УДК 004.056.5

О. В. Дичко

Т. Г. Кирилащук

ДОСЛІДЖЕННЯ ПРИХОВАНИХ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ ЗА ДОПОМОГОЮ ОПТИЧНИХ ВИПРОМІНЮВАЧІВ ІОТ-ПРИСТРОЇВ

Вінницький національний технічний університет

Анотація

У дослідженні приділено увагу проблемі витоку конфіденційної інформації через нетрадиційні канали зв'язку в системах Інтернету речей (IoT). Розглянуто спосіб створення прихованих оптичних каналів шляхом управління станом світлодіодних індикаторів пристроїв. Проведено аналіз потенційної можливості віддаленого перехоплення даних за допомогою фотоприймачів і камер мобільних пристроїв. Запропоновано рекомендації для зниження ризику використання таких каналів у корпоративному та приватному середовищі.

Ключові слова: кібербезпека; Інтернет речей; приховані канали; оптичне випромінювання; витік даних; стеганографія.

RESEARCH OF COVERT DATA TRANSMISSION CHANNELS USING OPTICAL EMITTERS OF IOT DEVICES

Abstract

The paper investigates the problem of sensitive information leakage through unconventional communication channels in Internet of Things (IoT) systems. The mechanism of creating optical covert channels by manipulating the state of device LED indicators is considered. The possibility of remote data interception using photodetectors and mobile device cameras is analyzed. Recommendations for minimizing the risks of using such channels in corporate and private networks are formulated.

Keywords: cybersecurity; Internet of Things; covert channels; optical radiation; data leakage; steganography.

Вступ

Інтеграція IoT-пристроїв у повсякденне життя значно змінює ландшафт кіберзагроз, виходячи за межі звичного мережевого моніторингу. Стандартні антивірусні програми та засоби мережевого захисту, зосереджені переважно на логічному рівні передачі даних, часто не здатні ефективно протистояти атакам через приховані фізичні канали. Одним із найдужчих ризиків є оптичний канал, який дозволяє використовувати світлові випромінювачі пристроїв для несанкціонованої передачі конфіденційної інформації, при цьому залишаючись практично невидимим для традиційних систем безпеки.

Тема набуває актуальності через кризу традиційних методів захисту периметра. Сучасні системи кібербезпеки здебільшого зосереджені на рівні програмного забезпечення та мережевих протоколів, при цьому часто упускають загрози, пов'язані з фізичним середовищем. Зокрема, використання прихованих оптичних каналів відкриває можливість витоку конфіденційної інформації

навіть із фізично ізольованих мереж (air-gapped networks). Це створює серйозну загрозу безпеці об'єктів інформаційної інфраструктури.

Головною метою є проведення комплексного аналізу вразливостей IoT-пристроїв до витоку даних через оптичні приховані канали.

Результати дослідження

1. Концептуальна модель оптичного прихованого каналу

Головна концепція аналізованої атаки зосереджується на використанні стандартного компонента IoT-пристрою – світлодіодного індикатора (LED) – у ролі імпровізованого засобу передачі даних. Теоретична модель такого каналу зв'язку складається із трьох ключових шарів: програмного запуску, фізичного випромінювання та віддаленого виявлення.

Сучасні мікроконтролери, які широко використовуються в пристроях Інтернету речей (зокрема, базовані на архітектурах ARM, ESP8266, MIPS), зазвичай взаємодіють зі світлодіодами через стандартні інтерфейси введення/виведення (GPIO). У випадку, коли шкідливе програмне забезпечення отримує привілеї на рівні ядра або доступ до відповідних драйверів, воно може змінювати логічний стан пінів GPIO. Це відкриває можливість створювати високочастотні сигнали, які керують яскравістю світлодіода. Використання таких операцій на апаратному рівні мінімізує навантаження на центральний процесор, що ускладнює виявлення цієї активності системами моніторингу ресурсів.

Носієм інформації виступає модуляційний світловий потік, який використовується для передачі даних. На відміну від класичних радіочастотних каналів, цей оптичний потік відзначається високою спрямованістю та стійкістю до електромагнітних перешкод, що робить його недоступним для виявлення стандартними системами аналізу вторгнень (IDS). У цьому випадку основним середовищем передачі даних є відкритий повітряний простір. Для успішної ексфільтрації інформації критичною умовою є дотримання прямої видимості (Line-of-Sight) між джерелом випромінювання, представленим світлодіодним (LED) пристроєм, та приймальним обладнанням, яке використовує зловмисник.

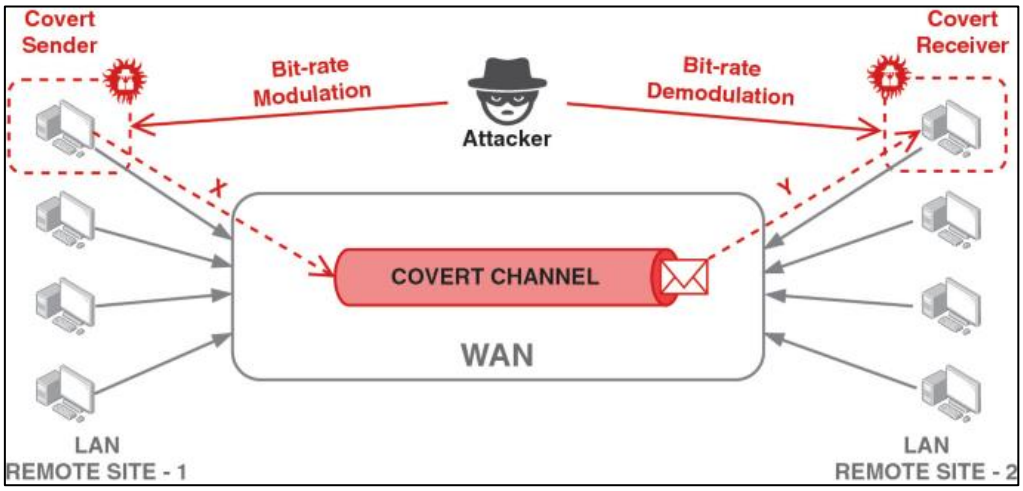

Рисунок 1 – Концептуальна модель передачі даних через оптичний прихований канал [1]

На рисунку 1 представлена модель, яка демонструє потенціал несанкціонованої ексфільтрації даних за межі захищеного периметра. Відмінно від звичних радіочастотних каналів, цей метод не генерує електромагнітних перешкод та залишається непомітним для стандартних систем виявлення.

2. Стратегія протидії та захисту

Мінімізація ризиків, пов'язаних із застосуванням оптичних прихованих каналів, вимагає інтегрованого підходу, який передбачає впровадження як програмних, так і фізичних заходів захисту в рамках інфраструктури.

Головним заходом протидії на рівні операційної системи є запровадження жорсткого контролю доступу до загальних інтерфейсів введення-виведення (GPIO).

Програмний рівень захисту – система спеціальних програм, що входять до складу програмного забезпечення, які реалізують функції захисту інформації [2].

До програмного захисту можна віднести:

1. Моніторинг системних викликів.
2. Аналіз патернів активності.
3. Віртуалізація індикаторів

Фізичні методи є найбільш надійними, оскільки вони діють безпосередньо на середовище передачі сигналу. Для нейтралізації загроз, пов'язаних із оптичною ексфільтрацією даних, доцільно застосовувати багаторівневий підхід, що включає як програмні, так і фізичні методи захисту. На рівні програмного забезпечення рекомендується здійснювати постійний моніторинг системних викликів до GPIO-інтерфейсів, а також впроваджувати алгоритми для виявлення аномальної активності індикаторів. Фізичні заходи протидії можуть включати екранування джерел випромінювання за допомогою непрозорих корпусів, використання поляризаційних фільтрів на вікнах приміщень для запобігання дистанційному перехопленню даних, а також встановлення низькочастотних фільтрів у лініях живлення світлодіодних індикаторів для обмеження їх здатності до швидкої модуляції.

Висновки

Проведене дослідження підтверджує, що використання штатних LED-індикаторів IoT-пристроїв як прихованих оптичних каналів становить серйозну загрозу для безпеки фізично ізольованих мереж. Запропонована модель модуляції та передачі даних через GPIO-інтерфейси демонструє недоліки традиційних методів захисту периметра. Встановлено, що лише поєднання програмного моніторингу активності, фізичного екранування та фільтрації сигналів може забезпечити надійний рівень захисту від несанкціонованої передачі конфіденційної інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. **Soderi S., Nicola R. D.** CONNECTION: COvert chaNnel NEtwork attaCk Through bIt-rate mOdulatioN. *Mobile and Wireless Technologies 2023. ICMWT 2023. Lecture Notes in Electrical Engineering*. Vol. 1146. Springer, Singapore, 2024. URL: https://link.springer.com/chapter/10.1007/978-981-99-9614-8_11 (дата звернення: 15.02.2026).
2. **Програмний захист даних.** *Офіційний сайт CIOU*. URL: https://ciou.lissa.cx.ua/articles/programnij-zahist-danih-e.html (дата звернення: 15.02.2026).

Олександр Віталійович Дичко – студент групи 1КІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: rugjgf524@gmail.com;

Науковий керівник: Тетяна Генадіївна Кирилащук – асистент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: kgt0998@gmail.com;

Oleksandr V. Dychko – student of group 1KITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: rugjgf524@gmail.com;

Scientific Supervisor: Tetiana H. Kyrylashchuk – assistant of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail: kgt0998@gmail.com.