується інтегральна оцінка ризику

$$R(x) \in [0; 1]$$

де менші значення відповідають нижчому ризику, а більші — вищому. Таким чином, система зводить набір різнорідних характеристик конкретної спроби логіну до єдиної кількісної оцінки, яка далі використовується для прийняття рішення.

Для прийняття рішення вводяться два пороги τ_1 і τ_2, причому $\tau_1 < \tau_2$. Тоді правило прийняття рішення має вигляд

$$d(x) = allow, \text{ якщо } R(x) \leq \tau_1 step - up, \text{ якщо } \tau_1 < R(x) \leq \tau_2 \, deny, \text{ якщо } R(x) > \tau_2$$

Отже, якщо значення ризик-скору є низьким, система дозволяє вхід без додаткових дій. Якщо значення ризику потрапляє до проміжної зони, ініціюється додаткова перевірка. Якщо ж ризик є високим, система відмовляє у вході. Такий підхід дає змогу перейти від двійкового рішення до більш гнучкої трирівневої моделі доступу, яка краще враховує невизначені та прикордонні ситуації.

Для оцінювання ефективності такої порогової політики доцільно використовувати кілька показників. Частка пропущених атак визначається як

$$APR = N^{allowattack} / N^{attack}$$

де N^{attack} — загальна кількість атакувальних спроб входу, а $N^{allowattack}$ — кількість атакувальних спроб, які система помилково дозволила. Частка легітимних спроб, для яких була призначена додаткова перевірка, визначається як

$$SUR = N^{legit}_{step-up} / N^{legit}$$

де N^{legit} — загальна кількість легітимних спроб входу, а $N^{legit}_{step-up}$ — кількість легітимних спроб, для яких система ініціювала додаткову перевірку. Частка хибних відмов для легітимних користувачів визначається як

$$FRR = N^{legit}_{deny} / N^{legit}$$

де N^{legit}_{deny} — кількість легітимних спроб, яким було помилково відмовлено у вході. У сукупності ці показники дають змогу оцінити, наскільки вдало вибрані пороги з точки зору безпеки та зручності користування системою.

Тоді задачу налаштування порогів можна подати як мінімізацію частки зайвих додаткових перевірок

$$SUR \to min$$

за умови

$$APR \leq \alpha$$

де α — допустима частка пропущених атак. За потреби додатково може враховуватись обмеження

$$FRR \leq \beta$$

де β — допустима частка хибних відмов для легітимних користувачів. У такій постановці пороги τ_1 і τ_2 визначаються не довільно, а з урахуванням конкретних вимог до безпеки системи. Це дає змогу орієнтувати налаштування моделі не лише на загальну точність, а насамперед на контроль найбільш критичних помилок.[3, 4]

Практична перевірка запропонованого підходу може виконуватися на валідаційній вибірці, яка містить як легітимні спроби входу, так і модельовані атакувальні сценарії, зокрема спроби з викраденим паролем. Для кожної спроби обчислюється ризик-скор R(x), після чого підбираються такі значення τ_1 і τ_2, які забезпечують виконання обмеження на APR. Серед допустимих варіантів обирається той, що мінімізує значення SUR, а за потреби також не перевищує допустимий рівень FRR. Такий підхід дозволяє пов'язати теоретичну модель порогового прийняття рішень із подальшою експериментальною перевіркою на даних, наближених до реальних умов автентифікації.[5]

Механізм прийняття рішення в RBA-логіні доцільно подати у вигляді окремої схеми на рисунку 1.

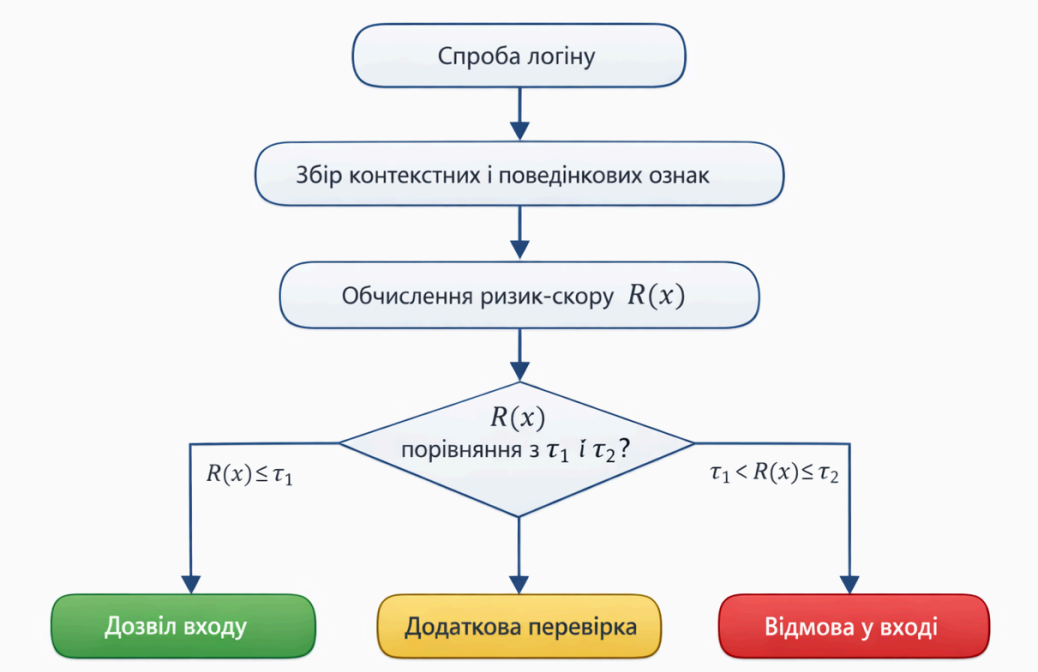

Рис. 1: Механізм прийняття рішення в RBA-логіні

Висновки

Отже, налаштування порогів allow / step-up / deny у ризик-орієнтованій автентифікації є не другорядним технічним кроком, а важливою частиною всієї логіки захисту. Саме від того, де проходять межі між дозволом входу, додатковою перевіркою та відмовою, залежить, чи зможе система вчасно зупинити підозрілу спробу і водночас не ускладнить вхід для справжнього користувача. Тому пороги доцільно визначати не лише з огляду на загальну точність моделі, а з урахуванням реальних ризиків для безпеки.

У роботі показано доцільність підходу, за якого налаштування порогів виконується за

обмеженням на частку пропущених атак. Такий підхід є більш практичним, оскільки дає змогу зосередитися на найнебезпечнішій помилці — пропуску атакувальної спроби як безпечної. Водночас це дозволяє не перевантажувати легітимного користувача зайвими додатковими перевірками, тобто краще збалансувати безпеку та зручність використання системи.

Крім того, важливо враховувати, що поведінкові ознаки під час логіну можуть бути неоднаково надійними в різних умовах. Через це система має зважати не лише на саму оцінку ризику, а й на якість сигналу, на основі якого вона отримана. У подальшому доцільно перевірити запропонований підхід експериментально на наборах даних динаміки натискань клавіш і в сценаріях, пов'язаних із використанням викрадених облікових даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Курніцький Д. П., Квєтний Р. Н. Порогова оптимізація risk-based автентифікації під вартісні регуляторні обмеження PSD2. Оптико-електронні інформаційно-енергетичні технології. 2025. Т. 50, № 2. С. 79–87.
2. Verizon. 2025 Data Breach Investigations Report. [Електронний ресурс]. Режим доступу: https://www.verizon.com/business/resources/T16f/reports/2025-dbir-data-breach-investigations-report.pdf
3. NIST. Digital Identity Guidelines: Authentication and Authenticator Management (NIST SP 800-63B-4). [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf
4. Podapati V. H., Nigam D., Das S. SoK: A Systematic Review of Context- and Behavior-Aware Adaptive Authentication in Mobile Environments. [Електронний ресурс]. Режим доступу: https://arxiv.org/abs/2507.21101
5. Shadman R., Wahab A. A., Manno M., Lukaszewski M., Hou D., Hussain F. Keystroke Dynamics: Concepts, Techniques, and Applications. [Електронний ресурс]. Режим доступу: https://dl.acm.org/doi/full/10.1145/3733103

Курніцький Дмитро Петрович – аспірант групи 126-23а, факультету інтелектуальних інформаційні технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця, dmytro.kurnitskiy@gmail.com

Софина Ольга Юріївна – канд. техн. наук, доцент кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця, *olsofina@gmail.com*

Kurnitsky Dmytro P. – post-graduate student, group 126-23a, faculty of intellectual information technologies and automation, Vinnytsia National Technical University, Vinnytsia, dmytro.kurnitskiy@gmail.com

Sofina Olga Yu. - Cand. Sc. (Eng), Docent of the Department of Automation and Intelligent Information Technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: *olsofina@gmail.com*