Андрій Блозва
Кандидат педагогічних наук, доцент
Національний університет біоресурсів і природокористування України, м. Київ, Україна
ORCID: 0000-0002-4377-0916
blozvaand@gmail.com

Валерій Лахно
Доктор технічних наук, професор, завідувач кафедри,
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0001-9695-4543
valss21@ukr.net

БЕЗПЕКА В МЕРЕЖАХ LORAWAN

Анотація. Інтернет речей характеризується збільшенням поширеності об'єктів і об'єктів з автоматичним можливостями передачі даних, кожен з унікальними ідентифікаторами. Збільшений трафік IoT в основному викликаний зв'язком між машинами (M2M): сенсорні системи, такі як ті, що використовуються в розумних будинках і розумних містах, процесах промислової автоматизації, портативних мобільних обчислювальних пристроях, системах зв'язку транспортних засобах і т.д.

Ключові слова: Інтернет речей, безпека, мережі, LoRaWAN.

Інтернет речей характеризується збільшенням поширеності об'єктів і об'єктів з автоматичним можливостями передачі даних, кожен з унікальними ідентифікаторами. Збільшений трафік IoT в основному викликаний зв'язком між машинами (M2M): сенсорні системи, такі як ті, що використовуються в розумних будинках і розумних містах, процесах промислової автоматизації, портативних мобільних обчислювальних пристроях, системах зв'язку транспортних засобах і т.д.

При аналізі окремий пристрій в полі не слід розглядати окремо. Швидше за все, слід брати до уваги всі інтерфейси до шлюзів, додатків і систем зберігання даних, в яких обробляються і зберігаються великі обсяги даних.

Проблеми безпеки існують у всіх шарах архітектури IoT. Значні зусилля, необхідні для гармонізації конфіденційності даних і вимог компаній і суспільств.

Безпека не завжди розглядається при розробці продукції. Це велика проблема, яка заслуговує того, щоб її розглядали так само, як і підключення. Деякі продукти IoT надаються з застарілими операційними системами у вбудованій формі.

Встановлення системних оновлень або оновлень безпеки на пристроях IoT є складною процедурою. Вузли зазвичай встановлюються на відкритому повітрі або в приміщеннях замовника, щоб охопити географічні зони, що представляють інтерес. Через це іноді існує велика кількість спустошених вузлів, які дуже важко контролювати і керувати.

Доступ до кожного вузла для індивідуального зміни його налаштувань або конфігурацій - включаючи конфігурації безпеки - не є репрезентативним технічним рішенням. Автоматичне ініціювання цих вузлів виробниками також не забезпечує значного рівня довіри. Належні та перевірені процедури повинні запобігати тому, щоб оновлення стали самими отворами безпеки.

Деякі компанії безпеки наразі обмінюються ресурсами для забезпечення рішень безпеки IoT, таких як шифрування на диску в цілому або реалізація захищених від злому компонентів. Ці рішення дозволяють як вдосконалене управління цифровою безпекою, так і управління життєвим циклом за допомогою шифрування та обмеження доступу до чутливих даних.

Стек протоколу LoRaWAN складається з прикладного рівня, рівня MAC і рівня PHY. Дані з прикладного рівня відображаються в MAC Payload. Рівень MAC конструює кадр MAC з використанням корисного навантаження MAC. Корисна інформація MAC містить заголовок кадру (який містить як адреси джерела, так і адреси призначення плюс лічильник кадрів), порт кадру і корисне навантаження кадру (що містить дані програми). Порт кадру використовується, щоб визначити, чи містить кадр окремі команди MAC (коли він встановлений в 0) або конкретні дані програми. Нарешті, рівень PHY використовує кадр MAC як корисне навантаження PHY і конструює кадр PHY після вставки преамбули, заголовка PHY і CRC.

До параметрів RF належать частоти, рівні потужності, модуляція і основні протоколи RF. Всі вони інкапсульовані в параметри LoRaWAN RF або фізичному рівні.

Оскільки для будь-якої бездротової мережі надзвичайно важливо забезпечити безпеку, LoRaWAN використовує два шари безпеки: один для мережі і один для прикладного рівня. Мережевий рівень безпеки забезпечує автентичність пристрою в мережі. Захист рівня додатків гарантує, що оператор мережі не має доступу до даних додатків кінцевого користувача.

Кінцевий хост (вузол) повинен бути активований перед тим, як він може обмінюватися інформацією в мережі LoRaWAN. У мережах LoRaWAN доступні два способи активації: OTAA і ABP.

Over-the-Air Activation (OTAA) - Цей метод ґрунтується на повідомленнях про приєднання до мережі і повідомлень про приєднання, які працюють разом. Кожне кінцеве пристрій (вузол) розгортається з 64-розрядним DevEUI, 64-бітним AppEUI і 128-бітним AppKey. DevEUI є глобальним унікальним ідентифікатором для пристрою, який має 64-бітну адресу, порівнянну з MAC-адресою для пристрою TCP / IP. AppKey використовується для криптографічного підписання запиту на приєднання. Після цього всі три значення стають доступними для сервера додатків, до якого має бути підключено пристрій. AppKey використовується, коли вузол посилає повідомлення запиту на приєднання. Вузол посилає повідомлення запиту на приєднання, яке складається з його AppEUI і DevEUI. Він додатково посилає DevNonce, який є унікальним, випадково згенерованим, двобайтовим значенням, що використовується для запобігання атакам відтворення.

Ці три значення підписуються 4-байтовим MIC (Код цілісності повідомлення) за допомогою AppKey пристрою. Сервер приймає заявки на приєднання лише з пристроїв з відомими значеннями DevEUI і AppEUI під час перевірки MIC за допомогою AppKey.

Якщо сервер приймає запит на приєднання, він реагує на пристрій за допомогою повідомлення Приєднатися. Програми та мережні сервери обчислюють два 128-бітові ключі вузла: ключ сеансу додатків (AppSKey) і ключ мережевого сеансу (NwkSKey) відповідно. Вони обчислюються на основі значень, надісланих у повідомленні запиту приєднання від вузла.

Крім того, сервер додатків генерує власне значення nonce: AppNonce. Це ще одна унікальна, випадково створена величина.

Відповідь Join Accept включає AppNonce, NetID і адресу кінцевого пристрою (DevAddr) разом з конфігураційними даними для RF затримок (RxDelay) і каналів для використання (CFList). Адреса пристрою (DevAddr) у відповіді Join Accept - це 32-бітовий ідентифікатор, який є унікальним у мережі.

Можна використовувати адресу пристрою для розрізнення кінцевих пристроїв, які вже приєдналися до мережі. Це дозволяє серверам мереж і додатків використовувати правильні ключі шифрування і правильно інтерпретувати дані.

При отриманні даних назад дані шифруються за допомогою AppKey. Потім вузол використовує AppKey для розшифрування даних і отримує AppSKey і NwkSKey, використовуючи значення AppNonce, отримане у відповіді Join Accept.

Метод активації за допомогою персоналізації (ABP) - Цей метод відрізняється від OTAA, оскільки вузли постачаються з DevAddr і обома сеансовими ключами (NwkSKey і AppSKey), які повинні бути унікальними для вузла. Оскільки вузли вже мають необхідну інформацію та ключі, вони можуть почати спілкування з мережевим сервером без необхідності обміну повідомленнями.

Як тільки вузол приєднався до мережі LoRaWAN - або через OTAA або ABP - всі майбутні повідомлення будуть зашифровані і підписані за допомогою комбінації конкретних клавіш (див. Також Безпека в LoRaWAN):

Мережевий ключ сеансу (NwkSKey) - це механізм безпеки мережевого рівня. Цей ключ є унікальним для кожного кінцевого пристрою та спільний між кінцевим пристроєм та мережним сервером. Ключ мережної сесії забезпечує цілісність повідомлень під час комунікації та безпеки для кінцевого пристрою для зв'язку з мережним сервером.

Ключ сеансу додатків (AppSKey) - Цей ключ відповідає за шифрування корисного навантаження (додаток до програми). Це також 128-бітний ключ AES, унікальний для кожного кінцевого пристрою. Він розділяється між кінцевим пристроєм і сервером додатків. Ключ сеансу програми шифрує і розшифровує повідомлення даних програми і забезпечує безпеку корисних навантажень програми.

Ці два сеансові ключі (NwkSKey та AppSKey) унікальні для кожного пристрою та кожного сеансу. Якщо пристрій динамічно активується (OTAA), ці клавіші регенеруються кожною активацією. Якщо пристрій статично активовано (ABP), ці клавіші залишаються незмінними, поки вони не будуть змінені вручну.

Розширений стандарт шифрування (AES) - Шифрування AES з обміном ключа, реалізованого в LoRaWAN, на основі безпеки для бездротових мереж IEEE 802.15.4.

LoRaWAN пропонує простий процес конфіденційної та цілісної конфіденційності даних, який має бути сумісним між виробниками та мережевими провайдерами. Реалізований механізм шифрування гарантує, що мережа LoRaWAN залишається захищеною.

Поточний стандарт LoRaWAN 1.0.x вже містить порівняно високий рівень безпеки. Перелічені тут ризики та сценарії нападу є легітимними і повинні оцінюватися окремо для кожного випадку використання. Рішення вже обговорювалися вище.

З метою задоволення підвищених вимог безпеки в мережах IoT Альянс LoRa постійно працює над вдосконаленням стандарту. Лора Альянс - це некомерційна асоціація організацій, які працюють разом для стандартизації мереж LPWAN.

ПОСИЛАННЯ

[1] LoRaServer. – Електронний ресурс – Режим доступу: https://www.loraserver.io/overview/architecture/
[2] Stacet in IoT – Електронний ресурс – Режим доступу: https://staceyoniot.com/