АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ У ПРИСТРОЯХ IoT

Трилецький Д. Г., Сєвєрінов О. В.
Харківський національний університет радіоелектроніки, Харків, Україна

Автентифікація – це процедура встановлення належності користувачеві інформації в системі його ідентифікатора. Автентифікація в системі IoT є важливим компонентом кібербезпеки.

Метою доповіді є дослідження способів автентифікації у пристроях системи IoT. У результаті дослідження було виявлено три способи, які залежать від пристроїв, місцезнаходження і характеру даних, які пристрій передає або отримує [1]:

1) Розподілена одностороння автентифікація. Один пристрій реєструється як дійсний на другому пристрої за допомогою гешу паролю чи цифрового сертифікату. Коли перший пристрій намагається з'єднатися, другий пристрій перевіряє пароль або сертифікат та порівнює його зі збереженою інформацією. Якщо інформація співпадає, пристрій дозволяє підключення. Такий вид автентифікації краще за все підходить для пристроїв, які з'єднуються лише один з одним.

2) Розподілена двостороння автентифікація. Кожен пристрій має містити унікальний цифровий ідентифікатор, що збережений для цього пристрою. З'єднання можливе лише тоді, коли перший пристрій довіряє цифровому сертифікату другого пристрою і навпаки. Протокол безпеки транспортного рівня обмінюється сертифікатами і порівнює їх. Така автентифікація зазвичай використовується для онлайн-транзакцій електронної комерції і передачі особливо конфіденціальних даних.

3) Централізована трьохстороння автентифікація. Адміністратор реєструє пристрої на сервері і зв'язує пристрої з дійсними цифровими сертифікатами. При трьохсторонній автентифікації сертифікати безпеки не зберігаються на пристроях і не можуть бути викрадені зловмисниками, але пристрої досі забезпечують надійний захист [2]. Цей підхід краще за все працює для постійно підключених пристроїв або пристроїв з доступом в Інтернет по запиту, оскільки він ліквідує будь-які затримки автентифікації. Служба керування життєвим циклом сертифікатів і ключів може централізовано керувати сертифікатами і під'єднуватись до будь-якого пристрою в мережі, який потребує перевірки.

Список літератури

1. How to use IoT autherntication and authorization for security. URL: http://surl.li/brxhe (date of access: 06.04.2022).

2. Д'якова Н. Є., Сєвєрінов О. В. Аналіз загроз безпеки у системах розумного будинку / ВА ЗС АР; НТУ" ХПІ"; НАУ, ДП" ПДПРОНДІАВІАПРОМ"; УмЖ, 2021.