КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.11.124135
УДК 004.77

Черненко Роман Миколайович
аспірант кафедри Інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-1439-961X
r.chernenko.asp@kubg.edu.ua

Рябчун Олена Петрівна
аспірант кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-4400-0112
Santalen@bigmir.net

Ворохоб Максим Віталійович
Аспірант кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0001-5160-7134
m.vorokhob.asp@kubg.edu.ua

Аносов Андрій Олександрович
кандидат військових наук, доцент,
доцент кафедри Інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-2973-6033
a.anosov@kubg.edu.ua

Козачок Валерій Анатолійович
кандидат технічних наук, доцент,
доцент кафедри Інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ ЗА РАХУНОК ШИФРУВАННЯ ДАНИХ НА ПРИСТРОЯХ З ОБМЕЖЕНИМИ ОБЧИСЛЮВАЛЬНИМИ РЕСУРСАМИ

Анотація. Оскільки пристрої мережі Інтернету речей, працюють з даними що можуть в тому числі мати конфіденційний або секретний характер, ці дані повинні бути захищені. Через особливості платформ та реалізацію таких систем, а саме: по-перше використання пристроїв з обмеженими обчислювальними характеристиками, що унеможливлює використання традиційних засобів захисту інформації, та протоколів передачі даних, по-друге нестандартне розташування пристроїв, що не дозволяє вчасно реагувати на загрози, оновлювати системи, та забезпечувати їх достатньою кількістю обчислювальних ресурсів через неможливість прокладання електричних ліній, по-третє відсутність стандартів для впровадження цих пристроїв до існуючої інфраструктури, існують серйозні загрози в забезпеченні конфіденційності, цілісності та доступності інформації. У статті розглядається модель системи IoT, стандарту oneM2M представлена Європейським інститутом стандартів зв'язку. Пристрої IoT розроблені з необхідними можливостями підключення до мережі, але часто не реалізують надійну мережеву безпеку. Мережева безпека є критичним фактором при розгортанні пристроїв IoT. Ситуацію ускладнює те що IoT багато в чому складається з обмежених пристроїв. Обмежений пристрій зазвичай має дуже обмежений цикл потужності, пам'яті та обробки. Пристрої IoT особливо вразливі для суб'єктів загрози, оскільки багато пристроїв IoT, які зараз випускаються, не підтримують шифрування. Для аналізу було відібрано декілька відомих алгоритмів шифрування: RSA, шифр Вернама, схема Эль-

Гамаля. Проаналізувавши наведені алгоритми, був розроблений прототип системи IoT з використанням обмежених пристроїв, що забезпечує абсолютну криптографічну стійкість. Прототип складається з шлюзу в ролі якого виступає мікрокомп'ютер Raspberry pi 3 B+, обмеженого пристрою Arduino Nano з підключеним датчиком та програмною реалізацією вище згаданого шифру Вернама з усіма поставленими задачами.

Ключові слова: Інтернет речей; IoT; мережева безпека; пристрої з обмеженими обчислювальними ресурсами; алгоритми шифрування; шифр Вернама.

ВСТУП

Інтернет речей (IoT) - це система взаємопов'язаних обчислювальних пристроїв, механічних і цифрових машин, предметів, яким надаються унікальні ідентифікатори (UID) та можливість передавати дані по мережі без необхідності взаємодії людини з комп'ютером.

Оскільки пристрої мережі Інтернету речей, працюють з даними що можуть в тому числі мати конфіденційний або секретний характер, ці дані повинні бути захищені. Через особливості платформ та реалізацію таких систем, а саме: по-перше використання пристроїв з обмеженими обчислювальними характеристиками, що унеможливлює використання традиційних засобів захисту інформації, та протоколів передачі даних, по-друге нестандартне розташування пристроїв, що не дозволяє вчасно реагувати на загрози, оновлювати системи, та забезпечувати їх достатньою кількістю обчислювальних ресурсів через неможливість прокладання електричних ліній, по-третє відсутність стандартів для впровадження цих пристроїв до існуючої інфраструктури, існують серйозні загрози в забезпеченні конфіденційності, цілісності та доступності інформації. Для вирішення проблем в безпеці пристроїв мережі IoT, проводяться дослідження та розробляються методики та алгоритми захисту цих пристроїв. Зокрема Національним інститутом стандартів та технологій США було ініційовано проект у 2015 році з назвою Lightweight Cryptography [1], метою якого є розробка алгоритмів шифрування які могли б працювати на пристроях з обмеженими обчислювальними ресурсами, але станом на сьогоднішній день, конкретних результатів досягнуто не було.

Постановка проблеми. Пристрої IoT розроблені з необхідними можливостями підключення до мережі, але часто не реалізують надійну мережеву безпеку. Мережева безпека є критичним фактором при розгортанні пристроїв IoT. Виникає необхідність розробки методів для забезпечення достовірності, цілісності та безпеки даних, на шляху від датчика до колектора та підключення до пристрою.

Відповідно до списку вразливостей складеного Відкритим проектом з безпеки веб-застосунків OWASP [2] пристрої IoT мають вразливості на трьох рівнях функціонування:

- апаратному;
- комунікаційному;
- програмному.

Ситуацію ускладнює те що IoT багато в чому складається з «обмежених» пристроїв. Обмежений пристрій зазвичай має дуже обмежений цикл потужності, пам'яті та обробки. У RFC 7228 спеціальна група Internet Engineering (IETF) визначила класи для обмежених пристроїв [3], як показано в таблиці 1.

ISSN 2663 - 4023

Таблиця 1

Класифікація обмежених пристроїв

Назва	Розмір пам'яті (RAM)	Розмір коду (флеш-пам'ять)
Class 0, C0	< 10 Кілобайт	< 100 Кілобайт
Class 1, C1	~ 10 Кілобайт	~ 100 Кілобайт
Class 2, C2	~ 50 Кілобайт	~ 250 Кілобайт

Можливості комунікації також обмежені. Для зв'язку цих пристроїв, шифрування не реалізується через обмежену потужність обробки пристроїв, особливо пристроїв класу 0, хоч в таблиці не вказані обчислювальні ресурси процесору, було прийнято рішення вважати їх пропорційно малими відносно використання пам'яті.

Якщо частина проблем може бути вирішена шлюзом який зазвичай має достатньо обчислювальних ресурсів для підтримки шифрування та сучасних інтерфейсів обміну інформацією, то проблема з шифруванням даних на всіх етапах життєвого циклу залишається не вирішеною. Шифрування застосовує алгоритм до даних, який зробить його нечитабельним для тих, хто не має права бачити інформацію. Шифрування повинно бути оборотним для того, щоб зашифровані передані дані зробили читабельними приймаючим пристроєм або процесом.

Пристрої IoT особливо вразливі для суб'єктів загрози, оскільки багато пристроїв IoT, які зараз випускаються, не підтримують шифрування. Але ситуація виглядає ще гірше оскільки, пристрої IoT зазвичай вимагають певної форми бездротового зв'язку, яка спрощує перехоплення передач даних, якщо немає шифрування. Через характер та розмір пристроїв IoT вони, як правило, мають обмежений обсяг ресурсів. Наслідком цього є те, що більшість пристроїв IoT не мають потужності обробки або ресурсів, необхідних для більш надійних алгоритмів шифрування. Оскільки шифрування все ще є необхідним компонентом для їх функціональності, можна використовувати легкі алгоритми шифрування. Ці алгоритми можуть бути реалізовані в програмному забезпеченні або через інтегральну схему (IC) в апаратному забезпеченні. Кожен із цих методів збільшує вартість для виробника IoT, оскільки обидва методи потребують додаткових ресурсів. Наразі не існує стандарту, і багато пристроїв IoT взагалі не підтримують шифрування.

Національний інститут стандартів і технологій США нещодавно розпочав «ініціативу легкої криптографії». Мета - розробити стандартний криптографічний алгоритм, який можна використовувати в невеликих пристроях IoT з мінімальними ресурсами, щоб захистити ці пристрої та їх дані. Станом на листопад 2019 року ця ініціатива ще перебуває на стадії розвитку.

Проаналізувавши список вразливостей авторами було визначено, що відсутність шифрування при передачі інформації між пристроями з обмеженими обчислювальними ресурсами є однією найсерйозніших вразливостей, перелічених OWASP.

Отже необхідно проаналізувати існуючі методи та засоби для забезпечення захисту цих пристроїв, та розробити алгоритми шифрування даних в пристроях Інтернету речей для забезпечення конфіденційності інформації під час її життєвого циклу.

Аналіз останніх досліджень і публікацій. Перед будь-яким пристроєм, що передає дані, постає основна проблема – захист каналу зв'язку між пристроями від

зловмисників. Оскільки кількість пристроїв інтернету речей невпинно зростає, з такою ж швидкістю підвищується рівень небезпеки. Проблемою пристроїв інтернету речей є те, що апаратні засоби, на яких вони побудовані, не є обчислювально потужними, а також не мають постійного стабільного зв'язку з інтернетом, а також достатньо складного програмного забезпечення, щоб отримати доступ до центрів авторизації. Для розв'язання цієї задачі було вирішено взяти за основу декілька алгоритмів – протокол обміну ключами Діффі–Хельмана, алгоритм DSA для створення цифрового підпису даних, необхідних для вищезгаданого протоколу, а також алгоритм AES з різними режимами шифрування для автентифікації та симетричного шифрування даних. Вибір вищезгаданих протоколів пояснюється взаємною компенсацією проблемних місць у протоколах. Наприклад, AES потребує ключ шифрування, однаковий для двох сторін, адже використовується як для зашифровування даних, так і навпаки. Цю проблему вирішує протокол Діффі–Хельмана, проте кожна зі сторін повинна впевнитись у тому, що вона створює спільний ключ із кінцевим користувачем, а не зловмисником, що діє як посередник. Цю проблему вирішує алгоритм DSA [4].

Оскільки Інтернет речей включає в себе такі пристрої, що постійно збирають і обробляють інформацію про оточуюче середовище, то вони є потенційно небезпечними для кінцевого користувача. Зважаючи на зростання рівня кіберзлочинності особливу увагу слід приділяти саме таким пристроям, адже не тільки втрата даних є основною проблемою. Можливе також використання обчислювальних ресурсів систем у проектуванні різноманітних кібератак. Недоліками даних систем є потреба у сучасних датчиках, контролерах, методах та способах передачі інформації тощо. Тому впровадження пристроїв IoT та вирішення найбільш поширених задач і проблем пов'язаних із ними є досить актуальним напрямом досліджень. Доцільним у системах Інтернету речей є наскрізне шифрування. При використанні такого методу ключі шифрування є відомими тільки пристроям-учасникам однієї системи. У такому випадку, інформація може бути розшифрована тільки кінцевими пристроями і не буде доступна у відкритому вигляді третім сторонам (сторонні сервери, постачальник Інтернет-послуг тощо) [5].

Безпека IoT стає головним завданням для організацій, оскільки без міцної архітектури безпеки великі обсяги даних, що надходять через мережі і зберігаються в хмарах, можуть стати легкою здобиччю для хакерів. Щоб зменшити ризик кібератак та злому, розробники повинні підтримувати конфіденційність даних, цілісність і доступність у всій IT-інфраструктурі всіма доступними їм способами, зважаючи на ресурсні обмеження пристроїв IoT. У зв'язку з обмеженими ресурсами для забезпечення процесу шифрування на якісному рівні, в IoT почали імплементувати алгоритми LW-криптографії. Як один із алгоритмів було обрано та реалізовано XTEA на мові JavaScript [6].

Для забезпечення належного рівня безпеки інфраструктури IoT необхідна комплексна стратегія захисту. Вона забезпечує захист даних у хмарі, захист цілісності даних під час передачі через Інтернет, а також безпечний зв'язок між пристроями. Мінімальні накладні витрати, наявність класів обслуговування та ієрархічна структура тем є незаперечною перевагою протоколу MQTT, про що свідчить велика різноманітність як програмного забезпечення клієнта, так і сервера, включаючи програмне забезпечення з відкритим кодом. Таким чином, спостерігається зрушення парадигми від маршрутизації на транспортному рівні до маршрутизації на рівні програми [7].

Мета статті. Мета статті полягає у підвищенні рівня захищеності систем мережі Інтернету речей за рахунок оптимального використання засобів та методів захисту даних при їх передачі пристроями з обмеженими обчислювальними характеристиками.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У статті розглядається модель системи IoT, стандарту oneM2M представлена Європейським інститутом стандартів зв'язку (ETSI) [8], яка є репрезентативною системою IoT від кінця до кінця (рис. 1). Необхідно зауважити, що вона характеризується як система «машина до машини» (M2M).

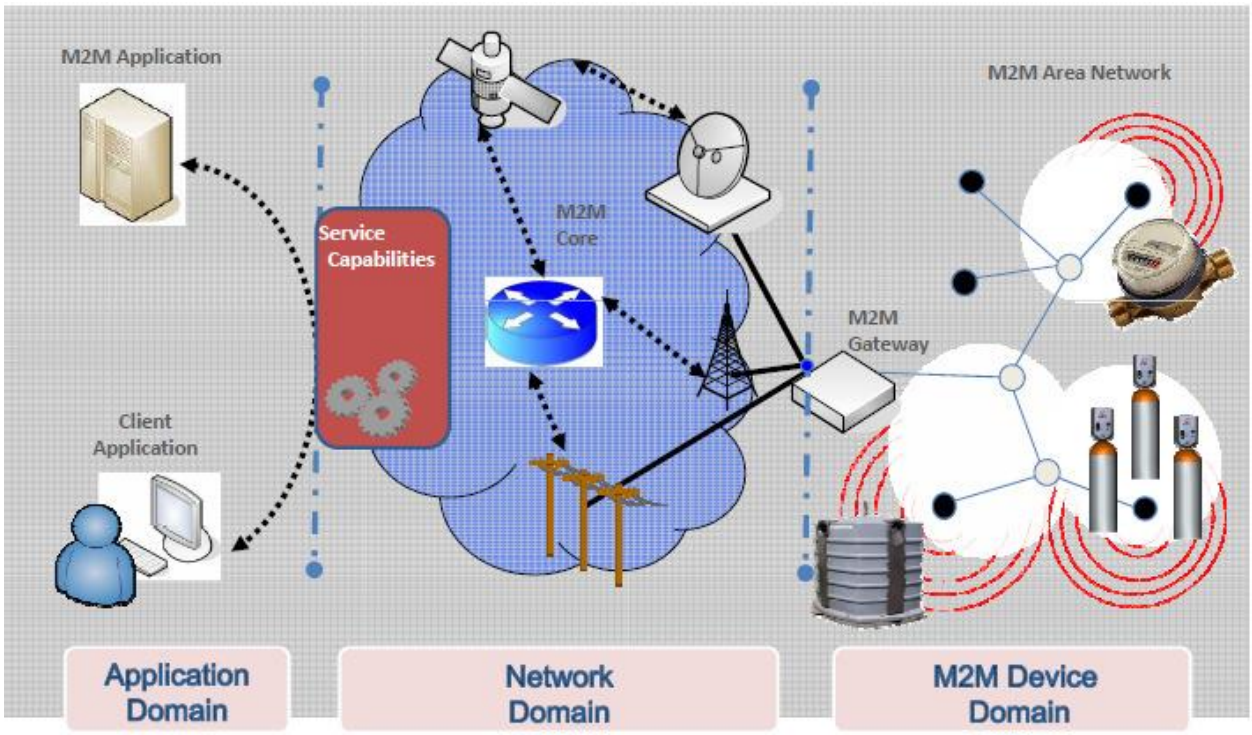

Рис. 1. Модель системи IoT стандарту oneM2M

Багато вузлів датчиків IoT обмежені ресурсами, потужністю та обробкою. Це означає, що канали зв'язку повинні реалізовуватись між пристроями малої потужності та шлюзом. Шлюз переводить трафік бездротової мережі давачів (WSN) в трафік протоколу IP, який може подорожувати в традиційних мережах передачі даних.

Деякі WSN можуть складатися з сотень, а то й тисяч, сенсорних вузлів. Ці вузли можуть використовувати лише заряд акумулятора і дуже обмежену кількість ресурсів для обробки. Через обмеження живлення, ці вузли можуть використовувати лише радіоприймачі дуже малої дальності. У цьому випадку використовуються протоколи, які дозволяють датчикам відправляти дані від вузла до вузла поки вони не дійдуть до шлюзу.

Для проведення дослідження у статті використовувались методи криптоаналізу, а саме атака на основі шифротексту, а також метод порівняння.

ISSN 2663 - 4023

Аналіз сучасних алгоритмів шифрування даних

Для аналізу було відібрано декілька відомих алгоритмів шифрування:

- RSA;
- шифр Вернама;
- схема Эль-Гамаля.

Алгоритм шифрування RSA - криптографічний алгоритм з відкритим ключем, що базується на обчислювальній складності задачі факторизації великих цілих чисел. RSA став першим алгоритмом такого типу, придатним і для шифрування, і для цифрового підпису. Алгоритм застосовується до великої кількості криптографічних застосунків. Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів.

Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий (public) і секретний (private), разом відкритий і відповідний йому секретний ключі утворюють пари ключів (keypair). Відкритий ключ не потрібно зберігати в таємниці, він використовується для шифрування даних. Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним секретним ключем. Для того, щоб відправити секретне повідомлення, потрібно спочатку передати відкритий ключ однієї сторони (n, e) іншій стороні через надійний, але не обов'язково секретний маршрут. Секретний ключ d ніколи не розповсюджується.

RSA є односторонньою перестановкою, тобто для будь-якого дієвого алгоритму A ймовірність $\Pr[A(n,e,c) = c^{1/e}$ дуже мала, що означає неможливість обернення RSA без секретної інформації — d.

RSA алгоритм є дуже надійним, але для його роботи необхідно робити велику кількість обчислень з числами так званої довгої алгебри, оскільки число n повинно бути більше 1024 біт. Це унеможливлює використання його на обмежених пристроях.

Схема Ель-Гамаля — криптосистема з відкритим ключем, яку засновано на труднощі обчислення дискретних логарифмів в кінцевому полі. Криптосистема включає в себе алгоритм шифрування і алгоритм цифрового підпису. Нині криптосистеми з відкритим ключем вважаються найперспективнішими. До них належить і схема Ель-Гамаля, криптостійкість якої засновано на обчислювальній складності проблеми дискретного логарифмування, де за відомими p, g та y потрібно обчислити x, що задовольняє рівнянню: $y = g^x (mod\ p)$.

Через те, що в схему Ель-Гамаля вводиться випадкова величина k, шифр Ель-Гамаля можна назвати шифром багатозначної заміни. Через випадковість вибору числа k таку схему ще називають схемою імовірнісного шифрування. Імовірнісний характер шифрування — це перевага для схеми Ель-Гамаля, тому що у схем імовірнісного шифрування спостерігається більша стійкість у порівнянні зі схемами з певним процесом шифрування. Вадою схеми шифрування Ель-Гамаля можна назвати подвоєння довжини зашифрованого тексту в порівнянні з початковим текстом. Для схеми імовірнісного шифрування саме повідомлення M і ключ не визначають шифротекст однозначно. У схемі Ель-Гамаля необхідно використовувати різні значення випадкової величини k для шифрування різних повідомлень M і M'. Якщо використовувати однакові k, то для відповідних шифротекстів (a, b) і $(a', b')\}$ виконується співвідношення $b(b') = M(M')^{-1}$. З цього виразу можна легко обчислити M', якщо відоме M. За однакової довжини ключа криптостійкість дорівнює RSA, тобто $2{,}7 * 10^{28}$ для ключа завдовжки 1300 біт. Проаналізувавши схему Ель-Гамаля можна

ISSN 2663 - 4023

зробити висновки що вона не підходить для реалізації в обмежених пристроях, через складнощі обчислень при шифруванні, збільшення розміру зашифрованого повідомлення в два рази порівняно з оригінальним повідомленням та необхідністю передачі сесійного ключа для шифрування.

Шифр Вернама - система симетричного шифрування. Шифр є різновидом криптосистеми одноразових блокнотів. У ньому використовується булева функція «Виключна диз'юнкція» відома як операція XOR. Шифр Вернама є прикладом системи з абсолютною криптографічною стійкістю. При цьому він вважається однією з найпростіших криптосистем.

Для отримання шифротекста відкритий текст об'єднується операцією «виключне АБО» з секретним ключем. Так, наприклад, при застосуванні ключа (11101) на букву «А» (11000) отримуємо зашифроване повідомлення (00101): $11000 \oplus 11101 = 00101$. Знаючи, що для прийнятого повідомлення маємо ключ (11101), легко отримати вихідне повідомлення тієї ж операцією: $00101 \oplus 11101 = 11000$. Для абсолютної криптографічної стійкості ключ повинен володіти трьома критично важливими властивостями:

- мати випадковий рівномірний розподіл: $P_k(k) = 1 / 2^N$ де k - ключ, а N - кількість бінарних символів в ключі;
- збігатися за розміром з заданим відкритим текстом;
- застосовуватися тільки один раз.

Також добре відомий так званий шифр Вернама по модулю m, в якому знаки відкритого тексту, шифрованого тексту і ключа приймають значення з кільця відрахувань Z_m. Шифр є узагальненням оригінального шифру Вернама, де m=2.

Наприклад, кодування шифром Вернама по модулю

$$m = 26\ (A = 0, B = 1, \ldots, Z = 25).$$

Ключ: EVTIQWXQVVOPMCXREPYZ

Відкритий текст: ALLSWELLTHATENDSWELL

Шифротекст: EGEAMAIBOCOIQPAJATJK

Без знання ключа таке повідомлення не піддається аналізу. Навіть якби можна було перепробувати всі ключі, як результат ми отримали б усі можливі повідомлення даної довжини плюс колосальну кількість безглуздих дешифровок, що виглядають як безладне нагромадження букв. Але і серед осмислених дешифровок не було б ніякої можливості вибрати потрібну. Коли випадкова послідовність (ключ) поєднується з невипадковою (відкритим текстом), результат цього (шифротекст) виявляється абсолютно випадковим і, отже, позбавленим тих статистичних особливостей, які могли б бути використані для аналізу шифру

У 1945 році Клод Шеннон написав роботу «Математична теорія криптографії» [9] (розсекречену тільки після Другої світової війни в 1949 р як «Теорія зв'язку в секретних системах»), в якій довів абсолютну стійкість шифру Вернама. Тобто перехоплення шифротекста не дає ніякої інформації про повідомлення. З точки зору криптографії, неможливо придумати систему безпечніше шифру Вернама. Вимоги до реалізації подібної схеми досить нетривіальні, оскільки необхідно забезпечити накладення унікальною гами, що дорівнює довжині повідомлення, з подальшим її гарантованим знищенням.

Наведемо доказ абсолютної криптографічного стійкості. Нехай повідомлення представлено двійковою послідовністю довжини $N: m = m_1, m_2, \ldots, m_n$. Розподіл ймовірності повідомлень $P_m(m)$ може бути будь-яким. Ключ так само представлений

ISSN 2663 - 4023

двійковій послідовністю $k = k_1, k_2 \dots, k_n$ тієї ж довжини, але з рівномірним розподілом $P_k(k) = 1 \,/\, 2^N$ для всіх ключів.

У відповідності зі схемою шифрування, зробимо шифротекст, покомпонентно підсумовуючи по модулю 2 послідовності відкритого тексту і ключа:

$$C = M \oplus K = (m_1 \oplus k_1, m_2 \oplus k_2, \dots, m_N \oplus k_N)$$

Легальний користувач знає ключ і здійснює розшифрування:

$$M = C \oplus K = (c_1 \oplus k_1, c_2 \oplus k_2, \dots, c_N \oplus k_N)$$

Знайдемо імовірнісний розподіл N-блоків шифротекста, використовуючи формулу:

$$P(c = a) = P(m \oplus k = a) = \sum_m P(m)\, P(m \oplus k = a|m) = \sum_m P(m)\, 1/2^N = 1/2^N$$

Результат підтверджує відомий факт про те, що сума двох випадкових величин, одна з яких має рівномірний розподіл, є випадковою величиною з рівномірним розподілом. Таким чином, в нашому випадку розподіл шифротекста рівномірний.

Запишемо спільний розподіл відкритих текстів і шифротекста:

$$P(m = a, c = b) = P(m = a)P = (c = b|m = a)$$

Знайдемо умовний розподіл

$$P(c = b|m = a) = P(m \oplus k = b|m = a) = P(k = b \oplus a|m = a) = P(k = b \oplus a) = 1/2^n$$

так як ключ і відкритий текст є незалежними випадковими величинами. Разом:

$$P(c = b|m = a) = 1/2^N$$

Підстановка правій частині цієї формули в формулу для спільного розподілу дає

$$P(m = a, c = b) = P(m = a)1/2^N$$

Що доводить незалежність шифротекста і відкритих текстів в цій системі. Це і означає абсолютну криптографічну стійкість [10].

Прийняття рішення на основі аналізу.

Проаналізувавши наведені алгоритми, а саме необхідну кількість обчислень та пам’яті пристрою для організації цих обчислень, було досліджено що для роботи алгоритмів RSA та схеми Эль-Гамаля, необхідно використання обсягу пам’яті що перевищує наявну кількість у пристроях класу 0, та 1. Відповідно вони не можуть бути реалізовані на обмежених пристроях.

Оскільки побітова операція XOR, що використовується в шифрі Вернама має алгоритмічну складність рівну одиниці, тобто виконується за один такт процесора, а реалізація самого алгоритму не вимагає використання великої кількості флеш пам’яті то шифр Вернама може бути реалізований на пристроях навіть класу 0. Але для забезпечення абсолютної криптографічної стійкості потрібно згенерувати абсолютну або близьку до абсолютної випадкову послідовність бітів. Для генерації близької до абсолютної послідовності було прийняте рішення використовувати в якості зерна для генерації випадкових величин значення зчитане з непідключеного аналогового входу на мікроконтролері що піддається електронному шуму і спотворенню, що спричинені каналами передачі і операцій з обробки сигналів, тобто отримане значення шуму практично неможливо спрогнозувати, після чого виконати ряд арифметичних операцій з отриманим шумом та показами датчиків що вимірюють фізичні величини, отже згенерована послідовність буде практично абсолютно випадковою. Але оскільки шифр Вернама є симетричним алгоритмом шифрування, потрібно щоб ключ для шифрування був на обох сторонах, тобто на обмеженому пристрої та на шлюзі, оскільки для

кожного нового пакету даних буде генеруватись абсолютно нова послідовність випадкових значень, то ключ потрібно передати на шлюз, і звичайно теж зашифрувати перед відправкою.

Було прийняте рішення забезпечувати кожен обмежений пристрій N кількістю ключів для шифрування випадкових ключів шифром Вернама, якими буде шифруватись повідомлення, оскільки для кожного повідомлення що передається буде використовуватись новий унікальний ключ шифрування, то дізнатись предвстановлені ключі з пакету що передається буде неможливо.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Відповідно до вище вказаного аналізу був розроблений прототип системи IoT з використанням обмежених пристроїв, що забезпечує абсолютну криптографічну стійкість. Прототип складається з шлюзу в ролі якого виступає мікрокомп'ютер Raspberry pi 3 B+, обмеженого пристрою Arduino Nano з підключеним датчиком та програмною реалізацією вище згаданого шифру Вернама з усіма поставленими задачами. Шлюз використовується за необхідності тільки для передачі даних далі на сервери підприємства, в цьому випадку розшифрування відбувається вже на серверах, відповідно дані абсолютно не доступні на межі системи IoT, що у випадку взлому шлюзу, унеможливить крадіжку даних, оскільки вони зашифровані, а ключі розшифрування містяться тільки на сервері. З іншого боку прототип реалізовує інший сценарій в якому дані необхідні на межі мережі IoT, в цьому випадку шлюз здійснює прийом зашифрованих пакетів даних через незахищений канал зв'язку який підтримують обмежені пристрої, та здійснює по-перше підбір необхідного ключа для розшифрування випадково згенерованого ключа для шифрування повідомлення, по-друге розшифровує саме повідомлення та зберігає дані необхідні для обробки та передачі у форматованому вигляді на сервер для подальшої обробки та зберігання.

У будь-якому випадку кінцевий пристрій що відповідає за розшифрування зберігає N кількість ключів для кожного обмеженого пристрою, відповідно якщо зловмисник зможе отримати фізичний доступ до одного обмеженого пристрою, наприклад фізично вкравши його та діставши ключі для шифрування випадково згенерованих ключів, то це не вплине на захист всієї системи.

Обмежений пристрій в свою чергу зчитує дані з датчиків, та формує пакети, після чого за вище згаданим правилом формує абсолютно випадковий ключ для шифрування повідомлення, довжина якого дорівнює повідомленню, після чого шифрує отриманий випадковий ключ одним із предвстановлених ключів (що теж обираються випадково) для безпечної передачі разом з повідомленням. Після відправки зашифрованого пакету, його не можливо розшифрувати без доступу до предвстановлених ключів на обмеженому пристрої.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *Lightweight Cryptography | CSRC*. (б. д.). NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/Projects/Lightweight-Cryptography

2 *oneM2M Security solutions oneM2M TS-0003.* Європейський інститут телекомунікаційних стандартів ETSI. World Wide Web. https://www.etsi.org/deliver/etsi_ts/118100_118199/118103/02.12.01_60/ts_118103v021201p.pdf.

3 *OWASP Internet of Things*. (б. д.). OWASP Foundation | Open Source Foundation for Application Security. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities

4 Бачинський, Р. В., & Купецький, А. В. (2018). Серія: Інформаційні системи та мережі. *Вісник Національного університету "Львівська політехніка"*, (887), 18–24. http://nbuv.gov.ua/UJRN/VNULPICM_2018_887_5

5 Кузнєцов, Д. І. & Рябчина, Л. С. (2019). Інформаційна безпека систем Інтернету речей. *Вісник Криворізького національного університету*, (49), 80-83.

6 Петренко, А. І. (2019). Криптологія в Інтернеті речей. *Моделювання та інформаційні системи в економіці*, (97), 155-163. http://nbuv.gov.ua/UJRN/Mise_2019_97_18

7 Белей, О. І. & Логутова, Т. Г. (2019). Безпека передачі даних для Інтернету речей, *Кібербезпека: освіта, наука, техніка*, *2* (6), 6-18.

8 Bormann, C., Ersue, M., Keranen A. (2014). *Terminology for Constrained-Node Networks*. Internet Engineering Task Force (IETF). World Wide Web. https://tools.ietf.org/html/rfc7228.

9 Shannon, C. E. (б. д.). *A Mathematical Theory of Cryptography*. World Wide Web. https://www.iacr.org/museum/shannon/shannon45.pdf

10 Henk, C. A. (2005). Encyclopedia of Cryptography and Security. Springer Science+Business Media.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (11), 2021
ISSN 2663 - 4023

Chernenko M. Roman
graduate student of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-1439-961X
r.chernenko.asp@kubg.edu.ua

Riabchun P. Olena
graduate student of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-4400-0112
Santalen@bigmir.net

Vorokhob V. Maksym
graduate student of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0001-5160-7134
m.vorokhob.asp@kubg.edu.ua

Andriy O. Anosov
Candidate of sciences, associate professor, assistant professor of information and cybernetic security department
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-2973-6033
a.anosov@kubg.edu.ua

Valerii A. Kozachok
Phd, associate professor
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0003-0072-2567
v.kozachok@kubg.edu.ua

INCREASING THE LEVEL OF SECURITY OF INTERNET THINGS NETWORK SYSTEMS DUE TO ENCRYPTION OF DATA ON DEVICES WITH LIMITED COMPUTER SYSTEMS

Abstract. Because IoT devices work with data that may be confidential or confidential, that data must be protected. Due to the peculiarities of platforms and the implementation of such systems, namely: first, the use of devices with limited computing characteristics, which makes it impossible to use traditional means of information protection and data transmission protocols, and secondly. systems, and provide them with sufficient computing resources due to the impossibility of laying power lines, thirdly, the lack of standards for the implementation of these devices in the existing infrastructure, there are serious threats to the confidentiality, integrity and availability of information. The article considers the model of the IoT system, oneM2M standard presented by the European Institute of Communication Standards. IoT devices are designed with the necessary network connectivity, but often do not provide reliable network security. Network security is a critical factor in the deployment of IoT devices. The situation is complicated by the fact that IoT largely consists of limited devices. A limited device usually has a very limited cycle of power, memory, and processing. IoT devices are particularly vulnerable to threats because many of the current IoT devices do not support encryption. Several known encryption algorithms were selected for analysis: RSA, Vernam cipher, El Gamal scheme. After analyzing the above algorithms, a prototype of the IoT system was developed using limited devices, which provides absolute cryptographic stability. The prototype consists of a gateway in the role of a Raspberry pi 3 B + microcomputer, a limited Arduino Nano device with a connected sensor and a software implementation of the above-mentioned Vernam cipher with all the tasks.

Keywords: Internet of Things; IoT; network security; devices with limited computing resources; encryption algorithms; Vernam's cipher.

REFERENCES

1 Lightweight Cryptography | CSRC. (b.d.). NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/Projects/Lightweight-Cryptography
2 oneM2M Security solutions oneM2M TS-0003. European Institute of Telecommunication Standards ETSI. World Wide Web. https://www.etsi.org/deliver/etsi_ts/118100_118199/118103/02.12.01_60/ts_118103v021201p.pdf.
3 OWASP Internet of Things. (b.d.). OWASP Foundation | Open Source Foundation for Application Security. https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities
4 Bachinsky, R.V., & Kupetsky, A.V. (2018). Series: Information Systems and Frames. Bulletin of the National University "Lvivska Politechnika", (887), 18–24. http://nbuv.gov.ua/UJRN/VNULPICM_2018_887_5
5 Kuznetsov, D. I. & Ryabchina, L. S. (2019). Information security systems for Internet speeches. Bulletin of Kryvorizkiy National University, (49), 80-83.
6 Petrenko, A. I. (2019). Cryptology in the Internet of speeches. Model and information systems in economics, (97), 155-163. http://nbuv.gov.ua/UJRN/Mise_2019_97_18
7 Beley, O. I. & Logutova, T.G. (2019). Safe transmission of tributes for Internet speeches, Cyberbezpeka: education, science, technology, 2 (6), 6-18.
8 Bormann, C., Ersue, M., Keranen A. (2014). Terminology for Constrained-Node Networks. Internet Engineering Task Force (IETF). World Wide Web. https://tools.ietf.org/html/rfc7228.
9 Shannon, C. E. (b.d.). A Mathematical Theory of Cryptography. World Wide Web. https://www.iacr.org/museum/shannon/shannon45.pdf
10 Henk, C. A. (2005). Encyclopedia of Cryptography and Security. Springer Science + Business Media.