УДК 004.5 DOI: 10.33111/mise.97.16

Петренко А. І.,
студентка 3-го курсу спеціальності «Кібербезпека»,
інженер ННЛ «Полігон кібербезпеки»,
Київський національний економічний університет
імені Вадима Гетьмана

Petrenko A. I.,
3rd year Student at the «Cybersecurity» speciality,
Engineer of the «Polygon of Cyber Security» ESL,
Kyiv National Economic University named after Vadym Hetman

КРИПТОЛОГІЯ В ІНТЕРНЕТІ РЕЧЕЙ

CRYPTOLOGY ON THE INTERNET OF THINGS

Анотація: *«Інтернет речей» швидко увійшов в наше життя і життя мільярдів людей по всьому світу. Однак зростання кількості підключених пристроїв веде до збільшення ризиків безпеки: від заподіяння фізичної шкоди людям до простоїв і пошкодження обладнання — це можуть бути навіть трубопроводи, доменні печі і установки для вироблення електроенергії. Оскільки ряд таких об'єктів і систем «Інтернету речей» вже піддавалися нападу і було завдано значний збиток, забезпечення їх захисту стає критично важливим питанням, що потребує негайного вирішення. Це і зумовило актуальність вибраної теми.*

Більшість пристроїв IoT потенційно небезпечні через помилкове припущення, що забезпечення є надмірно дорогим і передбачає виділення певного періоду часу з графіку розробки продуктів IoT. Майже всім у спільноті IoT відомі заголовки ЗМІ, що стосуються ряду гучних порушень безпеки пристроїв IoT протягом останніх трьох років. У кожному з цих випадків після того, як хакер отримав запис, він здійснив несанкціоноване оновлення програмного забезпечення та взяв під контроль пристрій IoT.

Як професіонал IoT Security, найдивовижнішим аспектом порушень безпеки було те, що в цих системах безпека недостатня або її взагалі немає. Виявилося, що проблему безпеки при розробці навіть не розглядають. Колись деякі виробники IoT вважали, що вони можуть досягти безпеки за допомогою «непотрібность». Немає будівельників , які зводять будинки без замків на дверях. То чому виробники створювали пристрої IoT без замків на своїх «дверях»? Проінформовані керівники технологій та професіонали знають, що безпека через «незрозумілість» — це не що інше, як хибна надія.

Нещодавній парад збентежуючих, гучних порушень безпеки продукту IoT змушує порушити логічне запитання: слабка безпека в системах IoT це типово чи лише як виключення з правила? На жаль, здається, що типово.

Ключові слова*: Інтернет речей, кібербезпека, захищеність, вразливість, компоненти IoT.*

Annotation: *The Internet of Things has quickly entered our lives and the lives of billions of people around the world. However, increasing the number of*

connected devices leads to increased security risks: from physical harm to people to downtime and damage to equipment — it may even be pipelines, blast furnaces and power plants. As a number of such objects and systems of the Internet of Things have already been attacked and severely damaged, ensuring their protection becomes a critical issue that needs immediate resolution. This is what made the topic chosen relevant.
Most IoT devices are dangerously insecure because of a false assumption that reasonable security is prohibitively expensive and would add excessive time to the IoT product development schedule. Nearly everyone in the IoT community is aware of the media headlines involving a string of high-profile security breaches for IoT devices over the past three years. In each of these cases, after the hacker gained entry, he performed an unauthorized firmware update and took control of the IoT device.
As an IoT Security professional, the most surprising aspect of security breaches was that there appeared to be little or no security in these systems. It appeared that security wasn't even considered. It was once believed by some IoT manufacturers that they could achieve «security by obscurity.» I don't know of any builders who build homes without locks on the doors. So why would IoT device makers build IoT devices without locks on their «doors?» Informed technology executives and professionals know that «security by obscurity» is nothing more than false hope.
The recent parade of embarrassing, high-profile IoT product security breaches raises a logical question, is the lack of security in these IoT systems unusual or is this typical? Sadly, the answer appears to be that it's typical.
Keywords: *Internet of Things, cybersecurity, security, vulnerability, IoT components.*

Вступ: Інтернет речей — це нова і перспективна технологія, що має на меті глобальну зміну нашого світу шляхом об'єднання фізичних об'єктів («речей») і кіберпростору. Концепція Інтернету речей включає багато технологій, наприклад Інтернет, розподілені обчислення, машинне навчання, комунікації, великі дані, сенсорні технології, взаємодія машина-людина, машина-машина.

Постановка проблеми: Інтернет речей, аналітика великих даних і машинне навчання — це ті області науки і техніки, які бурхливо розвиваються та формують нове покоління комп'ютерних систем з використанням штучного інтелекту. Варто відмітити, що ці області є міждисциплінарними за своєю природою. Це дозволяє їм нагромаджувати як і теоретичні основи, так і розвиватися в практичній площині.

Виклад основного матеріалу: Термін «Інтернет речей» (Internet of things, IoT) був запропонований в 1999 році Кевіном Ештоном під час його роботи над створенням Procter&Gamble, який припустив, що можливо зв'язати кілька фізичних об'єктів («речей») на виробництві для обміну інформацією і взаємодії між собою і із зовнішнім оточенням. У 2010 році в результаті стрімкого поширення смартфонів і планшетних комп'ютерів під

поняттям «Інтернет речей» стали розуміти непросто автоматизацію процесів на локальному виробництві, але й глобальніше поняття, коли не тільки комп'ютер або смартфон, а й інші прилади, починаючи з кавомашини в офісі і закінчуючи холодильником у будинках, підключені до інтернету. У звичайних споживачів з використанням таких технологій життя стає комфортніше. У народному господарстві це спосіб економії ресурсів і оптимізації виробництва [2]. IoT дозволяє створювати динамічні мережі, що складаються з мільярдів елементів, що можуть взаємодіяти між собою. Таким чином забезпечується зв'язок між накопиченим обсягом даних і реальними об'єктами, для яких додатки, сервіси, самі пристрої — це джерела даних.

По суті, Інтернет речей — це одна величезна хмара. Сам по собі крихітний чіп примітивний за своєю архітектурою: він нічого не може сказати своєму власнику, лише приймати потрібну йому інформацію. Як тільки він зв'язується через Wi-Fi з відповідним комп'ютером або системою обробки цієї інформації, цей чіп прирівнюється до суперкомп'ютера, що обробив отриману інформацію.

Передбачається, що в майбутньому IoT стануть активними учасниками бізнесу, інформаційних і соціальних процесів, де вони зможуть взаємодіяти і спілкуватися між собою, обмінюючись інформацією про навколишнє середовище, реагуючи і впливаючи на процеси, що відбуваються в навколишньому світі, без втручання людини.

Роб Ван Краненбург стверджує, що IoT можна уявити як «чотирьох-шаровий пиріг» (рис. 1) [3]. Це класифікація за масштабністю використання IoT.

Рис. 1. Класифікація IoT за Робом Ван Краненбургом

Заглядаючи в майбутнє, Cisco прогнозує, що до 2020 року до Інтернету буде підключено 38 млрд, а до 2025 року — 56 млрд пристроїв [4]. Однак ці прогнози не враховують прискореного розвитку технологій і пристроїв. Комусь кількість підключених пристроїв може здатися заниженою. Це пов'язане з тим, що в розрахунках враховується все населення нашої планети, але біль-

шість людей до сих пір не має доступу в Інтернет. Якщо ж враховувати тільки тих, хто користується Інтернетом, то кількість підключених пристроїв на одного користувача виявиться набагато вище. У 2010 році кількість підключених пристроїв на одного користувача становило 6,25 одиниць, а не 1,11.

Історія часто повторюється. Сьогодні Інтернет речей підходить до етапу, на якому різнорідним мережам і безлічі датчикам належить об'єднатися для взаємодії під керуванням єдиних стандартів. Цю мету поставлять перед собою комерційні організації, державні установи, органи, що займаються розробкою стандартів, і навчальні заклади. Щоб Інтернет речей став популярним серед звичайних користувачів, постачальники послуг та інші учасники ринку повинні розробити додатки, які значно підвищують якість життя простих громадян, не порушуючи їх безпеки в кіберпросторі.

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 і злому, розробники повинні підтримувати конфіденційність даних, цілісність і доступність у всій IT-інфраструктурі всіма доступними їм способами, зважаючи на особливості пристроїв IoT.

Розвиток концепції Інтернету речей та її впровадження в різні сфери передбачає наявність десятків мільярдів автономних пристроїв. Усі вони підключені до мережі та передають через неї відповідні їх функціоналу дані. Ці дані і функціонал є мішенню для зловмисників, а отже, повинні бути захищені відповідним чином.

Фактично, більшість IoT-пристроїв не забезпечені елементами захисту, мають доступні ззовні інтерфейси управління, дефолтні паролі, тобто, мають всі ознаки веб-уразливості.

Всі ще пам'ятають події трьохрічної давності, коли ботнет Mirai шляхом підбору комбінацій дефолтних логінів і паролів зламав велику кількість камер і роутерів, які були в подальшому використані для наймогутнішої DDoS-атаки на провайдерські мережі UK Postal Office, Deutsche Telekom, TalkTalk, KCOM і Eircom. При цьому «брутфорс» IoT-пристроїв здійснювався за допомогою Telnet, а роутери зламувалися через порт 7547 з використанням протоколів TR-064 і TR-069 [5].

Але найрезонанснішою була атака у 2016 році, що порушила нормальне функціонування DNS-оператора DYN, а разом з ним практично роботу «пів-інтернету» США. Для атаки ботнетом

були використані ті ж самі встановлені за замовчуванням логіни і паролі пристроїв.

Зазначені події наочно демонструють проґалини IoT-системах і вразливості багатьох «розумних» пристроїв. Зрозуміло, що збої «розумних» годинників або фітнес-трекерів пересічних громадян особливої шкоди, крім для самих господарів, не принесуть. Але ось злом IoT-пристроїв, які входять у системи і сервіси M2M, зокрема, інтегровані в критичну інфраструктуру, загрожує непередбачуваними наслідками [6]. У цьому випадку ступінь їх безпеки повинна відповідати важливості тієї чи іншої інфраструктури: транспортної, енергетичної чи інший, від яких залежить життєдіяльність людей і робота економіки. Також і на побутовому рівні — збої і атаки на ту ж систему «розумний» будинок можуть привести до локальних комунальним або іншим аварійним і небезпечних ситуацій.

Більшість пристроїв IoT утворюють «закриті системи». В такій системі покупці не можуть змінювати наповнення пристроїв, а будь-яке втручання завдає непоправної шкоди системі. Тобто, усі заходи захисту мають бути вбудовані до виходу продукту на ринок. Для інформаційної безпеки така «безпека зсередини» є новою технологією захисту при виготовленні пристрою на заводі. Це стосується і класичних технологій безпеки, таких як шифрування, перевірка автентичності, перевірка цілісності, запобігання вторгнень і можливості безпечного оновлення. З огляду на тісний зв'язок апаратного і програмного забезпечення в моделі IoT, іноді простіше, щоб програми для захисту використовували розширення функцій апаратної частини і створювали «зовнішні» рівні безпеки. Апаратний рівень — це всього лише перший крок, необхідний для комплексного захисту зв'язку і пристроїв. Комплексний захист вимагає інтеграції функцій управління ключами, захисту на основі хосту, інфраструктури OTA і аналітики безпеки [7].

Безпеку інтернету речей можна побудувати на фундаменті з чотирьох наріжних каменів: безпека зв'язку, захист пристроїв, контроль пристроїв і контроль взаємодій у мережі.

Відсутність навіть одного з наріжних каменів у фундаменті безпеки залишить широкий простір діям зловмисників. Наше життя залежить від літаків, поїздів і автомобілів, які перевозять нас, від інфраструктури охорони здоров'я та цивільної інфраструктури, яка дозволяє нам жити і працювати. Неважко уявити, як незаконне маніпулювання світлофорами, медичним обладнанням або незліченними іншими пристроями може привести до плачевних наслідків.

Більшість сучасних алгоритмів захисту інформації і, зокрема, шифрування, розраховані на застосування в ЕОМ у складі програмних комплексів без урахування оптимізації на апаратному рівні забезпечення. Цей факт робить неможливим застосування більшості існуючих криптографічних алгоритмів в пристроях з обмеженою обчислювальною потужністю, малим обсягом і малим енергоспоживанням.

Особливої актуальності «низькоресурсної криптографії» (Lightweight cryptography, LW-криптографія) набуває в світлі розвитку ідеї «інтернету речей» [8].

Оскільки алгоритми LW-криптографії розробляються під конкретні вимоги з чіткими обмеженнями, тому неважко перерахувати всі переваги і недоліки даного сімейства алгоритмів. При цьому головною перевагою є вкрай низькі вимоги як до ресурсів, так і щодо споживання енергії, що робить ці алгоритми вкрай швидкими в роботі і «невибагливими» до середовища, у якому буде здійснюватися їх робота. Крім того, це робить такі алгоритми вкрай дешевими у впровадженні та використанні.

Однак, оскільки LW-алгоритми призначені для обробки малого обсягу інформації, вони не володіють високою пропускною спроможністю.

Перш ніж говорити про приклади реалізації схем LW-криптографії, ми повинні сформулювати критерії пошуку таких криптографічних алгоритмів [9]. По-перше, це вічний пошук балансу між надійністю, продуктивністю і ціною (рис. 2).

Рис. 2. Схема взаємодії надійності, продуктивності і ціни

Розширений алгоритм крихітного шифрування (Extended Tiny Encryption Algorithm, XTEA) — один з найшвидших і найефективніших криптографічних алгоритмів, що існують (рис. 3). XTEA — це симетричний алгоритм шифрування ключів, створений Девідом Уілером та Роджером Нудхемом з Кембриджського університету та опублікований у 1997 році [10].

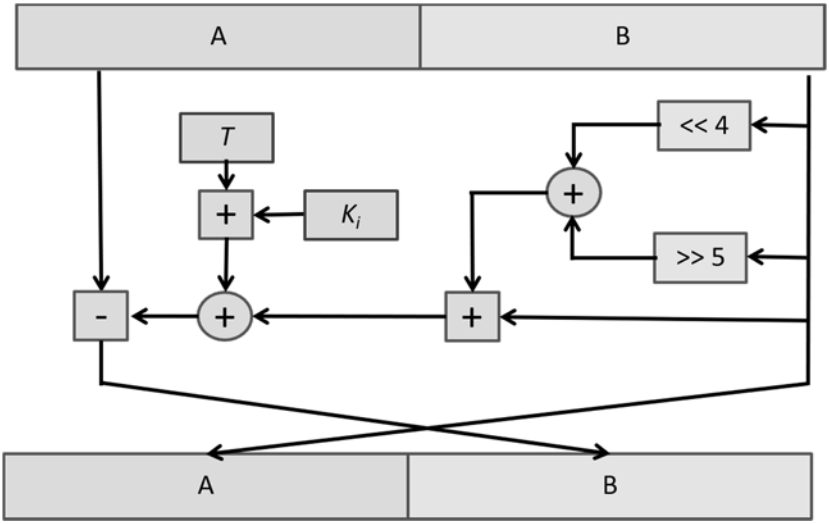

Рис. 3. Схема шифрування

Як і TEA, шифр заснований на операціях з 64-бітним блоком, має 32 повних цикли, в кожному повному циклі за два раунди Мережі Фейстеля, що означає 64 раунди мережі Фейстеля. Однак, кількість раундів для досягнення кращої дифузії може бути збільшена за рахунок продуктивності. Крім того в XTEA, як і в TEA, використовується 128-бітний ключ, який складається з чотирьох 32-бітних слів K[0], K[1], K[2] і K[3].

XTEA за технічними характеристиками нічим не відрізняється від повноцінних алгоритмів, які функціонують на суперкомп'ютерах і носять державне значення. Варто звернути увагу на те, що приналежність XTEA до алгоритмів LW-криптографії не означає жертвувати його стійкістю заради низьких ресурсів. Компроміс завжди можна знайти.

Висновки: 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. Простого універсального рішення не існує, і для забезпечення безпеки недостатньо замкнути двері, залишивши вікна відкритими. Безпека повинна бути комплексною, інакше хакери просто скористаються найслабшою ланкою.

У зв'язку з обмеженими ресурсами для забезпечення процесу шифрування на якісному рівні, в IoT почали імплементувати алгоритми LW-криптографії, що детально було розглянуто у останньому розділі. Як один із алгоритмів було обрано та реалізовано XTEA на мові JavaScript.

IoT — це новий етап еволюційного розвитку Інтернету, який не повинен стати технологією заради технології. Він може кардинально змінити усталений устрій світу. Наскільки швидко — залежить лише від нас самих.

Література

1. Смирнов О.С. Розвиток «Інтернету речей», доповненої реальності та комунікаційних технологій: стаття / К. С. Голохваст, О. В. Тумялис. — Далекосхідний федеральний університет — Режим доступу: https://arxiv.org/ftp/arxiv/papers/1902/1902.08008.pdf

2. Щербинина М.Ю., Стефанова Н.А. Концепция интернет вещей // Креативная экономика. — 2016. — Т. 10. — № 11. — с. 1323–1336 — Режим доступу: https://www.researchgate.net/publication/311863315_Koncepcia_internet _vesej

3. UK Government Chief Scientific Adviser The Internet of Things: making the most of the Second Digital Revolution / посібник, 2014 — 40 с.

4. Лекція №1. Вступ до інтернету речей //навчальний посібник з дисципліни «Архітектура і технології IoT», 2017 — 13с.

5. Тюрин В.А. Інтернет речей: нові можливості для світу та бізнесу — Мережа. Фактори — Режим доступу: https://megamozg.ru/post/25334/

6. Sundmaeker H. Vision and Challenges for Realising the Internet of Things / European Commission — Information Society and Media DG

7. Вічугова А. Криптографія в IoT та Big Data: захищенні протоколи та мікросхеми [Електронний ресурс] — Режим доступу: https://www.bigdataschool.ru/bigdata/iot-protocol-microchip-crypto-big-data.html

8. Rishi R., Saluja R. EY Future of IoT // Ernst & Young Associates LLP, 2019 — 32 с. Режим доступу: https://www.ey.com/Publication/vwLUAssets/EY_-_Future_of_IoT/$FILE/EY-future-of-lot.pdf

9. Эванс Д. Интернет вещей: как изменится вся наша жизнь на очередном этапе развития сети // Компанія Cisco Systems. — 2011 [Електронний ресурс] — Режим доступу: http://www.cisco.com/web/RU/news/releases/txt/2011/062711d.html

10. IoT і проблеми безпеки — блог компанії Unet — 2018. [Електронний ресурс] — Режим доступу: https://habr.com/ru/company/unet/blog/410849/

References

1. Smirnov O.S. Development of the Internet of Things, Augmented Reality and Communication Technologies: Article / KS Holokhvast, OV Tumyalis. — Far Eastern Federal University — Access Mode: https://arxiv.org/ftp/arxiv/papers/1902/1902.08008.pdf

2. Shcherbinina M.Y., Stefanova N.A. The concept of the Internet of Things // Creative Economy. — 2016. — Vol. 10. — № 11. — p. 1323–1336 — Access Mode: https://www.researchgate.net/publication/311863315_Koncepcia_internet_vesej

3. UK Government Chief Scientific Adviser The Internet of Things: Making the Most of the Second Digital Revolution / Manual, 2014 — 40 p.

4. Lecture №1. Introduction to the Internet of Things // Tutorial on IoT Architecture and Technology, 2017 — 13p.

5. Tyurin V.A. Internet of Things: New Opportunities for the World and Business — Networking. Factors — Access Mode: https://megamozg.ru/post/25334/

6. Sundmaeker H. Vision and Challenges for Realizing the Internet of Things / European Commission — Information Society and Media DG

7. Vichugova A. Cryptography in IoT and Big Data: Secure Protocols and Chips [Electronic resource] — Access mode: https://www.bigdataschool.ru/bigdata/iot-protocol-microchip-crypto-big-data.html

8. Rishi R., Saluja R. EY Future of IoT // Ernst & Young Associates LLP, 2019 — 32 p. Access Mode: https://www.ey.com/Publication/vwLUAssets/EY_-_Future_of_IoT/$FILE/EY-future-of-lot.pdf

9. Evans D. The Internet of Things: How Our Life Will Change at Another Stage of Network Development // Cisco Systems. — 2011 [Electronic resource] — Access mode: http://www.cisco.com/web/EN/news/releases/txt/2011/0627 11d.html

10. IoT and Security Issues — Unet Blog — 2018. [Electronic resource] — Access mode: https://habr.com/en/company/unet/blog/410849/

Статтю подано до редакції 27.03.2019 р.