УДК 004.056

ПОКРАЩЕННЯ ЗАХИЩЕНОСТІ ПРОЦЕСУ ВІДДАЛЕНОГО ОНОВЛЕННЯ ПРОШИВКИ IOT ПРИСТРОЇВ ЗА ДОПОМОГОЮ ХМАРНИХ БЕЗПЕКОВИХ СЕРВІСІВ AWS

С. А. Іщик[1,а], О. М. Барановський[1,б]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

У даній роботі досліджено проблематику захищеності віддаленого оновлення прошивок пристроїв Інтернету речей. Запропоновано рішення на основі хмарної інфраструктури Amazon Web Services з використанням цифрового підпису, mTLS та HMAC. Розроблений метод було протестовано на стійкість до типових атак.

Ключові слова: Інтернет речей, прошивка, віддалене оновлення, хмарні сервіси AWS

Вступ

З розвитком Інтернету речей зростає потреба у захищеному віддаленому оновленні прошивок, особливо для пристроїв, що використовуються в критичній інфраструктурі, зокрема у військовій сфері. Поширені практики, як–от оновлення через незахищені протоколи HTTP або FTP, а також ручне оновлення, є застарілими та не відповідають вимогам безпеки, особливо в умовах масового використання та відсутності фізичного доступу до пристроїв. За останні роки було виявлено ряд вразливостей, що використовувались для атак на системи віддаленого оновлення прошивок. Нижче наведено декілька прикладів:

- Вразливість у продукті Bitdefender Box використовувалась для атаки MiTM через застосування незашифрованого протоколу HTTP, що призводило до віддаленого виконання коду на пристрої [1].
- Вразливість в маршрутизаторі Asus DSL–N14U_B1 дозволяла інсталювати версії прошивок, не призначені для цієї моделі, що призводило до атак типу DoS [2].
- У лютому 2024 року повідомлялося про атаку на сервери оновлення російських модифікованих дронів DJI, внаслідок чого було припинено процес оновлення близько 200,000 пристроїв агресора [3].

З огляду на актуальні вимоги до захисту пристроїв IoT, доцільно звернути увагу на хмарні рішення, зокрема на платформу AWS. Основна перевага AWS — інтеграція всіх необхідних інструментів: зберігання та обробка даних, автоматизація, та контроль доступу. Модель спільної відповідальності дозволяє розподілити обов'язки між користувачем та провайдером, при цьому гарантується високий рівень безпеки на інфраструктурному рівні з боку AWS. AWS забезпечує більшу гнучкість та масштабованість порівняно з локальними рішеннями, що дозволяє оперативно реагувати на зміни вимог. Крім того, забезпечується висока доступність, відмовостійкість та інтеграція з сучасними системами безпеки.

Існуючі підходи до оновлення прошивок пристроїв IoT є застарілими, використовують незахищені протоколи з'єднання, не передбачають автентифікацію пристроїв, та не мають функціоналу підтвердження автентичності та цілісність переданого файлу.

Мета цієї роботи — запропонувати та оцінити рішення для безпечного механізму віддаленого оновлення прошивок пристроїв IoT на базі хмарної платформи AWS з використанням технології mTLS, цифрового підпису з перевіркою контрольної суми на пристрої та підтвердженням коду HMAC після встановлення. Такий підхід забезпечить надійний захист каналу оновлення, перевірку автентичності та цілісності прошивки, контроль доступу до ресурсів, а також гнучке масштабування.

1. Запропоноване рішення

Для покращення захищеності віддаленого оновлення прошивки, було запропоновано використовувати mTLS, порівняння контрольної суми файлу прошивки при отриманні, та HMAC код для підтвердження операції. Технологія mTLS забезпечить автентифікацію з'єднання усіх пристроїв, та сервера оновлень, за допомогою сертифікатів. За потреби сертифікат можна деактивувати або оновити. Контрольна сума файлу оновлення надсилається разом з повідомленням про оновлення, що дозволяє порівняти значення, а також перевірити цифровий підпис файлу прошивки перед встановленням. HMAC код, створений пристроєм на основі контрольної суми файлу прошивки, унікального ідентифікатора пристрою, та поточного часу, надсилається після встановлення нової версії,

[а] sericy-ipt25@lll.kpi.ua
[б] o.baranovskyi@kpi.ua

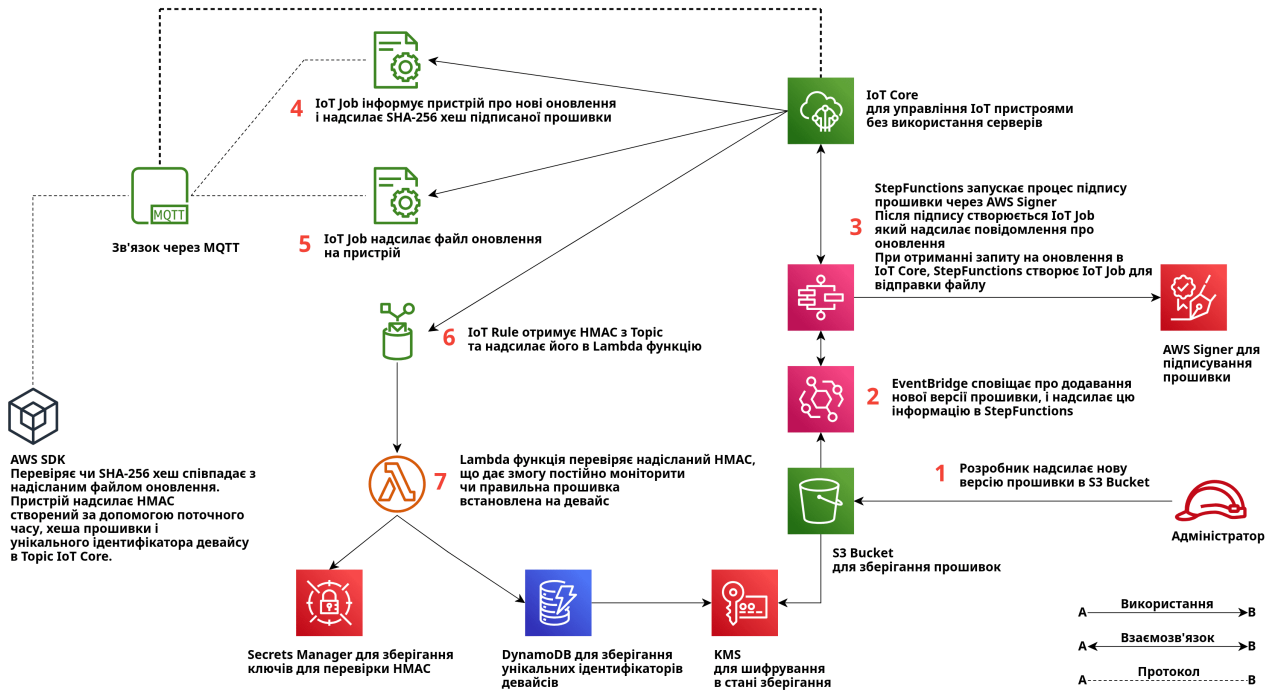

Рис. 1. Діаграма архітектури процесу оновлення прошивки

та повідомляє сервер про те, що на пристрої було встановлено цілісний та автентичний файл прошивки. В залежності від отриманого HMAC коду, адміністратор може виконати організаційні операції над пристроєм. На рис. 1 представлено архітектуру рішення для безпечного оновлення прошивки пристроїв Інтернету речей із використанням сервісів AWS:

1. **Ініціалізація оновлення:** адміністратор завантажує нову версію прошивки до S3 Bucket.
2. **Обробка події оновлення:** сповіщення про завантаження нової версії активується службою Amazon EventBridge, передаючи інформацію про оновлення до AWS StepFunctions.
3. **Підписування прошивки:** AWS Step Functions ініціює процес цифрового підписування програмного забезпечення в сервісі AWS Signer. Після цього створюється відповідне IoT Job в AWS IoT Core, для сповіщення пристрою про оновлення.
4. **Сповіщення пристрою:** AWS IoT Job надсилає пристрою повідомлення про оновлення та контрольну суму підписаної прошивки через протокол MQTT.
5. **Транспортування файлу прошивки:** після підтвердження готовності пристрою до оновлення через запит в MQTT Topic, формується IoT Job для передачі файлу прошивки за допомогою Presigned URL.
6. **Генерація та передача HMAC коду:** після встановлення прошивки, пристрій локально обчислює HMAC код. Обчислене значення передається до MQTT Topic в AWS IoT Core.
7. **Перевірка цілісності отриманого файлу:** HMAC код передається з MQTT Topic через AWS IoT Rule до функції AWS Lambda, в якій виконується верифікація отриманого коду.

2. Тестування розробленого методу

MiTM атака: система ефективно протидіє перехопленню трафіку завдяки використанню двосторонньої автентифікації (mTLS) між пристроєм та платформою AWS.

DDoS атака на сервер оновлень: архітектура рішення базується на сервісах, які мають вбудовані механізми масштабування й автоматичного захисту від перевантаження. Захист на мережевому рівні забезпечується сервісом AWS Shield, що зменшує ризик виведення сервера оновлень з ладу при високій кількості запитів.

Replay атака на сервер: для запобігання повторному використанню повідомлень використовується часова мітка в коді HMAC. На сервері здійснюється верифікація актуальності повідомлення, що унеможливлює реалізацію цієї атаки.

Rollback атака на пристрій: механізм цифрового підпису та перевірка контрольної суми бінарного файлу прошивки на стороні пристрою гарантують встановлення виключно авторизованої та актуальної версії. У разі невідповідності контрольної суми або цифрового підпису, оновлення автоматично відхиляється. Однак, за наявності фізичного доступу до пристрою зазначений захисний механізм може бути обійдений через перезапис пам'яті.

Підміна сервера оновлень (spoofing): пристрій перевіряє автентичність сервера за допомогою сертифікатів mTLS. Передача прошивки здійснюється виключно через підписані URL із Amazon S3, а цифровий підпис гарантує автентичність файлу.

Підміна пристрою: кожен пристрій автентифікується за допомогою сертифікату mTLS. Додаткова

Таблиця 1. Оцінка ризиків для активів розробленої системи оновлення прошивок

Актив	**Загроза**	$V_{\text{цінн.}}$, **у.о.**	$P_{\text{ймов.}}$ **(0–1)**	$R_{\text{ризик}}$, **у.о.**	$R_{\text{норм.}}$	**Оцінка ризику**
Пристрій та сервер	MiTM атака	1000	0.1	100	0.111	Дуже низький
Сервер	DDoS	800	0.2	160	0.178	Дуже низький
Сервер	Replay атака	800	0.4	320	0.356	Низький
Пристрій	Rollback атака	200	0.1	20	0.022	Дуже низький
Сервер	Spoofing	800	0.3	240	0.267	Низький
Пристрій	Spoofing	200	0.3	60	0.067	Дуже низький
Сума:				900	1	

перевірка HMAC коду з використанням секретного ключа унеможливлює підміну навіть при доступі до мережі. Проте, сертифікат або приватний ключ може бути викрадений за наявного фізичного доступу до пристрою.

Для аналізу проведеного тестування, було використано метод якісної оцінки ризиків. Результати наведено в табл. 1.

1. Ризик для активу:

$$R_{\text{ризик}} = V_{\text{цінн.}} \times P_{\text{ймов.}}$$

де:
- $R_{\text{ризик}}$ — ризик для активу (у.о.),
- $V_{\text{цінн.}}$ — цінність активу (у.о.),
- $P_{\text{ймов.}}$ — ймовірність загрози (від 0 до 1).

2. Нормалізований ризик:

$$R_{\text{норм.}} = \frac{R_{\text{ризик}}}{\text{Макс. ризик}}$$

де:
- $R_{\text{норм.}}$ — нормалізований ризик,
- $R_{\text{ризик}}$ — ризик для активу,
- Макс. ризик — максимальний ризик серед усіх активів — 900 у.о.

3. Оцінка ризику:

Для оцінки ризику визначено категорію за рівнем нормалізованого ризику:
- $R_{\text{норм.}} \leq 0.2$ — Дуже низький,
- $0.2 < R_{\text{норм.}} \leq 0.4$ — Низький,
- $0.4 < R_{\text{норм.}} \leq 0.6$ — Середній,
- $0.6 < R_{\text{норм.}} \leq 0.8$ — Високий,
- $R_{\text{норм.}} > 0.8$ — Дуже високий.

Результати тестування підтвердили здатність запропонованого методу забезпечити комплексний захист процесу віддаленого оновлення прошивки. Атаки типу Rollback та Spoofing пристрою все ще можливі, але тільки при фізичному доступі до пристрою, тому вплив потенційних наслідків істотно зменшується.

Висновки

Огляд актуального стану захищеності процесу віддаленого оновлення показав, що значна частина пристроїв залишається вразливою. У роботі запропоновано використовувати технологію mTLS, перевірку контрольної суми файлу прошивки на стороні пристрою, та підтвердження успішності оновлення за допомогою HMAC коду. Було обрано хмарну платформу AWS завдяки її надійності, легкій інтеграції з IoT та вбудованим механізмам безпеки. Під час дослідження було здійснено аналіз стійкості розробленого методу до типових атак на процес віддаленого оновлення прошивок IoT–пристроїв. Тестування розробленої архітектури показало, що запропоноване рішення суттєво зменшує ризики атак на процес оновлення.

Запропоноване рішення створює передумови до інтеграції додаткових сервісів для роботи з пристроями IoT, зокрема AWS IoT Analytics та AWS Greengrass, що дозволить будувати більш комплексні рішення із розширеним моніторингом, локальною обробкою даних, автоматизацією процесів та інтеграцією з іншими хмарними компонентами для підвищення гнучкості та рівня безпеки.

Перелік використаних джерел

1. *National Vulnerability Database.* CVE-2024-13872 / National Institute of Standards, Technology. — 03/12/2025. — URL: https://nvd.nist.gov/vuln/detail/CVE-2024-13872 (visited on 04/28/2024).
2. *National Vulnerability Database.* CVE-2021-3166: Authentication Bypass in OpenCart / National Institute of Standards, Technology (NIST). — 01/18/2021. — URL: https://nvd.nist.gov/vuln/detail/CVE-2021-3166.
3. *Hambling D.* British Software Will Protect Ukrainian Drones From Cyber Attack. — 03/20/2025. — URL: https://www.forbes.com/sites/davidhambling/2025/03/20/british-software-will-protect-ukrainian-drones-from-cyber-attack/.