

5. Huang X. et al. Trends, research issues and applications of artificial intelligence in language education. *Educational Technology & Society*. 2023. Т. 26. № 1. С. 112–131.

6. García-Peñalvo F. J. The perception of Artificial Intelligence in educational contexts after the launch of ChatGPT: Disruption or Panic. 2023, <http://repositorio.grial.eu/handle/grial/28-38>

7. Huang X. et al. Trends, research issues and applications of artificial intelligence in language education. *Educational Technology & Society*. 2023. Т. 26. № 1. С. 112–131.

УДК 004.08: 621.37

Ярова І.А., канд. техн. наук, доцент

yarova@op.edu.ua

Дідик Є.Ю., бакалаврант

Національний університет «Одеська політехніка», 10252751@stud.op.edu.ua

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ RFID-СИСТЕМ В КІБЕРПРОСТОРИ

В сучасних промислових і комерційних процесах контроль переміщення різноманітних об'єктів або осіб реалізується шляхом впровадження технологій радіочастотної ідентифікації, або RFID-технологій (Radio-Frequency Identification Technology). Використання RFID-технологій для ідентифікації, відстеження й управління матеріальними ресурсами має низку переваг, до яких належать висока швидкість та ефективність функціонування систем, відсутність вимог, пов'язаних із прямим візуальним контролем міток (що дозволяє зекономити на системах освітлення), підвищена стійкість до природних впливів (забруднення, висока вологість). Але водночас самі принципи функціонування інтелектуальних автоматизованих систем зумовлюють загрози, пов'язані з можливістю несанкціонованого доступу до даних, переданих між RFID-мітками і зчитувачами. Можливість використання RFID-систем у різних сферах – від логістики та торгівлі до контролю безпеки та доступу до об'єктів – підтверджує важливість захисту цих систем від загроз в кіберпросторі.

RFID-системи є програмно-апаратними комплексами, що складаються з трьох основних компонентів: RFID-міток для збереження і передавання даних по переміщуваних об'єктах, RFID-зчитувачів – пристроїв для зчитування і передавання інформації, та програмного забезпечення – централізованої системи управління даними. Ці елементи спільно забезпечують передачу інформації між об'єктами і системою управління, що дозволяє автоматизувати процеси відстеження та ідентифікації неживих і живих об'єктів. RFID-зчитувачі можуть встановлюватися у різних об'єктах: торгових центрах, підприємствах, транспортних засобах, забезпечуючи безконтактний обмін даними в режимі реального часу. Використання цих систем дозволяє контролювати доступ до приміщень, вести облік продукції на складі та організовувати різні автоматизовані процеси.

Процес функціонування RFID-системи зазвичай складається з кількох етапів. На першому етапі за допомогою RFID-терміналу завантажуються завдання по інвентаризації. Далі на терміналі обирається тип інвентаризації (повна або за певним фільтром) і за допомогою курка або кнопки запускається процес зчитування міток. Для цього не потрібно наводити термінал на мітку, а достатньо здійснювати рух в бік ОЗ з мітками на відстані від 10 см до 10 м, періодично змінюючи положення терміналу. Про всі виявлені мітки термінал сповіщає звуковим сигналом, а знайдені мітки позначаються відповідним символом на екрані. Натиснувши на терміналі на назву мітки, можна зайти в картку ОЗ, переглянути і при необхідності змінити інформацію про ОЗ (наприклад, місцезнаходження, стан тощо). Після закінчення інвентаризації результати вивантажуються на сервер.

Вразливості RFID-систем можна поділити на чотири основні групи [2]. Перш за все, це вразливості, пов'язані з клонуванням RFID-міток. Використання відкритих стандартів без захищених каналів зв'язку дозволяє зловмисникам клонувати мітки для отримання

несанкціонованого доступу в систему. Під час атаки спуфінгу зловмисник видає себе за законну RFID-мітку або зчитувач, щоб отримати неавторизований доступ і таким чином - можливість маніпулювати системою. Цього можна досягти шляхом клонування міток RFID або створення підроблених зчитувачів, які імітують поведінку легальних пристроїв.

Актуальними для RFID-систем є загрози пасивного та активного перехоплення даних. При несанкціонованому перехопленні сигналу можлива підробка інформації, яка передається між міткою і зчитувачем. Оскільки RFID-зв'язок відбувається через радіохвилі, він чутливий до перехоплення. При наявності відповідного обладнання зловмисник може перехопити зв'язок між міткою і зчитувачем, потенційно отримуючи доступ до конфіденційної інформації або відстежуючи переміщення людей чи об'єктів.

Окрему групу загроз створюють вразливості RFID-зчитувачів. Використання спеціального обладнання для атаки на зчитувачі може призвести до відмови в обслуговуванні або передачі помилкових даних у систему. Зловмисне програмне забезпечення, наприклад віруси чи хробаки, становить значний ризик для RFID-систем. Зараження ним RFID-зчитувача може призвести до несанкціонованого доступу або маніпулювання даними, що зберігаються на мітках.

Фізичні атаки на RFID-системи можуть бути реалізовані у випадку, коли зловмисник має доступ на територію об'єкта, на якому впроваджена подібна система. Атаки подібного типу являють собою включають втручання в RFID-мітки або зчитувачі для отримання несанкціонованого доступу або порушення функціональності системи. Наприклад, зловмисник може фізично видалити або замінити RFID-мітку, щоб отримати доступ до зони обмеженого доступу.

Існують певні методи і заходи забезпечення кібербезпеки RFID-систем, які можна визначити як програмні і фізичні. Перш за все, для забезпечення конфіденційності інформації в системі рекомендується застосовувати шифрування переданих даних. З метою усунення можливостей перехоплення сигналів, слід впроваджувати криптографічні протоколи та безпечні канали зв'язку для захисту конфіденційності та цілісності даних.

Ефективним методом захисту є динамічне шифрування сигналу: регулярна зміна ключів шифрування допомагає мінімізувати ризики перехоплення.

Аутифікація між RFID-міткою та зчитувачем зменшує ризики реалізації атак підробки. Для подібної аутифікації можуть використовуватися унікальні ідентифікатори, криптографічні ключі, а також протоколи типу «запит – відповідь». Вказані методи гарантують, що лише авторизовані мітки та зчитувачі можуть взаємодіяти з системою.

Захист від клонування RFID-міток шляхом використання сучасних протоколів захисту з динамічною автентифікацією робить неможливим копіювання міток.

Контроль доступу до RFID-зчитувачів через надійне адміністрування з використанням програмного забезпечення дозволяє контролювати налаштування прав доступу і обробляти отримані дані з мінімальною затримкою. Для зменшення ризику зараження шкідливим програмним забезпеченням, на RFID-зчитувачах слід проводити регулярне антивірусне сканування та оновлення програмного забезпечення.

Важливим заходом захисту є моніторинг і аналіз підозрілих сигналів з метою своєчасного виявлення несанкціонованого втручання. Постійний моніторинг трафіку дозволяє виявляти аномальні патерни, які можуть свідчити про атаку на систему.

Не слід нехтувати також і фізичними заходами безпеки. Пломби, що захищають від несанкціонованого доступу до апаратного забезпечення RFID-системи, а також надійні огороження територій і приміщень повинні бути використані для зменшення ризику втручання в RFID-мітку або зчитувач.

Регулярні аудити та оцінки вразливості також можуть допомогти виявити та усунути будь-які потенційні недоліки в інфраструктурі RFID-систем.

Вразливості RFID-систем можна значно знизити завдяки впровадженню багаторівневих засобів захисту. Впровадження динамічного шифрування, захищених протоколів автентифікації та моніторингу трафіку зменшує ризик несанкціонованого доступу та перехоплення даних, підвищуючи надійність і безпеку RFID-технологій у різних сферах застосування.

Список посилань

1. Програмні рішення для автоматизації обліку [Електронний ресурс]. – Режим доступу: <https://ardix.systems/portfolio/>
2. Top RFID Cybersecurity Vulnerabilities. [Електронний ресурс]. – Режим доступу: <https://bluegoatcyber.com/blog/top-rfid-cybersecurity-vulnerabilities/>

УДК 004

Лисенко Д. Е., докт. техн. наук, професор
lysenko.d@stu.cn.ua

Мороз Д. В., студент

Національний університет «Чернігівська політехніка», dmytromoroz17854@gmail.com

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ КОНФІГУРУВАННЯ ПРОГРАМНО-ВІЗНАЧЕНОЇ МЕРЕЖІ

У зв'язку зі стрімким розвитком інформаційних технологій постає питання ефективного та оптимального керування мережевою інфраструктурою. Перспективним вирішенням даного питання є впровадження програмно-визначеної мережі(SDN) та її протоколів, які є новим підходом до керування комп'ютерними мережами. Дана технологія надає змогу централізованого керування мережами, що дозволяє гнучке керування та високу масштабованість.

Протоколи програмно-визначених мереж, такі як OpenFlow, є ключовими елементами, що забезпечують зв'язок між SDN-контролером та периферійними пристроями.[1]

Концепція SDN набула популярності після впровадження протоколу OpenFlow, і більшість наукових досліджень і програмних рішень з відкритим вихідним кодом засновані саме на ньому. Архітектура програмно-визначеної мережі з OpenFlow складається з трьох рівнів:

- 1) Інфраструктурний – використовується для пересилання пакетів між мережевими пристроями, що підтримують OpenFlow,
- 2) Управління – SDN-контролер, який використовується як операційна система, містить в собі площину управління і має централізоване подання, щоб виконувати рішення переадресації, засновані на врахуванні станів всіх пристроїв мережі. Контролер використовує північний(взаємодія з додатками і сервісами) та південний(взаємодія з мережевими пристроями) інтерфейси, які є основою логічної архітектури, що розділяє площину управління і площину передачі даних.
- 3) Прикладний рівень, який відповідає за мережеву логіку, політики і бізнес-додатки, що використовують мережеві дані, а також використовує північний інтерфейс для взаємодії з контролером. [2]

Комп'ютерна мережа в хмарі має відповідати таким вимогам:

- 1) Адаптивність до змін у трафіку, потреб додатків і бізнес-політик, інтегруючи при цьому нові функції без порушення роботи мережі,
- 2) Використання високорівневих абстракцій для гнучкого керування мережею, відкидаючи потребу в налаштуванні кожного мережевого пристрою окремо;
- 3) Масштабування мережі на вимогу.