DOI 10.34185/1562-9945-3-152-2024-08
УДК 044.056

В.Б. Мазуренко

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

Анотація. В роботі досліджується захист мікроконтролера ESP32, який широко використовується для побудови інтернету речей, від кібернетичних загроз шляхом аналізу відповідності платформи розробника вимогам міжнародних стандартів з кібербезпеки.
Ключові слова: інтернет речей, автоматизація, кібербезпека, мікроконтролер, комп'ютерно інтегровані технології.

Постановка проблеми. 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. Оскільки саме економічний фактор є рушійною силою в глобальному розповсюдженні систем IoT, постає актуальне питання: чи здатні популярні бюджетні мікроконтролери забезпечити потрібний рівень кібернетичної безпеки?

Мета дослідження. Метою дослідження, результати якого представлені в даній статті, 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 операцій-

ної 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.

Аналіз останніх досліджень і публікацій. Питанню створення та розвитку систем IoT і, зокрема питанню забезпечення кібернетичної безпеки, присвячено велику кількість наукових та науково-технічних статей та книг, з яких достатньо вказати, наприклад, такі роботи, як [1] та [2]. Важливо зазначити, що більшість публікацій на цю тему відображають, розкривають вже існуючі стандарти у цій галузі, надаючи тлумачення, роз'яснення та приклади до них, що є, безумовно, вкрай важливим. Проте, основою є саме міжнародні стандарти. 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. Всі ці організації мають свої стандарти з кібернетичної безпеки IoT. Не вдаючись до опису відмінностей цих стандартів, зазначимо, що в першу чергу вони розрізняються за сферою застосування IoT, як то: промислова автоматизація, медицина, «розумний город», транспортні засоби, загальне призначення та таке інше. Зважаючи на те, що в цій роботі 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» [3]. Надалі в тексті будемо називати його просто «стандарт».

Викладення основного матеріалу дослідження. 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.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

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.

Звичайно, 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. Звичайно, й всі інші пункти залежать від розробників та користувачів, проте їх не вдасться виконати, якщо мікроконтролер, ОС, API та підтримка виробника (тобто – платформа) не мають відповідних інструментів. Тому послідовно розглянемо саме пункти 2, 3, 4, 5, 7.

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 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 усува-

ються 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 (NVS – Non-volatile storage), 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.

Таким чином, аналіз відповідності технічних характеристик ESP32, властивостей ОС та специфікацій API з вимогами міжнародного стандарту ETSI EN 303 645 показує, що платформа ESP32 в цілому надає всі можливості задля створення безпечної IoT-системи. Невідповідність фіксується лише стосовно пункту 1 вимог, оскільки виробник – компанія Espressif, – не публікує своєї політики щодо виявлення вразливостей. З точки зору використання ESP32 для побудови звичайної, побутової системи IoT рівень кібернетичної безпеки цього контролера слід визнати достатньо високим. Реальний рівень безпеки такої

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

системи буде залежати від коректної розробки програмного забезпечення, вдалої конструкції пристроїв та правильної експлуатації у відповідності до стандарту.

Проведений аналіз був би неповним, якби ми не згадали задекларованих сторонніми особами вразливостей ESP32. Зокрема, база даних NIST включає опис деяких зафіксованих вразливостей ESP32 [4]. Усунення цих вразливостей виконується виробником мікроконтролера за звичайною процедурою й завершується випуском нової версії програмного забезпечення. В той же час, доволі часто зустрічаються й інші спроби компрометації платформи ESP32, наприклад [5, 6]. Проте злом системи IoT в цьому разі базується на вразливостях не мікроконтролера як такого, а загально відомих вразливостях безпеки WiFi мереж, до цього ж умовою злому є слабкий пароль доступу до мережі. Тому такі випадки не є специфічними для ESP32.

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

1 Дугінець Г.В. Концепція «Інтернет речей» у глобальному виробництві: досвід України // Економіка і регіон, Науковий журнал. – Випуск № 1 (68) – ПолтНТУ, 2018 – С.127 – 133

2. IoT Security and Privacy Paradigm / Edited by Souvik Pal, Vicente García Díaz and Dac-Nhuong Le – Boca Raton, FL: Taylor & Francis Group, LLC, 2020. 398p

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

4. 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*
5. WiFi Vulnerabilities on ESP32/ESP8266 IoT Devices. [Електронний ресурс], URL: https://www.micro.ai/blog/wifi-vulnerabilities-on-esp32-esp8266-iot-devices
6. Барибін О.І., Зайцева Е.Є., Бражний В.В. Тестування безпеки пристроїв інтернету речей на базі мікроконтролера ESP-32 // Кібербезпека: освіта, наука, техніка, Електронне фахове наукове видання. – Том 2 №6 (2019) – Київський університет імені Бориса Грінченка, 2019 – С.71 – 81

REFERENCES

1. Duhinets H.V. Conception of the “Internet of Things” in Global Manufacturing: Experience for Ukraine // Economics and Region, Science Jornal. – Issue № 1 (68) – PoltNTU, 2018 – P.127 – 133
2. IoT Security and Privacy Paradigm / Edited by Souvik Pal, Vicente García Díaz and Dac-Nhuong Le – Boca Raton, FL: Taylor & Francis Group, LLC, 2020. 398p
3. ETSI EN 303 645 V2.1.1 «Cyber Security for Consumer Internet of Things: Baseline Requirements». Sophia Antipolis, Fr: ETSI, 2020. 34p
4. NATIONAL VULNERABILITY DATABASE. [Electronic source] / NIST Site, 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*
5. WiFi Vulnerabilities on ESP32/ESP8266 IoT Devices. [Electronic source], URL: https://www.micro.ai/blog/wifi-vulnerabilities-on-esp32-esp8266-iot-devices
6. Barybin O.I., Zaitseva E.Y., Brazhnyi V.V. Testing the Security ESP32 Internet of Things Devices // Cybersecurity: Education, Science, Technique CYBERSECURITY: EDUCATION, SCIENCE,TECHNIQU, Electronic professional scientific publication. – Vol. 2 №6 (2019) – Borys Grinchenko Kyiv University, 2019 – P.71 – 81.

Received 15.04.2024.
Accepted 17.04.2024.

Assessment of ESP32 microcontroller compliance with international standards of cyber security for internet of things

Internet of Things becomes more and more accessible for ordinary people. This fact brings cybersecurity threats. Thus there is necessity to assess how microcontroller platforms that are quite popular for producing home IoT system are really secure. One of such platforms is ESP32. This study has an aim to asses ESP32 cybersecurity level. Method of assessment is analyzing how international standard requirements are fulfilled by ESP32 microcontroller platform. The ETSI standard ETSI EN 303 645 V2.1.1 «Cyber Se-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

curity for Consumer Internet of Things: Baseline Requirements» is chosen as a base. In particular, the "Cyber security provisions for consumer IoT" requirements was considered. First of all, those requirements are under analyze that depend only on platform (microcontroller, OS, API, manufacturer support) performance and not on IoT-system designers or consumers. 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, and ESP32 cybersecurity level should be considered as a quite high to produce a regular, household IoT system. The non-compliance with European standard ETSI EN 303 645 is only in relation to vulnerability reporting controls, as the ESP32 manufacturer does not publish its vulnerability disclosure policy. But on the other hand, the NIST database includes a description of some recorded ESP32 vulnerabilities. Management of these vulnerabilities is performed by the microcontroller manufacturer in the usual procedure and it is completed by the release of a new version of the software. Thus, the real cybersecurity level of home IoT system on the base of ESP32 will depend on how correctly hardware and software design is, and does an IoT system operation is provided in accordance with the cybersecurity standards.

Мазуренко Валерій Борисович – Дніпровський національний університет, фізико-технічний факультет, канд. техн. наук, доцент кафедри кібербезпеки та комп'ютерно-інтегрованих технологій.

Mazurenko Valeriy Borisovich – Oles Honchar Dnipro National University, Physical and Technical Faculty, Doctor of Philosophy, docent of Chair of cyber security and computer-integrated technologies.