АНАЛІЗ КРИПТОГРАФІЧНИХ ПРИМІТИВІВ В МЕРЕЖАХ IoT

Журіло О., Комарець К., Ляшенко О.
Харківський національний університет радіоелектроніки, Харків, Україна

Останнім часом все більше уваги приділяється концепції IoT, яка являє собою єдину інформаційну систему, що об'єднує речі кіберфізичного простору. До таких речей відносять не тільки звичні комп'ютери, смартфони, мережеве обладнання, але і пристрої, що виконують специфічні функції: розумні термостати, автомобілі з безпілотним керуванням, трекери фізичної активності та інші. Тобто IoT має різноманітні сценарії застосування, що і визначає актуальність цієї концепції і підвищений до неї інтерес з боку розробників. Зокрема, об'єднані мережею розумні речі можуть знайти застосування в управлінні здоров'ям, в розумних будинках, в управлінні здоров'ям, в організації транспортних мереж. Основними характеристиками кожного сценарію для розумних речей є отримання, передача і обробка критично важливої для людини інформації: дані про його здоров'я, житло, звичках і пересуванні. Тому питання інформаційної безпеки, особливо конфіденційності інформації, обов'язковий для дозволу при побудові IoT [1].

Метою доповіді є аналіз криптографічних примітивів та протоколів, які використовуються в мережах IoT. В доповіді розглядається різні підходи до захисту інформації в IoT, це шифрування на основі атрибутів (ШОА) та «легкі» криптографічні алгоритми. В рамках ШОА можна виділити два підходи до реалізації: шифрування на основі закритого ключа та шифрування на основі шифротексту. Безпека інтернету речей на основі «легких» криптографічних примітивів безпосередньо пов'язана з використовуванням в протоколах: шифрів, хеш-функцій. Здебільшого для таких пристроїв використовують блочне шифрування, так як воно вимагає менше ресурсів і пам'яті, ніж асиметричні криптографічні алгоритми. Проаналізовані наступні шифри Present-80, MIBS-80, Khudra та PRINCE. Таким чином, існує ряд блокових шифрів, які можуть бути використані для ряду завдань в IoT. В ряді випадків IoT-пристрої фізично доступні зловмиснику, що робить можливим, силові атаки.

Таким чином ШОА дозволяє здійснювати контроль доступу та адресувати одне зашифроване повідомлення за допомогою декількох пристроїв, що мають однакові набори атрибутів, що є полезним у IoT-системах. З іншого боку, такі схеми повинні бути розроблені, щоб задовольнити умови обмеженості ресурсів. «Легкі» криптографічні примірники задовольняють цьому умові, однак не всі з них достатньо стійкі.

Список літератури

1. Ляшенко О. Моделювання можливих загроз інформаційної безпеки в системах з використанням мікроконтроллерів AVR / О. Ляшенко, О. Журіло– «GLOBAL CYBER SECURITY FORUM 2019» 14 – 16 листопада 2019, Харьков, С 68-69.