DOI: 10.34185/1991-7848.itmm.2024.01.070

ДОСЛІДЖЕННЯ РІВНЯ ВІДПОВІДНОСТІ МІКРОКОНТРОЛЕРА ESP32 МІЖНАРОДНИМ СТАНДАРТАМ З КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Мазуренко В.Б.

Дніпровський національний університет, Україна

Анотація. *Досліджується захист мікроконтролера ESP32 від кібернетичних загроз шляхом аналізу відповідності платформи (мікроконтролер, ОС, API, підтримка виробника) вимогам міжнародних стандартів з кібербезпеки. Зокрема розглядаються: засоби керування звітами щодо вразливості, оновлення програмного забезпечення, надійне зберігання конфіденційних параметрів безпеки, безпечне спілкування та захист персональних даних. Отримано висновок, що мікроконтролер ESP32 в цілому відповідає стандартам з кібернетичної безпеки інтернету речей. Єдиний виняток, який було знайдено, полягає в тому, що виробник ESP32 не публікує свою політику розкриття вразливостей. Таким чином, рівень кібернетичної безпеки платформи ESP32 слід визнати достатньо високим для побудови звичайної, побутової системи IoT.*

Ключові слова: *інтернет речей, автоматизація, кібербезпека, мікроконтролер, комп'ютерно-інтегровані технології*

Вступ. Інтернет речей (IoT – Internet of Things) безперервно збільшує свою присутність в нашому житті. Цьому процесу розширення в першу чергу сприяє зменшення вартості сенсорів, мікроконтролерів, приладів мережевої інфраструктури вкупі з активним розвитком різноманітних хмарних сервісів. Сьогодні самі звичайні люди мають доступ до технологій, які дозволяють збирати інформацію з різноманітних джерел, створювати автоматизацію для роботи побутової техніки та реалізовувати потрібні сценарії взаємодії технічних об'єктів. Проте, як тільки користувач починає використовувати ці нові технології, відразу з'являється небезпека викрадання конфіденційних даних, підміни або знищення важливої інформації, появи спроб реалізації шкідливого функціювання системи та таке інше, – тобто всього того, що носить назву кібернетична загроза. Запобігти зазначеним загрозам можливо завдяки впровадженню в системах IoT стандартів з забезпечення кібернетичної безпеки.

Основний матеріал. Метою дослідження є аналіз можливостей одного з найбільш популярних мікроконтролерів, які використовуються для створення IoT, а саме – мікроконтролера ESP32, надавати потрібний рівень кібернетичного захисту. Дослідження проведено шляхом порівняння технічних характеристик, властивостей операційної системи (ОС) та специфікацій прикладного програмного інтерфейсу (API – Application Programming Interface), якими оснащується мікроконтролер ESP32, а також підтримки розробника з вимогами міжнародного стандарту ETSI EN 303 645.

Найбільш авторитетними організаціями, які створюють стандарти з кібербезпеки є такі: ETSI (European Telecommunications Standards Institute) – Європейський інститут телекомунікаційних стандартів; IoTSF (Internet of Things Security Foundation) – Організація з безпеки інтернету речей; GSMA (Groupe Speciale Mobile Association) — Асоціація «Спеціальна група мобільних технологій»; NIST (National Institute of Standards and Technology) – Національний інститут стандартів і технології, США; IEEE (Institute of Electrical and Electronics Engineers) – Інститут інженерів з електротехніки та електроніки; IEC (International Electrotechnical Commission) – Міжнародна електротехнічна комісія; ENISA (European Union Agency for Network and Information Security) – Агентство Європейського Союзу з питань мережевої та інформаційної безпеки. Зважаючи на те, що в даному разі розглядається бюджетний мікроконтролер, який використовується для потреб загального користування, таких, наприклад, як «розумний будинок», буде доцільним спиратися на стандарт ETSI, який має назву «Кібербезпека Інтернету речей користувачів: основні вимоги» [1]. Цей стандарт встановлює наступні основні положення забезпечення кібербезпеки інтернету речей:

1) не використовуйте універсальних паролів за замовчуванням;

2) впроваджуйте засоби керування звітами щодо вразливості;

3) постійно оновлюйте програмне забезпечення;

4) надійно зберігайте конфіденційні параметри безпеки;

5) спілкуйтеся безпечно;

6) зведіть до мінімуму відкритий простір для нападу;

7) забезпечте цілісність програмного забезпечення;

8) переконайтеся, що персональні дані захищені;

9) зробіть системи стійкими до збоїв; 10) перевіряйте дані системної телеметрії;

11) спростить для користувачів видалення даних користувачів;

12) зробіть установку та обслуговування пристроїв простими;

13) перевіряйте введені дані.

Не всі з цих вимог стосуються самого мікроконтролера, його ОС та API. Пункти 1, 6, 8, 9, 10, 11, 12, 13 – в першу чергу залежать від розробників та користувачів IoT. За належного програмування, вдалої конструкції та правильної експлуатації всі ці пункти можуть буть реалізовані практично на всіх популярних платформах. Всі інші пункти (2, 3, 4, 5, 7) також залежать від розробників та користувачів, але їх не вдасться виконати, якщо мікроконтролер, ОС, API та підтримка виробника (тобто – платформа) не мають відповідних інструментів. Розглянемо послідовно саме ці пункти.

Почнемо з другого пункту стандарту. Стосовно засобів керування звітами щодо вразливості стандарт потребує відкритої публікації політики виробника щодо виявлення вразливостей. Це перша вимога з якої витікають усі наступні. На жаль, виробник – фірма Espressif цього не зробила. Відповідно, й наступні вимоги стандарту щодо публікації та термінів усунення вразливостей наразі не заявляються фірмою Espressif як такі, що постійно виконуються. Проте в базі даних NIST [2] відслідковуються інциденти, пов’язані з продукцією Espressif, так само, як й Espressif публікує звіти, щодо виявлених вразливостей, однак це не можна сприймати, як виконання вимог стандарту.

Щодо третього пункту основних вимог зазначимо, що випуск оновленого програмного забезпечення для мікроконтролера ESP32 відбувається на постійній основі. Операційною системою реального часу, якою виробник оснащує ESP32 є FreeRTOS. Вона включає в себе ядро та бібліотеки. Останній реліз вийшов в грудні 2022 року. Засобом розробки програмного забезпечення від виробника є Espressif IoT Development Framework (ESP-IDF). Найновішою

версією цього інструментального забезпечення на сьогодні є версія 5.1 від червня 2023 року. В кожній новій версії системного та інструментального програмного забезпечення проводиться оновлення засобів кібернетичної безпеки та усуваються виявлені, або потенційні вразливості. Тому в розробника системи IoT на базі ESP32 завжди є можливість виконати вимоги щодо виконання пункту 3 стандарту. Крім того ESP32 забезпечує механізм, відомий як Over the Air Update (OTA), який дозволяє проводити безпечне обновлення програмного забезпечення без зупинення робочих процесів. Таким чином, можна зробити висновок, що третій пункт основних положень забезпечення кібербезпеки інтернету речей стандарту ETSI по відношенню до платформи ESP виконується.

В мікроконтролері ESP32 надійне збереження конфіденційних параметрів безпеки (пункт 4 вимог стандарту) забезпечується шифруванням файлової системи (флеш-шифрування) за алгоритмом AES. Додатково відбувається шифрування енергонезалежної пам’яті, яке використовує стандартний алгоритм AES-XTS. Ключ зберігається в окремому розділі пам'яті, яка сама шифрується за допомогою звичайного шифрування.

Пункт 5 вимог стандарту («безпечне спілкування») передбачає використання криптографічного захисту під час передавання даних. Платформа ESP32 надає для цього необхідні інструменти у вигляді ESP-TLS, який є компонентом ESP-IDF і надає прикладний програмний інтерфейс для роботи з TLS – криптографічним протоколом захисту на транспортному рівні (Transport Layer Security). API надає функціональні можливості для перевірки сертифіката сервера, автентифікації сертифіката клієнта, підтримки попередньо спільних ключів PSK (pre-shared key) та протоколу переговорів прикладного рівня ALPN (Application-Layer Protocol Negotiation). На основі протоколу TLS реалізується протокол HTTPS, що дозволяє побудувати надійний зв’язок з хмарним сервером, так само, як й з IoT-пристроями.

Стандарт вимагає (пункт 7) наявності засобів забезпечення цілісності програмного забезпечення шляхом застосування механізму безпечної

загрузки, який передбачає використання цифрових підписів програмного коду. Такий механізм в ESP32 існує й він легко конфігурується.

Висновки. В результаті проведеного аналізу встановлено наступне:

1) Мікроконтролер ESP32 в цілому відповідає європейським стандартам з кібернетичної безпеки інтернету речей.

2) Невідповідність європейському стандарту ETSI EN 303 645 має місце лише стосовно засобів керування звітами щодо вразливості, оскільки виробник ESP32 не публікує своєї політики щодо виявлення вразливостей.

3) Для побудови звичайної, побутової системи IoT рівень кібернетичної безпеки мікроконтролера ESP32 слід визнати достатньо високим; умовою побудови захищеної IoT на базі цього мікроконтролера є використання всіх наявних в ESP32 інструментів кібернетичної безпеки та виконання вимог стандарту ETSI EN 303 645.

ЛІТЕРАТУРА / REFERENCES

1. ETSI EN 303 645 V2.1.1 «Cyber Security for Consumer Internet of Things: Baseline Requirements». Sophia Antipolis, Fr: ETSI, 2020. 34p

2. NATIONAL VULNERABILITY DATABASE. [Електронний ресурс]/Сайт NIST, URL: https://nvd.nist.gov/vuln/search/results?adv_search=true&isCpeNameSearch=true&query=cpe%3A2.3%3Ah%3Aespressif%3Aesp32%3A-%3A*%3A*%3A*%3A*%3A*%3A*%3A*

ASSESSMENT OF ESP32 MICROCONTROLLER COMPLIANCE WITH INTERNATIONAL STANDARDS OF CYBER SECURITY FOR INTERNET OF THINGS

Valeriy Mazurenko

Abstract. *The protection of the ESP32 microcontroller from cyber threats is studied by analyzing the compliance of the platform (microcontroller, OS, API, manufacturer support) with the requirements of international cybersecurity standards. In particular, the following topics are covered: means to manage reports of vulnerabilities, keeping software updated, securely storing sensitive security parameters, secure communication, and protecting personal data. Generally, it is concluded that the ESP32 microcontroller meets the cybersecurity standards of the Internet of Things. The only one exception that was found is the ESP32 manufacturer does not publish its vulnerability disclosure policy. Thus cybersecurity level of ESP32 platform should be considered as a quite high to produce a regular, household IoT system.*

Keywords: *Internet of Things, automation, cyber security, microcontroller, computer-integrated technologies*