УДК 004.94

П. П. Малініч
В. В. Войтко

ЗАСТОСУВАННЯ ДАНИХ ТЕЛЕМЕТРІЇ ВІДЕОІГОР ДЛЯ ПОВЕДІНКОВОГО ФІНГЕРПРИНТИНГУ КОРИСТУВАЧА

Вінницький національний технічний університет

Анотація

У роботі розглядається питання зловживань в онлайн-іграх, таких як використання ботів та колективне керування акаунтами, що спотворює ігрову статистику. Автори пропонують концепцію поведінкового фінгерпринтингу, яка базується на аналізі унікальних патернів моторики, логіки та соціальної взаємодії користувача. Впровадження такого біометричного підходу дозволяє суттєво підвищити ефективність античіт-систем та забезпечити надійний захист облікових записів через верифікацію реальної особистості гравця.

Ключові слова: фінгерпринтинг користувачів, поведінкова біометрія, мультиакаунтинг, машинне навчання, патерни ігрової взаємодії, ідентифікація гравців, безперервна автентифікація.

Abstract

The study addresses the issue of misconduct in online games, such as the use of bots and account sharing, which distorts game statistics. The authors propose a concept of behavioral fingerprinting based on the analysis of a user's unique patterns of motor skills, logic, and social interaction. Implementing this biometric approach significantly enhances the effectiveness of anti-cheat systems and ensures robust account protection through the verification of the player's real identity.

Keywords: user fingerprinting, behavioral biometrics, multi-accounting, machine learning, gameplay interaction patterns, player identification, continuous authentication.

Вступ

У сьогоднішніх реаліях є доволі розповсюджена практика, коли один гравець онлайн-гри зловживає її правилами для отримання переваг нечесним шляхом. Також існують ситуації, коли декілька людей використовують один акаунт, граючи по черзі. Або користувач може використовувати боти, які імітують діяльність гравця у грі (наприклад, автоклікери). Це створює спотворення у даних статистики поточних гравців та їх досягнень. Виходячи з цього, є потреба у підходах, що дозволили б виявити реальність користувача за допомогою поведінкової біометрії та уникнути колективного використання акаунтів, забезпечуючи більш коректними даними, на відміну від зібраних статичними методами, використовуючи IP-адресацію чи HWID [1]. Також використання подібних підходів дозволить підвищити ефективність застосування античіту.

Опис концепції поведінкового фінгерпринтингу

Для ідентифікації користувача за допомогою поведінкової біометрії застосовується концепція поведінкового фінгерпринтингу (рис. 1), що включає ключові характеристики поведінки гравця, зокрема, патерни моторики, логіки та соціальні патерни поведінки [2]. Патерни моторики відповідають за підсвідому фізичну поведінку гравця, проте не є досить стабільними і залежать від поведінки, настрою та стану людини [3]. Хоч вони і вважаються надійним інструментарієм, аби зі значною ймовірністю відрізнити поведінку конкретного користувача від поведінки інших гравців, та базуються на одному з найнадійніших алгоритмів процесу виявлення недоброчесних проявів, проте метод фінгерпринтингу сам собою не є досить надійним [4]. Патерни логіки є доволі унікальними для кожної гри. Вони дозволяють сформувати інтелектуальний портрет гравця. Зазвичай ці аспекти включають навігацію, економічну поведінку та поведінку за надзвичайних обставин. Це дозволяє проаналізувати поведінку гравця у ситуаціях з різною тривалістю та з урахуванням різних особливостей. Соціальний аспект також є досить важливим, оскільки ідентифікує користувача як соціальну одиницю [5]. Він включає лінгвістичні патерни спілкування, соціальну взаємодію та поведінковий профіль. Це дозволяє зрозуміти, як гравець спілкується, визначити його типові особливості помилок, встановити коло його

спілкування у грі та відстежувати його поведінку. Тобто при зміні власника акаунта обов'язковою є зміна соціальної взаємодії.

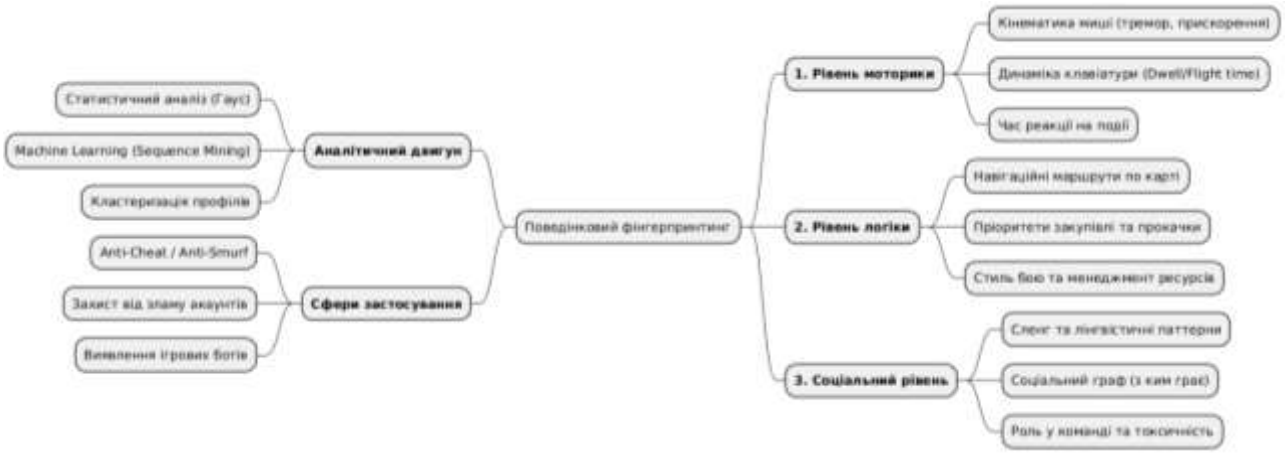

Рис. 1. Схема поведінкового фінгерпринтингу користувача

Таким чином, кожен із типів патернів є важливим, а за допомогою їх сукупнісного аналізу з'являється можливість формувати поведінкові фінгерпринти гравців. Для такого аналізу потрібні «сирі» дані кожного виду патерну, які слід аналізувати та класифікувати у сутності. Це дає розробникам можливість забезпечити кращий захист акаунтів у разі злому, оскільки, якщо зловмисник підбере пароль чи заволодіє ним, система виявить неспівпадіння поведінкового фінгерпринту. Тоді у розробників буде можливість підтвердити користувача за допомогою інших опцій, таких як поштова скринька чи застосунок автентифікації. Такий підхід дозволяє більш ефективно виявляти як недоброчесне використання поведінкових скриптів через аномалії поведінки, невластиві фінгерпринту, так і відслідковувати появу іншого гравця, що з різних причин грає почергово з власником акаунту.

Висновок

Впровадження поведінкового фінгерпринтингу на основі патернів моторики, логіки та соціальної взаємодії дозволяє вийти за межі малоефективних методів ідентифікації. Сукупний аналіз цих характеристик забезпечує точне виявлення ботів, автоклікерів та фактів передачі акаунтів, що є критичним для достовірності ігрової статистики. Такий підхід не лише автоматизує верифікацію реального користувача, а й суттєво підсилює античіт-системи, гарантуючи захист акаунтів навіть у випадку викрадення пароля.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Малініч П.П., Войтко В.В. Програмна архітектура взаємозв'язку аналітики телеметрії відеоігор та динамічної генерації ігрового контенту / П.П. Малініч, В.В. Войтко // Herald of Khmelnytskyi National University. Technical sciences. – 2025. – № 4 (355). – С. 365-372.

2. Crichton K. Rethinking Fingerprinting: An Assessment of Behavior-based Methods at Scale and Implications for Web Tracking / Crichton K., Cranor L. F., Christin N. // Proceedings on Privacy Enhancing Technologies. – 2025.

3. Мишок Р. Р. Концептуалізація кібербулінгу як технології у середовищі багатокористувацьких онлайн-ігор / Р. Р. Мишок, У. Д. Купяк // Перспективи : соціально-політичний журнал. – 2024. – № 3. – С. 237-242.

4. Інформаційні загрози та методи забезпечення безпеки в сучасних мережевих іграх / О. Полотай, Т. Брич, А. Ткаченко, М. Дітковський, М. Гуменюк // Кібербезпека: освіта, наука, техніка. – 2025. – №2(30). – С. 50-64. – DOI: https://doi.org/10.28925/2663-4023.2025.30.928.

5. Hammady R., Arnab S. Serious Gaming for Behaviour Change: A Systematic Review / R. Hammady, S.Arnab // Information. – 2022. – Vol. 13, № 3. – Art. 142. – DOI: https://doi.org/10.3390/info13030142.

Маліній Павло Павлович – аспірант кафедри програмного забезпечення, Вінницький національний технічний університет, Вінниця, e-mail: pavlo.malinich@vntu.edu.ua.

Войтко Вікторія Володимирівна – кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: dekanfki@i.ua.

Pavlo Malinich – postgraduate student of department of Software Development, Vinnytsia National Technical University, Vinnytsia, email: pavlo.malinich@vntu.edu.ua

Viktoria Voitko – Ph.D., Associate Professor of Software Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dekanfki@i.ua.