ДОСЛІДЖЕННЯ СУЧАСНИХ ПІДХОДІВ ДО ЗАХИСТУ МЕРЕЖЕВОГО ТРАФІКУ В ІГРОВИХ СЕРЕДОВИЩАХ

Полотай Орест
к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

Ткаченко Артур
викладач
Львівський державний університет безпеки життєдіяльності

Дітковський Максим
Здобувач вищої освіти
Національний університет Львівська політехніка

Забезпечення захисту мережевого трафіку в онлайн-комп'ютерних іграх є одним із пріоритетних напрямів у сфері інформаційної безпеки. Це пояснюється тим, що переважна частина потенційних загроз [1, 5], реалізується саме на рівні мережевої взаємодії. Ключовим завданням захисту мережевого обміну даними є гарантування конфіденційності, цілісності та доступності переданої інформації за умови мінімального впливу на швидкодію та стабільність ігрового процесу.

На відміну від класичних інформаційних систем, онлайн-ігрові платформи висувають підвищені вимоги до затримок передачі даних і пропускної здатності мережі. Навіть незначне зростання часу відгуку, спричинене використанням ресурсоємних або складних механізмів захисту, здатне суттєво погіршити якість взаємодії користувачів з ігровим середовищем. У зв'язку з цим методи забезпечення безпеки, що застосовуються в ігрових системах, зазвичай реалізуються як компромісне рішення між необхідним рівнем захищеності та вимогами до продуктивності [4].

Модель захисту мережевого трафіку в ігрових середовищах представлено на рисунку 1.

Рисунок 1 - узагальнена модель захисту мережевого трафіку в ігрових системах [власна розробка авторів]

На рисунку 1 подано узагальнену модель забезпечення захисту мережевого трафіку в ігрових системах, яка відображає основні принципи формування комплексної системи безпеки для онлайн-ігор. Запропонована модель охоплює ключові компоненти, що відповідають за захист інформації під час передавання та за контроль і виявлення мережевих атак у режимі реального часу.

З лівого боку схеми зображено клієнтський пристрій користувача, яким може виступати персональний комп’ютер або ноутбук із запущеним ігровим клієнтом. Клієнт формує запити до ігрового сервера, передає відомості про дії гравця та отримує актуальну інформацію щодо стану ігрового процесу. Обмін даними між клієнтською та серверною частинами відбувається через захищений канал зв’язку, що гарантує конфіденційність і цілісність пакетів, зокрема шляхом застосування механізмів шифрування або використання криптографічних протоколів TLS/SSL.

Праворуч на схемі розташовано ігровий сервер, який виконує обробку клієнтських запитів, підтримує актуальний стан гри та забезпечує синхронізацію ігрових сесій між учасниками. Серверна складова є критично важливим елементом системи, а її захист має вирішальне значення для забезпечення безперервної роботи, доступності та цілісності всієї ігрової платформи.

У центральній частині моделі виділено два допоміжні функціональні компоненти – систему моніторингу та модуль виявлення атак. Система моніторингу здійснює постійний аналіз мережевого трафіку й поведінкових характеристик користувачів у реальному часі, накопичує статистичні дані щодо кількості переданих пакетів, інтенсивності запитів та можливих відхилень від нормальної поведінки клієнтів. Це дає змогу своєчасно ідентифікувати потенційні загрози ще на ранніх етапах їх прояву.

Модуль виявлення атак відповідає за перевірку мережевого трафіку з метою виявлення підозрілих або шкідливих пакетів, сигнатур відомих типів атак, аномальних сценаріїв взаємодії клієнтів, а також спроб несанкціонованого

доступу або втручання в роботу системи. У разі фіксації загрози модуль формує відповідні сигнали, що можуть ініціювати блокування трафіку або запуск процедур додаткової перевірки.

Запропонована схема також ілюструє основні потоки даних та взаємодію між усіма компонентами системи: клієнт і сервер здійснюють обмін інформацією через захищений канал зв'язку, тоді як система моніторингу та модуль виявлення атак отримують копії трафіку або узагальнені статистичні показники для подальшого аналізу. Такий підхід забезпечує комплексний захист конфіденційності, цілісності та доступності ігрових даних у процесі функціонування онлайн-ігор.

Одним із фундаментальних підходів до забезпечення безпеки мережевого трафіку є застосування криптографічних методів шифрування. У сучасних онлайн-ігрових системах механізми шифрування використовуються з метою захисту переданих даних від перехоплення, аналізу та несанкціонованого доступу з боку третіх осіб.

Найбільш поширеними практиками в цій сфері є:

- використання алгоритмів симетричного шифрування для передачі основного ігрового трафіку [2];
- застосування асиметричних криптографічних алгоритмів для безпечного обміну ключовою інформацією;
- впровадження захищених протоколів транспортного рівня для організації безпечних каналів зв'язку.

Застосування шифрування дозволяє ефективно протидіяти пасивним атакам, зокрема перехопленню та прослуховуванню мережевого трафіку. Водночас цей підхід не гарантує повного захисту від активних загроз, спрямованих на підміну або модифікацію переданих даних. Крім того, зашифрований трафік може піддаватися аналізу за непрямими характеристиками, такими як обсяг, розмір або частота передавання пакетів, що потенційно може використовуватися зловмисниками.

Для підвищення рівня захищеності ігрових серверів від несанкціонованого доступу широко застосовуються механізми автентифікації та контролю доступу [3]. Ці механізми забезпечують перевірку легітимності клієнта та обмежують взаємодію з серверною частиною виключно для авторизованих користувачів.

До основних засобів автентифікації, що використовуються в онлайн-ігрових системах, належать:

- перевірка облікових даних користувачів;
- використання токенів доступу;
- застосування сесійних ключів для керування доступом у межах активних ігрових сеансів.

На рисунку 2 наведено узагальнену схему функціонування системи виявлення атак у мережі онлайн-гри. Вона ілюструє механізм взаємодії основних компонентів, спрямованих на забезпечення безпеки мережевого трафіку та оперативне виявлення потенційних загроз.

З лівої сторони представлено клієнтський пристрій гравця, на якому працює ігровий клієнт. Цей клієнт генерує мережевий трафік, що передається до ігрового сервера та відображає дії користувача і поточний стан гри. У нормальному режимі обмін даними відбувається безперервно та з мінімальними затримками, що забезпечує плавний ігровий процес.

Рисунок 2 - принцип роботи системи виявлення атак у мережі онлайн-гри [власна розробка авторів]

У центрі схеми розміщено модуль збору трафіку, який виконує роль ключового елемента системи виявлення атак. Цей модуль приймає копії мережевих пакетів і передає їх для подальшого аналізу. Збір інформації проводиться одночасно для сигнатурного та аномального аналізу, що дає змогу ідентифікувати як відомі, так і нові типи загроз [5].

Вгорі схеми розташована база сигнатур, що містить відомі шаблони атак і методів несанкціонованого втручання. Модуль збору порівнює отримані пакети з інформацією в базі сигнатур і передає результати сигнатурного аналізу, що дозволяє своєчасно виявляти відомі атаки, зокрема DDoS, підміни пакетів та спроби несанкціонованого доступу.

Нижче модуля збору розміщено модуль виявлення аномалій, який здійснює аналіз мережевого трафіку на основі статистичних і поведінкових характеристик. Цей компонент здатен ідентифікувати нові або змінені атаки, відсутні у базі сигнатур. У разі виявлення підозрілої активності модуль генерує сигнал тривоги, який може інформувати адміністратора або ініціювати автоматичне блокування потенційно небезпечних пакетів.

Праворуч на схемі знаходиться ігровий сервер, який приймає трафік від клієнтів і взаємодіє з модулем збору для моніторингу аномалій. Загалом система забезпечує комплексний захист цілісності, конфіденційності та доступності даних, мінімізуючи негативний вплив атак на хід ігрового процесу.

Захист мережевого трафіку в онлайн-ігрових системах є ключовим фактором забезпечення безпеки та стабільності ігрового процесу. Використання криптографічних алгоритмів шифрування, механізмів автентифікації та контролю доступу дозволяє ефективно протидіяти більшості відомих загроз,

зберігаючи при цьому високий рівень продуктивності та якості взаємодії користувачів із системою.

Запропонована модель із застосуванням системи моніторингу та модулю виявлення атак забезпечує своєчасне виявлення як відомих, так і нових типів загроз у мережевому трафіку, що сприяє підтриманню конфіденційності, цілісності та доступності даних. Такий комплексний підхід є ефективним засобом мінімізації негативного впливу атак на онлайн-ігри та підвищення їх загальної безпеки.

Список літератури:

1. Christophe Kiennert, Ismail Ziad, Hervé Debar, Jean Leneutre. A Survey on Game-Theoretic Approaches for Intrusion Detection and Response Optimization. August 2018ACM Computing Surveys 51(5):1-31 DOI:10.1145/3232848

2. Karen Scarfone, Peter Mell Guide to Intrusion Detection and Prevention Systems (IDPS). Recommendations of the National Institute of Standards and Technology. COMPUTER SECURITY. 2007. 127 p. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf

3. Полотай О.І., Брич Т.Б., Ткаченко А.М., Дітковський М.М., Гуменюк М.Р. Інформаційні загрози та методи забезпечення безпеки в сучасних мережевих іграх. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2025. Том 2 № 30: С. 50-64.

4. Полотай О.І., Дітковський М.М., Гуменюк М.Р. Використання слабких ланцюжків мережевих ігор як точки входу в корпоративні мережі. Матер. VII Всеукр. наук.-практ. конф. “Інформаційна безпека та інформаційні технології - 2025” (м. Львів, 27 листопада 2025 р.). Львів, ЛДУБЖД, 2025. С. 422–424.

5. Поширені загрози для геймерів: як суперники можуть впливати на хід гри. URL: https://www.eset.com/ua/about/newsroom/blog/home-security/osnovnyye-ugrozy-dlya-geymerov-kak-protivniki-mogut-vliyat-na-khod-igry/?srsltid=AfmBOoqmU3ieMyMCr7agDWUVKzO0Y7Z033LeULHz-5bTZgTok0_hqjz0