ПОЛІПШЕНИЙ ЗАХИСТ МІКРОКОНТРОЛЕРА ВІД ЧИТАННЯ

доцент, к.т.н. Воргуль О.В., студент Білоцерківець О.Г.
Харківський національний університет радіоелектроніки, кафедра мікропроцесорних технологій і систем,
e-mail: oleksii.bilotserkivets @nure.ua

Abstract. Embedded system designers need to regularly store confidential information, such as cryptographic keys, user data, proprietary algorithms, and other forms of intellectual property in the firmware of microcontrollers. To prevent the retrieval of confidential information stored in microcontrollers (MCUs), many MCUs implement functionality known as read protection. This limits the reading of the internal memory through debugging or software interfaces. But these methods of protection are not always reliable

Вступ. Проектувальникам вбудованих систем регулярно потрібно зберігати конфіденційну інформацію, таку як криптографічні ключі, дані користувача, власні алгоритми та інші форми інтелектуальної власності у прошивці мікроконтролерів . Для запобігання вилучення конфіденційної інформації, що зберігається в мікроконтролерах (MCU), багато MCU реалізують функціональні можливості, відомі як захист від від зчитування. Це обмежує читання внутрішньої пам'яті за допомогою налагоджувальних або програмних інтерфейсів.

Основна частина. Однак ці функції не є повністю надійними - багато MCU містять недоліки конструкції, які дозволяють обійти захист від читання. Розробники також часто неправильно налаштовують захист від читання, неправильно розуміють документацію постачальника або підривають захист читання через ненавмисно дозволену функціональність прошивки. Крім того, навіть при правильній реалізації та налаштуванні захист від читання часто може бути подоланий такими методами, як ін'єкція несправностей та інвазивні атаки кремнію. Для розробників важливо знати про ці обмеження, щоб точно оцінити ризик.

Однією з поширених помилок є вибір мікроконтролера, який забезпечує достатню безпеку для задоволення вимог до проектування. Це, як правило, виникає через нерозуміння функцій безпеки, пропонованих MCU, незнання дефектів функцій безпеки MCU або недостатнє визначення вимог безпеки на етапі вибору компонентів.

Спроби реалізувати захист від зчитування на мікроконтролерах, не призначених для забезпечення такого захисту, невдалі. Зазвичай вони включають спробу відключення налагоджувальних інтерфейсів (таких як JTAG або SWD) шляхом перепризначення виводів або відключення контактів на рівні друкованої плати. Як правило, ці методи не працюють.

Коли інтерфейси налагодження обмежуються, а не взагалі відключаються на все більш складних сучасних MCU, існує безліч способів, щоб постачальники мікроконтролерів ненавмисно добавили

вразливості кристалу, які дозволяють обійти захист від читання. Щороку нові атаки дозволяють обходити помилкові реалізації захисту від читання на мікроконтролерах. Зазвичай ці атаки можливі лише шляхом часткового обмеження налагоджувальних інтерфейсів, а не їх взагалі відключення.

Одним з таких випадків є функція PALL (Захистити всіх) популярної серії бездротових комунікаційних мереж nRF51. Якщо ця функція ввімкнена, вона запобігає доступу налагоджувача до адрес пам'яті флеш -пам'яті та оперативної пам'яті. Однак це не обмежує доступ до реєстру процесора. Захист від зчитування можна подолати, спостерігаючи за змінами в реєстраційних значеннях, одночасно змушуючи повторно виконувати інструкції завантаження, де адреса, що читається, є реєстром ЦП.

Інший резонансний недолік, опублікований Йоганнесом Обермайєром та Стефаном Тачнером, включає мікроконтролери серії STM32F0 у RDP (ReaDout Protection) рівня 1. У цьому режимі доступ до певних діапазонів пам'яті блокується, але інтерфейс налагодження залишається активним. Обмеження доступу до налагоджувача активуються лише після двох циклів синхронізації системної шини після початку першого доступу налагоджувача до шини.

У часи низького навантаження на системну шину одне слово даних можна прочитати через інтерфейс налагодження до того, як обмеження почнуть діяти. Повторно скидаючи налаштування процесора та читаючи одне слово за раз, можна прочитати весь вміст пам’яті мікроконтролера.

Подібні недоліки зазвичай зустрічаються у всіх основних брендах мікроконтролерів. Вибираючи компоненти та оцінюючи ефективність заходів захисту від зчитування, важливо дослідити атаки, які були опубліковані проти мікроконтролера. Більшість опублікованих логічних атак може бути зірвано повним вимкненням інтерфейсу налагодження, якщо це дозволено MCU. Навіть коли вразливості ще не були опубліковані щодо певного MCU, найкраще взагалі відключити налагоджувальні інтерфейси для поглибленого захисту, на випадок, якщо в майбутньому будуть виявлені логічні недоліки.

Висновки. Всім механізмам захисту від зчитування мікроконтролера можна запобігти за допомогою достатніх ресурсів і зусиль. Однак ретельний вибір компонентів, конфігурація та розробка прошивки можуть підвищити вартість атаки. Хоча жоден MCU не може повністю протистояти атакам, спеціально розроблені MCU високого рівня безпеки пропонують механізми для повного відключення інтерфейсів налагодження та запобігання зчитуванню.

Список використаних джерел.

1. AVR: Introductory Course, John Morton Kidlington, England 2002.

2. Microcontroller Readback Protection : Bypasses and Defensesi Sultan Qasim Khan, 2020