УДК 004.021
Маслова Ю.Ю., Довженко Н.М., Лавровський І.М.
DOI: 10.31673/2409-7292.2021.043643

ЗАХИСТ ПРИСТРОЇВ IOT НА БАЗІ ПРОТОКОЛУ LORA WAN

В роботі проведено аналіз життєвого циклу пристроїв IOT, цикл розробки ПЗ IOT, проаналізовано загрози та технології захисту пристроїв, а також протокол LoRaWAN, способи взаємодії пристроїв, архітектуру мережі та способи захисту інформації в рамках зазначеного протоколу. Досліджені основні етапи життєвого циклу пристроїв IOT, етапи розробки ПЗ IOT в контексті захисту інформації та проаналізовані загрози що можуть виникати на різних стадіях життєвого циклу пристроїв IOT. Висунуті рекомендації та пропозиції щодо організації процесів взаємодії з зацікавленими особами, безпосередньо, щодо процесів отримання певного пристрою IOT в контексті безпеки та оглянуті технології захисту пристроїв IOT на базі протоколу LoRaWAN.

Ключові слова: технології, Lora Wan, процеси, загрози, IoT, життєвий цикл.

Вступ

В наш час, одним з ключових напрямків розвитку мереж зв'язку є концепція Інтернету речей [1, 2, 3]. За переважною більшістю прогнозів, "Інтернет речей" продовжить бурхливо розвиватися, та відповідно до прогнозів, в 2023 році кількість підприємств та корпорацій у відсотковому відношенні, що будуть використовувати IOT рішення сягне 70%. Кількість самих кінцевих пристроїв в цьому сегменті досягне позначки в кілька мільярдів. Широкий спектр галузей, де є потреби в використанні IoT, а також різноманітність пристроїв і датчиків, що підключаються до мережі, збільшують попит в фахівцях, які знаються на таких системах і здатних з ними працювати. Збільшення популярності IoT призведе до нового буму на ринку праці. Тому напрямок захисту рішення на основі IoT фактично є надиктованим нашим часом.

Протокол LoRaWAN

LoRaWAN – це відкритий протокол для мереж, які володіють високою ємністю (близько 1 мільйона пристроїв), низьким енергоспоживанням і великим радіусом дії (до 15 км на відкритій місцевості). Даний протокол забезпечує зв'язок між вузлами мережі і використовує особливі методи шифрування, що забезпечує надійність і безпеку системи [4].

Стандарт LoRaWAN на ринку мережевих додатків з’явився нещодавно, але вже є маса прикладів його застосування. На рис. 1 показано, як станція LoRa - Інтернет речей проводить збір даних з кінцевих вузлів. Ці вузли за допомогою шлюзів утворюють невидимі мости, вони з'єднуються з центральним сервером. кінцеві вузли належать абонентам, а центральний сервер і шлюзи контролює оператор.

Типова бездротова мережа LoRaWAN являє собою сукупність шлюзів (gateways), які пересилають повідомлення між кінцевими пристроями (end-devices) і центральним сервером (Network Server, NS), і характеризується «зоряної» топологією «star-of-stars». Відображення отриманих метрик відбувається на сервері візуалізації (Application Server, AS), з’єднання NS та AS відбувається за допомогою IP-з'єднання.

У мережі LoRaWAN передбачено використання трьох класів пристроїв. Вони використовуються для вирішення різних завдань в залежності від області застосування [5]:

двонаправлені кінцеві пристрої «класу А» (Bi-directional end-devices, Class A). Ці кінцеві пристрої застосовуються, коли потрібна мінімальна споживана потужність при передачі даних на сервер;

двонаправлені кінцеві пристрої «класу Б» (Bi-directional end-devices, Class B). Відмітна особливість від класу А – додаткове вікно прийому. Його пристрій відкривається за розкладом. Це означає що передача даних з сервера буде здійснюватися тільки тоді, коли кінцеве пристрій вийде на зв'язок. Складання розкладу для кінцевого пристрою здійснить синхронізацію по сигналу від шлюзу;

двонаправлені кінцеві пристрої «класу С» (Bi-directional end-devices, Class C). У цих пристроїв максимальне вікно прийому. вони призначені для отримання великого обсягу

даних і мають майже безперервне вікно прийому даних. Таким чином, 1 шлюз мережі обслуговує, та може керувати близько 5 тисяч кінцевих пристроїв.

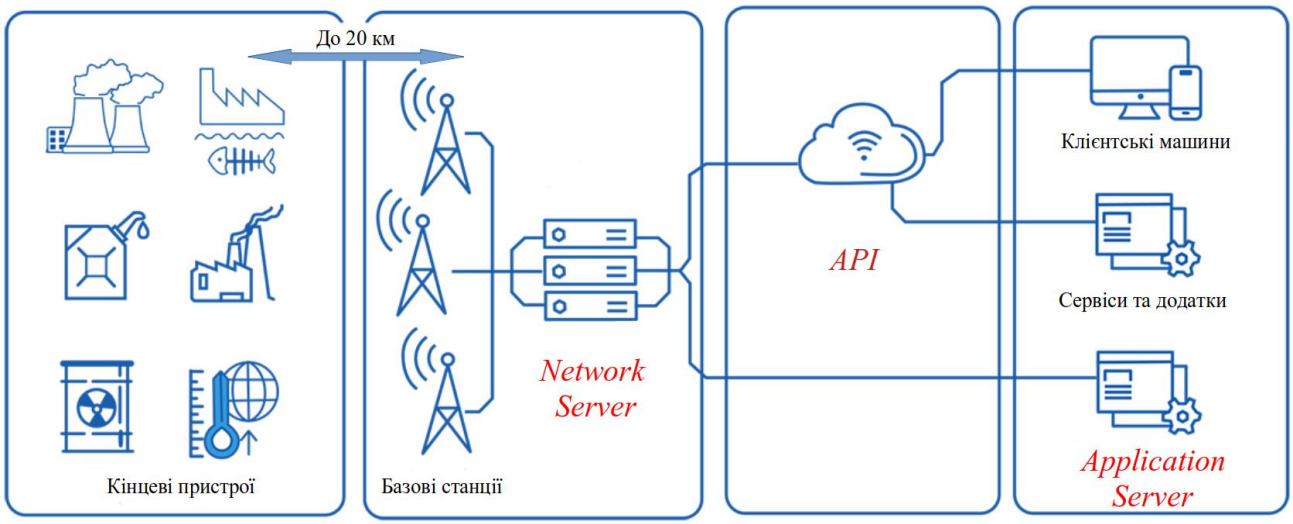

Рис. 1. Типова бездротова мережа LoRaWAN

Базова станція – типове поняття для багатьох радіосистем, включаючи мережі IoT. У мережі LoRaWAN базова станція (БС) виконує функції сполучення і взаємодії радіомережі з абонентським терміналом і концентрації навантаження з групи терміналів, тому в документації LoRa Alliance БС іменується шлюзом або концентратором. Сигнал від одного кінцевого пристрою або терміналу може прийматися декількома БС. Сукупність базових станцій оператора забезпечує радіопокриття мережі і прозору двосторонню передачу даних між кінцевими пристроями та сервером мережі. Базова станція оснащена приймально – передавальної антеною (секторної або всюди направленною), а також (опціонально) GPS / ГЛОНАСС – антеною для прецизійної синхронізації внутрішнього годинника і визначення точних координат приймально-передавальної антени [6].

Зв'язок шлюзів і центральним сервером відбувається як і між NS та AS, через стандартні IP-з'єднання а між шлюзами і кінцевими пристроями через бездротові з'єднання. Весь процес призначений для низько швидкісної бездротової передачі даних в неліцензійних діапазонах частот на великі відстані. Зв'язок є двосторонньої, але основний обсяг даних передається від кінцевих пристроїв до шлюзів.

Мережевий сервер (*NS*) – програмно-апаратний комплекс, який виконує наступні функції:

управління радіомережею. Мережевий сервер мережі LoRaWAN вибирає БС для передачі повідомлень в напрямку «вниз» (downlink), приймає рішення про необхідність зміни швидкості передачі даних для кожного терміналу, потужності передавача, контролює заряд батарей кінцевих пристроїв, шифрує дані і т.ін.;

контроль радіомережі включає моніторинг, збір статистики і аварійне інформування;

маршрутизація пакетів даних від кінцевих пристроїв або терміналів до відповідних серверів додатків. Кожен пакет даних, що відправляється абонентським терміналом, має в своєму складі унікальний ідентифікатор DevAddr, а на мережевому сервері зберігається запис про відповідність DevAddr і URL сервера додатків, якій призначена інформація від терміналу кінцевого пристрою. На підставі цієї відповідності мережевий сервер виконує маршрутизацію пакета до сервера додатків, де відбувається його подальша обробка додатком.

Сервер додатків, сервер візуалізації - платформа, яка виконує перший рівень шифрування / дешифрування і виробляє обробку даних, одержуваних від кінцевих пристроїв, терміналів і направляються до терміналів або кінцевих пристроїв. Крім роботи з даними, сервер додатків може управляти кінцевими пристроями з рівня додатки (наприклад,

переводити їх в режим роботи іншого класу, управляти опцією адаптивної передачі даних, мультикаст і т.ін.) [7].

Мета роботи: дослідження ефективних технологій захисту пристроїв IOT на базі протоколу LoRaWAN.

Забезпечення захисту даних в мережі LoRaWAN рівнем інфраструктури

Насамперед потрібно звернути увагу на те, яким чином можуть бути захищені кінцеві пристрої на етапі виготовлення а також на етапі під'єднання до мережі та подальшого обміну повідомленнями.

При виготовленні в абонентський пристрій заносяться наступні константи:

DevEUI (Device Identifier - унікальний ідентифікатор пристрою [64 біта]);

AppEUI (Application Identifier - унікальний ідентифікатор додатки [64 біта]). Починаючи з версії стандарту V1.1 називається JoinEUI - ідентифікатор Join-сервера;

AppKey (Application Key - унікальний кореневої ключ шифрування [128 біт]). Використовується в процесі обчислення сесійних ключів шифрування AppSKey і NwkSKey.

Активація пристрою (рис. 2) може здійснюватися як через радіоефір OTAA (рис. 3), так і оператором ABP (рис. 4). Під час процесу активації формуються наступні дані:

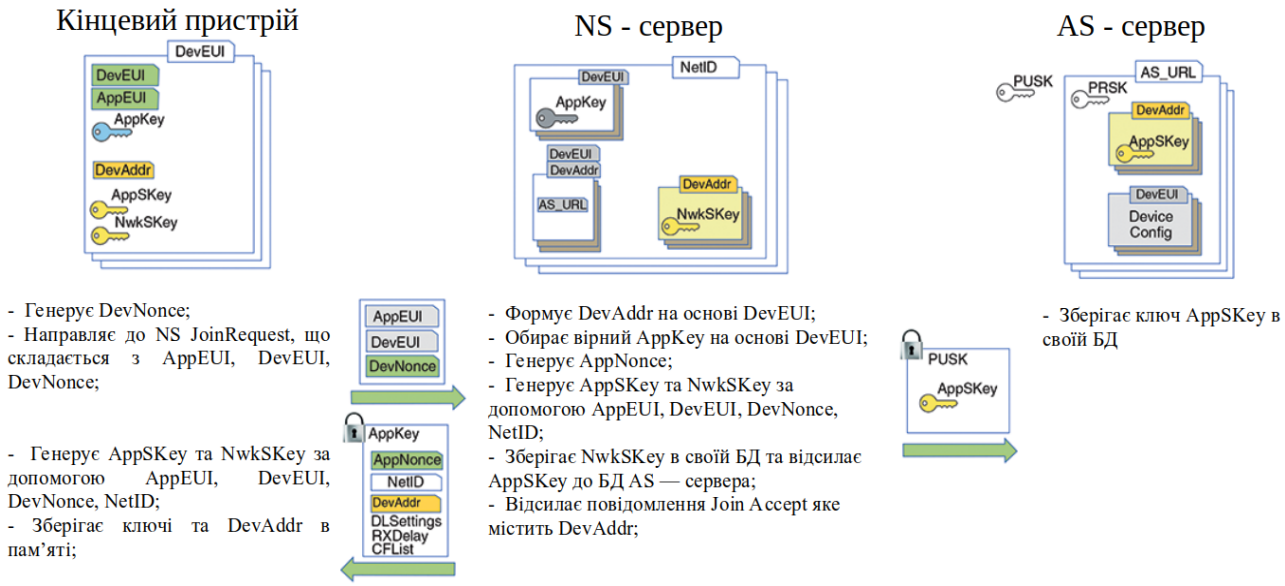

Рис. 2. Процедура активації кінцевого пристрою за допомогою радіоефіру (OTAA)

DevAddr (End-Device Address - локальна адреса пристрою в конкретній мережі [32 біта]). Складається з двох полів: NetID і NwkAddr. Чим коротше NetID (ідентифікатор мережі оператора, який присвоюється LoRa Alliance, мінімальний розмір - 6 біт), тим довше поле NwkAddr і тим більше різних пристроїв може бути зареєстровано в мережі (максимум на один NetID - 33,5 млн терміналів, кінцевих пристроїв);

NwkSKey (Network Session Key - мережевий сесійний ключ шифрування [128 біт]). Використовується для шифрування даних між терміналом і сервером, а також для обчислення поля MIC (Message Integrity Code) з метою перевірки цілісності даних при передачі їх по радіоефіру;

AppSKey (Application Session Key - сесійний ключ шифрування додатка [128 біт]). Служить для шифрування даних на рівні додатку (між абонентським терміналом і сервером додатка).

Сесійні ключі шифрування формуються незалежно на абонентському терміналі і на мережевий частини на підставі ідентифікаторів мережі (NetID) і пристрої (DevEUI), кореневого ключа безпеки AppKey, а також згенерованих унікальних для кожної сесії випадкових чисел DevNonce, JoinNonce. При активації терміналу оператором зміна сесійних

ключів шифрування без демонтажу пристрою неможлива, через що цей варіант активації використовувати не рекомендується [8].

DevAddr, NwkSKey і AppSKey зберігаються в пам'яті абонентського пристрою, DevAddr, NwkSKey - на мережевому сервері (NS), а AppSKey - на сервері візуалізації, додатків (AS).

В загальному випадку активація за допомогою OTAA приведена на рис. 3.

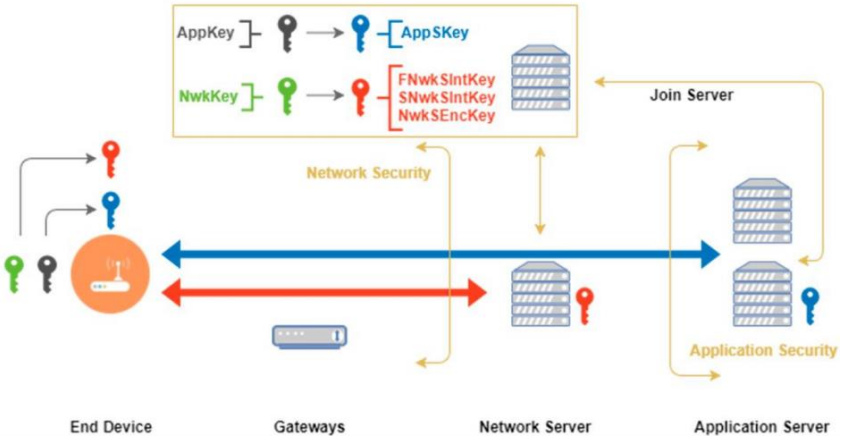

Рис. 3. Загальна схема активації пристрою за допомогою OTAA

У випадку активації за допомогою персоналізації (ABP) пристрою не потрібно DevEUI, AppEUI або AppKey. Замість цього ключі сеансу NwkSKey і AppSKey попередньо встановлені у вашому пристрої, і пристрій попередньо зареєстровано в мережі. Коли пристрій хоче встановити зв'язок, воно робить це, використовуючи ключі сеансу, без необхідності спочатку використовувати процедуру з'єднання. Загальна схема активації пристрою за допомогою ABP приведена на рис. 4.

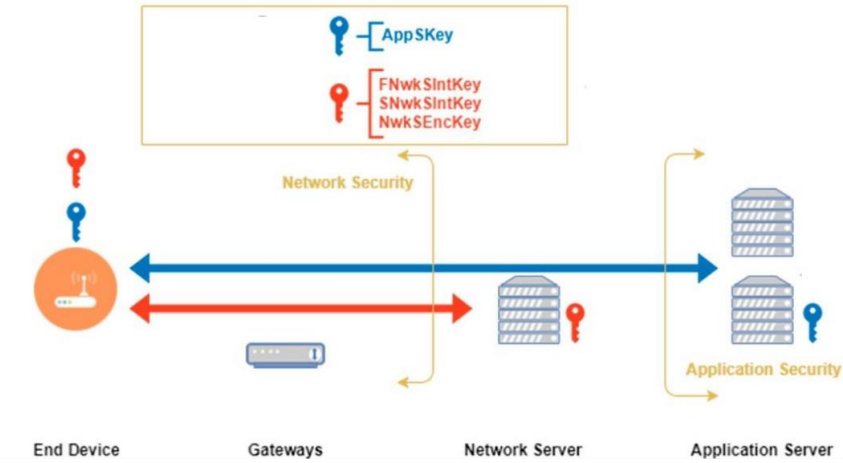

Рис. 4. Загальна схема активації пристрою за допомогою ABP

Шифрування повідомлень в мережі що працює за протоколом LoRaWAN

У мережі IoT LoRaWAN використовується багаторівнева система безпеки передачі даних (Рис. 5).

Перший рівень має AES – шифрування на рівні додатку (між кінцевим пристроєм і сервером додатків, візуалізації) за допомогою 128 — бітного змінного сесійного ключа Application Session Key (AppSKey). Цей ключ шифрування зберігається в абонентському терміналі і на сервері додатків і недоступний оператору зв'язку (доступ до AppSKey є тільки у клієнта — власника сервера додатків, візуалізації). Формування сесійного ключа AppSKey

відбувається паралельно в абонентському терміналі і на стороні мережі під час процедури активації кінцевого пристрою, через повітря (під час ефіру) AppSKey не передається [9].

Другий рівень передбачає AES – шифрування і перевірку цілісності повідомлень на мережевому рівні (між абонентським терміналом і сервером) за допомогою 128 — бітного змінного сесійного ключа Network Session Key (NwkSKey). Зазначений ключ шифрування також зберігається в абонентському терміналі і на мережевому сервері і недоступний клієнту (доступ до NwkSKey є тільки у оператора мережі - власника мережевого сервера). Формування сесійного ключа NwkSKey також відбувається паралельно в абонентському терміналі і на стороні мережі під час процедури активації терміналу, через ефір NwkSKey також не передається.

Третій рівень включає стандартні методи аутентифікації і шифрування інтернет-протоколу IPsec, TLS і т.ін. При передачі даних по транспортній мережі між вузлами мережі (базова станція, мережевий сервер, join-сервер, сервер додатків).

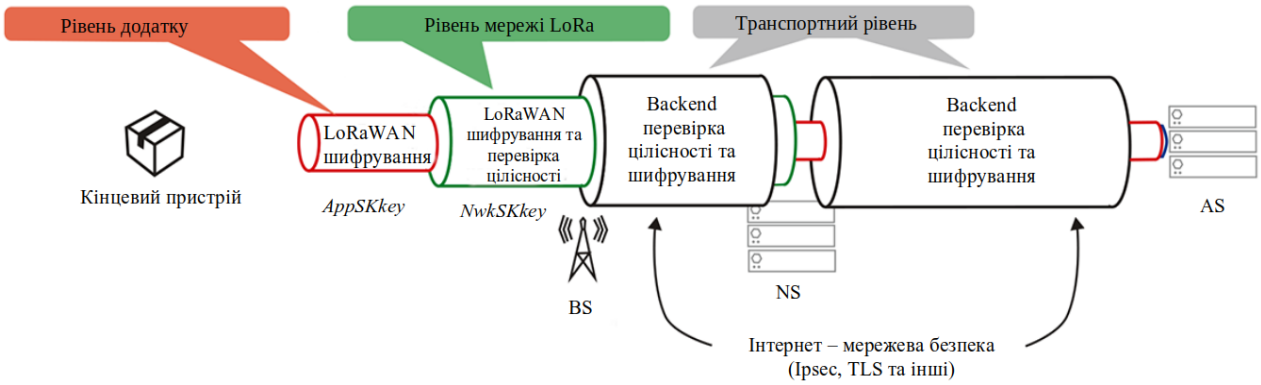

Рис. 5. Загальна схема безпеки даних в мережі LoRaWAN

За командою додатки або мережевого сервера в будь-який момент можливий перехід на нову сесію з генерацією нового комплекту ключів шифрування, що робить марними старі ключі шифрування. Також є можливість встановити періодичну генерацію нового комплекту ключів NwkSKey і AppSKey. У версії стандарту LoRaWAN V1.0.x формування сесійних ключів на стороні мережі проводиться на мережевому сервері (NS), однак у версії V1.1 для цих цілей використовується виділений сервер - так званий join-сервер. Join-сервер може бути додатково захищений окремим апаратним модулем безпеки HSM (Hardware Security Module).

В цьому випадку для безпечної передачі згенерованих сесійних ключів між серверами, а також для зберігання їх на мережевому сервері і сервері додатків впроваджуються додаткові ключі: AS_Key для ключа AppSKey і LRC_K для ключа NwkSKey. На абонентському пристрої ключі шифрування за потреби можуть захищатися спеціальним апаратним елементом безпеки Secure Element, що виключить їх компрометацію в разі фізичного впливу на термінал.

Впровадження апаратних засобів захисту в мережі і на терміналі робить марними спроби перехоплення сесійних ключів при передачі їх між серверами і спроби зламу мережевих серверів або абонентських пристроїв з метою отримання сесійних ключів. Розглянуті заходи також створюють умови для захищеного роумінгу даних - безпечну авторизацію датчиків в гостьовій мережі і захищену передачу даних домашньому сервера додатків з гостьової мережі. З метою додаткового захисту процесу генерації сесійних ключів Join — сервер може бути розміщений на території клієнта або виробника пристроїв. У цьому випадку навіть співробітники оператора не зможуть отримати доступ до сесійних і кореневих ключів шифрування [10].

Забезпечення безпеки даних в мережі LoRaWAN від розповсюджених загроз.

Перехоплення призначених для користувача даних

Найпростіша загроза - звичайне перехоплення даних.

Принцип реалізації атаки:

Через те, що радіохвилі поширюються неконтрольовано, будь хто може взяти приймач, налаштований на потрібний діапазон і тип модуляції, і слухати все, що передається від кінцевого пристрою до базової станції, шлюзу.

Спосіб захисту - шифрування даних.

Механізм реалізації:

У LoRaWAN призначені для користувача дані шифруються по алгоритму AES-128 з ключем довжиною, відповідно, 128 біт (16 байт).

Повторне відправлення даних

У LoRaWAN до кожного пакету додається лічильник. Якщо на сервер мережі приходить пакет з лічильником, рівним або менше попереднього, то цей пакет просто відкидається. Після переповнення від пристрою прийде пакет з номером 0, який, очевидно, буде менше будь-якого іншого номера, але при цьому сервер мережі повинен його сприйняти правильно і почати відлік пакетів з нуля. Крім того, пристрій може обнулити лічильник перезавантаженням.

Це досягається в одним з наступних способів:

перед відсиланням пакету пристрій повинен пройти процедуру реєстрації в мережі (Join);

сервер допускає прихід чергового пакета з номером 0, при цьому відлік починається заново.

У LoRaWAN використовуються обидві схеми в залежності від способу активації пристрою - OTAA або ABP.

Для OTAA використовується перший варіант, при цьому пристрою видаються нові ключі шифрування.

Для ABP, використовується другий варіант - втім, якщо термін переповнення лічильника помітно перевищує розрахунковий термін служби пристрою, він може бути відключений. На випадок випадкового перезавантаження, після відправлення кожного пакета таке кінцеве пристрій зберігає значення лічильника в незалежну пам'ять.

Друга схема, звичайно, менш безпечна, але на практиці допустима - зловмиснику в ній треба записати не будь-який пакет, а конкретно нульовий.

Підробка лічильника

Якщо лічильник підробити, можна покласти його в зашифровану частину пакета, але тоді реальний обсяг призначених для користувача даних зменшиться на два байта. Можна шифрувати не тільки призначені для користувача дані, але тоді, по-перше, доведеться підлаштуватися під 16 - байтний розмір блоку, а по - друге, збільшиться навантаження на сервер мережі, якому для будь-яких дій над пакетом доведеться його спочатку розшифровувати (в схемі ж, коли шифруються тільки призначені для користувача дані, якщо пакет за формальними ознаками ігнорується, то розшифровувати не треба нічого).

При цьому очевидно, що нам неважливо, знає зловмисник номер пакета чи ні - в схемі з перереєстрацією в мережі (OTAA) це знання йому взагалі нічим не допоможе, а в ABP він буде дуже довго чекати наступного приходу пакету з номером N-1. Тому цілком достатньо не дати йому цей номер змінити.

Для цього весь пакет в LoRaWAN підписується криптографічного підписом AES – CMAC, цей підпис в стандарті називається MIC, Message Integrity Code. По ньому перевіряється, що весь пакет, включаючи всі заголовки і дані, дійшов до сервера в незмінному вигляді.

Тобто, прийнявши черговий пакет, ми можемо швидко подивитися в його лічильник, і якщо він наш і коректний – тоді вже перевірити підпис, і якщо підпис теж коректний – розшифровувати дані і передавати їх далі.

Відстеження незмінних даних

Очевидно, що шифрування даних - процедура оборотна, їх можна розшифрувати, а відтак, одні і ті ж дані, зашифровані з одним і тим же ключем, завжди виглядають однаково.

Отримуючи пакети від кінцевого пристрою, у якого не змінюються дані, є можливість, не розшифровуючи пакет, зрозуміти, що вони не змінюються.

Протидія таким проявам не складна — повинні змінюватися або дані, або ключ.

Зловмисник дізнався ключ шифрування

Ц випадку, якщо всі пристрої мають один і той же ключ шифрування, власник будь — якого з них може слухати трафік будь-якого іншого пристрою. У LoRaWAN реалізовані дві схеми використання ключів, індивідуальних для кожного пристрою:

Over The Air Activation, OTAA - ключі генеруються сервером мережі кожен раз, коли пристрій в ній реєструється;

Activation By Personalization - ключі задані виробником і зберігаються на пристрої, ніколи не змінюючись.

Всього ключів використовується як мінімум два - AppSKey, яким шифруються призначені для користувача дані, і NwkSKey, яким підписується повідомлення.

Очевидно, схема з OTAA більш зручна і надійна - ключі можуть змінюватися з тією частотою, з якою хочеться, вони гарантовано унікальні і не відомі нікому, крім мережевого сервера. У ABP ключі не змінюються ніколи, унікальність залежить від сумлінності виробника пристрою (наприклад, ми генеруємо ці ключі з унікального ID мікроконтролера, тому ймовірність їх збігу на двох пристроях незначна), і їх треба десь зберігати в явному вигляді, щоб при підключенні пристрою до мережі прописати їх на сервері.

Перехоплення згенерованих ключів

Очевидно, якщо при реєстрації в мережі кожен раз генеруються нові ключі, то їх треба синхронізувати між пристроєм і сервером, а від так, зловмисник може перехопити їх. Тому у пристроїв LoRaWAN використовується третій ключ - AppKey, зашитий в пристрій і використовуваний в один момент — при реєстрації в мережі. З його допомогою підписується обмін сесійними ключами між пристроєм і сервером. В ідеалі AppKey повинен бути унікальний для кожного пристрою, але в багатьох випадках допускається використання одного і того ж AppKey - так як потрібен він всього один раз, що може бути визнано допустимим. AppKey перед підключенням пристрою заноситься в налаштування на сервері мережі.

Отже, пристрій формує запит на реєстрацію (JoinRequest), не шифруючи його, але підписуючи його ключем AppKey. Сервер мережі, отримавши цей пакет і перевіривши адреса відправника, підпис, відповідає пакетом JoinAccept, в якому передає налаштування мережі і підтверджує реєстрацію.

Генерація ключів AppSKey і NwkSKey. Це - результат шифрування AES-128 з ключем AppKey комбінації з переданого сервером у відповіді випадкового числа AppNonce, номера ключа (1 або 2), ID мережі і ще одного випадкового числа DevNonce:

NwkSKey = aes128_encrypt (AppKey, 0x01 | AppNonce | NetID | DevNonce)

AppSKey = aes128_encrypt (AppKey, 0x02 | AppNonce | NetID | DevNonce)

Так як і пристрій, і сервер після обміну пакетами реєстрації знають всі ці параметри, то вони згенерують однакові ключі. Таким чином, ні в який момент ніякі ключі по радіо передаватися самі по собі не будуть, але при цьому пристрій, і сервер отримають унікальні ключі шифрування і підпису пакетів.

Перехоплення потоку даних на себе

У разі, відсилання на сервер перехопленого раніше пакету JoinRequest без його корегування або зміни, сервер відповість на нього пакетом JoinAccept, згенерувавши нові ключі. Після цього пристрій що фактично атакується, просто перестане спілкуватися з сервером, через те, що кінцевий пристрій JoinRequest не ініціював і ніяких підстав оновлювати ключі не бачить. Тобто, та ж атака повтором - але вже на процедуру реєстрації в мережі.

Зловмисник не зможе підробити дані, так як для цього потрібно знати ключі, а для їх отримання потрібно знати AppKey, який він не знає. Але вибити пристрій з мережі - зможе. Щоб уникнути цього, при реєстрації пристрій передає на сервер випадкове число DevNonce.

Крім того, що на його базі генеруються ключі, він служить ще одній меті - сервер LoRaWAN зберігає архів DevNonce. Якщо від пристрою прийшов повторний запит реєстрації з уже використаним DevNonce, сервер його просто проігнорує. У свою чергу, пристрій повинен кожного разу при входженні генерувати новий DevNonce.

Висновок.

Існує велика кількість технологій, процесів а також підходів у напрямку захисту пристроїв IOT, що можуть бути задіяні в залежності від етапу життя пристрою або його розробки, невиконання яких вірогідніше за все призведе до компрометації, виводу з ладу, підроблення або знищення пристроїв IOT. Практичне значення дослідження полягає у тому, що в роботі зазначені деякі з проблем, які можуть виникнути на етапах життєвого циклу пристрою, а також акцентована увага на необхідності імплементації заходів забезпечення захисту та безпеки на ранніх етапах, які дозволили б суттєво скоротити коло загроз та вірогідність компрометації або будь якого неправомірного зовнішнього впливу. Результати проведеного дослідження можуть бути використані при описі, та визначенні підходів до протидії проблемам, пов'язаним з захистом та забезпеченням безпеки пристроїв IOT на різних етапах їх життєвого циклу.

Перелік посилань

1. Secure integration of IoT and Cloud Computing/ Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta 2016p.
2. InternetofThings:AsurveyonthesecurityofIoTframeworks/ MahmoudAmmara,GiovanniRussellob,BrunoCrispo 2017p.
3. The Web of Things: interconnecting devices with high usability and performance/ Simon Duquennoy, Jean-Jacques Vandewalle. 2019p.
4. Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing/ Angelo Furfaro ; Alfredo Garro ; Andrea Tundis 2014p.
5. Buchheit, Marcellus, Mark Hermeling, Frederick Hirsch, Bob Martin, and Simon Rix. 2020. "Software Trustworthiness Best Practices." An Industrial Internet Consortium White Paper. https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf .
6. Filkins, Barbara, and Doug Wylie. 2019. "SANS 2019 State of OT/ICS Cybersecurity Survey." https://radiflow.com/wp-content/uploads/2019/06/Survey_ICS-2019_Radiflow.pdf
7. Cascella, Roberto. 2019. "Challenges of Cybersecurity Certification and Supply Chain Management." ECSO - EUNITY Workshop.
8. Boyens, Jon M. 2020. "Key Practices in Cyber Supply Chain Risk Management: Observations from Industry." Preprint. https://doi.org/10.6028/NIST.IR.8276-draft
9. Boyens, Jon M., Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. 2020. "Case Studies in Cyber Supply Chain Risk Management: Summary of Findings and Recommendations." NIST CSWP 02042020-1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.02042020-1
10. Fagan, Michael, Katerina N Megas, Karen Scarfone, and Matthew Smith. 2020. "Foundational Cybersecurity Activities for IoT Device Manufacturers." NIST IR 8259. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8259.
11. Маслова Ю.Ю. Кушнір І.М. Інформаційна безпека і людський фактор // Сучасний захист інформації, № 4(44), 2020. – С. 41–45.
12. Коростель В.С., Кожухівський А.Д., Луценко І.М., Кітура О.В., Маслова Ю.Ю. Прогнозування часу здійснення кібератаки на основі результатів аналізу нестаціонарних процесів // Сучасний захист інформації, № 3(43), 2020. – С. 49–53.
13. Data Leak: Unsecured Server Exposed Bing Mobile App Data [Електронний ресурс] // -режим доступу: https://www.wizcase.com/blog/bing-leak-research/
14. Report: Popular Marketing Tool Exposes Dating Site Users in Massive Data Leak [Електронний ресурс] // -режим доступу: https://www.vpnmentor.com/blog/report-mailfire-leak/
15. The human factor is key to good security [Електронний ресурс] // -режим доступу: https://www.computerweekly.com/opinion/The-human-factor-is-key-to-good-security

Надійшла: 10.10.2021 Рецензент: д.т.н., професор Савченко В.А.