

МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ ВІД АТАК ЧЕРЕЗ ПЕРИФЕРІЙНІ ПРИСТРОЇ

В. Є. Шевченко¹, В. М. Луценко¹, В. М. Степаненко¹

¹ Навчально-науковий Фізико-технічний інститут

Анотація

У роботі здійснено аналіз основних векторів атак на інформаційні системи через периферійні пристрої з фокусом на апаратні вразливості протоколу USB. Розглянуто нормативні вимоги технічного захисту інформації згідно з НД ТЗІ 2.5-004-99 і ДСТУ 3396-96, а також принципи реалізації багаторівневої моделі безпеки. Запропоновано реалізацію системи контролю доступу до периферії на основі принципу обмеженої взаємодії, що унеможливує непередбачену маршрутизацію команд або передачу даних між компонентами, які не мають явно дозволеного каналу зв'язку.

Ключові слова: USB, ТЗІ, технічний захист інформації, peripheral attacks, off-path USB, USBGuard, BadUSB

Вступ

Периферійні пристрої є критичними елементами інформаційних систем, а їхній захист — обов'язкова вимога відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [1]. НД ТЗІ 2.5-004-99 [2] регламентує оцінювання захищеності технічних засобів, включаючи контроль портів та інтерфейсів. ДСТУ 3396-96 [3] визначає принципи зонування та розмежування доступу. Актуальним є виявлення нестандартної поведінки периферії, що може загрожувати цілісності чи доступності інформації.

1. Основні загрози витоку інформації через периферійні пристрої

Периферійні пристрої традиційно сприймаються як пасивні компоненти обчислювальної системи, однак численні дослідження останніх років демонструють їхню здатність виступати в якості активного вектора атаки. Класичні загрози включають підміну пристрою, експлуатацію вразливостей прошивки або використання пристроїв з подвійною функцією.

Особливо небезпечною є атака типу BadUSB [4], що базується на можливості перепрограмування контролера USB-пристрою так, щоб він виконував дії, які не відповідають його задекларованому типу. Наприклад, флешка може видавати себе за клавіатуру і вводити команди в систему без відома користувача.

Нещодавні дослідження також звертають увагу на off-path injection атаки [5], при яких шкідливий пристрій не замінює легальний, а просто перехоплює або дублює відповіді, отримані хостом, через спільний USB-хаб. Це можливо завдяки відсутності механізму автентифікації джерела даних у USB-протоколі.

Інші небезпеки — атаки з підвищеною потужністю

сигналу, перехоплення автентифікаційних даних, або зміна логіки взаємодії системи з зовні легітимним пристроєм.

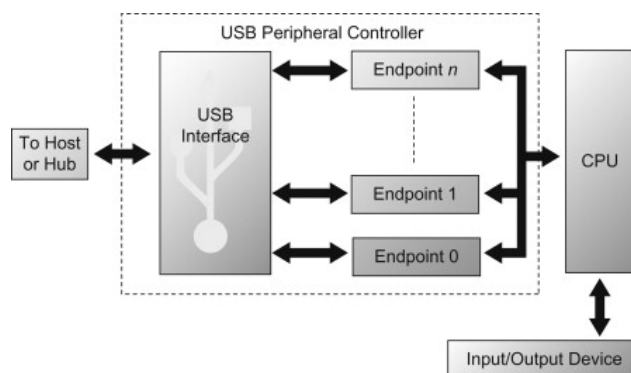


Рис. 1. Типова схема атаки через змінений периферійний пристрій

2. Методи та засоби захисту від витоку інформації

У відповідь на зростаючу кількість атак, у сфері технічного захисту інформації (ТЗІ) сформувалася багаторівнева модель захисту, яка включає фізичні, програмні та процедурні компоненти.

На фізичному рівні застосовуються блокатори USB-портів, екранування ліній зв'язку та використання USB-шлюзів, які ізолюють хост-систему від неперевіраних пристроїв.

Програмні рішення включають:

- Device Control Software — керують політиками доступу (USBGuard [6]);
- Моніторинг в реальному часі — за сигнатурами або поведінковими шаблонами;

- Реалізацію whitelist підходів — серійні номери, VID/PID.

НД ТЗІ 2.5-004-99 [2] вимагає обов'язкового контролю доступу до портів, ізоляції каналів введення-виведення, обмеження доступу до елементів ТЗІ-системи через периферію. ДСТУ 3396-96 [3] підтримує ці вимоги, деталізуючи принципи зонування доступу та технічного регламенту захищених інтерфейсів.

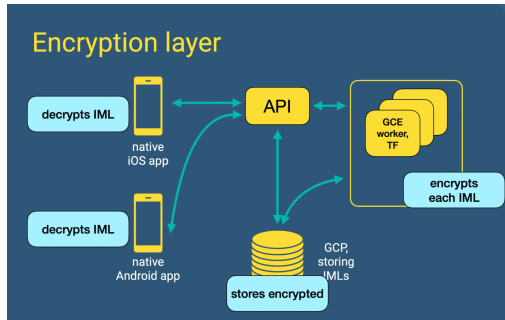


Рис. 2. Багаторівнева модель захисту периферійних пристроїв

3. Система захисту на основі принципу обмеженої взаємодії

У роботі запропоновано підхід до захисту інформаційних систем від атак через периферійні пристрої на основі принципу обмеженої взаємодії (PoLI — Principle of Limited Interaction), що дозволяє виявляти та блокувати нетипову активність на рівні USB-протоколу.

Цей підхід ґрунтується на тому, що після первинного підключення та авторизації пристрою, усі його подальші дії мають залишатися в межах попередньо визначеного профілю. Якщо пристрій намагається ініціювати іншу функціональність (наприклад, змінити клас інтерфейсу або додати нові endpoint-и), система вважає це відхиленням і блокує взаємодію.

Відмінність від існуючих рішень полягає в тому, що більшість сучасних засобів безпеки, таких як USBGuard чи Device Control Software, базуються на авторизації пристроїв на етапі підключення, орієнтуючись на ID або дескриптори пристроїв. Проте ці характеристики можуть бути змінені в обхід або підроблені, що робить традиційний контроль вразливим. PoLI, навпаки, враховує поведінкову послідовність та контекст команд, включаючи їхнє походження, затримки у відповіді, тип хабу (наприклад, TT або поп-TT) [7], та порівнює ці характеристики з шаблонами для дозволених сценаріїв.

Приклад реалізації: у системі, оснащений PoLI-контролем, звичайна флешка може бути авторизована лише як пристрій класу Mass Storage з доступом лише до bulk-endpoint. Якщо той самий пристрій починає надсилати запити або відповіді з ознаками класу HID (пристрій введення), система автомати-

чно фіксує відхилення та ізолює його. Подібне також стосується затримок — якщо відповідь приходить з нетиповою швидкістю або з іншого підключення (наприклад, внаслідок off-path атаки [5]), вона буде визнана потенційно небезпечною.

Переваги підходу:

- не потребує оновлення сигнатур чи довірених списків;
- забезпечує глибший контроль взаємодії на рівні протоколу;
- дозволяє протидіяти новим типам атак, зокрема протокольним інжекціям;
- узгоджується з принципами технічного захисту, викладеними в НД ТЗІ 2.5-004-99 [2].

Недоліки підходу:

- потребує профілювання дозволеної поведінки для кожного типу пристрою;
- можлива несумісність з деякими багатифункціональними пристроями;
- потребує інтеграції з хостовим стеком або апаратним USB-фільтром.

Таким чином, впровадження принципу обмеженої взаємодії дозволяє не лише підвищити рівень безпеки, а й забезпечити реалізацію вимог прикладних нормативних документів у сфері ТЗІ щодо контролю каналів взаємодії з технічними засобами обробки інформації.

Перелік використаних джерел

1. *Верховна Рада України*. Про захист інформації в інформаційно-телекомунікаційних системах. — 1994. — Закон України № 80/94-ВР.
2. *Державна служба спеціального зв'язку та захисту інформації України*. НД ТЗІ 2.5-004-99. Технічний захист інформації. Порядок контролю та оцінювання захищеності. — 1999. — Нормативний документ з технічного захисту інформації.
3. *Державний комітет України з питань технічного регулювання і споживчої політики*. ДСТУ 3396-96. Захист інформації. Загальні положення. — 1996. — Державний стандарт України.
4. Nohl K., Lell J. BadUSB: On accessories that turn evil // BlackHat USA. — 2014.
5. The Impostor Among US(B): Off-Path Injection Attacks on USB Communications / V. Dumitru, S. Chakrabarti, S. Savage, G. M. Voelker // Proceedings of the 32nd USENIX Security Symposium. — 2023. — URL: <https://www.usenix.org/conference/usenixsecurity23/presentation/dumitru>.
6. Hat R. USBGuard: A USB Device Authorization Policy Framework. — 2022. — URL: <https://usbguard.github.io>.
7. Anker. Understanding USB Hubs and Transaction Translators. — 2023. — URL: <https://www.anker.com/blogs/hubs-and-docks/brief-understanding-of-usb-hubs>.