Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії ім. В.В. Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА

Пояснювальна записка

другий (магістерський) .
(рівень вищої освіти)

Захист інформації послуг «Інтернет- речей» в локальних мережах
(тема)

Виконав: студент 2 курсу, групи ІКІм-19-1
Спеціальності 172 «Телекомунікації та радіотехніка»
освітньої професійної програми
«Інфокомунікаційна інженерія»
(шифр і назва спеціальності)
Рибас К.В. .
(прізвище, ініціали)
Керівник кафедри ІКІ ім.В.В.Поповського
доц. Холод Л.М.
(прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020 р.

Атестаційна робота не містить
відомостей, що заборонені
до відкритого друку

Студент гр. ІКІм-19-1 Рибас К.В.
Керівник доцент Холод Л.М.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій

Кафедра Інфокомунікаційної інженерії ім В.В. Поповського

Рівень вищої освіти другий (магістерський)

Спеціальність 172 «Телекомунікації та радіотехніка»

Освітня-професійна програма «Інфокомунікаційна інженерія»

(повна назва)

ЗАТВЕРДЖУЮ

Зав. кафедри_____

(підпис)

«____» _____2020р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студенту Рибасу Костянтину Віталійовичу.

(прізвище, ім'я, по-батькові)

1. Тема роботи: Захист інформації послуг «Інтернет- речей» в локальних мережах

Information Protection for Internet of Things Services in Local Networks

затверджена наказом по університету від «20» жовтня 2020р. №1396Ст

2. Термін здачі студентом роботи 15 грудня 2020р.

3. Вихідні дані до роботи: методи забезпечення безпеки послуг «Інтернет- речей» в локальних мережах,,стандарти TLS (DTLS)/SSL, алгоритми гібридного шифрування, захист трафіку IoT, стандарти ISO/IEC 27001:2018, COBIT, ISO/IEC 27007, оцінка якості безпеки WAF/IPS, параметри: $P_{СЗІN}$, $<P,a,R>$ і $<Д,Z,V>$, $P = (p1, p2, \ldots, pN)$ та $Q = (q1, q2, \ldots, qN)$ з $\sum i = 1Npi = \sum i = 1Nqi = 1$, $i = 1,2,\ldots, N$

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):

1. Аналіз перспектив розвитку концепції Internet of Things
2. Дослідження основних методів захисту інформації послуг Інтернет-речей в локальних мережах
3. Методи тестування елементів локальних мереж
4. Методика розрахунку, аналізу та оцінка методів захисту інформації локальних мереж нових поколінь

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, плакатів):

Демонстраційний матеріал у вигляді ppt-презентації;

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по-батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна Частина	доцент Холод Леонід Миколайович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	01.09.2020	Виконано
2	Виконання 1 розділу	24.10.2020	Виконано
3	Виконання 2 розділу	20.11.2020	Виконано
4	Виконання 3 розділу	01.12.2020	Виконано
5	Виконання 4 розділу	12.12.2020	Виконано
6	Оформлення пояснювальної записки	15.12.2020	Виконано
7	Оформлення слайдів та презентації	15.12.2020	Виконано

7. Дата видачі завдання 1 вересня 2020 року

Студент _____ Рибас К.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Холод Л.М.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка складається з: 78 сторінок, 34 рисунків, 21 посилань.

LAN, IoT, МЕРЕЖА, КОНТРОЛЬ, БЕЗПЕКА, ОЦІНКА ЯКОСТІ ЗАХИСТУ ПОСЛУГ IoT, ЕЛЕМЕНТИ, ТРАФІК, HTTP, КОНТРОЛЬ ПАРАМЕТРІВ, ТЕСТУВАННЯ, СКАНУВАННЯ

Об'єкт дослідження – процес функціонування елементів та послуг IoT в LAN.

Предмет дослідження – методи захисту інформації послуг Інтернет-речей в локальних мережах нових поколінь.

Мета атестаційної роботи – забезпечення нормативних вимог до параметрів якості захисту інформації послуг Інтернет-речей в локальних мережах нових поколінь.

Методи досліджень – аналіз науково-технічної літератури, опис, порівняння, зіставлення, формалізація, розрахунок, побудова діаграм, розроблення та використання програмних засобів.

Математичне моделювання, оптимізація, тестування, сканування, розрахунки, аналіз методів контролю забезпечення захисту об'єктів, трафіку послуг IoT та оцінка параметрів безпеки при обслуговуванні послугами IoT в локальних мережах нових поколінь.

ABSTRACT

The explanatory note consists of: 78 pages, 34 figures, 21 references.

LAN, IoT, NETWORK, CONTROL, SECURITY, QUALITY ASSESSMENT OF IoT SERVICES PROTECTION, ELEMENTS, TRAFFIC, HTTP, PARAMETER CONTROL, TESTING, SCANNING

The object of study - is the process of functioning of IoT elements and services in LAN.

The subject of research - methods of information protection of Internet of Things services in local networks new generation.

The purpose of certification work - to provide regulatory requirements for the quality of information protection of Internet of Things services in local networks new generation.

Research methods - analysis of scientific and technical literature, description, comparison, comparison, formalization, calculation, construction of diagrams, development and use of software .

Mathematical modeling, optimization of calculations, analysis of control methods to ensure the protection of objects, traffic of IoT services and evaluation of security parameters in the maintenance of IoT services in local networks of new generations.

ЗМІСТ

Перелік скорочень, умовних позначень, символів, одиниць і термінів…..... 9
Вступ……... 11
1 Аналіз перспектив розвитку концепції Internet of Things……... 14
1.1.Загальні положення…….. 14
1.2 Особливості розвитку концепції Internet of Things…….. 14
1.3 Пілотні проекти Інтернет речей…… 18
1.4 Споживчий Інтернет речей та побутова електроніка……. 22
1.5 Технологія iot: хмарні, туманні та крайові обчислення……. 28
1.6 Інфраструктура, безпека iot–платформ…….. 29
2 Дослідження основних методів захисту інформації послуг Інтернет-Речей в локальних мережах…….. 40
2.1 Загальні положення……. 40
2.2 Основні напрямки забезпечення безпеки архітектури Інтернету речей в локальних мережах…….. 41
2.3 Особливості забезпечення безпеки Інтернету речей в локальних мережах…… 44
2.4 Особливості захисту трафіку Інтернет-речей…….. 55
2.5 Метод захисту трафіку Інтернет-речей на базі використання алгоритмів гібридного шифрування…….. 59
2.6 Метод захисту трафіку Інтернет-речей на базі створення патернів мережного трафіку……. 60
3 Методи тестування елементів локальних мереж…… 63
3.1 Загальні положення……. 63
3.2 Основні вимоги нормативного забезпечення…… 65
3.3 Методологія тестування та сканування елементів локальної мережі…. 65
3.4 Методи тестування компонентів web-додатків…… 67
3.5 Тестування елементів мережі на можливості SQL–ін’єкцій……. 70
3.6 Тестування виконання сценаріїв міжсайтового обміну ……... 71
3.7 Тестування даних автентифікації…….. 72
3.8 Тестування можливостей витоку конфіденційних даних……. 75

4 Методика розрахунку, аналізу та оцінка методів захисту інформації локальних мереж нових поколінь……... 76
4.1 Загальні положення…… 76
4.2 Системи забезпечення безпеки локальних мереж нових поколінь……. 77
4.3 Методи розрахунку, аналізу та оцінка стійкості системи захисту інформації в локальних мережах нових поколінь……. 81
4.4 Метрики захисту транспортних ресурсів локальної мережи……. 87
Висновки……. 94
Перелік джерел посилання……. 98

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АСУ - автоматизовані системи управління
ВДТ - візуальний дисплейний термінал
ГІІ - глобальна інформаційна інфраструктура
НІІ - національна інформаційна інфраструктура
РІІ - регіональна інформаційна інфраструктура
ЦОД - центрів обробки даних
AMQP - advanced message queuing protocol
CAN - corporate area network
CIoT - Consumer Internet of Things
CoAP - constrained application protocol
COBIT - Control Objectives for Information and Related Technology
CPS - cyber-physical-system
C-UNB - cooperative ultra narrowband
DDoS - Distributed Denial of Service
DNS - domain name system
DPI - Deep Packet Inspection
DTLS - datagram transport layer security
ECC - elliptic curve cryptography
EID - electronic identification
EST - enrollment over secure transport
FE - flash event
FTP - file transfer protocol
HPE - hewlett packard enterprise
HTTP - hypertext transfer protocol
IEEE - institute of electrical and electronics engineers
IH - intellectual house
ISO/IEC 27007 - Guidelines for information security management systems auditing.
IIC - industrial internet consortium
IoT - Internet of Things

ISA - international society for automation
IT - information Technology
LAN – local area network
LoRa - long range
MAN - metropolitan area network
MQTT - message queuing telemetry transport
NGN - Next Generation Networks
OCSP - online certificate status protocol
OT - operational Technology
OTA - оновлення по повітрю
RFID - radio frequency identification
SCADA - supervisory control and data acquisition
SCEP - simple certificate enrollment protocol
TLS - transport layer security
WAF - Web Application Firewall
WLAN - wireless local area network
WMAN - wireless metropolitan area network
WPAN - wireless personal area network
WWAN - wireless wide area network
XMPP - extensible messaging and presence protocol

ВСТУП

У сімдесяті роки минулого століття, з того часу, коли комп'ютери перестали бути поодинокими і унікальними виробами, почалася масова автоматизація за двома практично незалежним напрямками. Одне – автоматизація бізнес-процесів, яку називають інформаційними технологіями (IT - IT, Information Technology). Інше - автоматизація технологічних процесів, цей напрямок на противагу IT стали називати операційними технологіями (OT, Operational Technology).

Варто уточнити, IT мають справу не з інформацією, а з даними, тому їх би так точніше варто було б називати «технології даних». IT об'єднують в собі комп'ютери, системи зберігання даних і мережі з процесами створення, обробки, зберігання, забезпечення безпеки і обміну будь-якими формами електронних даних. OT - це теж комплекс апаратного і програмного забезпечення, але призначеного для контролю і управління фізичними процесами.

Понад сорок років IT і OT розвивалися незалежно, і за цей час набули рис, істотно розрізняти їх. Але в третьому десятилітті XXI століття під впливом ряду факторів, в тому сенсорної революції, розвитку мережевих технологій, хмарного комп'ютингу, аналітики великих даних і інших сучасних трендів почався процес конвергенції (IT/OT convergence), який об'єднує два підходи - орієнтацію на дані і орієнтацію на події в фізичному світі.

Поняття «Інтернет речей» (IoT - Internet of Things) описує дуже важливий етап розвитку глобальної інформаційної інфраструктури (ГІІ), що характеризується підключенням великої кількості пристроїв, які здійснюють автоматизовану обробку даних без участі людини.

Основним призначенням мережі Інтернет є здійснення транспортної функції: об'єднання приватних обчислювальних мереж, індивідуальних користувачів і центрів обробки даних (ЦОД). Фізичний рівень ГІІ досить статичний і вдосконалюється в основному в кількісному відношенні шляхом підвищення пропускної здатності каналів інфокомунікацій і каналоутворюючого обладнання.

Значне збільшення трафіку призводить до розробки все більш потужних маршрутизаторів і вдосконалення протоколів маршрутизації і принципів функціонування ГІІ. У побудові сучасних мереж на рівнях: ГІІ, національної інформаційної інфраструктури (НІІ), регіональної інформаційної інфраструктури (РІІ), MAN (Metropolitan Area Network), CAN (Corporate Area Network) , LAN (Local Area Network), ІН (Intellectual House), крім традиційного інфраструктурного рівня передачі даних, що містить комутуюче обладнання, виділяється рівень управління.

Поділ функцій передачі та управління дозволяє віртуалізувати мережеву інфраструктуру і значно підвищити утилізацію і централізувати управління ресурсами, реалізуючи технологію програмно визначених мереж (Software Defined Network), призначену для роботи в умовах динамічних змін.

Такий підхід вже сьогодні знаходить своє застосування в ЦОД при побудові хмарних сервісів і стрімко набирає популярність в корпоративних мережах і мережах провайдерів.

В першому розділі представлені аналіз перспектив розвитку концепції Internet of Things. Розглянуто технології та стандарти для комутації та конвергенції інфраструктури Інтернету речей. Досліджені варіанти підключення IoT до існуючих мереж.

В другому розділі проведені дослідження основних методів захисту інформації послуг Інтернет-речей в локальних мережах. Проведено аналіз безпеки Інтернету речей локальних мереж.

Прикладний цінністю мережі Інтернет є ряд спеціалізованих сервісів, реалізованих на її базі - DNS, електронної пошти (e-mail), передачі файлів (FTP), всесвітньої павутини (World Wide Web), потокового мультимедіа і т.д. Надані сервіси знаходяться в безперервному розвитку, трансформуючи суспільство і соціологізіруя взаємодію в рамках мережі. Більшість web -додатків використовує модель взаємодії «користувач - сервіс» і є відображенням формованого інформаційного суспільства.

В третьому розділі представлені методи тестування елементів локальних мереж та особливості вимог нормативного забезпечення.

Запропонована методологія тестування та сканування елементів локальної мережі на базі сканеру Nmap, що входить до ОС Kali Linux. Nmap (“Network Mapper”).

Проведен детальний аналіз результатів тестування відкритих портів та сканування запущених служб на web-сервері, сценаріїв встановлення типу операційної системи, контролю сервісів та їх версій та різних типів ін’єкцій.

В четвертому розділі представлена методика розрахунку, аналізу та оцінка методів захисту інформації локальних мереж нових поколінь.

Проведен аналіз системи забезпечення безпеки локальних мереж нових поколінь та схеми захисту трафіку локальної мережі на основі брандмауера web–додатків WAF.

Запропонована та описана схема блокування ненормального трафіку з Інтернету.

Цій темі були присвячені публікації на: Шосту Міжнародну науково-технічну конференцію«Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС-2020)»; The 1st International scientific and practical conference «European scientific discussions» (November 28–30, 2020) Potere della ragione Editore, Rome, Italy. 2020; IV Міжнародну науково-практичну конференцію «PRIORITY DIRECTIONS OF SCIENCE AND TECHNOLOGY DEVELOPMENT», 20-22 грудня 2020 року Київ [6,7,8].

1 АНАЛІЗ ПЕРСПЕКТИВ РОЗВИТКУ КОНЦЕПЦІЇ INTERNET OF THINGS

1.1.Загальні положення

Під річчю в Інтернеті речей (IoT) розуміється або фізична річ (електричне обладнання, робот і т.д.), або елемент інформаційного світу (мультимедійний контент, ПЗ і т.д.), який може бути ідентифікований та інтегрований в мережу зв'язку. Фізична річ є об'єктом матеріального світу, має структуру, володіє функціональними, якісними і кількісними характеристиками. Її можна включити, привести в дію і т.д. Віртуальна річ має місце тільки в інформаційному світі, її можна зберігати, обробляти і отримувати до неї доступ. Фізична річ може мати кілька проекцій в інформаційному світі, віртуальна ж річ може існувати без відповідної їй фізичної речі.

Базова ідея IoT полягає в забезпеченні взаємодії різних речей в навколишньому просторі, надання безперебійної зв'язку і передачі контекстної інформації, яку ці речі генерують. Взаємодія речей відбувається на основі існуючих і розвиваються на основі інформаційно–комунікаційних технологій. У просторі IoT поряд з вже існуючими вимогами до інформаційно-комунікаційних технологій, такими як забезпечення зв'язку "в будь–який час" і "в будь–якому місці", з'являється нове – "зв'язок з будь–якою річчю". Ця вимога передбачає взаємодію, тобто обмін інформацією як між самими речами, так і між людиною і річчю.

1.2 Особливості розвитку концепції Internet of Things

Концепція IoT передбачає, що кожна фізична річ має пристрій – елемент обладнання, який надає можливість комунікації (обов'язкова вимога), а також ряд

додаткових можливостей. До них відносяться можливості проводити вимірювання, спрацьовувати, а також можливість введення, зберігання і обробки даних. Всі пристрої можна розділити на категорії: пристрої перенесення і збору даних, сенсорні і виконавчі пристрої, широкого / загального призначення.

До першої категорії відносяться пристрої, що дозволяють підключити фізичну річ до мережі зв'язку. Друга категорія – це зчитувальні або записуючі пристрої. У третій категорії знаходяться сенсорні пристрої, що дозволяють виявляти і вимірювати інформацію, а потім перетворювати її в цифрові електричні сигнали. Виконавчі пристрої виробляють зворотну операцію, перетворюючи цифрові електричні сигнали в різні дії. Четверта категорія включає пристрої, що відносяться до різних областей застосування IoT і володіють вбудованими можливостями обробки інформації та зв'язку.

В якості додатків IoT можуть виступати різні інтелектуальні транспортні системи, розумні будинки, розумні електромережі і т.д. Передача управляючих команд від додатків до пристроїв також виконується мережами зв'язку. Мережа повинна забезпечувати надійну, ефективну і безпечну передачу даних. Інфраструктури можуть бути використані як традиційні мережі на базі протоколу TCP/IP, так і нові технології, де розвиваються мережі, наприклад мережі наступного покоління (Next Generation Networks – NGN).

Чотирьохрівнева еталонна модель IoT

Розроблена четирехуровневая еталонна модель [1] дає уявлення про архітектуру і дозволяє зробити оцінку можливостей IoT(рис.1.1).

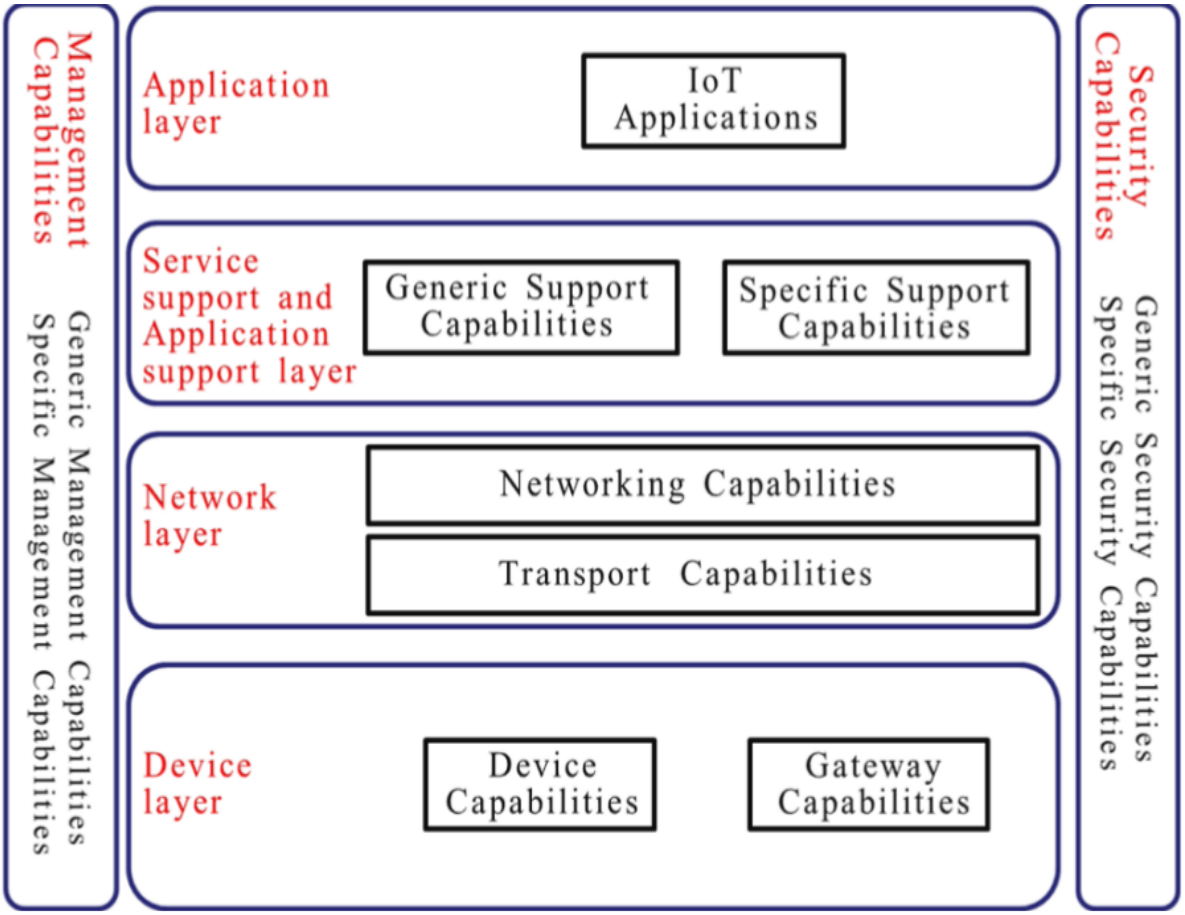


Рисунок 1.1 – Чотирьохрівнева еталонна модель IoT

Для цих цілей найбільш цікаві четвертий (верхній) і перший (нижній) рівні. На верхньому рівні моделі розташовані IoT–додатки, що виробляють інтерпретацію надходить від пристроїв інформації. IoT–додатки залежать від даних, які вони обробляють, і їх споживачів. Деякі додатки зосереджені на моніторингу даних, інші на управлінні ними.

Завдання моніторингу та управління породжують різні моделі додатків і шаблони програмування, а також торкаються питань операційних систем, мобільності, серверів додатків і багатопоточності. У загальному вигляді індивідуальні користувачі можуть застосовувати додатки для домашньої автоматизації, забезпечення безпеки, автоматичного моніторингу пристроїв і управління повсякденними завданнями.

В якості промислових рішень додатки надають необхідну контекстну інформацію в реальному масштабі часу і допомагають у прийнятті рішень. Нижній рівень моделі є фізичні речі пристрої, які можуть управляти іншими пристроями. Вони включають в себе широкий спектр кінцевих пристроїв, що

генерують і обробляють інформацію в локальних, корпоративних, місцевих, регіональних, національних та глобальних мережах.

З розвитком інформаційних технологій (IT) цей рівень буде постійно поповнюватися новими пристроями. Для самих пристроїв не існує ніяких обмежень, окрім одного: все вони повинні надавати можливість зв'язку. Без цього вони не можуть бути інтегровані в простір IoT.

Необхідність забезпечення комунікації з пристроєм призводить до виникнення проблеми сумісності, яка повинна бути вирішена шляхом розробки стандартів їх взаємодії. У загальному вигляді будь–яка фізична річ може бути включена в простір IoT, якщо вона здатна взаємодіяти або з мережею зв'язку, або з іншими речами.

Безпека

Потенційні загрози безпеки, що виникають в середовищі IoT, також можна розглядати з точки зору еталонної моделі. На кожному рівні моделі присутні загрози безпеки, як специфічні тільки для цього рівня, так і загальні для всієї моделі.

Так, на всіх рівнях моделі присутня загроза несанкціонованого доступу до додатка або пристрою. У разі виконавчих пристроїв несанкціонований доступ може привести до несанкціонованих дій самої речі.

На рівні додатку – це загрози витоку інформації, порушення цілісності даних і недоторканності приватного життя. На рівні мережі – загрози витоку даних про використання сигналізації та порушення їх цілісності[4].

На рисунку 1.2 представлена модель загроз безпеки IoT.

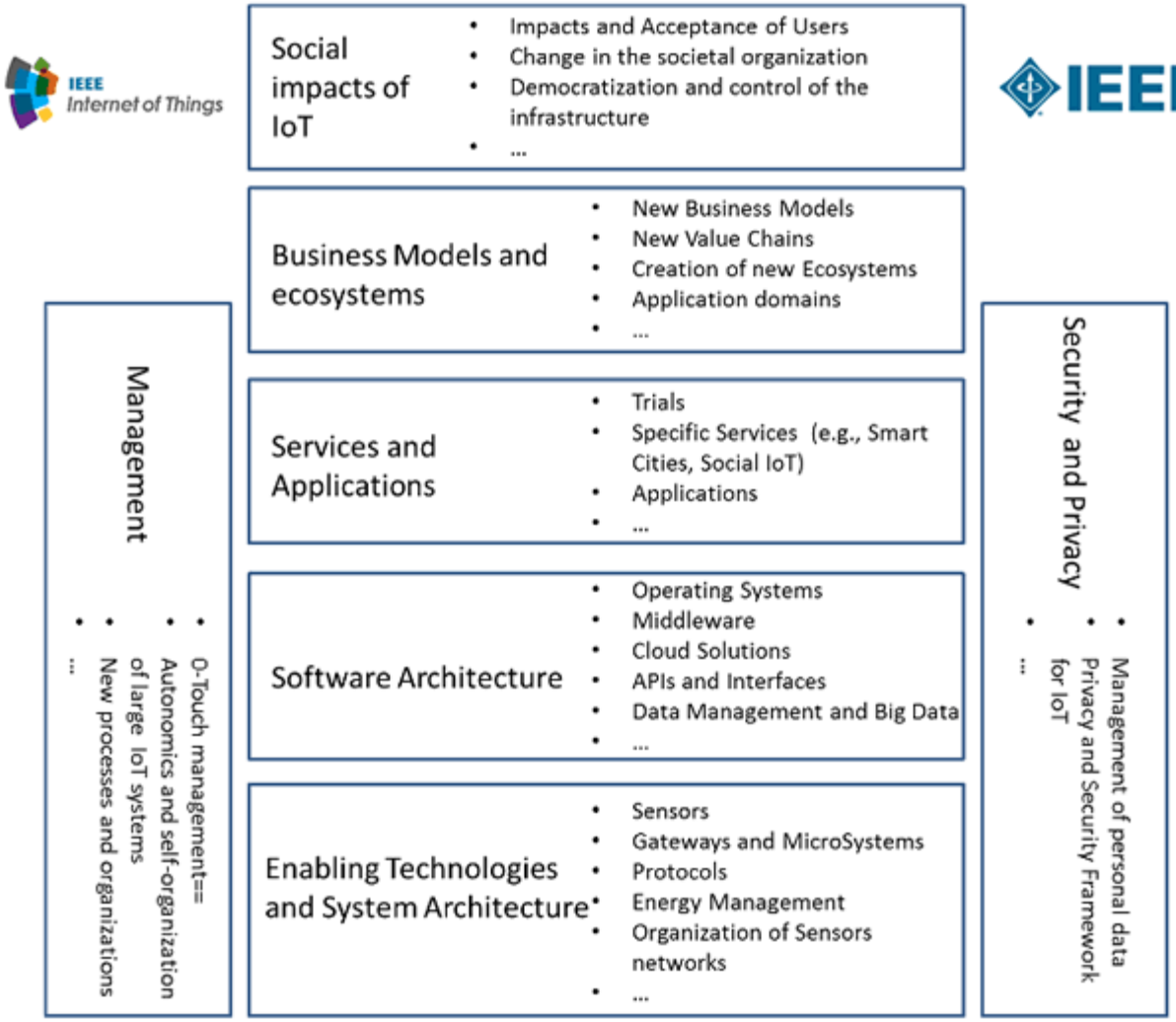


Рисунок 1.2 – Модель загроз безпеки IoT.

На рівні пристрою – загрози несанкціонованого розкриття, несанкціонованого контролю / управління, витоку даних, що зберігаються в пристрої, пошкодження їх цілісності.

Для нейтралізації описаних загроз безпеки застосовуються алгоритми авторизації та ідентифікації, проводиться шифрування переданих і збережених даних, проводиться аудит систем і застосовується антивірусне програмне забезпечення. Але не всі пристрої і додатки мають високу продуктивність, тому застосування криптостійкості алгоритмів не завжди є можливим.

Важливим моментом, на думку автора, з точки зору потенційних загроз також є аспект соціальних наслідків застосування IoT. По–перше, при взаємодії типу пристрій–пристрій роль людини вже в даний час обмежена.

А по–друге, в майбутньому загроза приватного життя буде виходити не від всезнаючого «клієнта», що відслідковує і реєструю кожен крок, а від сотень маленьких пристроїв, постійно втручаються в приватне життя.

Концепція IoT несе в собі величезний потенціал можливостей. Але поряд з цим виникає і цілий спектр загроз безпеки, в тому числі мають і соціальні наслідки.

Кінцевою метою розвитку IoT є створення проекцій для кожної фізичної речі в віртуальному просторі. Чим більше речей може контролювати IoT, тим більше можливостей він зможе надати. Якщо цей процес залишити без належного контролю, то, в кінцевому рахунку, у будь-якого реального об'єкта буде віртуальна копія, що представляє властивості фізичного об'єкта, але, можливо, володіє іншими здібностями у віртуальному світі.

Це призведе до появи централізованої системи, здатної до виробництва і управління великою кількістю даних. Тому виникає питання про те, хто буде управляти цією системою і до якого виду відносин між віртуальними об'єктами мереж це може привести.

1.3 Пілотні проекти Інтернет речей

Оскільки компанії все частіше починали інвестувати в технології Інтернету речей та масштабоване розгортання Інтернету речей, а не просто в пілотні проекти, швидко стало зрозуміло, що Інтернет речей як термін охоплює абсолютно різні реалії, які мають мало спільного.

Більшість галасу в Інтернеті речей зосереджувались на орієнтованих на споживача пристроях, таких як носимі пристрої або розумні домашні пристрої. Тим не менше, ми не можемо повторити це досить, існує величезна різниця між особистим фітнес-трекером та використанням IoT на промислових ринках, таких як виробництво, де IoT займає головне місце у баченні Індустрії 4.0 –IIoT (підключення до Інтернету речей або пристроїв з підтримкою Інтернету речей, такі як великі промислові роботи або логістичні системи IoT).

Ось чому для початку було розмежовано Індустріальний Інтернет речей та Споживчий Інтернет речей. Однак і тут траплялися перекриття і, зрештою, труднощі, як завжди, коли ви починаєте сегментувати реалії. Широкий спектр нових термінів було винайдено для пояснення різних існуючих та нових форм використання Інтернету речей: Інтернет робототехнічних речей, Інтернет медичних речей, список можна продовжувати.

У той же час деякі постачальники рішень Інтернету речей почали пропонувати альтернативні умови. Найвідоміший – це Інтернет всього Cisco, який мав на меті підкреслити роль людей, даних, процесів тощо. Хоча всі ці (і багато інших) зусиль намагалися зробити Інтернет речей більш відчутним, зрештою, звісно, що з 2016 до 2020 р.р. більшість людей та фірм (включаючи Cisco) просто знову починають говорити про IoT. Використання терміна "Індустріальний Інтернет речей" (або "Індустріальний Інтернет") також робить бренд для більш широкого контексту Індустрії 4.0, Інтернет речей – це частина реальності.

Індустріальний Інтернет речей (IIoT)

Інтернет речей, Інтернет всього, споживчий Інтернет речей, стільки термінів, що стає заплутаним.

Основне значення та додатки знаходять у так званому Індустріальному Інтернеті Речей або IIoT. Однією з головних причин, чому почали говорити про Індустріальний Інтернет речей, є відрізнити його від більш популярного погляду в Інтернеті речей, оскільки він все частіше використовується в останні роки: споживчого Інтернету речей або додатки побутової електроніки, такі як носимі пристрої у підключеному контексті або програми розумного будинку.

Індустріальний Інтернет речей визначається Індустріальним Інтернет-консорціумом як «машини», комп’ютери та клієнти, що забезпечують інтелектуальні промислові операції з використанням передової аналітики даних для трансформаційних результатів бізнесу. Деякі люди в основному розглядають «важкі» галузі, такі як виробництво, нафтогазова промисловість, транспорт. Інші також додають «менш важкі» програми для розумних міст чи розумного сільського господарства. Іноді є дещо тонка грань, оскільки, звичайно, ви також можете мати дуже прості програми в розумних містах.

На рисунку 1.3 представлена модель елементів Індустріального Інтернет-консорціума.

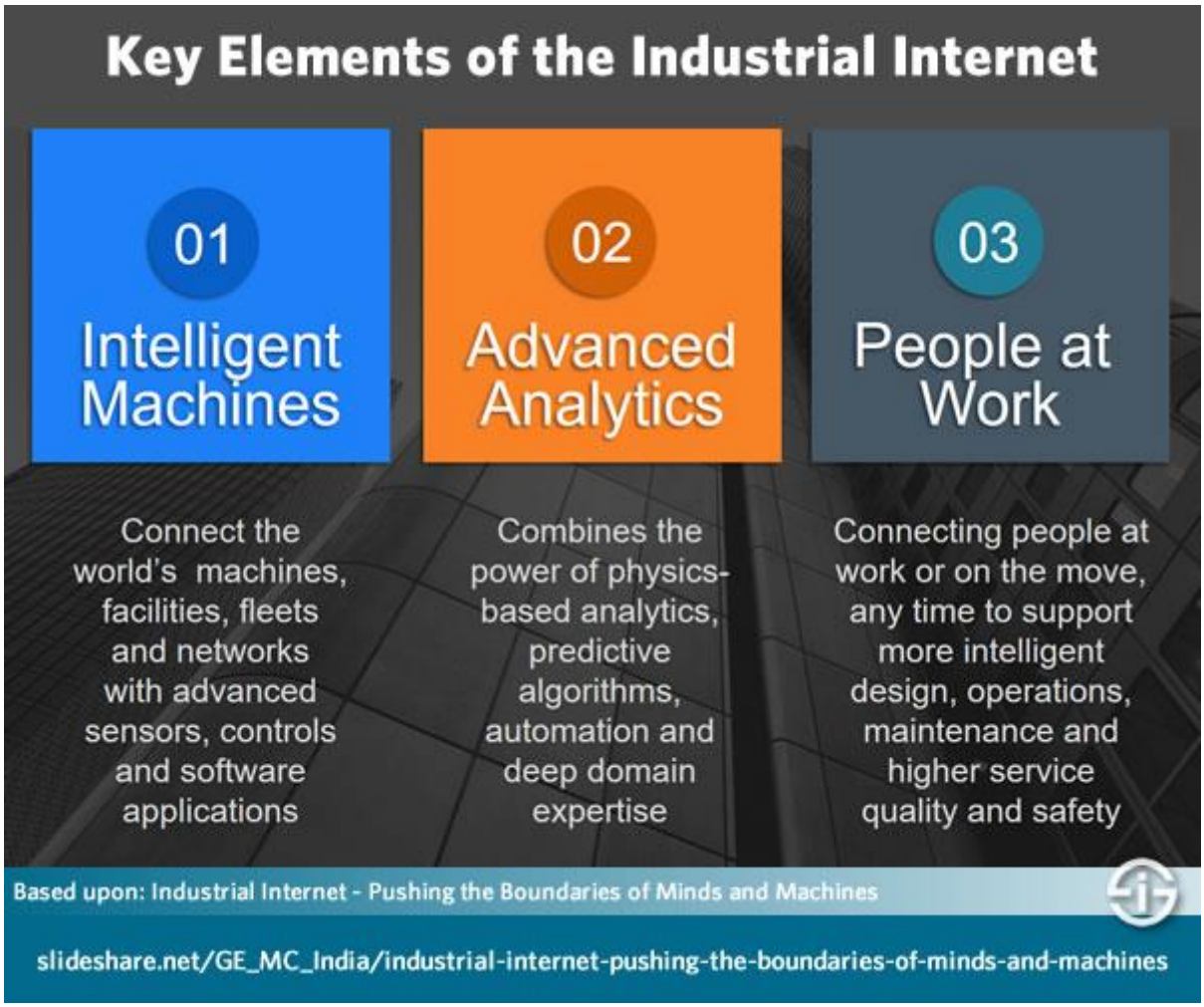


Рисунок 1.3 – Модель елементів Індустріального Інтернет–консорціума

У промисловому Інтернеті речей або IIoT вирішальне значення має згадана інтеграція (світів) IT (інформаційні технології) та OT (операційна технологія).

На даний момент IIoT є найважливішим сегментом Інтернету речей, набагато більше, ніж, наприклад, споживчі програми.

Промисловий Інтернет речей пов'язаний з Індустрією 4.0: усі програми Інтернету речей в Індустрії 4.0 є формами IIoT, але не всі випадки використання IIoT стосуються галузей, які класифікуються як Індустрія 4.0.

Типові випадки використання Індустріального Інтернету Речей включають інтелектуальні рішення щодо блискавки та інтелектуального руху в розумних містах, інтелектуальні машинні програми, програми промислового управління, випадки використання заводських підлог, моніторинг стану, випадки

використання в сільському господарстві, інтелектуальні мережі та застосування нафтопереробних підприємств.

Отже, навіть якщо цей термін є не стільки загальним, скільки Інтернет речей, він все одно охоплює багато потенційних додатків та випадків використання.

Переваги IIoT – індустріальні драйвери Інтернету речей

Багато організацій розглядають додатки IIoT, і багато хто вже розпочав роботу, звичайно, на тих ринках, які раніше рухались, таких як виробництво або нафта та газ. Але інші все ще чекають або не впевнені.

Згідно з дослідженнями IDG у 2019 році, 70 відсотків організацій все ще перебувають у стадії "розгляду", "ранніх обговорень" або "фази планування", як вказує інфографіка індустріальних драйверів Інтернету речей на рисунку.1.4.

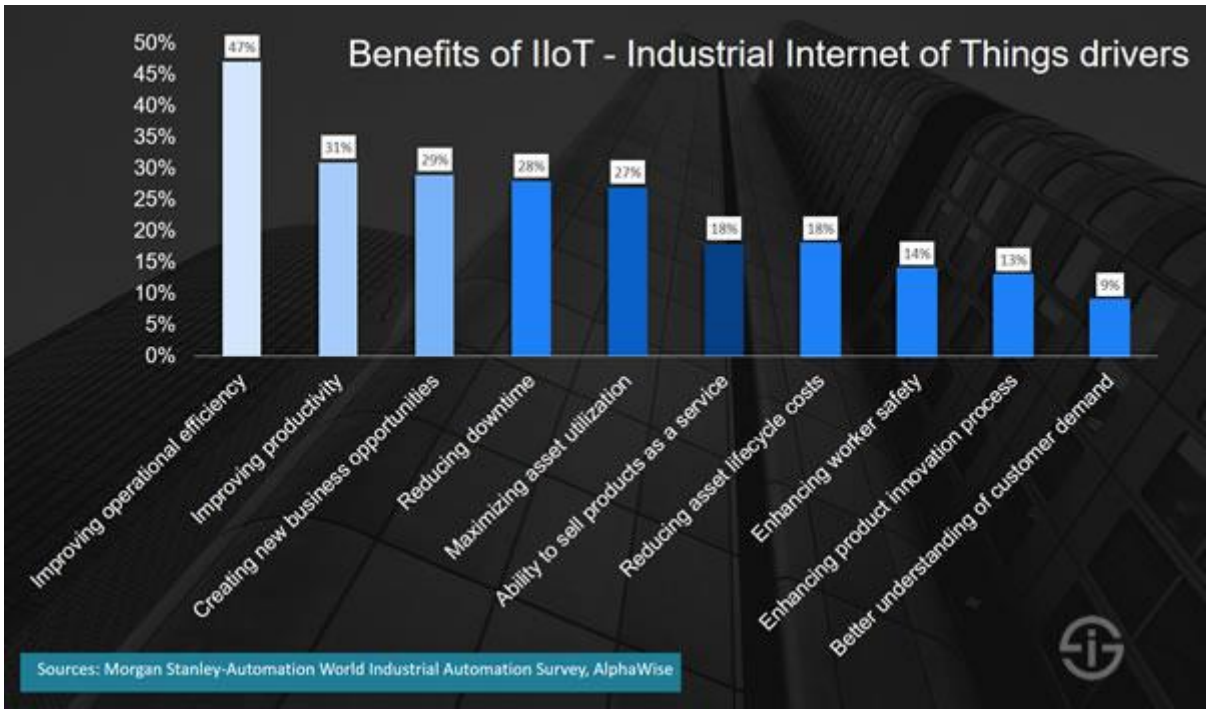


Рисунок 1.4 – Інфографіка індустріальних драйверів Інтернету речей

І це, незважаючи на безліч можливостей, зокрема щодо безперервності бізнесу, ефективності, зменшення витрат тощо. Але є також багато викликів, що стосується промислових даних.

Споживчий Інтернет речей (CIoT, Consumer Internet of Things)

Так чи інакше 5 років тому споживачі не бачили, що Інтернет речей буде означати для їхнього приватного життя. Сьогодні вони все частіше це роблять: не лише тому, що їх цікавить технологія, а головним чином тому, що на ринок вийшов ряд нових додатків та підключених пристроїв.

Ці пристрої та їх можливості привертають велику увагу практично на кожному інформаційному порталі та web–сайті, які охоплюють нові технології. Носії та розумні годинники та розумні домашні програми (причому Google Nest є популярним, але, безумовно, не першим), прикладів достатньо багато.

Хоча кажуть, що виникає певна втома від технологій, поєднання програм у споживчому контексті та захоплення технологіями, безсумнівно, відіграє роль у зростанні уваги до Інтернету речей. Цей аспект захоплення споживачів перевершує всі реальні можливості, коли вони починають впроваджуватися, а також контекстуальні та технологічні реалії, що робить Інтернет речей одним із багатьох поширених технологічних брендів. Очевидно, що споживчий ринок Інтернету речей не просто обумовлений захопленням новими технологіями: їх виробники сильно натискають на ринок, оскільки прийняття означає новинні можливості для бізнесу з ключовою роллю передачі даних.

1.4 Споживчий Інтернет речей та побутова електроніка

Що стосується Інтернету споживчих речей, можна знаходитися в реальності побутової електроніки.

Хоча деякі програми в цьому просторі вже є популярними (наприклад, фітнес та особисте здоров’я), реальне зростання все одно має настати.

Нижче наведено кілька проблем із споживчою електронікою, на які слід звернути увагу спочатку:

– Розумніші пристрої. Споживачі чекають розумніших поколінь носіїв та продуктів послуг Інтернету речей, які можуть виконувати більше функцій, не будучи надто залежними від смартфонів, як це відбувається з багатьма такими пристроями сьогодні (перші покоління розумних годинників, яким потрібен смартфон).

– Безпека. Споживачі ще не довіряють Інтернету речей, який ще більше посилюється порушеннями та висвітленням цих порушень. Більше того, мова йде

не лише про безпеку пристроїв, а й, зокрема, про безпеку протоколів передачі даних із низьким рівнем передачі даних (та операційних систем Internet of Things). Приклад: стандарт домашньої автоматизації Zigbee було виявлено легко зламати в листопаді 2020 року.

– Дані та конфіденційність. Окрім проблем безпеки, існують також проблеми щодо використання даних та конфіденційності. Відсутність довіри до даних, конфіденційності та безпеки вже була проблемою до цих порушень, як показано в огляді розвитку побутової електроніки.

– «Вагома причина купувати». Нинішні пристрої, які класифікуються як побутові прилади Інтернету речей, все ще відносно дорогі, «німі» та важкі у використанні. Також їм часто не вистачає унікальної вигоди, яка змушує споживачів масово купувати їх.

Тому цифрові технології стають все доступніше і є основним елементом підвищення продуктивності праці, впровадження інновацій та підвищення якості життя. Все більше найрізноманітніших пристроїв, що використовують технологію міжмашинної взаємодії –M2M, «machine to machine», підключаються до мережі Інтернет[3]. В рамках такого технологічного рішення використовується ряд спеціалізованих пристроїв, які збирають інформацію телеметричного характеру.

Ключовою властивістю таких систем є їх індустріальна спрямованість і необхідність участі людини в прийнятті управлінських рішень. Саме цей аспект сильно обмежує застосування M2M-технологій і привів до вдосконалення концепції і появи поняття «Інтернет речей» (рис.1.5).

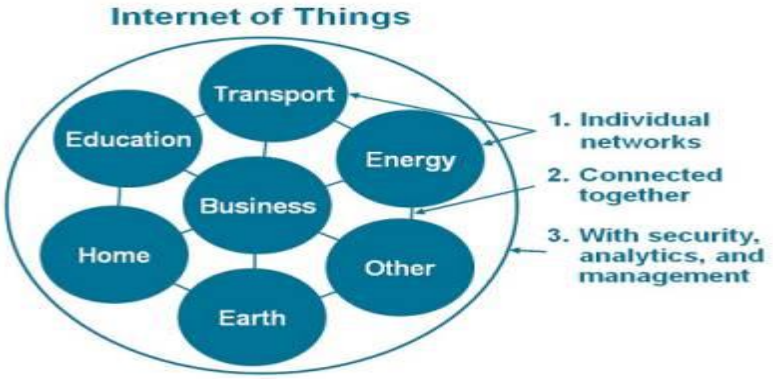


Рисунок 1.5 – Internet of Things

«Інтернет речей» або, як його ще називають, Мережа Мереж є мережею різноманітних підключених до Інтернету пристроїв, що реалізують різні моделі взаємодії – «Річ – Річ» (Thing–Thing), «Річ – Користувач» (Thing–User) і «Річ – Web -Об'єкт »(Thing-Web Object). З'єднання «розумних речей» (Smart Things) в єдину мережу надає критично важливі якісні зміни для розвитку людської життєдіяльності.

Інтернет речей складається з слабко пов'язаних між собою розрізнених мереж, кожна з яких була розгорнута для вирішення своїх специфічних завдань. Наприклад, в сучасних автомобілях працюють відразу кілька мереж: одна управляє роботою двигуна, інша – системами безпеки, третя підтримує зв'язок і т.д. В офісних і житлових будівлях також встановлюється безліч мереж для управління опаленням, вентиляцією, кондиціюванням, телефонним зв'язком, безпекою, освітленням. У міру розвитку Інтернету речей та багато інших мереж будуть підключатися один до одного і набувати все більш широкі можливості в сфері безпеки, аналітики та управління (див.рис. 1.1). В результаті Інтернет речей придбає ще більше можливостей відкрити людству нові, більш широкі перспективи.

Примітно, що ця тенденція відображає те, що спостерігалося на ранніх етапах розвитку мережевих технологій. В кінці 1980-х – початку 1990-х років Cisco сформувалася як велика компанія саме завдяки своїм зусиллям щодо встановлення зв'язку між різнорідними мережами за допомогою многопротокольної маршрутизації, яка в кінцевому підсумку зробила протокол IP загальноприйнятим мережевим стандартом. У тому, що стосується Інтернету речей, історія повторюється, але в значно більших масштабах.

З'єднання розумних об'єктів в єдину мережу за допомогою IP-протоколу утворює мережу мереж, продукує велику кількість найрізноманітніших телеметричних даних. Цінність одержуваної інформації цілком визначається протоколами прикладного рівня, що працюють поверх мережі.

Однією з головних передумов до цього є перехід до використання в мережі Інтернет–протоколу IPv6, що дає можливість надати виділений унікальну адресу кожного підключеного пристрою. При цьому основну частину з підключаються об'єктів будуть складати різноманітні спеціалізовані пристрої, що мають в своєму складі мікроконтролер з різними платами розширення: модуль передачі даних,

модуль пам'яті, засоби вимірювання (датчики) і засоби ідентифікації. Для управління пристроєм, обробки і передачі даних на контролері використовується операційна система реального часу, що відповідає за збір і первинну обробку даних для мінімізації трафіку.

Повсюдне поширення розумних речей робить нераціональним використання традиційної моделі «Клієнт – Сервер» з точки зору обміну трафіком. У місцях їх знаходження часто дуже важко забезпечити високошвидкісні канали з низькою затримкою, а власна обчислювальна потужність дозволяє проводити необхідну обробку даних, реалізуючи концепцію «хмарних обчислень» (Fog Computing). Функціональним елементом хмарних обчислень є мікроконтролери, які об'єднуються в розподілену обчислювальну мережу. Їх завдання здійснювати зберігання та обробку інформації, що надходить, надаючи обчислювальні потужності для різноманітних прикладних задач, які здійснюють адміністрування систем без участі людини.

Канали інфокомунікацій використовуються у конвергентних мережах на базі протоколу IP, а місця установки датчиків настільки різноманітні, що використання провідної інфраструктури дуже обмежене. Їх підключення все частіше здійснюється за допомогою безпроводових технологій. До недавнього часу для цього використовувалися традиційні технології для користувальницької передачі даних – WiFi, 2G, 3-4G.

Зараз в технології міжмашинної взаємодії для зв'язку все ще застосовують ієрархії протоколів, які розроблені IEEE (Institute of Electrical and Electronics Engineers).

Відповідно до стандартних принципів всі безпроводові мережі сьогодні прийнято ділити на чотири типи: персональні WPAN (Wireless Personal Area Network), локальні WLAN (Wireless Local Area Network), міські WMAN (Wireless Metropolitan Area Network) і глобальні WWAN (Wireless Wide Area Network) фіксовані та безпроводові мережі.

На вертикальних ринках вже використовується ряд технологій – C–UNB (Cooperative Ultra Narrowband), LoRa (Long Range), але найперспективнішими для Інтернету речей є технології EC–GSM (Extended Coverage GSM) і NB–CIoT (Narrowband Cellular IoT), які передбачають використання мереж мобільного зв'язку. Для цієї мети планується виділяти смуги частот нижче використовуваних

в мобільних мережах, і операторам необхідно тільки додати відповідні трансивери на базових станціях і оновити програмне забезпечення (ПЗ).

На рисунку 1.3 представлені варіанти підключення IoT до існуючих мереж.

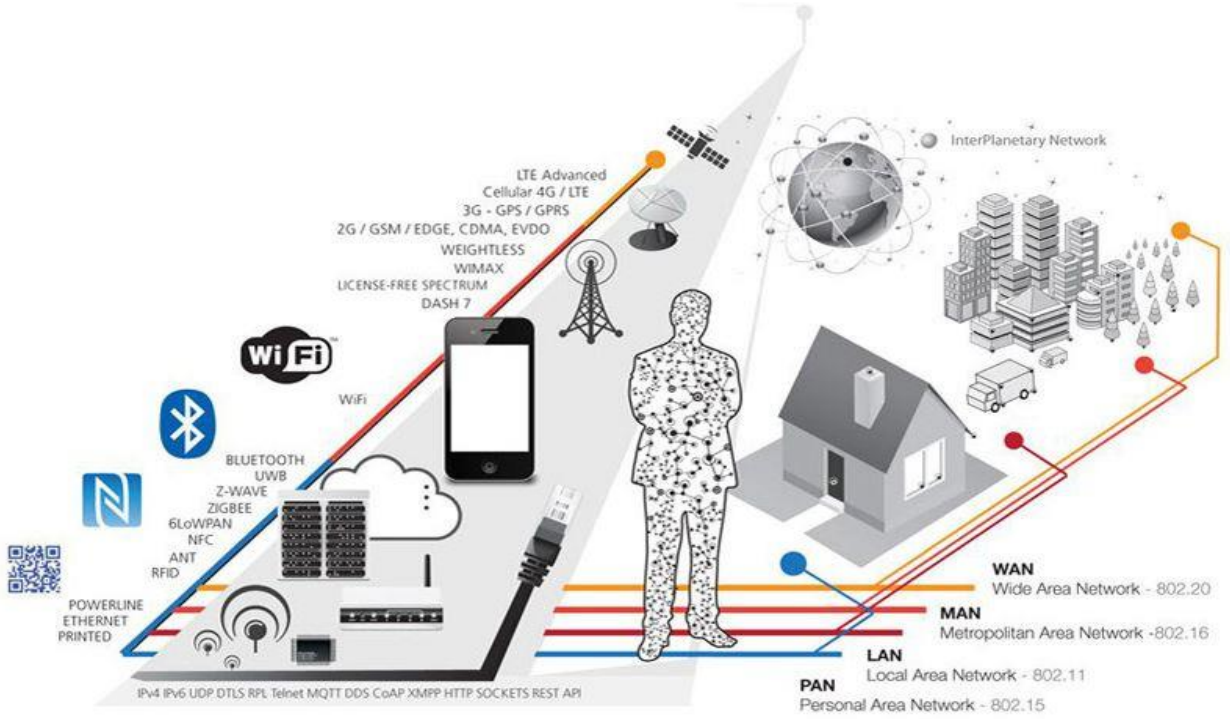


Рисунок 1.3 – Варіанти підключення IoT до існуючих мереж

IT-корпорація Hewlett Packard Enterprise (HPE) опублікувала результати дослідження, присвяченого Internet of Things (IoT). Для складання звіту було опитано близько 3100 керівників і фахівців з інформаційних технологій в 20 країнах світу.

За даними HPE, приблизно 57% компаній вже впровадили IoT–технології, а до 2020 року ця частка може зрости до 85%. Багато (88%) з тих, хто вже користується Інтернетом речей, відзначили швидку окупність інвестицій в ці проекти.

У 80% медичних установ, що вже освоїли Інтернет речей, відзначили зростання інновацій, наприклад, пов'язаних з наявністю постійного доступу до медичних даних пацієнтів і можливістю оперативної постановки діагнозу.

Майже таке ж респондентів (76%) відзначили, що Інтернет речей підвищив прозорість процесів, що проходять в організаціях, спростивши спільну роботу

медичного персоналу. 73% закладів охорони здоров'я змогли скоротити витрати за рахунок IoT–рішень (рис 1.4).

Можливостями Інтернету речей користуються близько 72% комерційних організацій. Найчастіше це виражено в застосуванні «розумних» систем кондиціонування і освітлення (56% опитаних працюють з ними) і персональних мобільних пристроїв (51%).

Крім того, деякі компанії підключені до локаційним IoT-сервісів і служб контролю комунальних ресурсів (електроенергії і т. П.).

Стверджується, що застосування IoT-технологій дозволило підвищити ефективність IT-відділів у 78% компаній.

Інтернет речей все сильніше проникає і в державні органи. Близько 42% серед них використовують IoT–нововведення, в тому числі в системах безпеки (57%), вуличне освітлення (32%) і автотранспорті (20%). 70% держустанов заявили, що Інтернет речей допоміг підвищити прозорість роботи організації в цілому. [5].

Рисунок 1.4 – Можливості Інтернету речей технологій

Майже всі компанії (97%), які взяли участь в опитуванні, висловили впевненість в тому, що впровадження IoT–технологій окупиться протягом п'яти років.

IoT Analytics: число IoT–платформ в світі досягло 450.Кількість IoT–платформ в усьому світі за минулий рік зросла на 25% і склало 450 – такі дані наводяться в звіті Global IoT Platform,2019, підготовленому IoT Analytics. [6]

Ринок IoT–платформ як і раніше стає більш насиченим і фрагментованим. Однак динаміка змінюється незважаючи на те, що продовжуємо спостерігати появу стартапів в цьому сегменті, більшість великих постачальників уже пропонують свої IoT–платформи. Ймовірно, що поява нових IoT–платформ від IT–гігантів стане рідкісним явищем.

За оцінками галузевих аналітиків, кількість IoT–платформ досягне 20–55 млрд одиниць до 2021 р.

1.5 Технологія IoT: хмарні, туманні та крайові обчислення

Оскільки стільки даних створюється і дедалі більше буде створюватися за допомогою Інтернету речей, децентралізовані способи формування цих даних потребують різних підходів, серед інших у способах їх транспортування, обробки та аналізу, управління (автоматизованими) діями.

Одним із таких підходів є обчислення туману, архітектура системного рівня (і форма граничних обчислень), яка розширює обчислювальні, мережеві та сховищні можливості хмари до краю мережі (рис.1.5).

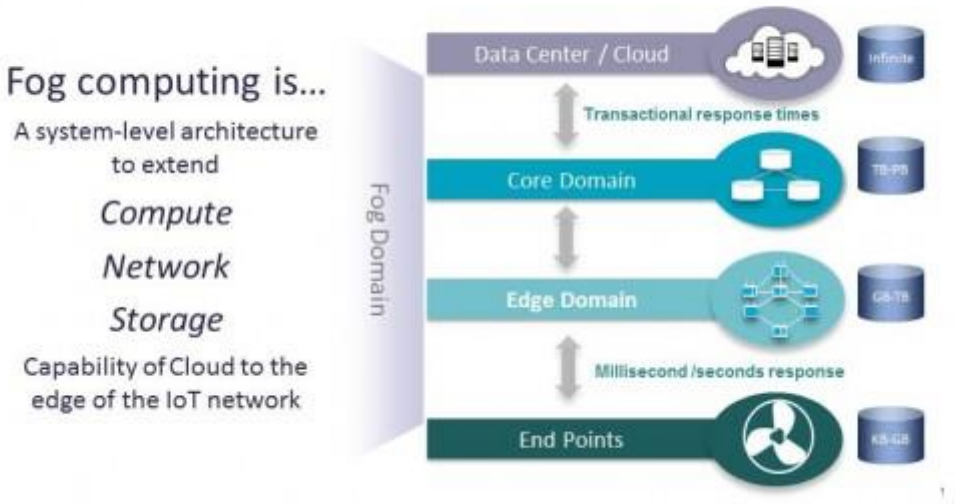


Рисунок 1.5 – Сховищні можливості хмари

Це особливо важливо, коли задіяна велика географічна область, коли дані потрібно обробляти надзвичайно швидко і дані збираються на крайньому краю мережі, як це називає Cisco, наприклад, на нафтових вишках або на суднах.

1.6 Інфраструктура, безпека IoT–платформ

Державні послуги IoT–платформ підводять до нової інфраструктури. Знову ж таки, це широка категорія, яку можуть організувати декілька партнерів з урядової екосистеми. Прикладом є інтелектуальна мережа, іншою IoT–платформ інтелектуальна дорога (у випадках, коли дорожня інфраструктура є національною або «спільною» справою). Також існують такі програми, як збір мита. Далі йде безпека. На національному рівні це, безумовно, також включає оборону та промислово–військовий комплекс. На більш регіональних рівнях такі програми, як розумне освітлення (існує зв'язок між освітленням громадських приміщень та злочинністю), різні форми контролю особи, спостереження тощо.

Нарешті, але не менш важливим є роль Інтернету речей у сповіщеннях про безпеку, боротьбі зі стихійними лихами тощо. Це призводить до охорони здоров’я, іншого сектору, який проходить цифрову трансформацію та тісно пов’язаний з урядом. Охорона здоров’я організована по–різному в усьому світі, від фінансування до медичного страхування та фактичного догляду. Однак завжди є урядова складова. Охорона здоров’я – ключовий ринок Інтернету речей.

Більше того, уряди відіграють певну роль у галузі охорони здоров'я, яку можна посилити, ініціюючи використання Інтернету речей та у співпраці з приватними державними партнерами. Те ж саме стосується і громадської безпеки. Приклад: співпраця між урядами та страховими компаніями, використовуючи телематику.

Вездесущність Інтернету речей в уряді – можливості, регулювання та проблеми. Існують насправді сотні способів, за допомогою яких уряди використовують і можуть використовувати Інтернет речей для покращення досвіду громадян, економії витрат і, не забуваючи, створення нових потоків доходів. Останнє є досить важливим, оскільки багато проектів IoT впливають

на фінансування міст. Простий приклад: якщо є ідеально працююче інтелектуальне рішення для паркування в місті, можна втрачати доходи з усіх очевидних причин. Отже, справа не лише в технологіях, а й у пошуку творчих способів перетворити розширений досвід громадян та громадянські послуги на глобальну картину, вигідну кожному.

Це вимагає часу, планування і, як можна собі уявити, враховуючи складність урядових екосистем, багато узгоджень та координації.

У деяких країнах та на наднаціональному рівні України проводяться ініціативи, і передбачається фінансування для цілого ряду «розумних» ініціатив, де часто також міста та державні установи можуть отримати вигоду в рамках проектів у визначеній зоні та порядку денному з чіткою метою . У той же час уряди дедалі активніше беруть участь у сфері безпеки та регулювання Інтернету речей, як уже зазначалося, завжди поруч[2].

Як приклад, підключений автомобіль майбутнього. Цілком очевидно, що уряди будуть до цього дуже залучені, і це менш очевидно, ніж може здатися. Тільки, щоб дати уявлення: у деяких країнах правила дорожнього руху вже є повною халепою через появу швидких електричних велосипедів. Можна собі уявити, що станеться, коли транспортні засоби будуть підключені та «розумні».

Інтернет речей у будівлях та спорудах

Інтернет речей відіграє важливу роль в управлінні об'єктами, серед іншого, включаючи розумні будівлі.

Інтеграція IT (Інформаційні технології) та OT (Операційні технології) відіграють важливу роль у цьому відношенні, як це було у швидкому піднесенні Індустріального Інтернету Речей. Завдяки Інтернету речей та цій конвергенції IT/OT менеджери будівель та спеціалісти з будівництва можуть реалізувати різні цілі. Вони залежать від характеру та обсягу об'єкта/будівлі.

Розумні будівлі є одними з найбільш швидкозростаючих міжгалузевих випадків використання Інтернету речей у період до 2023 року. Більше того, дослідження показують, що збір даних з будівель та інших споруд вже є високим. І останнє, але не менш важливе: Інтернет речей сильно впливає на ринок та розвиток BMS (Система управління будівлями). Згідно з дослідженнями, Інтернет речей є одним з основних факторів як витрат, так і розвитку ринку BMS, який, за

прогнозами, зросте на рівні CAGR–16,7 % між 2017 і 2023 роками, згідно з одним із багатьох досліджень, що стосуються цього ринку BMS .

Системи управління будівлями стають центрами підключення у світі дедалі більше кінцевих точок у будинках, які використовуються кількома системами управління будинками, але при цьому BMS відіграє центральну та сполучну роль, оскільки врешті-решт, це все про аналітику та дії, завдяки яким власник будівлі хоче мати центральну платформу, якою буде BMS, а де–факто це є вже в основному.

На рисунку 1.6 представлена платформа системи управління будівлями.

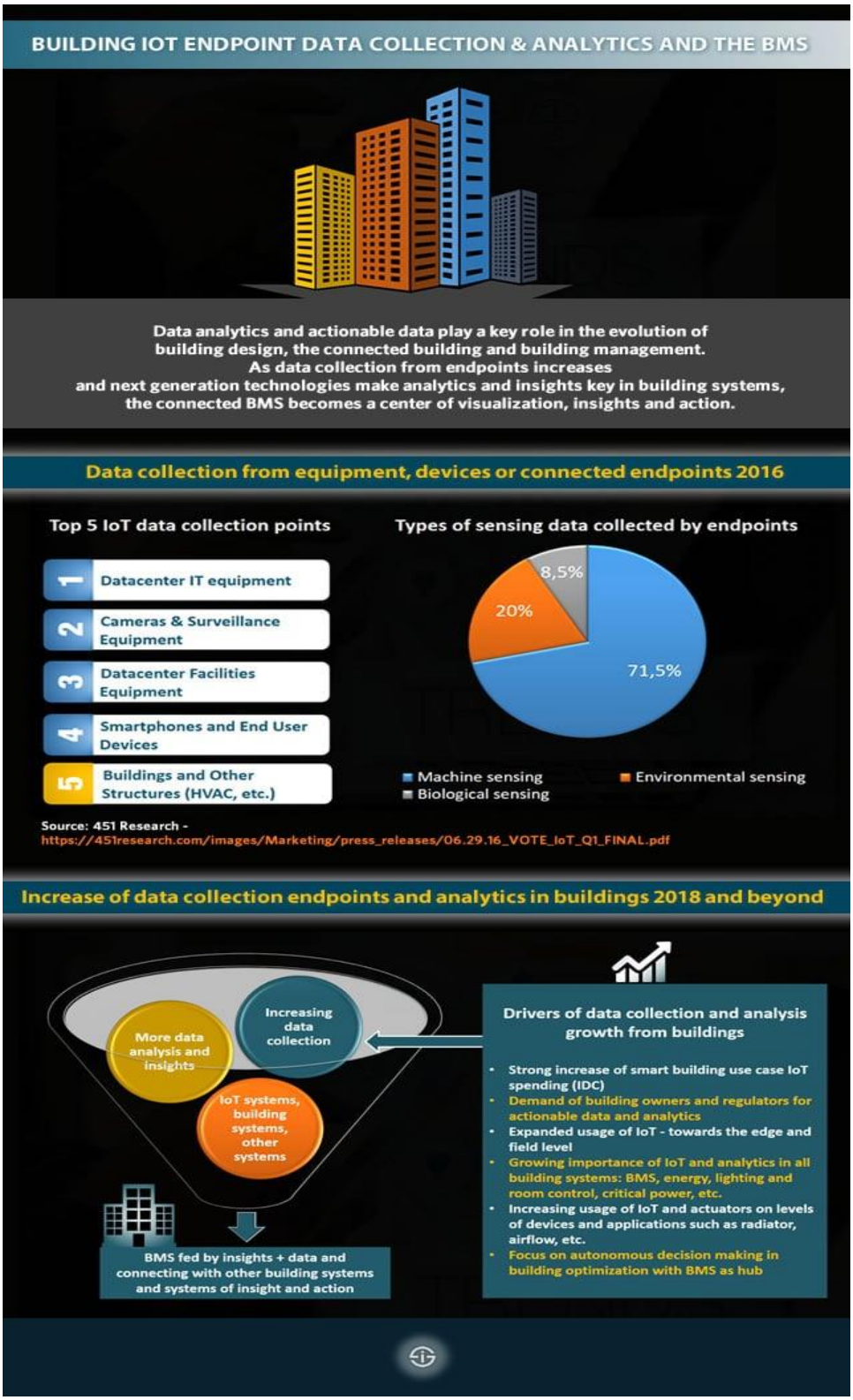


Рисунок 1.6 – Платформа системи управління будівлями

Використання даних з активів об’єктів, що підтримують IoT, а також нові платформи Інтернету речей та управління об’єктами із вбудованими можливостями призводять до можливостей та переваг у таких областях управління будівлею, як:

Використання даних з активів об’єктів, що підтримують IoT, а також нові платформи Інтернету речей та управління об’єктами із вбудованими можливостями призводять до можливостей та переваг у таких областях управління будівлею, як:

– Розумніші системи безпеки будівлі.

– Розумніше опалення, вентиляція та кондиціонування повітря (HVAC).

– Безпечніші та комфортніші/здоровіші робочі місця та будівлі.

– Оптимізація якості обслуговування об'єкта.

– Зниження витрат, також у контексті екологічного будівництва та зменшення споживання енергії та води.

– Краще планування, операційна ефективність та посилений розподіл ресурсів.

– Прогнозне технічне обслуговування та планування технічного обслуговування об'єкта.

– Контроль, конфігурація та регулювання обладнання.

– Управління будинками та автоматизація будівель.

– Енергоефективність.

– Контроль освітлення та приміщення, комфорт, вичерпний. Оскільки існують різні типи будівель, кожна зі своїми проблемами, інфраструктурою, технологіями та головним чином, ландшафт автоматизації та управління будинками дуже широкий.

Тільки в режимі управління світлом і кімнатою існує кілька елементів управління, таких як шторки, елементи управління змінного струму і буквально десятки інших.

Шлюзи IoT

Шлюзи IoT функціонують як мости між «речами» Інтернету речей, включаючи дані, які вони генерують за допомогою датчиків, з одного боку, та

мережі, хмари, платформи IoT, центри обробки даних і, зрештою, програми, що використовують ці та інші (агреговані та проаналізовані) дані , з іншого боку.

Шлюзи IoT відіграють важливу роль у шифруванні, дешифруванні, попередній обробці та навіть аналізі даних. Вони функціонують як розумні мости з набагато більшою кількістю типів та функцій[9].

Шлюзи IoT – це апаратне, програмне забезпечення або їх поєднання. Існує кілька типів шлюзів IoT, завдяки яким функції та можливості, які вони пропонують, збільшуються. Це пов’язано з тим, що дедалі більше пристроїв IoT, збільшується обсяг даних IoT і, нарешті, але не менш важливо, зміна способу аналізу даних до краю, як пояснювалося раніше.

Якщо у клієнта є більше даних, а також більш складні та різноманітні способи використовувати більше даних та створювати проекти IoT, це означає, що все технологічне середовище змінюється, щоб мати справу з різними робочими навантаженнями IoT там, де це найкраще підходить. Таким чином, шлюзи IoT виходять за рамки свого початкового обсягу як своєрідний фільтр і міст на перетині пристроїв IoT і даних, з одного боку, та мереж, хмарних служб або центрів обробки даних, де вони зазвичай зберігаються та / або аналізуються.

На рисунку 1.7 представлена структурна схема взаємодії шлюзу IoT з хмарними технологіями.

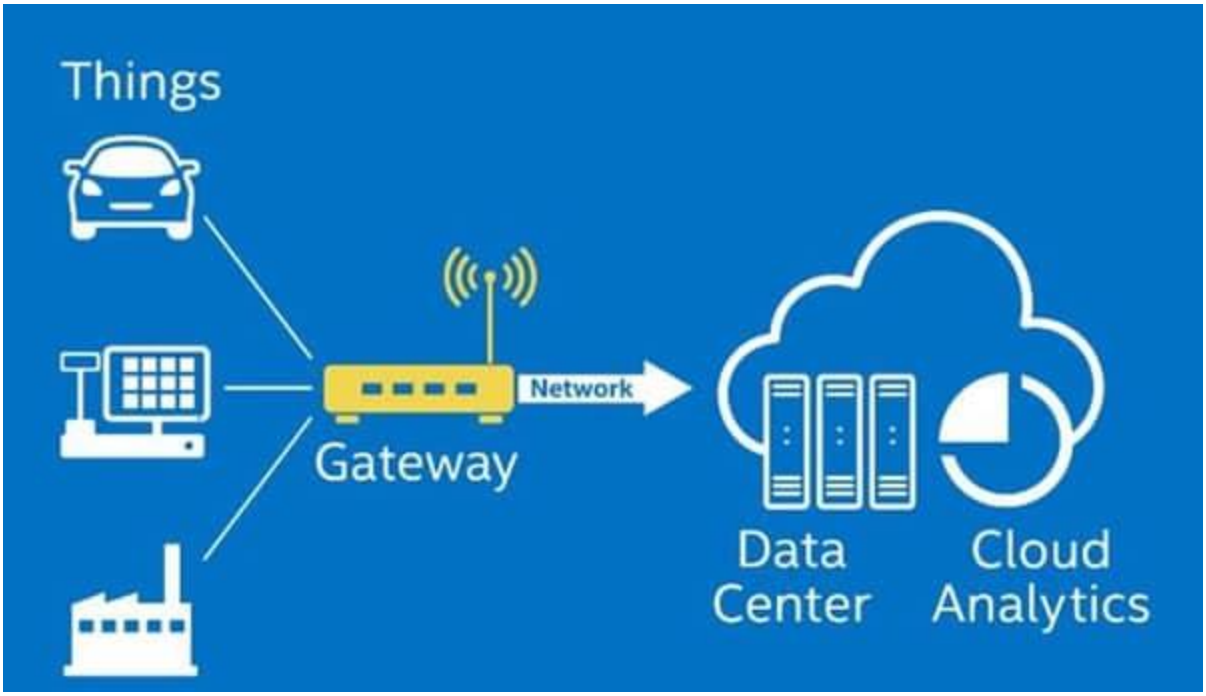


Рисунок 1.7 - Структурна схема взаємодії шлюзів IoT з хмарними технологіями

Типовою «новою» формою шлюзів IoT є граничний шлюз. Це пов’язано із згаданим зростанням обчислень і, отже, аналізом до хмари, мережі або центру обробки даних[3].

На практиці більшість даних IoT все ще аналізуються в центрах обробки даних згідно з дослідженнями. Однак трохи менше половини компаній займаються обробкою даних IoT (аналіз даних, агрегування даних або фільтрування даних на межі).

Комутація та мережеві технології

Комутація традиційно ділиться на рішення для персональної мережі PAN - (Personal Area Network), локальної мережі - LAN (Local Area Network), глобальна мережа – WAN (World Area Network), місцева мережа – MAN (Megapolis Area Network) та мережа мікрорайнів – NAN (Neighbourhood Area Network).

Для комутації з PAN до LAN та WAN або, скажімо, до Інтернету, потрібні шлюзи.

На рисунку 1.8 показано модель комутації споживача PAN до LAN, WAN та Інтернету.

Рисунок 1.8 – Модель комутації споживача PAN до LAN, WAN та Інтернету

Мережі Інтернету речей та зв’язок в процесі еволюції

Сьогодні різні рішення для зв’язку дозволяють це робити, але в не так далекому минулому потрібні були смартфони, мобільні мережі та інші рішення, які не були створені для IoT, не гарантували достатньої безпеки та якості.

Зростання таких компаній LPWAN, як Semtech (LoRA), Sigfox тощо, слід розглядати з тієї точки зору, коли основна увага була приділена достатній пропускній здатності, низькому енергоспоживанню тощо за нижчими цінами, ніж існуючі можливості. Побудова конкретних мереж, серед іншого, що зробило рішення, що не пов’язані зі стільниковим каналом, успішними.

Сьогодні цей ландшафт продовжує розвиватися та змінюватися. Нові стандарти 3GPP, перехід на 4G LTE в галузі та за її межами – ось деякі з цих еволюцій. Очікується, що протоколи та технології безпроводового Інтернету речей стануть більш важливими в мережевому рівні IoT в цілому. Однак це є і залишається реальністю, яка постійно змінюється.

Перехід до більш безпроводових з’єднань Інтернету речей та безпроводових мережевих технологій

Серед причин, чому технології безпроводових мереж стають все більш важливими, є їх гнучкість у порівнянні з проводовими мережами.

Очевидно, що різні технології в межах п’яти сегментів безпроводової мережі Інтернету речей, які представлені у інфографіці та мають різні діапазони, різні характеристики на інших рівнях, таких як швидкість передачі даних та багато іншого[5].

Щоб класифікувати декілька безпроводових технологій та протоколів на мережевому рівні можна зазначити, що, один із попередніх згаданих типів мереж додає NAN все більш важливий сегмент, безумовно, оскільки 4–а платформа наближається.

Класифікація безліч безпроводових протоколів та технологій Інтернету речей:

– мережа мікрорайнів – NAN

– безпроводова PAN: від Bluetooth та Zigbee до Z-Wave, Enocean та WirelessHART, щоб назвати декілька.

– безпроводова локальна мережа: різні варіанти Wi-Fi, включаючи Wi-Fic HaLow, який був представлений Wi-Fi Alliance для цілей IoT та DASH7.

– безпроводовий NAN: Wi-SUN та JupiterMesh.

– безпроводова глобальна мережа: будь-яка LPWAN, від неклітинної LPWA (Sigfox, LoRa тощо) до мобільниих технологій та стандартів у просторах 2G, 3G та 4G та поза ними.

На рисунку 1.9 зображена інфографіця п’яти сегментів безпроводової мережі Інтернету речей.

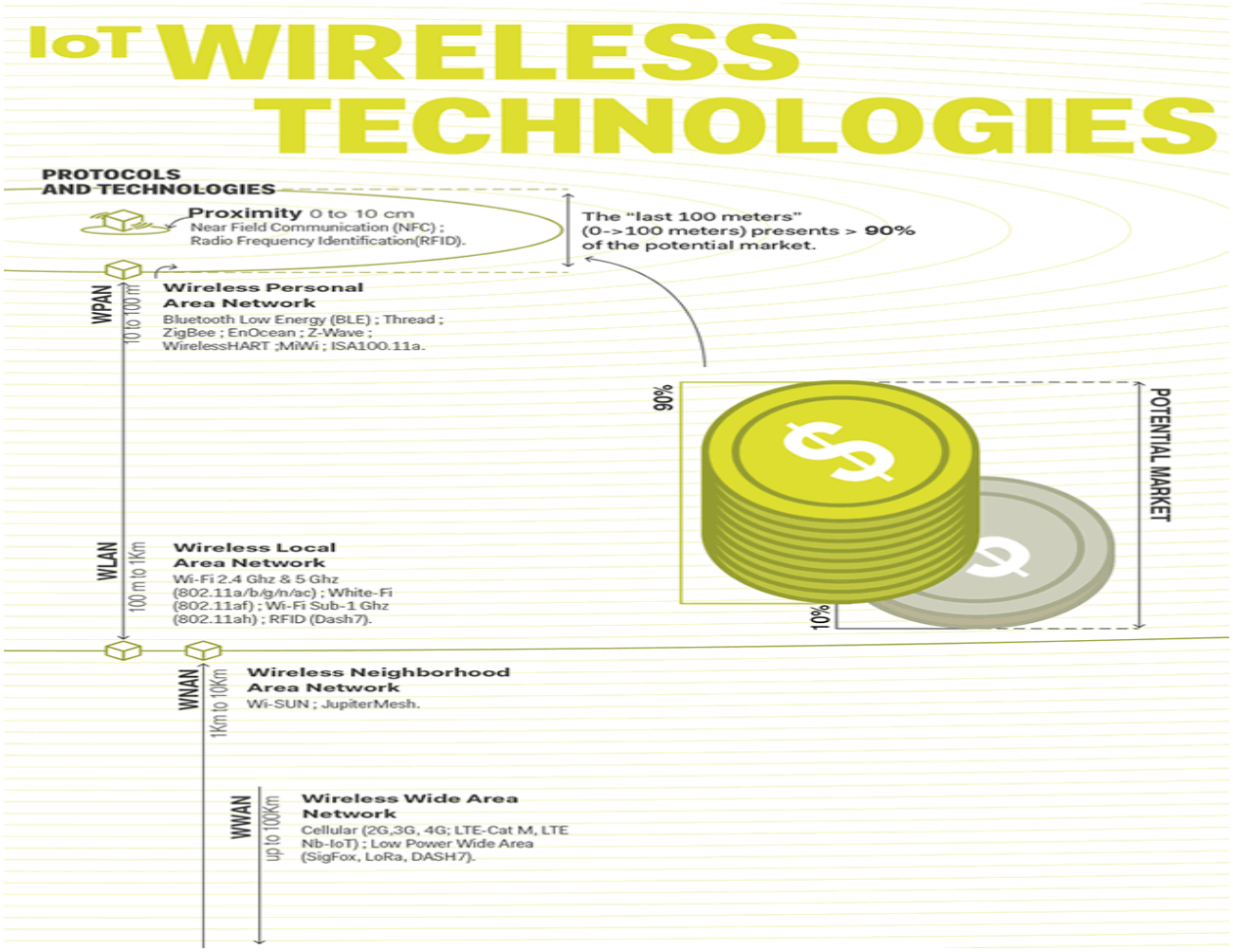


Рисунок 1.9 – Інфографіця п’яти сегментів безпроводової мережі Інтернету речей

Більше того, в рамках кожного типу рішень для підключення часто є різні гравці, кожен зі своїми характеристиками та специфікаціями.

Як приклад: у широкопотужному широкосмуговому підключенні (LPWA), що використовується в додатках, які потребують тривалого часу автономної роботи, мають обмежені потреби в даних і мають охоплювати ширшу область, існує кілька позаклітинних (поза ліцензованим мобільним спектром), серед яких LoRA, Sigfox, Ingenu та Weightless (SIG) є одними з найбільш відомих.

Однак є також новіші мобільні рішення (ліцензований спектр мобільних операторів) із знову різними формами: NB-IoT (NarrowBand IoT або CAT-NB1), LTE-M (CAT-M1) тощо. У мобільному просторі також потрібно згадати 5G, а також 3G тощо. Те саме різноманіття стосується і рішень інфокомунікації в умовах короткого радіусу дії тощо.

Ось чому кілька постачальників IT-рішень, оператори зв'язку та ін. на практиці пропонують поєднання рішень для комутації та конвергенції, щоб дозволити своїм клієнтам використовувати Інтернет речей для своїх конкретних потреб.

На цей час підключення IoT стає все більш стандартизованою, але стає не простіше, оскільки нові технології та стандарти інфраструктури Інтернету речей, такі як нові версії Bluetooth (Bluetooth 5, Bluetooth MESH), нові мобільні рішення, інші форми Wi-Fi тощо виникають поверх і без того величезні вимоги системи QoS та всіляких других рішень для комутації, заснована на різних стандартах, які використовуються в конкретному контексті, таких як Zigbee, Z-Wave та багато інших, включаючи підходи, що стосуються постачальників, безумовно, простору в розумному домі (рис.1.10).

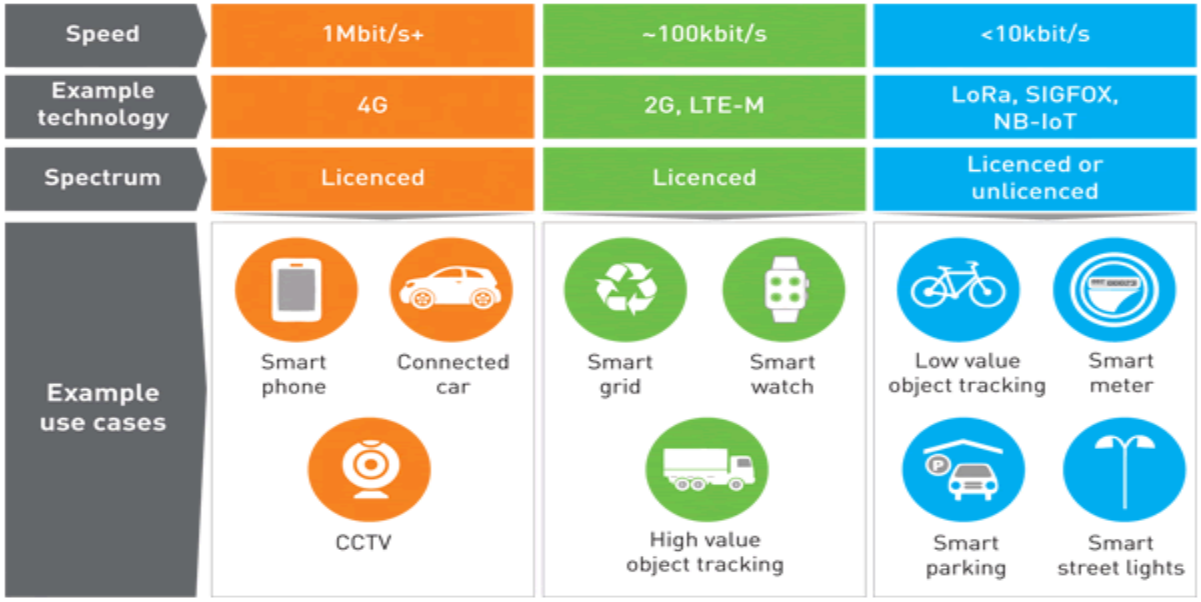


Рисунок 1.10 – Технології та стандарти для комутації та конвергенції інфраструктури Інтернету речей

Інтернет речей та безпека

Інтернет речей все ще є проблемою безпеки, хоча потрібно відрізнятися і не узагальнювати, а краще розглядати різні випадки.

Тим не менше, як у споживчих програмах, так і в промислових, існує багато питань, які потрібно вирішити.

Як контролери даних, так і обробники даних також мають кілька обов'язків щодо захисту та безпеки персональних даних, коли вони обробляються в проектах IoT у нових правилах. Більше того, є дедалі більше норм законодавства та дотримання нормативних актів, завдяки яким захищаються не лише персональні дані, а й регулюються IoT та нові технології, а безпека також займає центральне місце.

Безпека є викликом у споживчому та промисловому Інтернеті речей

Про споживчий IoT-простір, мабуть, найбільш задачі з точки зору безпеки, оскільки існує кілька питань і оскільки проблеми безпеки серйозно впливають на ринок.

Зі зростанням ринку побутової електроніки та наступним етапом зростання, який, як очікується, управління споживчими додатками в просторі Інтернету речей та пристроями, постачальники повинні вирішити ці проблеми безпеки.

Багато проблем безпеки в Інтернеті речей стосуються не лише простору побутової електроніки. У бізнес-додатках виклики безпеки гіперпов'язаної реальності Інтернету речей принаймні такі ж високі, не кажучи вже про вплив на IT-інфраструктуру та можливості передачі даних.

Загальний ландшафт автоматизації та управління будівлями існує ще задовго до існування Інтернету речей і складається з різних спеціалізацій, кожна зі своїх стандартів (наприклад, в контролі приміщень або BACnet в системах управління будинками), програм сертифікації зелених будівель (екологія та енергетика / екологічні норми є ключовими рушіями), а для партнерів OT-каналу, технологій, мереж, рішень і, звичайно, цілей (мета офісного приміщення, будівлі чи навіть кімнати для переговорів, що підтримує IoT, не є такою самою, як лікарня, навіть якщо є завжди перекривається).

Однак з Інтернетом речей ці світи зближуються (а стандарти вже перетворилися на IC). Це виклик і можливість для різних гравців, котрі мають усі свої навички, але рідко можуть запропонувати повну картину.

Наприклад, HVAC вимагає зовсім інших можливостей, ніж системи управління енергією або системи управління будівлею. Ось чому такі компанії, як Schneider Electric, розробили програми сертифікації партнерів та системних інтеграторів для різноманітних спеціалізацій інтелектуального будівництва, завдяки яким так звані EcoXperts (EcoXpert - це назва партнерської програми) можуть навчитися новим навичкам, зв’язатися, розширитися на нові домени та навіть піти багаторазові сертифікаційні значки, оскільки Інтернет речей все більше домінує у всіх сферах будівлі. Деякі гравці в цих сегментах мають більш механічний фон, інші електричний фон, а треті, такі як системні інтегратори, досвід налаштування та програмне забезпечення (ПЛК).

Серед цих постачальників оскільки Інтернет речей є:

– Експерти з управління світлом та приміщеннями.

– Експерти в дуже конкретних областях.

– Гравці в більш широкій галузі управління будівлями, переважно у великих будівлях.

– Підрядники електрики, які часто більше займаються меншими та середніми будинками, де вони можуть запропонувати розумні енергетичні рішення або, наприклад, спеціалізуються на автоматизації будинків.

– Фахівці з критичної потужності, яку ви зазвичай зустрічаєте в аеропортах, лікарнях та інших будівлях, де якість та надійність електроенергії є критично важливою у всіх сенсах.

– Менеджери служб безпеки.

2 ДОСЛІДЖЕННЯ ОСНОВНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПОСЛУГ ІНТЕРНЕТ-РЕЧЕЙ В ЛОКАЛЬНИХ МЕРЕЖАХ

2.1 Загальні положення

Будь–яку групу інфраструктури інфокомунікацій, з'єднаних системами передачі, можна назвати мережею передачі даних, а процес обміну ресурсами між комп'ютерами через мережу передачі даних – опорною мережею. У найпростішій формі мережа – це два або більше комп’ютери, з’єднані за допомогою syahfcnhernehb передачі для обміну даними. Концепція створення мереж почалася, коли хтось визначив, що існує потреба у спільному користуванні програмним забезпеченням та ресурсами даних, і що існує кращий спосіб це зробити, ніж зберігати дані на диску та буквально переходити з одного комп’ютера на інший.

До речі, цю ручну техніку переміщення даних на дисках іноді називають мережею кросівок. Найважливішими міркуваннями мережі передачі даних є продуктивність, швидкість передачі, надійність та безпека. Програми, що працюють у сучасних комп’ютерних мережах, сильно відрізняються від компанії до компанії.

Мережа повинна бути розроблена з урахуванням передбачуваного додатка. Конкретний додаток впливає на ефективність роботи мережі. Кожна мережа має обмежену пропускну здатність. Тому дизайнери та інженери мереж повинні знати про тип, частоту інформаційного трафіку та методи захисту інфраструктури в мережах.

При проектуванні інфраструктури мереж ((LAN/WAN/MAN/GAN) пов’язано багато факторів, зокрема такі:

1. Цілі інфраструктури, які визначені організаційним управлінням.
2. Безпека інфраструктури.
3. Вимоги до безперебійної роботи інфраструктури.
4. Вимоги до часу відгуку інфраструктури.
5. Інфраструктурніі та ресурсні витрати.

На рисунку 2.1 представлені основні компоненти інфраструктури мереж (LAN/WAN/MAN/GAN).

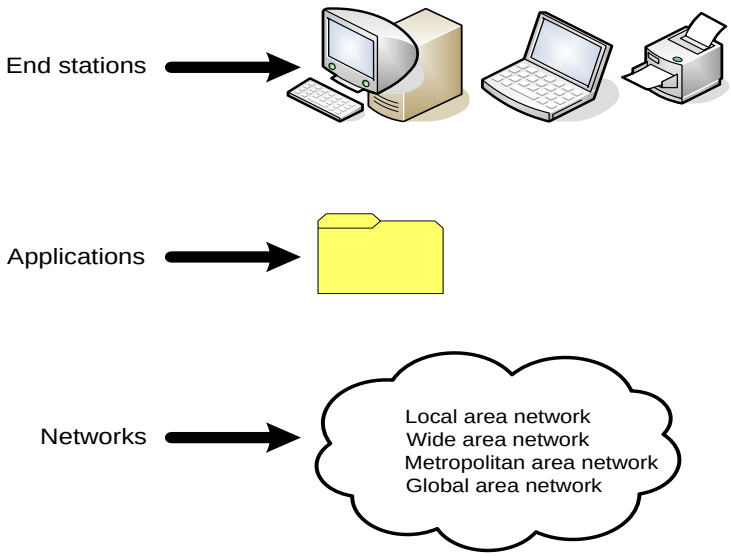


Рисунок 2.1 – Основні компоненти інфраструктури мереж (LAN/WAN/MAN/GAN)

2.2 Основні напрямки забезпечення безпеки архітектури Інтернету речей в локальних мережах

Все частіше стаються випадки злому пристроїв і їх використання в шкідливих цілях, а всі питання безпеки вирішуються індивідуально кожним виробником пристроїв і програмного забезпечення для локальних мереж. З огляду на широту поширення розумних об'єктів і ускладнення цільових атак, не дивно, що посилена увага в розробці протоколів приділяється безпеці.

З'єднання розумних об'єктів в єдину локальну мережу за допомогою IP-протоколу утворює мережу мереж, продукує велику кількість найрізноманітніших телеметричних даних. І цінність одержуваної інформації цілком визначається протоколами прикладного рівня, що працюють поверх локальної мережі.

Головним завданням при цьому є однозначна ідентифікація кожного елемента локальної мережі. З огляду на необхідну розрядність найкраще для цього підходить унікальний IPv6 адресу, що виділяється кожному пристрою в сучасних локальних мережах.

Ідентифікатор використовується не тільки для маршрутизації пакетів, але і для зіставлення з фізичними параметрами властивими пристроїв (mac-адресу, RFID, Electronic Identification (EID), QR-кодами).

Розумні об'єкти локальних мереж що володіють унікальним ідентифікатором, в залежності від конструкції, здатні не тільки передавати потоки даних, що збираються сенсорами, а й здійснювати передачу команд для зміни стану підключених до них пристроїв.

Протоколи взаємодії між цими компонентами є стеком добре зарекомендували себе стандартів, адаптованих для використання через низько швидкісні канали. Обмін повідомленнями працює за схемою видай/підпишись (publish/subscribe). Для цього виділяється спеціалізований «сервер» для передачі інформації – брокер. Вся передана інформація поділяється за напрямками на різні канали. Різноманітні датчики передають інформацію про різних фізичних величинах по відповідних каналах, в той час як споживачі локальних мереж підписуються на їх отримання, дуже гнучко обмінюючись необхідною інформацією.

Описаний принцип набув широкого поширення в цілому ряді протоколів – MQTT (MQ Telemetry Transport), XMPP (Extensible Messaging and Presence Protocol), AMQP (Advanced Message Queuing Protocol) [6].

Найбільш цікавим є протокол CoAP (Constrained Application Protocol). Він є адаптацією протоколу Web (web transfer protocol) для роботи за технологією межмашинного взаємодії. Він не тільки добре інтегрується з HTTP, а й підтримує адміністрування підключених пристроїв локальної мережі [6].

Система управління відповідає за конфігурацію, оновлення програмного забезпечення та моніторинг роботи обладнання локальної мережі. Можливості управління розумними об'єктами істотно менше в порівнянні з «класичними» пристроями (маршрутизаторами, комп'ютерами, серверами) і мають свою специфіку. Для цих цілей розроблено ряд стандартів, які працюють за технологією Клієнт – Сервер – CWMP, OMA-DM, Lightweight M2M [6].

Заходи щодо забезпечення безпеки можна умовно розділити за чотирма напрямками – підключення, ідентифікація, шифрування трафіку і безпеки додатків в локальної мережі.

Збереження цілісності та конфіденційності даних досягається застосуванням шифрування для аутентифікації і збереження цілісності повідомлень. Процедура передбачає підтвердження даних користувача і ліквідності використовуваних сертифікатів, що досить складно реалізувати в глобальних масштабах, тому виробники часто жорстко вбудовують облікові дані в програмно-апаратний комплекс. Ця інформація дозволяє чітко ідентифікувати пристрій, але не годиться для забезпечення цілісності даних. На транспортному рівні питання безпеки передачі даних вирішується в рамках протоколів Transport Layer Security (TLS) і Datagram TLS (DTLS) шляхом створення захищеного тунелю для додатків. Спрощена схема роботи протоколів зображена на рисунку 2.2 [7].

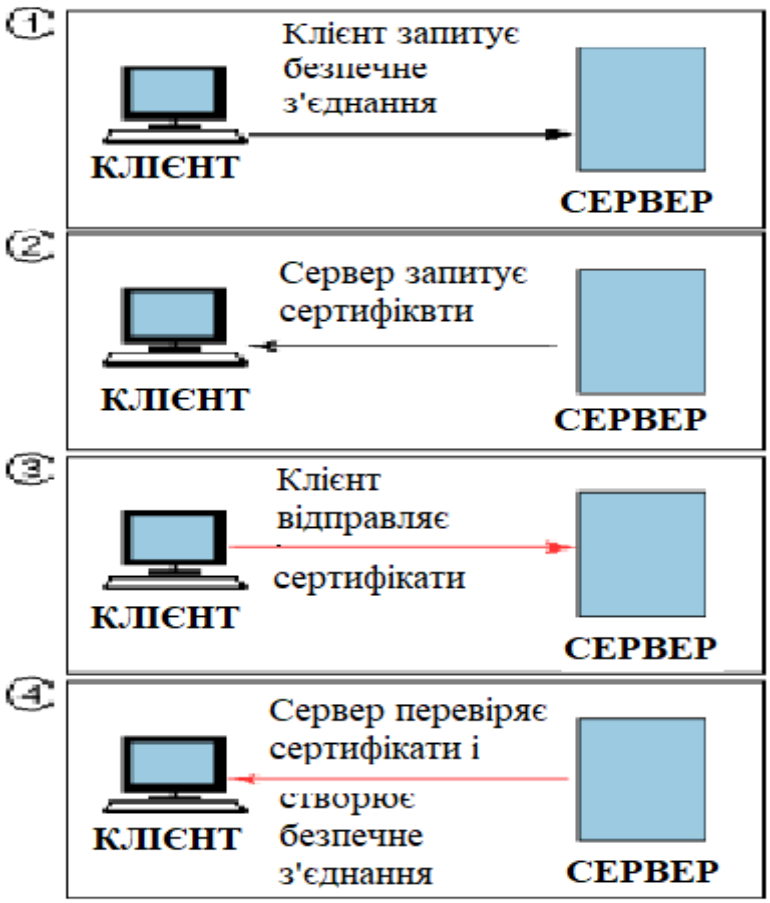


Рисунок 2.2 – Схема роботи протоколу Transport Layer Security

Але незважаючи на це, додатки є найбільш вразливою частиною рішення. Їх безконтрольне поширення становить серйозну загрозу. Надання розподіленої

платформи для обробки даних різними додатками – одна з особливостей архітектури Інтернету речей в локальних мережах, і основні тенденції в удосконаленні протоколу їх безпечного підключення OAuth 2.0 Internet of Things – виявлення розумних речей і їх аутентифікація, використання цифрових ідентифікаторів і централізоване управління доступом до ресурсів. Майбутнє, наприклад, глобальних хмарних обчислень цілком залежить від можливості взяти процеси під контроль і забезпечити безпечну самостійну конфігурацію розподілену інформаційну локальну мережу.

2.3 Особливості забезпечення безпеки Інтернету речей в локальних мережах

Впровадження повсюдного Інтернету речей – це все-таки віддалена перспектива. Розумна держава, розумні міста і навіть розумний будинок на базі локальних мереж – поки ще проблема для багатьох клієнтів. Впровадження Інтернету речей відбуваються не в глобальних масштабах, а в середині корпоративних та локальних мережах компаній.

Технологія розумних речей здатна підвищити продуктивність праці в першу чергу в виробничому сегменті, логістичному бізнесі, транспортних і енергетичних компаніях. Складність впровадження полягає в тому, що жоден виробник не має в своєму складі закінченого рішення, що включає всі компоненти. Необхідно використання великої кількості систем від різних виробників і від їх правильного підбору, інтеграції та захисту залежить те, наскільки точно реалізоване рішення буде відповідати завданням і вимогам конкурентного середовища.

У віддаленій перспективі варто очікувати появи єдиного цілого, що складається з традиційних технологій для роботи з даними і з промисловим систем управління (ICS) і автоматизованих систем диспетчерського управління та збору даних (SCADA). Можливо, в кінцевому підсумку це будуть кіберфізичні системи або навіть соціальні кіберфізичні системи.

Кіберфізичні системи (Cyber-Physical-System) – це системи, що складаються з різних природних об'єктів, штучних підсистем і управляючих контролерів, що дозволяють уявити таку освіту як єдине ціле. У CPS забезпечується тісний зв'язок і координація між обчислювальними і фізичними ресурсами.

Область дії CPS поширюється на робототехніку, транспорт, енергетику, управління промисловими процесами і великими інфраструктурами. Соціальні кіберфізичні системи Cyber-Physical-Social Systems (CPSS) об'єднують фізичний, кібернетичний і соціальний світи, забезпечують взаємодію між ними в реальному часі.

Процес об'єднання IT і IoT надзвичайно складний, він обговорюється на різних рівнях, в першу чергу в діалозі між двома найбільшими комітетами по стандартизації International Society for Automation (ISA) і Industrial Internet Consortium (IIC).

На маркетинговому рівні, в мас-медіа для позначення рішень, націлених на IT/IoT convergence, найчастіше використовують термін Industrial Internet або Industrial Internet of Things (IIoT). Те, як це робиться, найчастіше відображає надмірно захоплене ставлення до феномену IoT і спрощене ставлення до перенесення принципів IoT в індустрію.

У локальних мережах IIoT проблем буде ще більше, тому що обсяги даних, що генеруються промисловими машинами, більше, ніж побутовими, а питання безпеки – критичніше. Забезпечити адресацію до всіх можливих пристроїв по протоколу IPv6 (Internet Protocol version 6) далеко не достатньо для вирішення проблем IT/OT convergence.

Безпеку Інтернету речей локальних мережах можна побудувати на фундаменті з чотирьох напрямів:

- безпека зв'язку;
- захист пристроїв;
- контроль пристроїв;
- контроль взаємодій в мережі [7].

На цьому фундаменті можна створити потужну і просту в розгортанні систему безпеки в локальної мережі, яка здатна послабити негативний вплив більшості загроз безпеки для Інтернету речей, включаючи цілеспрямовані атаки.

Існують чотири фундаментальні напрямки. Необхідно надати базові рекомендації, які застосовуються до всіх областей, включаючи автомобільну промисловість, енергетику, виробництво, охорону здоров'я, фінансові послуги, державний сектор, роздрібну торгівлю, логістику, авіацію, товари широкого вжитку та інші напрямки.

Канал зв'язку в локальної мережі повинен бути захищений, для цього застосовуються технології шифрування і перевірки автентичності, щоб пристрої знали, чи можуть вони довіряти віддаленій системі корпоративної мережі в рамках телефонної мережі загально користування (ТМЗК) та Інтернет.

Нові криптографічні технології, такі як ECC (Elliptic Curve Cryptography), працюють в десять разів краще попередників в малопотужних чіпах IoT 8-bit 8MHz [8]. Не менш важливим завданням тут є управління ключами для перевірки достовірності даних та достовірності каналів їх отримання. Провідні центри сертифікації (CA) уже вбудували «сертифікати пристроїв» в більш ніж мільярд пристроїв IoT, надавши можливість виконувати перевірку автентичності широкого спектру пристроїв, включаючи мобільні станції, базові станції, телевізори і багато іншого.

Захист пристроїв – це в першу чергу забезпечення безпеки і цілісності програмного коду. Підписання коду потрібно для підтвердження правомірності його запуску, також необхідний захист під час виконання коду, щоб атаки не перезаписали його під час завантаження [8]. Підписання коду криптографічно гарантує, що він не був зламаний після підписання і безпечний для пристрою. Це може бути реалізовано на програмному рівні і на рівні прошивки та навіть на пристроях з монолітним чином прошивки. Всі критично важливі пристрої, будь то датчики, контролери або щось ще, повинні бути налаштовані на запуск тільки підписаного коду. Пристрої повинні бути захищені і на наступних етапах, вже після запуску коду. Тут допоможе захист на основі хоста, який забезпечує харденінг, розмежування доступу до системних ресурсів і файлів, контроль підключень, пісочницю, захист від вторгнень, захист на основі поведінки і репутації. Також в цей довгий список можливостей хостового захисту входять блокування, протоколювання і оповіщення для різних операційних систем IoT. Останнім часом багато засобів хостового захисту були адаптовані для IoT і тепер добре опрацьовані і налагоджені, не вимагають доступу до хмари і дбайливо витрачають обчислювальні ресурси IoT-пристроїв в локальних мережах.

Та все одно уразливості в пристроях IoT все одно будуть, їх потрібно буде патчити, і це може відбуватися протягом тривалого часу після передачі обладнання споживачеві. Навіть код із застосуванням обфускації в критичних системах зрештою реконструюється, і зловмисники знаходять в ньому

уразливості. Ніхто не хоче, а часто і не може відправляти своїх співробітників для очного візиту до кожного пристрою IoT для оновлення прошивки, особливо, якщо мова йде, наприклад, про парк вантажівок або про мережу датчиків контролю, розподілених на сотні кілометрів в корпоративних мережах. З цієї причини «управління по повітрю» (over the air, OTA) [8], повинна бути вбудована в пристрої до того, як вони потраплять до покупців.

Деякі загрози зможуть подолати будь-які вжиті заходи, незалежно від того, наскільки добре все захищено. Тому вкрай важливо мати можливості аналітики безпеки в IoT локальних мереж.

Системи для аналітики безпеки допоможуть краще зрозуміти локальну мережу, помітити підозрілі, небезпечні або зловмисні аномалії.

Еволюція парадигми. Більшість пристроїв IoT вдають із себе «закриті системи». Покупці не зможуть додавати програмне забезпечення безпеки після того, як пристрої покинуть завод. Таке втручання анулює гарантію, а часто просто не представляється можливим. З цієї причини, захисні функції повинні бути спочатку вбудовані в пристрої IoT, щоб вони були безпечними за своєю архітектурою в локальних мережах.

Для більшої частини індустрії інформаційної безпеки така «безпека всередині», тобто вбудована при виготовленні пристрою на заводі – це новий спосіб забезпечення захисту, що стосується і класичних технологій безпеки, таких як шифрування, перевірка справжності, 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. Багато виробників чіпів вже вбудували функції безпеки в обладнання. Але апаратний рівень – це всього лише перший шар, необхідний для комплексного захисту зв'язку і пристроїв. Комплексний захист вимагає інтеграції і функцій управління ключами, захисту на основі хоста, інфраструктури локальної мережі і аналітики безпеки [7].

Відсутність навіть одного з наріжних каменів у фундаменті безпеки залишить широкий простір діям зловмисників. Оскільки промисловий Інтернет і IoT привносять мережний інтелект в фізичні речі навколо, повинно уважно ставитися до питань їх безпеки. Життя залежить від літаків, поїздів і автомобілів,

інфраструктури охорони здоров'я та цивільної інфраструктури, яка дозволяє жити і працювати. Неважко уявити, як незаконне маніпулювання світлофорами, медичним обладнанням або незліченними іншими пристроями може привести до плачевних наслідків. Також ясно, що прості громадяни і покупці IoT не хочуть, щоб незнайомі люди зламували їх будинку або машини, щоб хтось робив їм шкоду, влаштовуючи збої локальних мереж на автоматизованих промислових об'єктах.

У цій ситуації необхідно запропонувати такі рекомендації, які сформують цілісну безпеку для IoT, одночасно зробивши її ефективної і простий в реалізації.

Що стосується безпеки зв'язку, посилена модель довіри для IoT - шифрування, перевірка справжності і управляюмості незмінно є основою стійкої безпеки. Є відмінні бібліотеки з відкритим вихідним кодом, які виконують шифрування навіть в пристроях IoT з обмеженими обчислювальними ресурсами. Але, на жаль, більшість компаній як і раніше піддаються небезпечним ризикам, допускаючи помилки при управлінні ключами для IoT в локальних мережах.

Транзакції на $4 млрд в день електронної торгівлі захищені простою і надійною моделлю довіри, яка обслуговує мільярди користувачів і понад мільйон компаній по всьому світу. Ця модель довіри допомагає системам безпечно проводити перевірку достовірності інфраструктури систем інших компаній і взаємодіяти з ними по зашифрованих каналах зв'язку. Модель довіри сьогодні є критичним фактором безпечного взаємодії в локальних середовищах і грунтується на дуже короткому списку довірених центрів сертифікації (CA). Ці ж CA встановлюють сертифікати в мільярди пристроїв щороку.

Сертифікати пристроїв дозволяють, наприклад, перевіряти справжність мобільних телефонів для безпечного підключення до базових станцій, перевіряти справжність інтелектуальних лічильників для електроенергетики, а також приставок в індустрії кабельного телебачення. Надійні CA дозволяють легко і безпечно генерувати, видавати, реєструвати, контролювати і відкликати сертифікати, ключі та облікові дані, які мають вирішальне значення для надійної перевірки автентичності. З огляду на реалізовані обсяги сертифікатів безпеки для IoT, більшість сертифікатів пристроїв продаються великими партіями за вельми скромну суму грошей за одиницю (в доларовому вираженні йдеться про десятки центів за сертифікат).

Небезпечно використовувати дані від неперевірених пристроїв або неперевірених сервісів. Такі дані можуть пошкодити або скомпрометувати систему, передати контроль над обладнанням зловмисникам. Використання надійної перевірки автентичності для обмеження небажаних підключень допомагає вберегти системи IoT від подібних небезпек і зберегти контроль над пристроями і сервісами локальних мереж.

Незалежно від того, чи з'єднується пристрій з якимось іншим пристроєм або відбувається обмін даними з віддаленим сервісом, наприклад, хмарним, зв'язок завжди повинна бути захищена локальна мережа. Всі взаємодії вимагають надійної перевірки автентичності і взаємної довіри. Виходячи з цих міркувань, економія на сертифікатах пристроїв видається спірною.

Безліч стандартів було розроблено для спрощення розгортання надійної перевірки автентичності всіх ланок ланцюга обміну даними [8]. Стандарти існують для форматів сертифікатів, і надійні центри сертифікації підтримують як стандартні, так і кастомні формати. У більшості випадків сертифікатами можна легко управляти віддалено за допомогою стандартних протоколів, таких як Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) і Online Certificate Status Protocol (OCSP) [8]. Завдяки надійному центру сертифікації, який надає можливість обробляти сертифікати, ключі та облікові дані, фактичну перевірку справжності можна робити за допомогою потужних стандартів Transport Layer Security (TLS) і Datagram TLS (DTLS) – родинних SSL.

Взаємна перевірка справжності, коли обидві кінцеві точки перевіряють один одного, має вирішальне значення для якісного захисту систем IoT. В якості додаткового бонусу, одного разу виконавши перевірку достовірності за TLS або DTLS, дві кінцеві точки можуть обмінюватися ключами шифрування або отримувати їх для обміну даними, які неможливо розшифрувати підслуховуючими пристроями.

Для багатьох додатків IoT потрібно абсолютна конфіденційність даних, це вимога легко виконується використанням сертифікатів і протоколів TLS/DTLS [8].

Однак, коли конфіденційність не є обов'язковою вимогою, справжність переданих даних може перевірятися будь-якою стороною, якщо вони були підписані під час їх появи на датчику – такий підхід не обтяжує канал

шифруванням, що переважно в архітектурі multi-hop. має вирішальне значення для якісного захисту систем IoT.

Часто виникають питання щодо вартості та продуктивності чіпів IoT для криптографічних операцій. Тут потрібно взяти до уваги, що Elliptic Curve Cryptography (ECC) в 10 разів швидше і ефективніше, ніж традиційне шифрування навіть в обмежених обчислювальними ресурсами пристроях [7]. Така швидкість і ефективність досягаються без зниження рівня безпеки. ECC навіть продемонстрував рівень захисту industry best practice, еквівалентний RSA 2048, в тому числі на надзвичайно обмежених в ресурсах чіпах – на 8-bit 1-MHz процесорах і 32-bit 1-KHz процесорах, при споживанні лише мікроват енергії. DTLS, варіант TLS був розроблений спеціально для малопотужних пристроїв, які періодично працюють між циклами сну. І нарешті, ціна таких 32-розрядних чіпів становить всього кілька десятків центів (при розрахунку в доларах), тому ціну або потужність чіпів не вийде використовувати в якості аргументу для зниження вимог щодо захисту нижче розумних порогових значень, коли безпека має значення [7].

В силу описаних факторів пропонуються наступні рекомендації по довжині ключа для перевірки справжності пристрою IoT, де безпека має значення [7]:

– мінімум 224-bit ECC для сертифікатів кінцевих об'єктів з перевагою 256-bit і 384-bit;

– мінімум 256-bit ECC для кореневих сертифікатів з перевагою 384-bit.

Сьогодні не можна уявити собі таку незручність, як ручну установку сертифікатів в браузери для кожного web–сервера локальної мережі. В той же час, не можна уявити собі, як це буде шкодити, якщо сліпо вірити будь–якому сертифікату.

Ось чому кожен браузер має кілька коренів довіри, за якими верифікуються всі сертифікати. Вбудовування цих коренів в браузери дало можливість масштабувати захист на мільйони серверів в Інтернеті. Оскільки мільярди пристроїв стають онлайн щорічно, в рівній мірі важливо, щоб в пристрої вбудовувалися і коріння довіри, і сертифікат пристрою.

Дані, пов'язані з IoT, повинні зберігатися в безпеці весь час. Надійність локальних мереж часто залежить від правильності, цілісності і належного функціонування систем більше, ніж від конфіденційності даних. Перевірка

справжності інформації, пристроїв і походження інформації можуть мати вирішальне значення. Дані часто зберігаються, кешуються і обробляються декількома вузлами, а не просто передаються з точки А в точку Б (клієнт – сервер). З цих причин дані завжди повинні бути підписані в той момент, коли вони були вперше зафіксовані і збережені. Це допомагає знизити ризики будь–якого втручання в інформацію. Підписання об'єктів даних, як тільки вони були зафіксовані, і ретрансляція підписи з даними навіть після їх дешифрування є все більш поширеною і успішною практикою.

Ще одним важливим пунктом є захист пристроїв та захист програмного коду IoT. При включенні кожен пристрій завантажується і запускає певний виконуваний код. Нам вкрай важливо бути впевненими в тому, що пристрої будуть робити тільки те, на що ми їх запрограмували, а сторонні не зможуть перепрограмувати на зловмисне поведінка. Тобто першим кроком у захисті пристроїв є захист коду, щоб гарантовано завантажувався і запускався тільки потрібний нам код. На щастя, багато виробників вже вбудували можливості безпечного завантаження в свої чіпи. Схожим чином справи йдуть і з високорівневих кодом – різні перевірені часом клієнтські бібліотеки з відкритим вихідним кодом, на кшталт OpenSSL, можуть використовуватися для перевірки підпису і дозволу коду тільки з авторизованого джерела. Внаслідок цього все більшого поширення набувають підписані прошивки, образи завантаження і більш високорівнева вбудований код, в тому числі підписані базові програмні компоненти, куди входять будь–які операційні системи. Все частіше зустрічаються не просто підписані прикладні програми, а взагалі весь код на пристрої. Такий підхід гарантує, що всі критичні компоненти систем IoT: датчики, механізми, контролери та реле сконфігуровані правильно – на запуск тільки підписаного коду і ніколи не запустять непідписаний код.

Доброю манерою було б дотримуватися принципу «ніколи не довіряти не підписаним коду». Логічним продовженням було б «ніколи не довіряти не підписаним даними і, тим більше, не підписаним конфігураційним даними». Використання сучасних засобів перевірки підпису і поширення апаратної реалізації безпечного завантаження, ставлять серйозне завдання перед багатьма компаніями – управління ключами і контроль доступу до ключів для підпису коду і захисту програмно-апаратних засобів.

Однак, деякі центри сертифікації пропонують хмарні сервіси, які роблять простіше, безпечніше і надійніше адміністрування програм для підписування коду і гарантують суворий контроль, хто може підписувати код, відкликати підписи, і як ключі для підписання і відкликання захищені.

Виникають ситуації, коли програмне забезпечення потрібно оновити, наприклад, в цілях безпеки, але при цьому необхідно врахувати вплив оновлень на заряд батареї. Операції перезапису даних збільшують споживання енергії і скорочують період автономної роботи пристрою.

З'являється необхідність підписати і оновити окремі блоки або фрагменти таких оновлень, а не монолітні образи цілком або бінарні файли. Тоді програмне забезпечення, підписана на рівні блоків або фрагментів, можна оновлювати з набагато більш тонкої деталізацією, не жертвуючи безпекою або зарядом батареї. Для цього не потрібна обов'язкова апаратна підтримка, таку гнучкість можна досягти за допомогою перед завантажувальної інфраструктури, яке може працювати на безлічі embedded–пристроїв.

Якщо час автономної роботи настільки важливий, можна було б просто конфігурувати пристрій з незмінної прошивкою, яку ніхто не може змінити або оновити, але пристрої в польових умовах схильні до реверс-інжинірингу для шкідливих цілей. Після його проведення виявляються і експлуатуються уразливості, які необхідно патчити якомога швидше.

Обфускація і шифрування коду можуть істотно уповільнити процес реверс-інжинірингу та відбити охоту продовжувати атакувати у більшості зловмисників. Але ворожі спецслужби або міжнаціональні деструктивні організації все-таки здатні це зробити навіть для програм, захищених за допомогою обфускації і шифрування, перш за все тому, код повинен бути дешифрований для запуску. Такі організації знайдуть і скористаються уразливими, які не були вчасно пропатчити. У зв'язку з цим можливості віддаленого поновлення мають вирішальне значення і повинні бути вбудовані в пристрої до того, як вони покинуть завод. Оновлення дуже важливі для підтримки високого рівня захищеності пристрою. Проте, обфускація, сегментування підписання коду і оновлення в кінцевому рахунку повинні бути щільно об'єднані між собою для ефективної роботи.

До речі, і сегментоване, і монолітне підписання коду використовують модель довіри на основі сертифікатів, а використання ECC при підписанні коду може забезпечити ті ж самі переваги високого рівня безпеки в поєднанні з високою продуктивністю і низьким енергоспоживанням. У цій ситуації пропонуються наступні рекомендації по довжині ключа для підпису коду IoT, де безпека має значення [7]:

– мінімум 224-bit ECC для сертифікатів кінцевих об'єктів з переважним 256-bit і 384-bit;

– мінімум 521-bit ECC для кореневих сертифікатів, оскільки, як правило, очікується, що підписаний код буде використовуватися роками або навіть десятиліттями після підписання, а підписи повинні бути досить сильними, щоб залишатися надійними протягом такого тривалого часу.

Захист пристроїв. Ефективний хостовий захист для IoT. Вище було розглянуто перший аспект захисту пристроїв, який визначає основні принципи управління ключами, перевірки автентичності для IoT, підписання коду і конфігурації для захисту цілісності пристрою, основи управління таким кодом і конфігурацією. Однак, після захисту зв'язку і реалізації безпечного завантаження добре керованого пристрою, необхідний захист на етапі експлуатації. Хостовий захист вирішує цю задачу.

IoT–пристрої стикаються з багатьма загрозами, в тому числі шкідливим кодом, який може поширюватися через перевірені з'єднання, скориставшись уразливими або помилками в конфігурації.

В таких атаках часто експлуатуються кілька слабких місць, включаючи, але не обмежуючись:

– невикористання перевірки підпису коду і безпечну завантаження;

– погано реалізовані моделі перевірки, які можна обійти.

Атакуючі часто використовують ці недоліки для установки бекдор, сніфферів, програмного забезпечення для збору даних, можливості передачі файлів для витягання конфіденційної інформації з системи, а іноді навіть для інфраструктури command & control (C&C) для маніпулювання поведінкою системи [9]. Особливо тривожить здатність деяких зловмисників експлуатувати вразливості для установки шкідливих програм прямо в пам'ять вже працюючих систем IoT. Причому іноді вибирається такий спосіб зараження, при якому

шкідлива програма зникає після перезавантаження пристрою, але встигає наносити величезної шкоди. Це працює, тому що деякі системи IoT і багато промислових системи майже ніколи не перезавантажуються.

Для відділу безпеки локальної мережі в цьому випадку ускладнюється можливість виявлення використаної уразливості в системі і розслідування походження атаки. Іноді такі атаки відбуваються через IT-мережу, підключену до промислової мережі або до мережі IoT, в інших випадках атака відбувається через Інтернет або через прямий фізичний доступ до пристрою.

Не важливо, який був вихідний вектор інфекції, але якщо він не виявлений, то перше скомпрометований пристрій як і раніше залишається довіреною і стає провідником для зараження іншої мережі, будь то автомобільна мережа транспортного засобу або локальна мережа заводу.

Таким чином, безпека IoT повинна бути комплексною. Закриваючи вікна, залишати двері відчиненими – неприйнятно. Всі вектори загроз повинні придушуватися. Іноді такі атаки відбуваються через локальну мережу, які підключені до промислової мережі або до локальної мережі IoT, в інших випадках атака відбувається через Інтернет або через прямий фізичний доступ до пристрою.

В поєднанні з надійним підписом коду і моделлю перевірки, хостовий захист може допомогти захистити пристрій від безлічі небезпек. У хостовому захисті використовується ряд технологій захисту, в тому числі харденінг, розмежування доступу до системних ресурсів, захист на основі репутації і поведінки, від шкідливих програм і, нарешті, шифрування. Залежно від потреб конкретної системи IoT комбінація цих технологій може забезпечити найвищий рівень захисту для кожного пристрою локальної мережі.

Харденінг, розмежування доступу до ресурсів, захистять все «двері» в систему. Вони обмежують мережні підключення до додатків і регламентують вхідний і вихідний потік трафіку, захищають від різних експлойтів, переповнення буфера, цілеспрямованих атак, регулюють поведінку додатків, при цьому дозволяють зберегти контроль над пристроєм. Такі рішення ще можуть використовуватися для запобігання несанкціонованого використання знімних носіїв, блокування конфігурації та налаштувань пристрою і навіть для деескалації користувальницьких привілеїв, якщо потрібно.

Хостовий захист має можливості аудиту і оповіщення, допомагаючи відстежувати журнали і події безпеки. Технології на основі політик можуть працювати навіть в середовищах без підключення до інформаційної мережі або при обмеженій обчислювальної потужності,

Технологія захисту на основі репутації може використовуватися для визначення сутності файлів по їхньому віку, поширеності, розташування і до решти для виявлення небезпек, що не виявляються іншими засобами, а також давати уявлення про те, чи слід довіряти новому пристрою навіть при успішній перевірці автентичності. Таким способом можна ідентифікувати загрози, які використовують мутуючий код або адаптують свою схему шифрування, просто відокремлюючи файли з високим ризиком від безпечних, швидко і точно виявляючи шкідливі програми, незважаючи на всі їхні хитрощі.

Зрозуміло, поєднання застосовуваних технологій буде залежати від конкретної ситуації, але наведені вище методи можуть об'єднуватися для захисту пристроїв, навіть в середовищах з обмеженими обчислювальними ресурсами локальних мереж.

2.4 Особливості захисту трафіку Інтернет-речей

Інтернет речей є ключовим напрямком в корпоративних та локальних мережах, обговоренню якого останнім часом приділяють багато уваги. У зв'язку з цим, з'являються нові загрози мережної безпеки для Інтернету речей, починаючи від атак на енергетичну систему, клонування вузлів сенсорної мережі, перехоплення даних від Інтернет-пристрою і підміни самого пристрою до злому сервісів, на базі яких здійснюється обробка і зберігання даних.

Класичні підходи для виявлення таких проблем не завжди підходять, з огляду на те, що для Інтернету Речей використовується велика кількість нових пропрієтарних протоколів, яких зараз налічується близько 25.

Концепція Інтернету речей передбачає можливість використання хмарних сервісів для зберігання і обробки даних [10]. У свою чергу, хмарний сервіс є сполучною ланкою між Інтернет-пристроєм і людиною, або є кінцевим елементом при зборі даних з датчиків. На всьому маршруті проходження даних від Інтернет-пристрою до хмарного сервісу може відбутися знищення спотворення і

блокування інформації, що передається, в силу втручання третіх осіб. Такий вид атаки називається «людина посередині».

Однак, найбільш простий вид атак, який може бути реалізований на рівні доступу, є відправка даних від Інтернет-речі в альтернативний хмарний сервіс. Для отримання доступу до конфіденційних даних, що йде від типової Інтернет-речі до віддаленого хмарного сервісу, пропонується використовувати метод клонування пакетів, що містять конфіденційну інформацію і їх подальшу відправку до дублюючому хмарного сервісу (хибну хмару). Під хмарним сервісом розуміється сукупність програмно–апаратних засобів (серверів), що мають підключення до Інтернет і здійснюють обробку та зберігання даних локальних мереж. У спрощеному варіанті хмарний сервіс може бути представлений Web і Data Base–сервером, який є одним з ключових компонентів локальної мережі для Інтернету речей [10].

Для реалізації перехоплення і відправки конфіденційних даних на дублюючий сервер локальної мержі необхідно мати доступ до каналу зв'язку або обладнання на рівні доступу, що відповідає за транспортування даних від Інтернет–речі до хмарного сервера.

В даний час технологія Wi-Fi є найбільш популярною серед безпроводових мереж і використовується для підключення Інтернет-речей в додатках «розумний будинок», «розумне місто» і ін. Для відправки даних на хмарний сервіс Інтернет-річ повинно мати підключення локальної мережі до точки доступу до мережі зв'язку загального користування.

Перехоплення і перенаправлення даних може бути реалізовано в безпосередній близькості до каналу зв'язку на ділянці доступу «Інтернет-річ – точка доступу». Для реалізації атаки необхідно перехопити мережний трафік, що йде до легального хмарного сервісу. Фільтрацію заданих пакетів від другорядного трафіку виконувати за IP-адресою і портом с призначенням перехоплених пакетів. Пакети, що мають в поле IP-адреса – адреса легального хмарного сервісу, дублюються та перенаправляються на альтернативний (хибний) хмарний сервер.

Програмна частина має виконувати аналіз заголовків кожного захопленого пакета, і при виявленні в полях Адреса одержувача (мережний рівень) і Порт одержувача (транспортний рівень) відповідної адреси і порту легального хмарного сервісу, або IP – адреси Інтернет-речі в поле Адреса відправника,

здійснювати копіювання змісту пакета в оперативну пам'ять і подальшу заміну полів Адреса одержувача і порт одержувача на IP-адресу і порт хибного хмарного сервера. Далі здійснити відправку такого пакета в мережу зв’язку загального користування (МЗЗК).

Якщо IP-адреса легального хмарного сервера була невідома, то здійснюється аналіз структури трафіку від Інтернет-речі. Основні характеристики трафіку Інтернет-речі можуть значно відрізнятися в залежності від типу пристрою (сенсорний вузол, актуатор, комбінований пристрій і т. д.), а також виду виконуваного завдання.

Для виявлення даних від Інтернет-речі і подальшої їх відправки на хибний хмарний сервер спочатку визначалася IP-адреса легального хмарного сервісу. Для цього необхідно проаналізувати поведінку трафіку від Інтернет-речі і отримати параметри основних характеристик. Протокол MQTT має стандартизований формат обміну повідомленнями між Інтернет-річчю і MQTT-брокером, як показано на рисунку 2.3 [11].

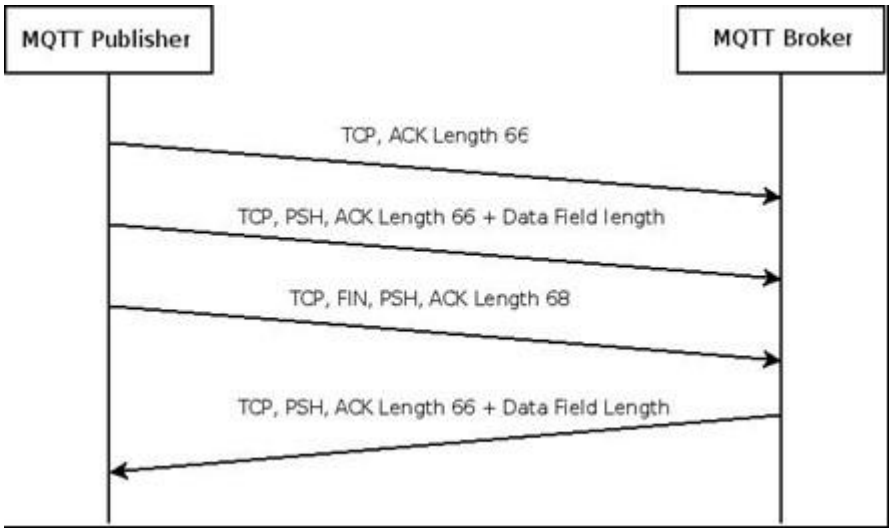


Рисунок 2.3 – Обмін повідомленнями між Інтернет-річчю і MQTT брокером

Першим критерієм для фільтра мережного трафіку протоколу MQTT є виявлення 4 послідовно вихідних пакетів від Інтернет- речі, а саме:

− пакету, що сигналізує про початок передачі даних (транспортний протокол TCP);

− пакету з даними від Інтернет-речі (транспортний протокол TCP);

- протокол прикладного рівня MQTT;
- пакету сигналізації про закінчення передачі даних (транспортний протокол TCP);
- пакету, що підтверджує отримання даних MQTT-брокером (протокол прикладного рівня MQTT).

Для фільтрації пакетів по даним критеріям необхідно здійснити порівняння поля Адреса відправника в пакеті, що йде від Інтернет-речі, і поля Адреса одержувача в пакеті, що йде від сервера. Цей критерій допустимо за умови, якщо пакет від сервера отримано не далі, ніж через 7 пакетів після пакета від самої інтернет-речі, і при їх збігу здійснювалося порівняння полів даних. Якщо поля даних виявлялися ідентичні, то включався лічильник, який при досягненні певного значення записував IP-адреса сервера одержувача, IP-адреса інтернет-речі і порт одержувача в ОЗУ для подальшого використання при дублюванні пакетів. Цей критерій підходить для аналізу трафіку за умови використання протоколів мережного рівня IPv4, IPv6, протокол транспортного рівня UDP, TCP і використанні протоколу прикладного рівня MQTT.

Також в якості критерію для фільтрації трафіку Інтернет-речі здійснюється аналіз всіх захоплених пакетів на предмет їх схожості на базі непрямих характеристик. Для цього можна використовувати масив з структур, що містять IP-адреса відправника, адресу порту відправника, IP-адреса одержувача, передбачуваний тип даних (символи або число), розмір поля даних пакета (з невеликим ймовірним відхиленням в залежності від типу перехоплених даних), масив з 3 і більше чисел, що зберігають час надходження останніх 3 і більше пакетів даного типу, і лічильник кількості перехоплених пакетів. Дана структура описує кількість отриманих пакетів, схожих між собою. У разі, якщо більше 3 пакетів мали схожі адреси та порти відправника, адреса одержувача, тип даних, розмір поля даних і тимчасова різниця між двома послідовно що йдуть пакетами була приблизно дорівнює різниці інших двох послідовно йдуть пакетів, в ОЗУ записувалося значення адреси одержувача, адреса відправника та порт одержувача для подальшого використання при дублюванні пакетів. Цей критерій доцільно використовувати для аналізу трафіку інтернет-речі за умови використання протоколів мережного рівня IPv4, IPv6 і протоколів транспортного

рівня UDP, TCP, однак вивчення структури інформаційного обміну може зайняти деякий час [14].

Після визначення IP-адреси сервера одержувача (легальний хмарний сервіс), IP-адреси Інтернет-речі і порту одержувача, кожен пакет, який підходить під дані критерії, дублюється і записується в ОЗУ. Потім відбувається заміна IP-адреси сервера і порту одержувача на адресу сервера дублювання даних і порт 10001.

Для захисту даних, що надходять від Інтернету-речей до віддаленого хмарного сервера через мережі зв’язку загального доступу пропонується використовувати такі методи захисту.

2.5 Метод захисту трафіку Інтернет-речей на базі використання алгоритмів гібридного шифрування

Дані алгоритми (наприклад, RSA-512 і AES-128) вимагають великих обчислювальних потужностей від Інтернет-речей і не підходять для малопотужних додатків, реалізованих на базі мікроконтролерів, що мають 8-ми або 16-ти бітну розрядність ЦПУ (наприклад, AVR або ARM), також, як і пристрої з малим об'ємом пам'яті. Приклад такого алгоритму складається з наступної послідовності кроків, як показано на рисунку 2.4 [11]:

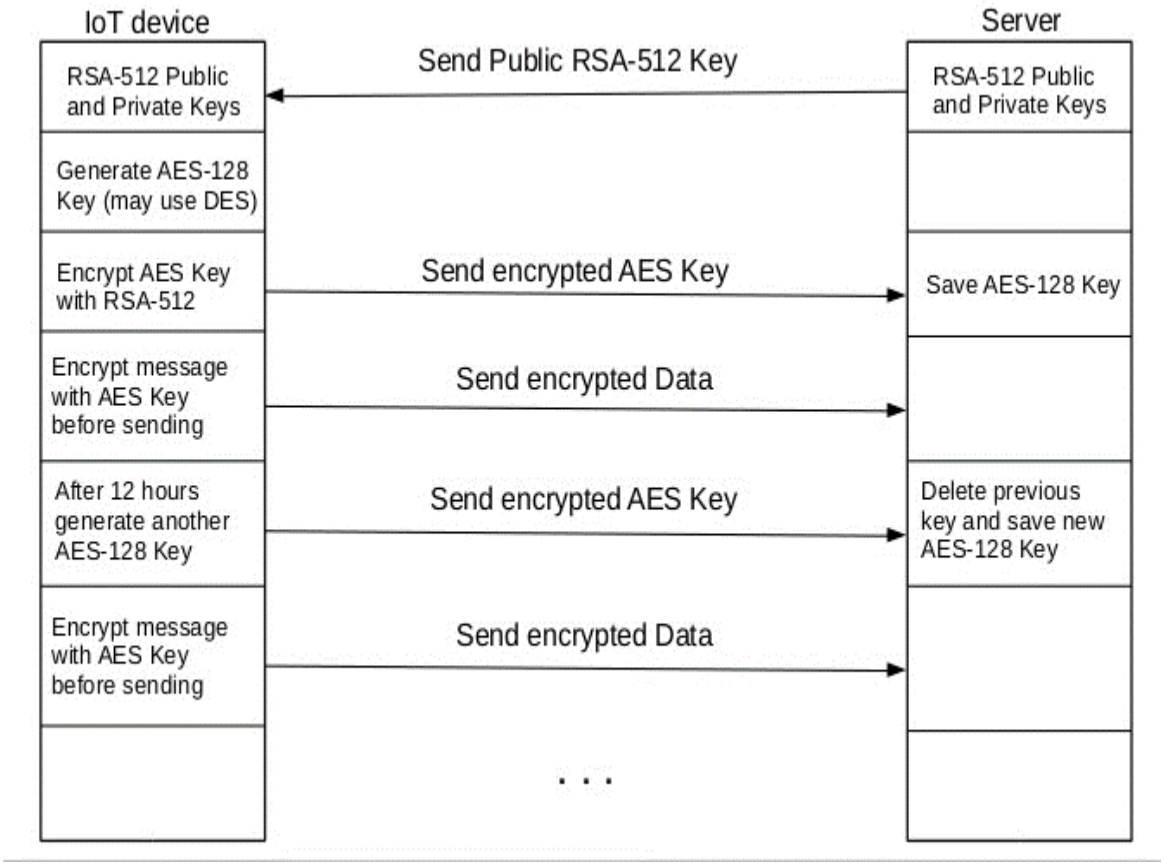


Рисунок 2.4 – Алгоритм гібридного шифрування для Інтернет-речей

Крок 1. Генерація відкритого і закритого ключів на сервері для організації асиметричного шифрування (наприклад RSA-512).

Крок 2. Генерація відкритого і закритого ключів для мікроконтролера і їх запис в пам'ять Інтернет-речі.

Крок 3. Проводиться обмін відкритими ключами між сервером і Інтернет-річчю.

Крок 4. Інтернет-річ генерує за допомогою набору випадкових символів ключ для симетричного шифрування (наприклад, DES).

Крок 5. Отриманий ключ симетричного шифрування шифрується за допомогою відкритого ключа та відправляється на сервер.

Крок 6. На сервері відбувається дешифрування і запис у ПЗУ симетричного ключа за допомогою закритого ключа.

Крок 7. Усі наступні дані, що відправляються з Інтернет-речі, шифруються за допомогою симетричного ключа, наявного на Інтернет-речі і на сервері.

Крок 8. В залежності від складності дешифрування симетричного ключа методом повного перебору (bruteforce) через заданий час потрібно повторити Кроки 4-7.

2.6 Метод захисту трафіку Інтернет-речей на базі створення патернів мережного трафіку.

Метод передбачає внесення випадкових змін в структуру інформаційного обміну між Інтернет-річчю і хмарним сервером, а також використання декількох портів на сервері для створення нетипового для Інтернет-речі трафіку, як показано на рисунку 2.5[5].

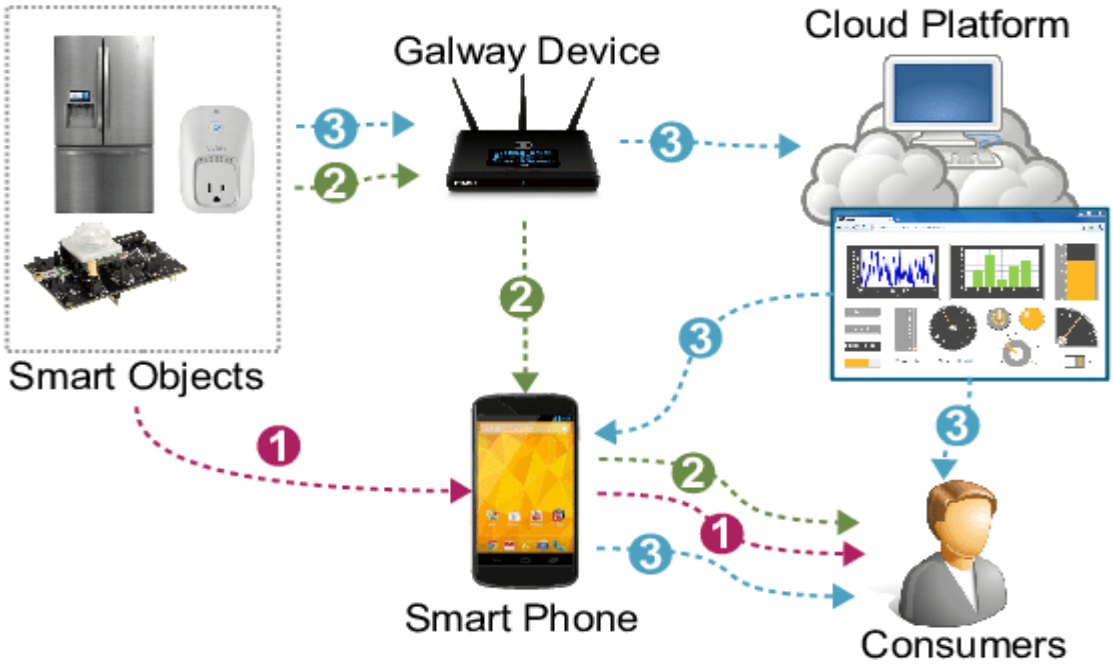


Рисунок 2.5 – Загальні патерни комунікації в додатках послуг Інтернет речей

Даний метод підійде для більшості Інтернет-речей, включаючи малопотужні 8-й розрядні мікроконтролери.

Розглянемо наступну послідовність кроків, як показано на рисунку 2.6 [11]:

Крок 1. Хешування всієї інформації, що знаходиться в полі даних всіх пакетів, що відправляються з Інтернет-речі (наприклад, за допомогою алгоритму MD5).

Крок 2. Внесення випадкових затримок перед черговим циклом відправки даних (дифференцируемость часу) з Інтернет-речі.

Крок 3. Використання з боку сервера декількох IP-адрес для прийому даних, що дозволить Інтернет-речі випадковим чином записувати різні значення в поле Адреса приймача.

Крок 4. Використання методу portknocking перед початком кожної передачі даних.

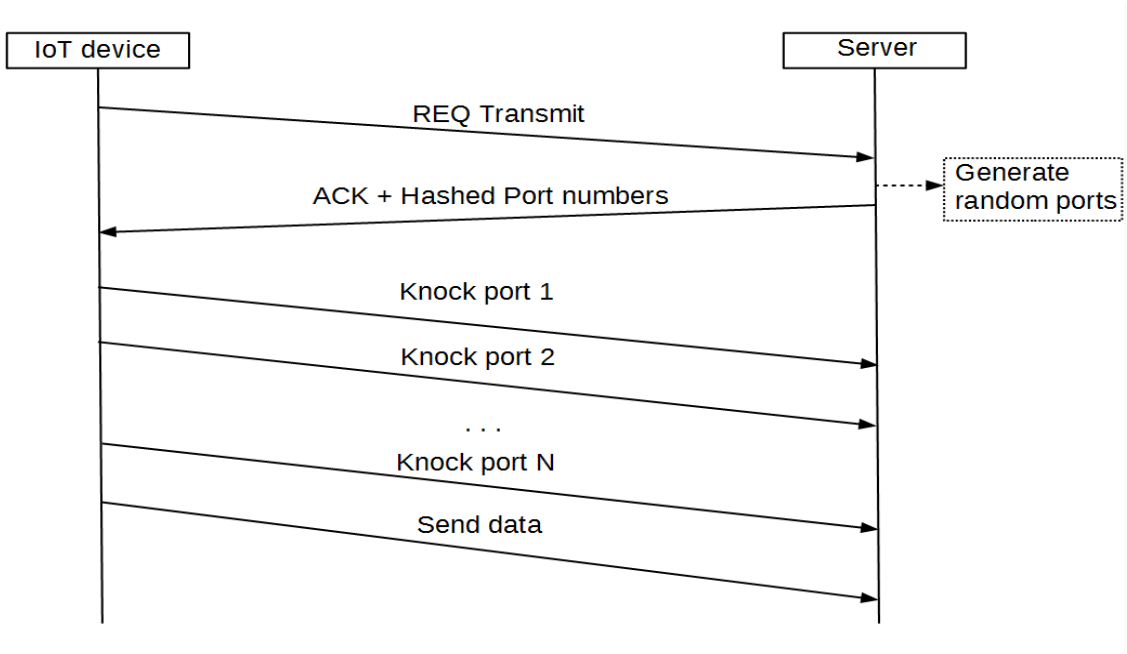


Рисунок 2.6 – Структура інформаційного обміну для методу portknocking

Метод portknocking полягає в зверненні до певних портів для розблокування доступу до порту, по якому, в кінцевому підсумку, відбувається передача даних. В даному випадку пропонується перед кожною передачею даних (або раз в певний період) проводити зміну портів передачі даних за допомогою даного методу. Для цього Інтернет-річ попередньо відправляє запит на передачу даних. Сервер у відповідь надсилає хешировать список портів для передачі, а потім пристрій робить поперемінні запити до кожного порту і відправляє дані за обраним порту.

Крок 5. Створення помилкового потоку даних.

Запропонований метод дозволяє значно збільшити складність перехоплення трафіку від Інтернет-речі, що дасть можливість зберегти конфіденційну інформацію.

3 МЕТОДИ ТЕСТУВАННЯ ЕЛЕМЕНТІВ ЛОКАЛЬНИХ МЕРЕЖ

3.1Загальні положення

Метою захисту інформації є діяльність, спрямована на запобігання витоку інформації по різних каналах локальних мереж і їх блокування. Захист включає в себе визначення можливих каналів витоку інформації, оцінку важливості самої інформації і розробку заходів щодо запобігання її витоку і розкрадання. Визначення потенційної цінності інформації дозволяє подумати, в першу чергу, про безпеку найбільш важливих секретів, витік яких здатна завдати шкоди. Тому об'єктом технічного захисту і є інформація, яка потрапляє під дію Закону України «Про інформацію» або конфіденційна інформація передана державі у володіння або використання. Виходячи з цього визначається мета захисту, якої є запобігання витоку або порушення цілісності інформації. Вона може бути досягнута методами тестування та моніторингу, які представляють собою організовану сукупність методів і засобів ефективного забезпечення захисту інформації[20].

Захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльністю, програмних і технічних засобів захисту інформації і засобів контролю, що мають сертифікат відповідної вимоги нормативних документів з технічного захисту, також застосуванням спеціальних споруд, засобів і систем.

Оперативне вирішення задач тестування та моніторингу досягаються організацією управління системою захисту інформації (ЗІ), для чого необхідно:

– постійно аналізувати технології проходження інформації в процесі інформаційної діяльності;

– виявляти схильність інформації впливу загроз в конкретний момент часу;

– оцінювати очікувану ефективність застосування засобів забезпечення ЗІ;

– визначати додаткову потребу в коштах забезпечення ЗІ;

– здійснювати збір, обробку, аналіз та реєстрацію даних, які стосуються захисту інформації;

– розробляти і реалізовувати пропозиції щодо коригування ЗІ в цілому або окремих її елементів.

Основи стратегії захисту інформації при загальному підході - це вибір основних і найбільш важливих базових системно-концептуальних положень і орієнтирів при плануванні, розробці та реалізації цієї стратегії. При цьому центральним питанням управлінського рішення стратегічного характеру є оцінка обсягу необхідних ресурсів захисту і їх оптимальне або найбільш розподіл не тільки необхідного, але і безперервного адаптивно–управляючого рівня гарантованого захисту інформації.

Гарантованість захисту інформації – вимога дуже серйозне і з практичних, і з теоретичних позицій. Тому про вірогідність можна говорити тільки з достовірністю і в контексті обов'язкового виконання вимог і рекомендацій використовуваних при цьому стандартів безпеки.

З метою забезпечення ефективних методів захисту від атак пропонуються методи тестування елементів локальних мереж.

Основні вимоги до моніторингу та тестуванню елементів локальних мереж та веб – додатків на появу уразливостей риску включають:

– розробка ефективних методів та порядок тестування;
– методологія та особливості тестування:
– нормативне забезпечення безпеки інформації;
– розробка процедур та метрики з контролю параметрів якості забезпечення безпеки інформації;
– методи технічної підтримки та контролю якості безпеки локальної мережи;
– програмне забезпечення для реалізації тестування.

Методи тестування вразливостей, як правило, включають важливі сценарії тестування:

– програмно–конфігуруємої локальної мережі;
– компонентів кожного web–додатка, які можуть містити відомі вразливості;
– елементів контролю вхідних даних до web – додатка;
– засобів автентифікації;
– наявності витоку конфіденційних даних;
– доступу до послуг IoT;
– web–додатка на послуги IoT.

3.2 Основні вимоги нормативного забезпечення

Методи тестування базуються на виконанні вимог згідно з міжнародними та державними стандартами України:

– міжнародний стандарт ISO/IEC 27001:2018, який забезпечує підтримку рішень на основі ITIL (Information Technology Infrastructure Library-бібліотека IT інфраструктури), що описує найкращу світову практику організації підприємства, що надає послуги у сфері IoT)

– COBIT (Control Objectives for Information and Related Technology - Задачі інформаційних і суміжних технологій) – відкритий IT-стандарт, який, своєю чергою, містить ряд документів зі стандартами щодо оптимізації управління IT: аудитом IT та IT-безпекою)

– ISO/IEC 27007: Guidelines for information security management systems auditing.

– «Положенні про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», затвердженого Постановою Правління Національного банку України від 28.09.2017 №95» - необхідність проведення тестування на проникнення/

Необхідно сформувати політику безпеки, яка дасть змогу уникнути або мінімізувати ризики безпеки локальної мережі з розробкою методології збереження, конфіденційності та цілісності послуг наступних поколінь IoT.

3.3 Методологія тестування та сканування елементів локальної мережі

Для дослідження елементів локальної мережі та перевірки безпеки по сценарію збору інформації використовується сканер Nmap, що входить до ОС Kali Linux. Nmap (“Network Mapper”) - це безкоштовна утиліта з відкритим кодом[26].

Сканер Nmap фактично фіксує топологію та програмну конфігурацію локальної мережі, які сервіси програмного забезпечення (назва програми та версії) функціонують, які впроваджені операційні системи (і версії ОС), який тип фільтрів/брандмауерів і інші характеристики, де результати сканування залежать від параметрів, які задані.

Список параметрів:

-sL: Список сканування - просто список цілей для сканування

-sn: Ping Scan - відключення сканування портів

-sS / sT / sA / sW / sM: сканування TCP / SYN / Connect () / сканування

- sU: Сканування UDP

-sN / sF / sX: сканування TCP Null, FIN та Xmas

-p <діапазони портів>: сканувати тільки вказані порти

-sV: Досліджуйте відкриті порти, щоб визначити інформацію про сервіс / версію

-O: Увімкнути виявлення ОС

-A Включає додаткові функції, такі як виявлення операційної системи та служби.

На рисунку 3.1 показано результати тестування відкритих портів та сканування запущених служб на web-сервері.

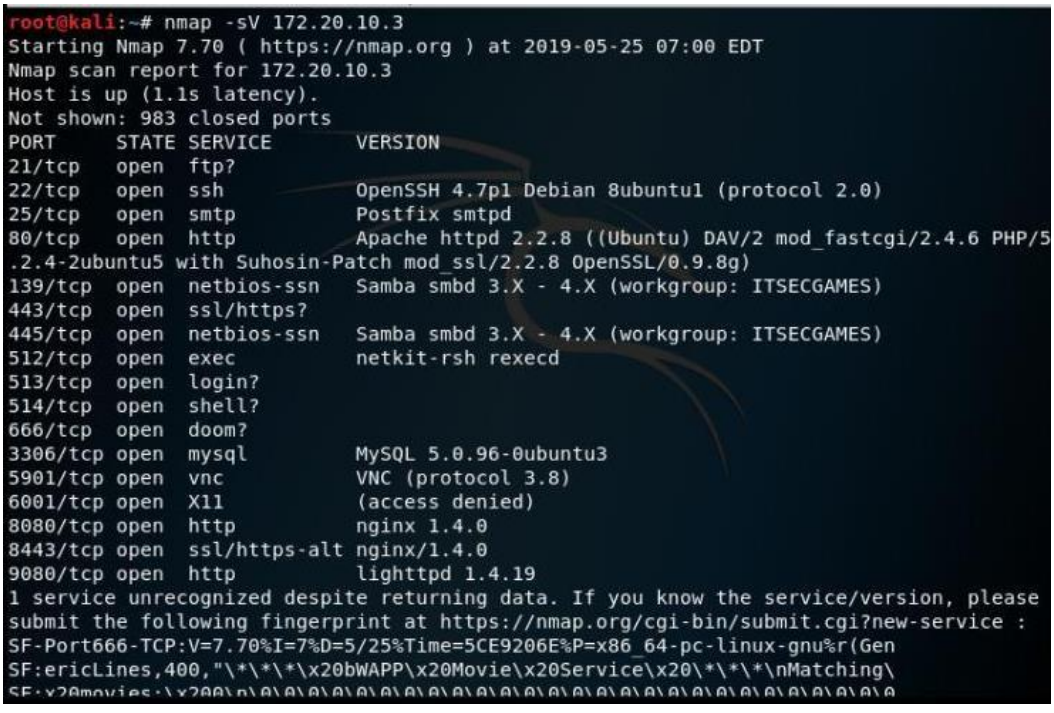


Рисунок 3.1 – Результати тестування відкритих портів та сканування запущених служб на web-сервері

На рисунку 3.2 показано сценарій встановлення типу операційної системи за використанням команди «nmap–0 172.20.10.3».

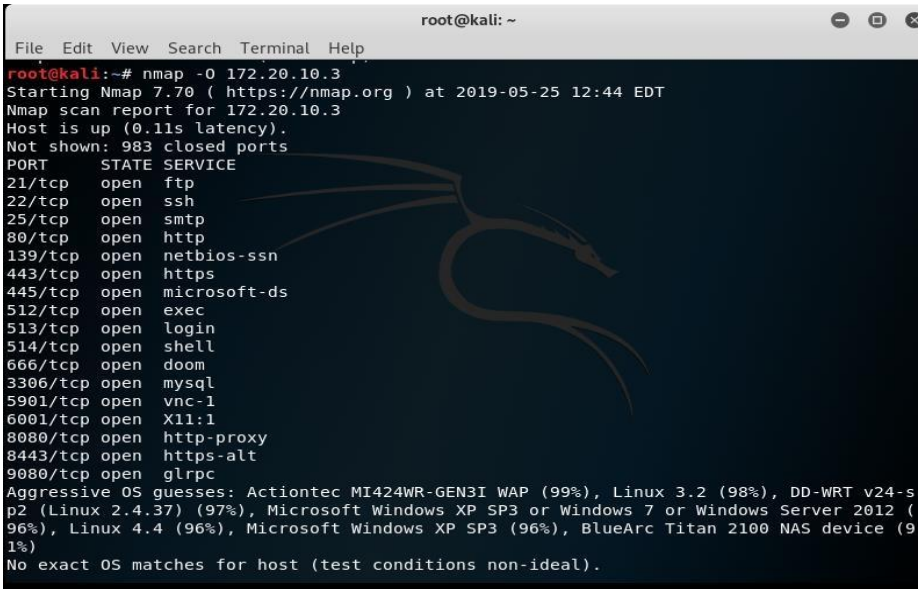


Рисунок 3.2 –Сценарій встановлення типу операційної системи за використанням команди «nmap –0 172.20.10.3»

За допомогою утиліті nmap отримані дані інформації, що на web-сервері містяться сервіси: OpenSSH 4.7p1, Apache 2.2.8, Samba smbd 3.x -4.x, MySQL 5.0.96.

А також такі операційні системи: Actiontec MI424WR-GEN3I WAP (99%), Linux 3.2 (98%), DD-WRT v24-sp2 (Linux2.4.37) (97%).

3.4 Методи тестування компонентів web-додатків

При наявності результатів аналізу даних інформації проводиться контроль появи експлойтів для web–серверів та операційних систем за допомогою сценаріїв.

В випадках наявності негативної інформації по першому сценарію та утиліти searchsploit з ОС Kali Linux можуть бути виявлені вразливості для програмного забезпечення (ПЗ) web–сервера. Утиліта searchsploit на основі бази даних експлойтів Exploit Database на наявність атак з боку існуючих вразливостей[19].

Тому всі версії сервісів перевіряються, які були виявлені по першому сценарію.

На рисунку 3.3 – представлено контроль сервісів та їх версій по сценарію – експолітів для apache.

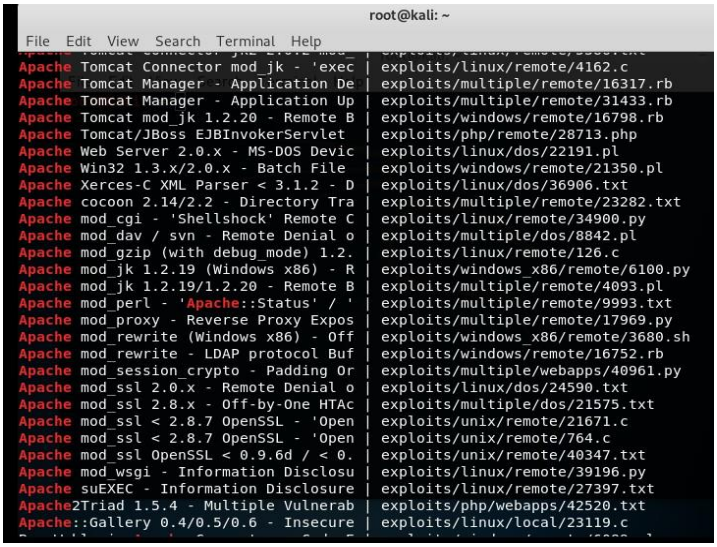


Рисунок 3.3–Дані контролю сервісів та їх версій по сценарію –експолітів для apache

На рисунку 3.4 представлено контроль сервісів та їх версій по сценарію - Searchsploit mysql.

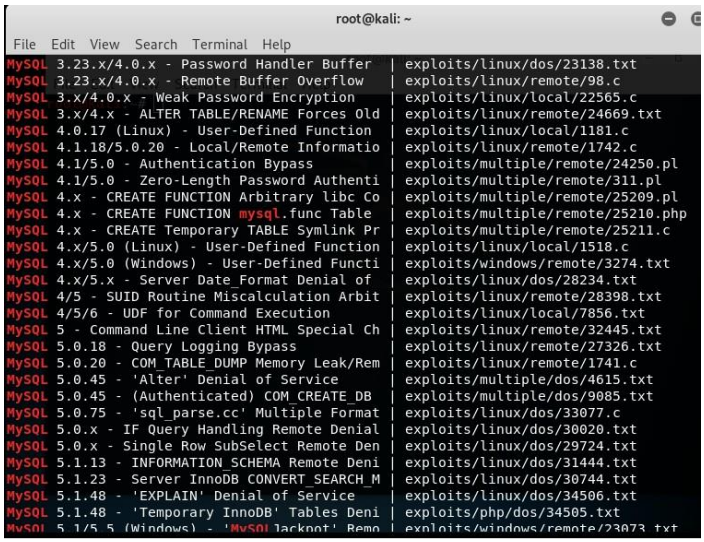
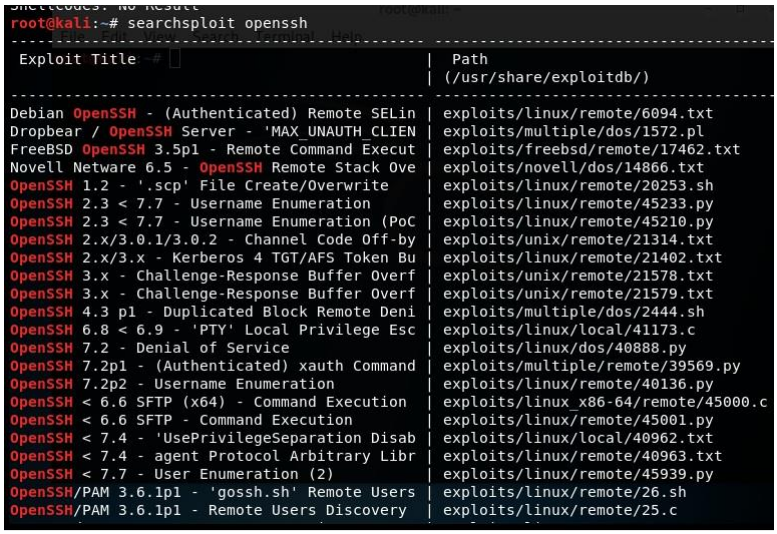


Рисунок 3.4 – Дані контролю сервісів та їх версій по сценарію – Searchsploit mysql

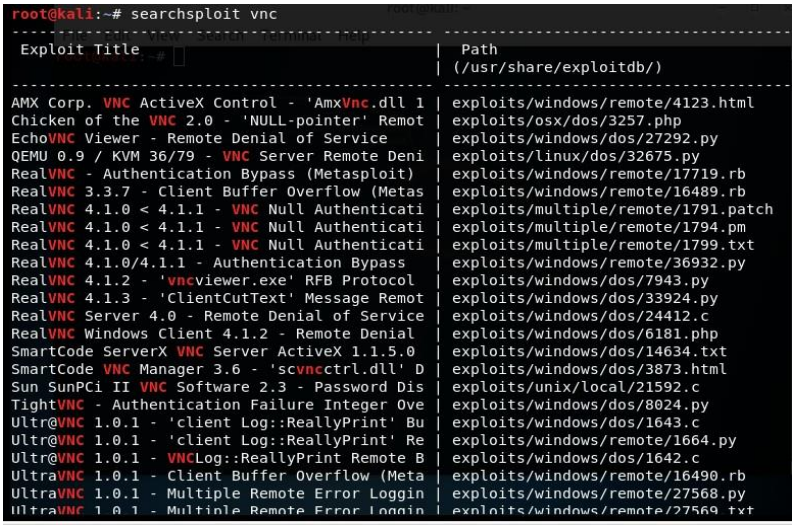
На рисунку 3.5 представлено контроль сервісів та їх версій по сценарію - Searchsploit openssh.



```
root@kali:~# searchsploit openssh
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
                                                | (/usr/share/exploitdb/)
------------------------------------------------ ---------------------------------
Debian OpenSSH - (Authenticated) Remote SELin | exploits/linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIEN | exploits/multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execut | exploits/freebsd/remote/17462.txt
Novell Netware 6.5 - OpenSSH Remote Stack Ove | exploits/novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite    | exploits/linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration      | exploits/linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC | exploits/linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by | exploits/unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Bu | exploits/linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overf | exploits/unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overf | exploits/unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Deni | exploits/multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Esc | exploits/linux/local/41173.c
OpenSSH 7.2 - Denial of Service               | exploits/linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command | exploits/multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration          | exploits/linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution  | exploits/linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution        | exploits/linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disab | exploits/linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Libr | exploits/linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)          | exploits/linux/remote/45939.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users | exploits/linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery  | exploits/linux/remote/25.c
```

Рисунок 3.5 – Дані контролю сервісів та їх версій по сценарію - Searchsploit openssh

На рисунку 3.6 представлено контроль сервісів та їх версій по сценарію – Searchsploit vnc.



```
root@kali:~# searchsploit vnc
------------------------------------------------ ---------------------------------
 Exploit Title                                  |  Path
                                                | (/usr/share/exploitdb/)
------------------------------------------------ ---------------------------------
AMX Corp. VNC ActiveX Control - 'AmxVnc.dll 1 | exploits/windows/remote/4123.html
Chicken of the VNC 2.0 - 'NULL-pointer' Remot | exploits/osx/dos/3257.php
EchoVNC Viewer - Remote Denial of Service     | exploits/windows/dos/27292.py
QEMU 0.9 / KVM 36/79 - VNC Server Remote Deni | exploits/linux/dos/32675.py
RealVNC - Authentication Bypass (Metasploit)  | exploits/windows/remote/17719.rb
RealVNC 3.3.7 - Client Buffer Overflow (Metas | exploits/windows/remote/16489.rb
RealVNC 4.1.0 < 4.1.1 - VNC Null Authenticati | exploits/multiple/remote/1791.patch
RealVNC 4.1.0 < 4.1.1 - VNC Null Authenticati | exploits/multiple/remote/1794.pm
RealVNC 4.1.0 < 4.1.1 - VNC Null Authenticati | exploits/multiple/remote/1799.txt
RealVNC 4.1.0/4.1.1 - Authentication Bypass   | exploits/windows/remote/36932.py
RealVNC 4.1.2 - 'vncviewer.exe' RFB Protocol  | exploits/windows/dos/7943.py
RealVNC 4.1.3 - 'ClientCutText' Message Remot | exploits/windows/dos/33924.py
RealVNC Server 4.0 - Remote Denial of Service | exploits/windows/dos/24412.c
RealVNC Windows Client 4.1.2 - Remote Denial  | exploits/windows/dos/6181.php
SmartCode ServerX VNC Server ActiveX 1.1.5.0  | exploits/windows/dos/14634.txt
SmartCode VNC Manager 3.6 - 'scvncctrl.dll' D | exploits/windows/dos/3873.html
Sun SunPCi II VNC Software 2.3 - Password Dis | exploits/unix/local/21592.c
TightVNC - Authentication Failure Integer Ove | exploits/windows/dos/8024.py
Ultr@VNC 1.0.1 - 'client Log::ReallyPrint' Bu | exploits/windows/dos/1643.c
Ultr@VNC 1.0.1 - 'client Log::ReallyPrint' Re | exploits/windows/remote/1664.py
Ultr@VNC 1.0.1 - VNCLog::ReallyPrint Remote B | exploits/windows/dos/1642.c
UltraVNC 1.0.1 - Client Buffer Overflow (Meta | exploits/windows/remote/16490.rb
UltraVNC 1.0.1 - Multiple Remote Error Loggin | exploits/windows/remote/27568.py
UltraVNC 1.0.1 - Multiple Remote Error Loggin | exploits/windows/remote/27569.txt
```

Рисунок 3.6 – Дані контролю сервісів та їх версій по сценарію - Searchsploit vnc

Сценарій завершується, коли експлоітів на атакуючому сервері не знайдено.

3.5 Тестування елементів мережі на можливості SQL–ін’єкцій

Тестування на цю вразливість може бути виконана при введенні « або» на полях, які контролюються. При зворотному зв’язку може бути поява незвичного повідомлення, то в результаті SQL–ін'єкція присутня на даному полі[24].

При пошуку, наприклад, фільму з назвою «halk» зі символом, як показано на рисунке 3.7 буде получено підтвердження наявності sql-ін’єкції. `

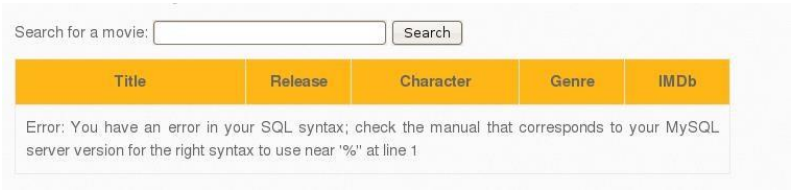


Рисунок 3.7 – Іконка підтвердження наявності sql–ін’єкції

Така помилка викликає ОС Kali Linux з виконанням наступної команди:

sqlmap –u `http://192.168.31.130:80/bWAPP/sqli_1.php?title=` --cookie=`PHPSESSID= b2a7d02cc634679f754fe391fb25f304` -T users , де

-u – параметр, якій необхідно вести перед веб-URL;

PHPSESSID – це ідентифікатор сессії, його ми знаходимо у cookies менеджері;

-T вказівка імені таблиці

На рисунку 3.8 представлено результат виконаної команди зі sqlmap.

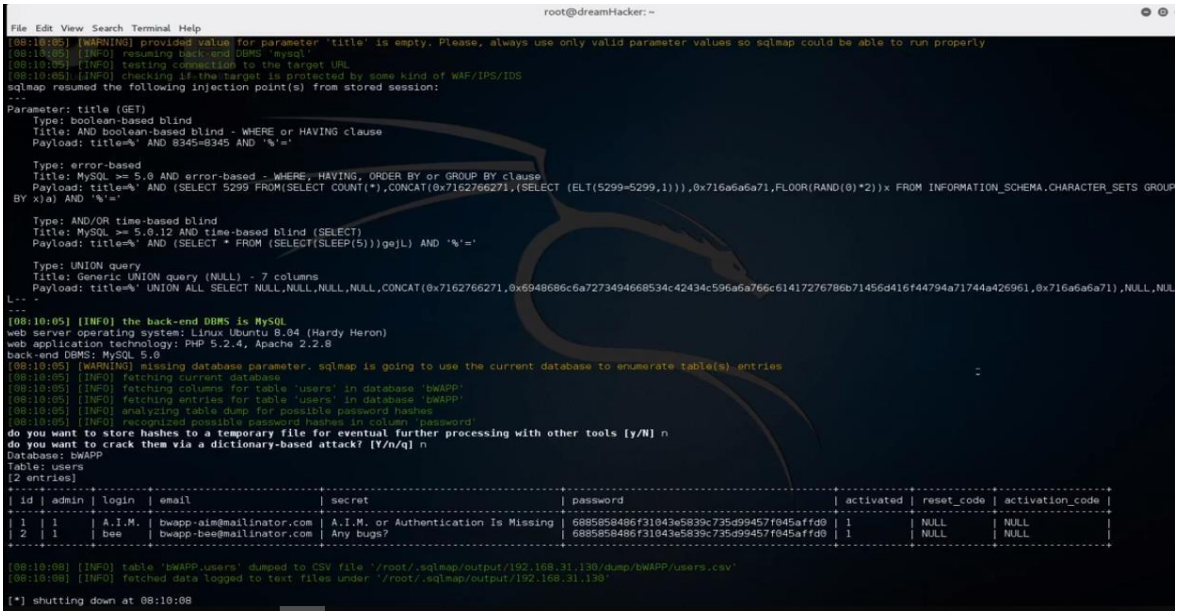


Рисунок 3.8 – Сценарій виконання команди sqlmap

3.6 Тестування виконання сценаріїв міжсайтового обміну між елементами мережі

Наявність вразливостей XSS потребує перевірки можливості на момент міжсайтового сеансу відповидати на запит web–додатка або веб-сервера по сценарію, який може бути виконаний браузером з відповіддю HTTP[21].

Тому у формі реєстрації для користувача необхідно заповнити поля та для перевірки відправити їх на веб-сервер. Приклад даних, які можна вести в форму: <script> alert(1) </script>. На стороні користувача може появитися вікно при наявності вразливостей, які призводять до міжсайтового виконання сценаріїв XSS атаки.

На рисунке 3.9 наведено вікно з результатами XSS атаки.

Рисунок 3.9 – Результати XSS-атаки

3.7 Тестування даних автентифікації

Процес аутентифікації, і використання цієї інформації для тестування схеми аутентифікації означає розуміння того, як працює механізм для обходу аутентифікації[31].

Тому необхідно:

1. Використання Wireshark для захоплення заголовків пакетів і їх перевірки дозволяє контролювати дані аутентифікації користувача, які передаються по зашифрованому каналу, щоб блокувати вторгнення зловмисників.

Наприклад, коли на вході каналу діє форма з полями User, Pass і кнопкою Submit для аутентифікації при доступі до web–додатку.

Тоди можно побачити заголовок запиту:

POST http:// www.siteexample.com /AuthenticationServlet HTTP/1.1

Таким чином, запит POST відправляє дані на сторінку www.siteexample.com/Authenticationform за допомогою HTTP. В такому випадку, коли дані передаються без шифрування, зловмисник має можливості перехопити ім'я користувача і пароль на етапі прослуховування мережі.

Наприклад, коли передача даних реалізується методом POST через HTTPS необхідна детальна перевірка. Нехай web–додаток для шифрування даних використовує протокол HTTPS, тоді заголовок POST-запиту буде виглядати наступним чином:

POST https://www. siteexample.com:443/cgi-bin/login.cgi HTTP/1.1

Це буде підтверджено запитом, якій адресовано по протоколу HTTPS. Дані не можуть бути прочитані зловмисником, що використовує аналізатор при гарантії використання клієнтом зашифрованому каналу.

Контроль та перевірка достовірного пароля та логіну за замовчуванням:

1. Можливи випробування даних імен клієнтів «admin», «administrator», «root», «system», «guest», «operator» або «super». Вони часто використовуються тому, що популярні серед системних адміністраторів локальних мереж. Якщо зловмиснику вдається успішно ідентифікувати будь-яке з вищезазначених імен користувачів - програма є вразливою до переліку імені користувача, і тому буде необхідно підібрати подібним чином паролі. Можливо вказати вільний пароль або, наприклад: "pass123", "password123", "admin" або "guest". Щоб заощадити час, подальші перестановки вищезгаданих можна також спробувати через написания скріпту.

2. Користувачі також задають собі ім’я по бренду компанії. Наприклад, при тестуванні web–додатку з назвою "Obscurity", можна впровадити комбінацію obscurity/obscurity або другу, як ім'я клієнта та пароль.

3. Можна спробувати знайти імена системних адміністраторів у соціальних мережах і вгадати ім'я клієнта, застосовуючи цю інформацію тому, що часто адреси електронної пошти клієнта розсилають угоду про імена облікових записів користувачів: якщо співробітник John Doe має адресу електронної пошти jdoe@example.com.

4. Як варіант можливо переглянути джерело сторінки та JavaScript або переглянувши джерело, або через проксі. Також знайти паролі в джерелі будь-якого посилання на електронну пошту користувачів. Можна увійти і переглянути кожен запит і відповідь для дійсного входу в порівнянні з недійсним Крім того, якщо є дійсний обліковий запис, входом, наприклад, цікавий запит GET та додаткові приховані параметри. Можливо шукати паролі, написані в коментарях у вихідному коді та імена облікових записів. Є інформація в резервних каталогах вихідного коду (або резервних копій вихідного коду), які можуть містити цікаві коментарі та код.

2. Тестування для оцінки можливості механізму блокіровки облікового запису на слабкий механізм блокування, щоб зменшити спроби підбору пароля:

– зайти в систему з неправильним паролем 3,4,5разів;

– увійти в систему з правильним паролем, щоби впевнитися, що механізм блокування не запускається після 3,4,5 помилок після кожної невдалої спроби;

– обліковий запис заблоковано після 3,4,5 помилок, спробувати увійти з правильним паролем через 5,10,15 хвилин у тому випадку, коли програма повертає «Ваш обліковий запис заблоковано»;

3. Методи тестування обходу схеми автентифікації.

Використання web додатком методів обходу схеми автентифікації:

– намагання отримання доступу до захищеної сторінки через адресний рядок у web–переглядачів через прямий запит на сторінку (примусовий перегляд);

– користувач може змінити параметри, щоб отримати доступ до захищених територій, не надаючи дійсних облікових даних, якщо web додаток може перевіряти успішну реєстрацію на основі параметрів фіксованого значення;

– можна знайти дійсний ідентифікатор сеансу і отримати несанкціонований доступ зловмисником до програми, видаючи себе за попередньо аутентифікованого користувача, через передбачення ідентифікатора сеансу - якщо генерація ідентифікатора сеансу передбачувана.

Ін'єкція SQL

4. Тестування функціональності пароля на запам’ятовування:

– Шукanb паролі, які зберігаються у файлі cookie. Необхідно переглядати файли cookie, збережені програмою. Облікові дані не зберігаються в прозорому тексті, а хешировані;

– освоєння механізму хешування: якщо він є загальним, відомим алгоритмом, перевірка його міцності та опробування декілька імен користувачів, щоб перевірити, чи можна легко угадати хеш-функцію;

– контролювати інші чутливі поля форми, наприклад, необхідно ввести в форму відновлення пароля або розблокування облікового запису в умовах ідповіді на таємне запитання.

3.8 Тестування можливостей витоку конфіденційних даних

Чутливі дані повинні бути захищені, коли передаються через мережу. На першому кроку перенесення SSL/TLS служби полягає у визначенні портів[25].

Наприклад, клієнт шукає SSL-служби за допомогою nmap з опцією “-sV”, яка використовується для ідентифікації сервісів, і вона також може ідентифікувати SSL-сервіси.

Реалізується за використанням сканера nmap та команди:

nmap -sV --reason -PN -n --top-ports 100 www.example.com, де:

-sV – на портах перевірка сервісів;

--reason – до порту спосіб підключення;

-PN - перевірка всіх хостів, які доступні на цей час;

--top-ports 100 – команда сканування портів та їх кількість;

www.example.com – веб – адреса, які сканується.

Забезпечення контролю та перевірки інформації про надійность алгоритмів шифрування, в складі SSL/HTTP – служби на порту 443 можна за допомогою команди:

nmap -sV --script ssl-enum-ciphers -p 443 <host>,

в випадках, коли web–додаток не використовує захищений протокол, наприклад, HTTPS, SSL або TLS. Може бути налаштовано нюхаюче спілкування за допомогою wireshark і tcpdump, щоб отримали ім'я користувача, пароль і конфіденційні дані компанії та розкрити конфіденційні дані web–додатка.

Тестування необхідно при наявності важливої інформації в вихідному коді або журналах. Пароль або encyrption ключ обов’язково кодуються з вихідного коду або конфігураційних файлів:

* grep -r –E "Pass | password | pwd |user | guest| admin | encry | key | decrypt | sharekey " ./PathToSearch/

За допомогою Metasploit Frameork методи тестування можливості витоку конфіденційних даних полягають в пошуку експлойтів до запущених служб, інформації про web–сервери та операційні системи.

4 МЕТОДИКА РОЗРАХУНКУ, АНАЛІЗУ ТА ОЦІНКА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ЛОКАЛЬНИХ МЕРЕЖ НОВИХ ПОКОЛІНЬ

4.1 Загальні положення

Одним з найцінніших активів (якщо не найбільше) локальних мереж компанії є її дані. Зловмисники, які віддані справі того, щоб бути злодіями локальних мереж, також це знають, тому вони намагаються різними методами атакувати мережу компанії та отримувати доступ до їх цінної інформації.

Нові типи досконалої «хакерської зброї», що здійснюють кібератаки, настільки урізноманітнилися, що вже недостатньо поставити брандмауер або будь-який інший Брандмауер наступного покоління - NGFW (Next-Generation Firewal) на межі локальної мережі.

Антивіруси також вже давно відіграють ключову роль у безпеці, особливо на робочих станціях користувачів, але в тому ж випадку їх недостатньо, щоб зупинити хитрі атаки. Адміністратор мережі знає, що це було б як заблокувати вхідні двері нашого будинку, але залишити всі вікна та задні двері відкритими. Тепер, коли атаки відбуваються в різних «рівнях» мережевих протоколів, для чого нам потрібні різні захисні системи для кожного типу трафіку.

Той факт, що все більше компаній постійно займаються веб-додатками, може зробити їх ще більш вразливими. Згідно з наступною діаграмою Statista, компанії RIA вкладають багато інвестицій у кібербезпеку[4].

На рисунку 4.1 представлено сегмент інвестування у кібербезпеку нових поколінь.

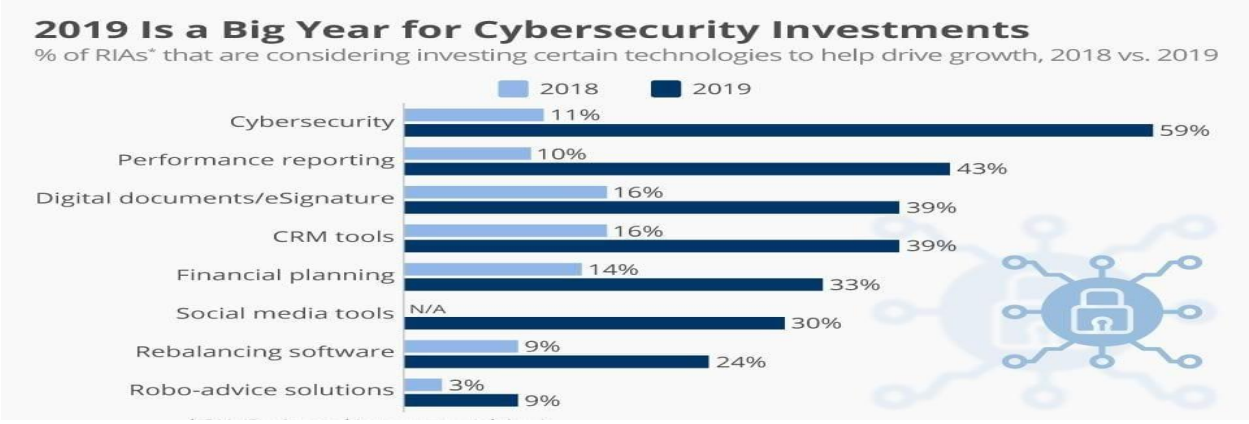


Рисунок 4.1 – Сегмент інвестування у кібербезпеку нових поколінь

4.2 Системи забезпечення безпеки локальних мереж нових поколінь

Існують два варіанти: брандмауер веб-додатків (WAF) та систему запобігання проникненню – IPS (Intrusion Prevention System).

Брандмауер web–додатків – WAF (Web Application Firewall) – це рішення (апаратне чи програмне забезпечення), яке працює як посередник між зовнішніми користувачами та веб–додатками.

Це означає, що весь зв'язок HTTP (запит-відповідь) аналізується WAF перед тим, як потрапити до web–програм або користувачів. Для здійснення моніторингу та аналізу трафіку HTTP WAF застосовує набір попередньо визначених правил, які роблять можливим виявлення шкідливих HTTP-запитів, таких як міжсайтові сценарії (XSS), SQL Injection, Dos або DDoS-атаки, маніпулювання файлами cookie, та багато інших[18].

Як тільки WAF виявляє загрозу, він блокує трафік і відхиляє шкідливий веб-запит або відповідь із конфіденційними даними. Якщо немає загроз або атак, весь трафік локальної мережі повинен протікати нормально, таким чином, щоб усі перевірки та захист були прозорими для користувачів.

На рисунку 4.2 представлено схема захисту трафіку локальної мережі на основі брандмауера web -додатків WAF.

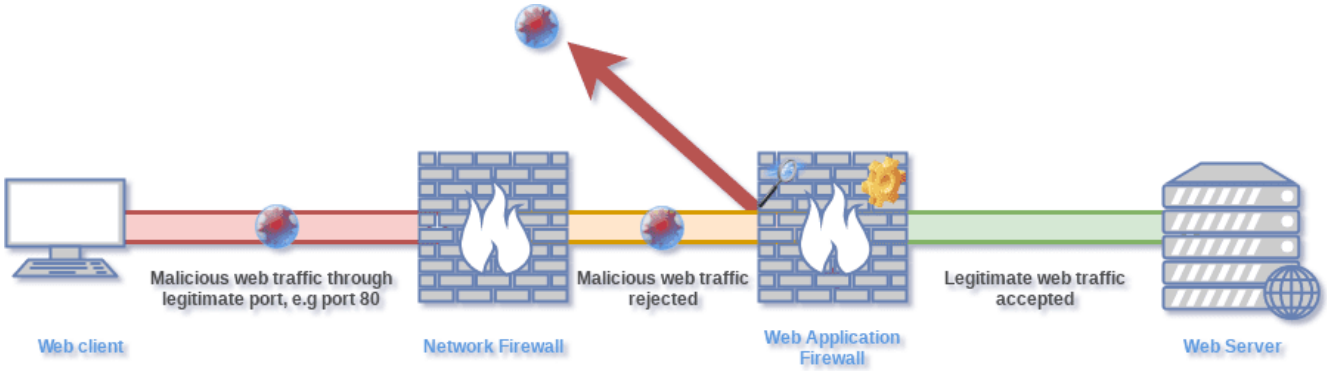


Рисунок 4.2 – Схема захисту трафіку локальної мережі на основі брандмауера web–додатків WAF

WAF розпізнає законний web-трафік і пропускає його. Це не впливає на повсякденні операції з діловими web–додатками.

Система запобігання проникненню (IPS). У випадку із системою запобігання проникненню (IPS) це більш загальний пристрій захисту або

програмне забезпечення. Він забезпечує захист від трафіку з різних типів протоколів, таких як DNS, SMTP, TELNET, RDP, SSH та FTP. IPS виявляє зловмисний трафік за допомогою різних методів, наприклад, виявлення на основі:

- підписів: IPS використовує виявлення на основі підпису так само, як це робить антивірус. Фірма може розпізнати загрозу та надіслати попередження адміністратору. Щоб цей метод працював коректно, усі підписи повинні мати останнє оновлення.
- політики: IPS вимагає, щоб політики безпеки були декларовані дуже конкретно. IPS розпізнає трафік, що не входить до цих правил, і автоматично відхиляє ненормальну поведінку або незвичний трафік.
- аномалій: за зразком нормальної поведінки дорожнього руху, цей метод можна використовувати двома способами - автоматичним або ручним. IPS автоматично виконує статистичний аналіз та встановлює стандарт порівняння. Коли трафік рухається занадто далеко від цього стандарту, він надсилає попередження.
- іншого способу - вручну встановити нормальну поведінку трафіку, щоб сповіщення надходили, коли трафік знову відходить від цього правила. Недоліком ручного способу є те, що, будучи менш гнучким і динамічним, він може надсилати помилкові попередження.
- Pot Detection: працює за допомогою комп’ютера, налаштованого на привернення уваги хакерів без шкоди для безпеки реальних систем. За допомогою цієї приманки атаки можна відстежувати та аналізувати, щоб після виявлення їх можна було використовувати для встановлення нових політик.

Пристрій IPS можна використовувати для підвищення безпеки та підтримки брандмауера. Очевидно, що навіть обидва рішення додають додатковий рівень безпеки для локальної мережі, вони працюють на різних типах трафіку. Тож, замість змагань, вони здебільшого доповнюють одне одного.

Незважаючи на те, що IPS, схоже, захищає ширший тип трафіку, є дуже конкретний, з яким може працювати лише WAF.

Як показано на рисунке 4.3, пристрій IPS блокує весь ненормальний трафік з Інтернету, який не був заблокований першою лінією оборони або брандмауером в локальної мережі.

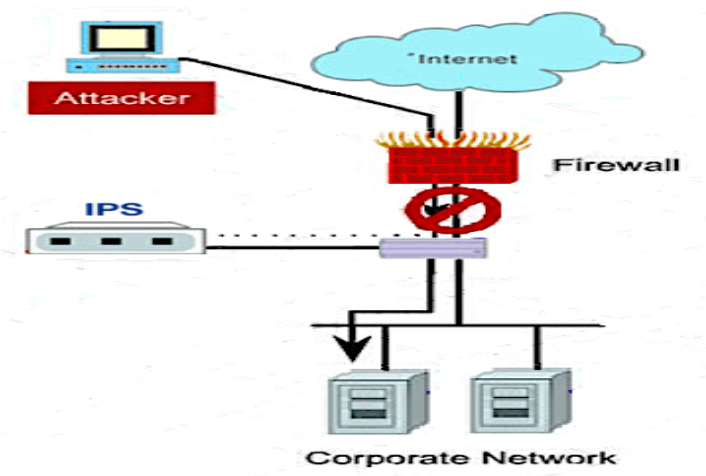


Рисунок 4.3 – Схема блокування ненормального трафіку з Інтернету

Споживачі мають можливості використовувати обидва рішення, особливо якщо локальні та корпоративні мережі тісно співпрацюють з технологіями Інтернету та IoT [5].

На рисунку 4.4 показано діаграма детального порівняння обох варіантів.

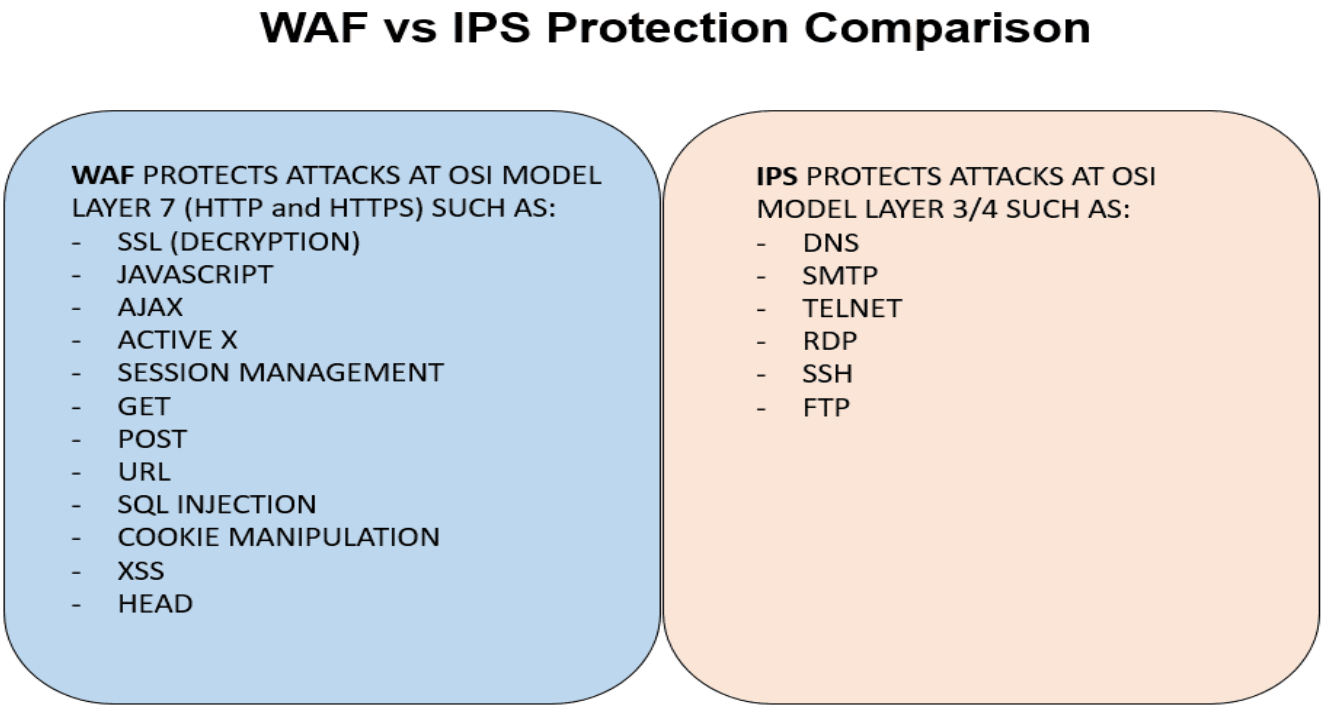


Рисунок 4.4 – Діаграма детального порівняння обох варіантів WAF та IPS

Зараз існує повне пакетне рішення, яке дає найкраще з обох світів. Завдання

полягає у виборі правильної апаратної системи WAF для ефективної роботи програмних механізмів безпеки. Найбільш практичним способом захисту корпоративного центру обробки даних від хакерів є впровадження програмно-апаратних чи гібридних рішень [14].

Вибираючи брандмауер web–додатків, необхідно враховувати наступні вимоги: прискорення SSL: SSL є критично важливим для WAF, оскільки це метод розвантаження процесора для надширокого шифрування відкритим ключем. Для оптимальної продуктивності реалізацій безпеки локальної мережі необхідно мати апаратний прискорювач.

DPI: Оскільки WAF розміщений між корпоративним сервером та користувачами, однією з основних задач WAF є відстеження трафіку та блокування будь–яких зловмисних спроб. Для цього потрібна ефективна глибока перевірка пакетів DPI (Deep Packet Inspection), яка підкріплена потужним обладнанням локальної мережі.

Висока продуктивність і висока пропускна здатність: оскільки DPI та SSL обидва вимагають наявність центрального процесора, тому необхідна апаратна архітектура для розгортання WAF повинна пропонувати спеціальні можливості обробки для запуска програмних продуктів.

Висока доступність: WAF працює цілодобово та без вихідних, і тому висока доступність щодо енергопостачання є критичною для оптимізації WAF. Масштабованість: Оскільки послуги web–додатків можуть розширюватися в міру зростання клієнтської бази, корпоративні WAF повинні масштабуватися за допомогою апаратних засобів, щоб підвищити продуктивність та пришвидшити критичні програми найпростішим способом.

Таким чином, WAF підходить для безпеки в програмах HTTP і зазвичай використовується для захисту серверів. WAF контролює веб-трафік, такий як HTTP GET, POST, URL, SSL тощо.

IPS, навпаки, забезпечує захист для широкого кола мережевих протоколів і може виконувати необроблене декодування протоколів і знаходити ненормальну поведінку, але не знає про сеанси (GET/POST), користувачів або навіть додатки. Інтегровані рішення можуть бути як апаратними, програмними, так і гібридними. Ці варіанти дають найкраще з обох рішень.

4.3 Методи розрахунку, аналізу та оцінка стійкості системи захисту інформації в локальних мережах нових поколінь

Універсальна система захисту всіх випадків не існує, так як захист створюється для конкретних елементів та об'єктів локальної мережі нових поколінь.

При швидкої зміні нових технологій та перспектив розвитку служб Інтернет та послуг IoT захист інформації повинен бути здатним адаптуватися до систем фіксованих та мобільних інфокомунікацій.

На практиці в більшості випадків захист системи суттєвий на портах та кордонах. Відомо, що при спробі подолати захист зловмисник спробує використовувати найбільш слабке напрям або кордон в цій системі.

З цієї причини підсумкова міцність систем ЗІ буде визначатися міцністю найбільш слабкого напрямку або кордону в цій системі. Якщо міцність слабкого кордону не задовольняє заданим вимогам, то цей рубіж зміцнюється або замінюється на більш міцний[27].

Отже, ймовірність ефективного захисту інформації при багаторубіжної системі визначається залежністю:

$$P_{\sum} = P_{CЗI1} * P_{CЗI2} * ... * P_{CЗIN} \quad , \qquad (4.1)$$

де *РСЗІN* – ймовірність ефективного захисту *N-го* рубіжу системи ЗІ, *N* - порядковий номер кордону.

Ефективність механізму захисту в значній мірі залежить від реалізації ряду принципів. По–перше, механізми захисту слід проектувати з урахуванням розподілу ресурсів між кордонами і можливістю їх перерозподілу.

По–друге, питання захисту слід розглядати комплексно в рамках єдиної системи захисту. Системний підхід забезпечує адекватний багаторівневий та багаторубіжний захист, що розглядається як комплекс організаційно-правових та технічних заходів.

Крім того, при реалізації механізмів захисту повинні використовуватися науково обґрунтовані технології захисту нових поколінь, що забезпечують необхідний рівень безпеки, прийнятність для користувачів і можливість

нарощування і модифікації систем ЗІ в перспективі.

Нехай комплексна система ЗІ характеризується великою кількістю рубежів *P*, які забезпечують протидію безлічі несанкціонованих дій – *Д*. Так як *P* складається з *n* рубежів, то *Д* містить – *m* дій.

Кожен рубіж $p_i \in P$ характеризується доступною потужністю – a_i. Відповідно до безліччю *P* маємо вектор ресурсів рубежів. Кожна несанкціонована дія відповідає набору дій зловмисника і має необхідний ресурс для виконання поставленого завдання (можливо і неодноразового) протягом доби – z_i (опер / сут).

За всім діям безлічі – *Д* маємо вектор $Z = (z_1, ..., z_m)$ необхідних ресурсів. По кожній дії дано два вектора, V_i *і* W_i де $V_i = (v_{i1}, ..., v_{in})$ безлічі *P*, вектор $W_i = (v_{i1}, ..., v_{im})$ визначає інтенсивність нападів під час нападу з завданнями інших протиправних дій безлічі – *Д*. Тут $w_{ii} = 0$.

По всій сукупності нападів маємо прямокутну матрицю *V* розміру *mxn* і квадратну матрицю *V* розміру *mxn*, складені з векторів і W_i, $1 \le i \le m$ відповідно. Будемо вважати, що ресурси несанкціонованої дії $d_i \in Д$ можуть бути реалізовані тільки проти одного будь-якого кордону безлічі *P*, тобто дія проводиться проти конкретного кордону.

Нехай дано безлічі *P* и *Д*, представлені кортежами <*P,a,R*> и <*Д,Z,V,W*>, де *a* - вектор доступності до інформації, *R* - матриця відстаней між рубежами, *Z* - вектор ресурсів протиправної дії, *V* - матриця інтенсивності нападів. Отже, потрібно знайти повне відображення: β: $Д \to P$, щоб середньоквадратична довжина $Д \to P$ маршруту несанкціонованих дій приймала мінімальне значення, тобто

Нехай дано безлічі P і Д, <P, a, R> і <Д, Z, V, W>, де a - вектор доступності до інформації, R - матриця відстаней між рубежами, Z - вектор ресурсів протиправної дії, V - матриця інтенсивності нападів. Отже, потрібно знайти повне відображення, щоб середньоквадратична довжина маршруту несанкціонованих дій приймала мінімальне значення, тобто:

$$L(\beta) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{i-1} S_{ij} Z_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{i-1} S_{ij}}, \qquad (4.2)$$

де $S_{ij} = \begin{cases} \sum_{k=1}^{n} v_{kj} h_{ki} + \sum_{k=1}^{m}\sum_{\alpha=1}^{k-1} w_{k\alpha} h_{ki} h_{\alpha j} \text{ при } i \neq j; \\ 0 \text{ при } i = j. \end{cases}$ $h_{ij} = \{0,1\}$

$h_{ij} = \{0,1\}$ визначає, цільову дію- a_i на конкретний рубіж- p_j,

$$h_{ij} = \begin{cases} 1, \ если \ \beta(d_i) = p_j; \\ 0 \text{ в противном случае} \end{cases}.$$

В умовах $\sum_{i=1}^{m} z_i h_{ij} \leq a$ для всіх $p_j \in P$.

Представимо вектор – Z в виді m–мірного вектору–стовбца, де z_i–обсяг протиправних дій під час нападу $-d_i$. Тоді функцію– β можна представити характеристичної функцією (характеристичної матрицею) H її трафіку, тобто:

$$H = \left\| h_{ij} \right\|_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}}.$$

Нехай p_i – номер деякого рубіжа. Двійковий m–мірний вектор–стовпець H_j, що містить одиницю на місцях з номерами складових протиправна дія, характеристичним способом, p_i – рубіжа.

Використовуючи описує скалярний добуток векторів Z і $H_i - ZH_i = \sum_{i=1}^{m} h_{ij}$ запишемо, що $H_j c_j$ дорівнює сумарній $a_i \in A$ з усіма рубежами, а добуток $-H_i c_j$, де $i \neq j$, так само інтенсивність потоку між рубежами p_i і p_j. Це значення S_{ij} вказано, тобто $S_{ij} = H_i c_j$. Квадратну матрицю рангу n значень S_{ij} позначено S.

Сумарний потік між рубежами составляє:

$$\lambda = \frac{1}{2}\sum_{j=1}^{n} H_j c_j . \qquad (4.3)$$

Тоді можна записати функціонал:

$$L(\beta) = L(H) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{i-1} s_{ij} r_{ij}}{\lambda}\ , \qquad (4.4)$$

$$\text{або}\quad L(\beta) = \frac{SR}{\frac{1}{2}\sum_{j=1}^{n} H_j c_j}\ . \qquad (4.5)$$

Таким чином, задача зводиться до мінімізації білінійного функціоналу на цілочисельних (довічних) векторах при лінійних обмеженнях виду $ZH_j \le a_j$ для всіх $-1 \le j \le n$.

При обраному критерії завдань нападів або розподілу по рубежах і зводиться розбиття до безлічі $Д$ на підмножини і призначенням цих продмножеств рубежів безлічі P, що відповідає спільним рішенням завдань розбиття графа на частини і завдання призначення.

Отримання оптимального рішення пов'язане з повним перебором різних варіантів розбиття. Для вирішення таких завдань використовується, як правило, метод гілок і меж. Недоліком цього методу є складність реалізації при порівняно невисокій ефективності.

Оскільки в системі ЗІ значення $m+n$ досить велике, доцільно використовувати для вирішення даного завдання евристичні алгоритми оптимізації. В основному відомі евристичні алгоритми можна віднести або до алгоритмів послідовної протидії підсистеми захисту, або до ітераційних алгоритмів послідовного поліпшення наближень за допомогою парних перестановок завдань між рубежами.

На практиці часто мають місце ситуації, коли кожне неправомірна дія $d_i \in Д$ представлена набором завдань, які можуть протистояти різні рубежі безлічі P, і коли нападу d_i протистоїть тільки один рубіж [26]. У цьому випадку розглянута задача кілька спрощується і може бути зведена до класичної транспортної задачі.

Нехай задані безлічі *P* и *Д*, де *P* має раніше вказані сенс і представляється кортежем <*P,a,R*>.

Безліч *Д* складено з *m* нападів $\{d_1,...,d_m\}$. Кожний напад $-d_i \in Д$ представлен набором завдань і характеризується необхідним ресурсом $-Z_i$ для їх реалізації. За всіма протиправними діями *Д* є вектор потрібних ресурсів $-Z=(z_1,...,z_m)$. Необхідний ресурс $-Z_i$ нападу $-d_i$ може бути припинений однією або декількома рубежами безлічі *P* при будь-якому розбитті $-Z_i$ між собою.

По кожному нападу $-d_i \in Д$ показан вектор $-V_i=(v_{i1},...,v_{1n})$, який визначає інтенсивність нападів $-d_i$, на рубежі безлічі *P*. Передбачається, що всі завдання пов'язані з нападом $-d_i \in Д$ мають однакову питому, щодо одиниці необхідного ресурсу, інтенсивністю – f_{ij} протиправних дій проти рубежів – $p_i \in P$, тобто:

$$\forall d_i \in Д, p_i \in P \left| f_{ij} = \frac{v_{ij}}{r_i}. \right. \qquad (4.6)$$

Отже, маємо в якості вихідної інформації безлічі *P* і *Д*, представлені відповідно кортежами:

$$<P,a,R> \; i \; <Д,Z,V>,$$

де *V* –матриця інтенсивностей нападів безлічі *Д* на рубіж безлічі *P*. Потрібно визначити розподіл ресурсів нападів Д по рубежах безлічі Р. В результаті розподілу ресурсів нападу формується матриця Q, в якій кожному протиправному дії повинна бути порівняно вектор–рядок $q_i=(q_{i1},...,q_{in})$ розмірності *n*, що представляє собою розподіл ресурсів протиправних дій d_i по рубежах безлічі Р, тобто по рубежах безлічі, де. *k*-й компонент q_{ik} вектора q_i являє собою обсяг завдань нападу $-d_i$ на *k*-й рубіж захисту.

Д – тут, n– сукупність розподілів протиправних дій безлічі Д визначено як відображення γ: $Д \to N^n$, тут N^n – векторний простір *n*– мірних векторів,

компоненти яких є цілими числами. Якість розподілу γ буде оцінено значенням середньозваженої довжини та з оцінкою значення середньозваженої довжини $L(\gamma)$ маршруту нападу.

Основою визначення $-L(\gamma)$ служить штраф для одиниці ресурсу нападу – $d_i \;\; i=1,2,...,m=[Д]$, закріпленного за p_j–м рубежом. Якщо одиниця ресурсу нападу діюча на p_j–й рубіж, то їй відповідає штраф:

$$c_{ij}=\sum_{k=1}^{n} f_{ik} r_{jk}=\sum_{k=1}^{n} r_{ik}\frac{v_{ik}}{z_i}. \tag{4.7}$$

Отже для кожного нападу $-d_i \in Д$ є вектор $-c_i=(c_{i1},...,c_{in})$, k-й компонент $-c_{ik}$ якого визначає збитки за одиницю ресурсу нападу закріплюється за кордоном $-p_k$.

Функція шкоди, яка характеризує вбрання розподіл протиправних дій $-\gamma$ по рубежах, має вигляд:

$$F(\gamma)=\sum_{i=1}^{m}\sum_{j=1}^{n} q_{ij} c_{ij}. \tag{4.8}$$

При складанні розкладу $-\gamma$ бажано мінімізувати функцію:

$$L(\gamma)=\frac{1}{\lambda}F(\lambda), \tag{4.9}$$

де λ – незалежна від розподілу величина, яка визначає сумарний потік нападів у відповідності з виразом:

$$\lambda=\sum_{i=1}^{m}\sum_{j=1}^{n} v_{ij} \;\text{ або }\; \lambda=\sum_{i=1}^{m}\sum_{j=1}^{n} q_{ij} j_{ij}. \tag{4.10}$$

Якщо $-\gamma$ – вбранний розподіл, то він, очевидно, має відповідати таким вимогам:

1) $\forall d_i \in Д \left| \gamma(d_i) = q \geq 0 = \overbrace{0,0,...,0}^{n} \right.$ (позитивність),

2) $\forall d_i \in Д \left| \sum_{j=1}^{n} q_{ij} \leq z_i \right.$ (обмеженість),

3) $\sum_{\forall d_i \in Д} q_i \leq a = (a_1,...,a_n)$ (реалізованість).

Таким чином, завдання розподілу необхідних ресурсів нападу між рубежами в наведених вище поняттях і позначеннях може бути сформульована таким чином, щоб <Д, Z, V> <P, a, R>.

Нехай задана система несанкціонованих дій <Д,Z,V> і система захисту <P,a,R>. Потрібно визначити позитивний, обмежений і реалізпцію розподілу $-\gamma$, щоб $L(\gamma)$ мав мінімальне значення.

Поставлений такий спосіб завдання, зводиться до класичної транспортної задачі:

$$\sum_{j=1}^{n+1} a_j = \sum_{i=1}^{m+1} z_i \,. \qquad (4.11)$$

Дана математична модель транспортної задачі має $n+m+1$ змінних. Для її вирішення може бути використана одна з модифікацій симплекс–методу (метод потенціалів).

4.4 Метрики захисту транспортних ресурсів локальної мережи

DDoS (Distributed Denial of Service) –атака – це така помітна атака, яка представляє собою дуже серйозну загрозу безпеці локальної мережі в цілому. Як правило, DDoS–атака запускається скоординованим чином, ставлячи під загрозу мільйони локальних та корпоративних систем, вільно доступних в Інтернеті, що становлять армію зомбі, званих ботнетами (Wang et al., 2012).

Існує дві категорії DDoS-атак (a) Мережеві (рівень 3/4) DDoS-атаки, які націлені на мережевий і транспортний рівні. Такі атаки відбуваються, коли кількість пакетів даних і іншого трафіку перевантажують мережу або сервер і споживають все його доступні ресурси, і (b) web–додаток (прикладний рівень 7

OSI) DDoS–атаки, що використовують порушення або вразливість в web–дизайні додатків для придушення web–сервера або бази даних, що приводить в дію web–додаток, з метою його пошкодження.

Такі атаки імітують законний трафік користувачів, ускладнюючи їх виявлення. В даний час DDoS–атаки прикладного рівня відбуваються частіше, коли досвідчені зловмисники використовують бот–мережі для відправки надлишкових законних запитів на вибірку або виконання запитів в базах даних пошукових систем, розгорнутих на web–серверах. Пік найбільшої атаки на рівні web–додатків в 2017 році досяг 173 633 RPS (кількість запитів в секунду).

Перш за все, існують два типи методів виявлення DDoS–атак:

- (a) методи виявлення на основі сигнатур, які працюють на основі вже збережених сигнатур атак, які відповідають відомим шаблоном з шаблоном вхідних пакетів;
- (b) методи виявлення аномалії, які засновані на порівнянні попередньо побудованої моделі поведінки мережі з вхідним поведінкою мережі в режимі реального часу.

Виявлення на основі аномалій має деякі внутрішні обмеження. По-перше, досвідчені зловмисники можуть відстежувати мережевий трафік для навчання своїх систем виявлення.

По–друге, труднощі в налагодженні оптимального порогу призводить до збільшення числа помилкових спрацьовувань.

По–третє, дуже важко витягти як якісно, так і точно відповідні ознаки законного і аномального поведінку мережі. З іншого боку, методи виявлення на основі сигнатур вимагають оновлених сигнатур для їх ефективної роботи. Виходячи зі швидкості трафіку, DDoS–атаки можна розділити на:

– (a) високошвидкісні DDoS–атаки (HR-DDoS), коли швидкість трафіку сильно відрізняється від допустимого трафіку;

– (b) низкоскоростной DDoS (LR-DDoS)–атака, коли швидкість трафіку дорівнює або менше, ніж законна швидкість трафіку.

Високошвидкісні DDoS–атаки (HR–DDoS) в даний час переважають, маючи обсяг трафіку понад 900 Гбіт / с. Вкрай важливо своєчасно виявляти такі атаки, щоб забезпечити своєчасну доставку широко використовуваних Інтернет–сервісів і додатків.

Атаки HR–DDoS часто об'єднуються з декількома низькошвидкісними атаками DDoS (LR–DDoS), які мають ту ж розподілену природу, що і атаки HR–DDoS, але мають низьку швидкість трафіку. Диференціація DDoS–атаки від легітимного трафіку є величезною проблемою для дослідників мережевої безпеки, оскільки зловмисники щоразу завдають жертві більш витончені прийоми. Відомі сайти є головними жертвами таких DDoS–атак.

З цього експоненціального збільшення трафіку атаки видно, що зловмисники постійно оновлюють свої навички, використання передових методів для генерації такої величезної кількості трафіку і в той же час поразки існуючих оборонних рішень.

Існує ще один вид мережевого трафіку, який називається флеш–подією (FE, flash event), що також викликає відмову в обслуговуванні. FE схожий на атаку HR–DDoS, коли тисячі законних користувачів намагаються одночасно отримати доступ до певного обчислювального ресурсу, такого як web–сайт. Це спричиняє несвоєчасну доставку відповідей від web–служби, подібно до випадку атаки HR–DDoS, і, отже, вимагає негайних дій. І атаки HR–DDoS, і IP мають багато загальних поведінкових характеристик, таких як збільшення обсягу трафіку, затримка відповідей web–сервера тощо, але все ж між ними є кілька параметричних відмінностей.

Крім того, подібність мережевих потоків, менша пропускна здатність і тривалість трафіку на IP–джерело є деякими обґрунтуваннями, які відрізняють атаку HR-DDoS від FE (Behal et al., 2017a, Behal et al., 2017b).

Важливо відзначити, що успішні схеми захисту DDoS–атак не тільки визначаються базовим алгоритмом виявлення, але й залежать від їх розміщення (Gulisano et al., 2015).

Насправді DDoS–атаки походять з різних джерел мереж. Кожен пакетний потік витікає із системи через web–сервер або маршрутизатор в Інтернет через один або кілька основних маршрутизаторів, що називаються автономними системами (AS), і, нарешті, до самої цілі.

Рішення DDoS Defense можна розгорнути в деяких або всіх цих місцях. Залежно від місць розгортання, захисні рішення можна класифікувати на вихідні, проміжні мережі та жертви. Звичайні методи безпеки, такі як списки контролю доступу елементів локальної мережі: маршрутизатора, міжмережеві екрани,

системи виявлення та запобігання вторгнень, не здатні ефективно захищати від DDoS-атак і FE[16].

Ось чому до цих пір не існує ідеального рішення для виявлення атак DDoS і FE. Деякі з причин можуть бути децентралізованим характером Інтернету, відсутністю співробітництва між Інтернет-провайдерами, змінами інфраструктури, побічними втратами, відсутністю останніх реальних наборів даних і застарілих методів, використовуваних для цілей перевірки, а також проблемами розгортання і т. д.

Тому DDoS web–атаки призводять до значних відхилень у розподілі трафіку в мережі. Метрики виявлення, засновані на теорії інформації, такі як ентропія або розбіжність, можуть швидко зафіксувати такі зміни в трафіку мережі. З безлічі метрик, заснованих на теорії інформації, використана нова метрика/дівергентность для виявлення DDoS–атак і FE, тому що вона більш ефективна і здатна вимірювати навіть лагідні варіації, невизначеність або випадковість в розподілі ймовірності. Пропонується розподілений підхід для виявлення різних типів DDoS–атак.

Кожне можливе місце розгортання має свої сильні та слабкі сторони. Вузли поблизу жертви можуть уважно спостерігати за повним трафіком атаки, моделювати його поведінку та ефективно виявляти аномалії, тоді як механізми, розгорнуті в інших місцях, можуть бачити лише частковий трафік атаки і, можливо, доведеться вжити заходів на основі неповної інформації про атаку. Однак під час типової атаки HR–DDoS або FE різні мережеві та серверні ресурси, такі як пропускна здатність, цикли процесора, пам'ять тощо, часто перевантажуються. У таких випадках розгортання оборони жертви не може ефективно виявити та охарактеризувати атаки на трафік. Через відсутність достатніх обчислювальних ресурсів він може почати скидати легітимні пакети замість того, щоб скидати атакуючі пакети, що призведе до збільшення кількості помилкових спрацьовувань. Звичайні методи безпеки, такі як списки контролю доступу маршрутизаторів, брандмауери, системи виявлення та запобігання вторгненню, не здатні ефективно захищати від DDoS–атак та IP. Ось чому немає ідеального рішення для цього поточного виявлення DDoS–атак та IP до теперішнього часу; деякими причинами можуть бути децентралізований характер Інтернету, відсутність співпраці між провайдерами, зміни інфраструктури,

побічний збиток, відсутність останніх реальних наборів даних та застарілих методів, що використовуються для перевірки, а також проблеми розгортання.

Помічено, що попередні видатні дослідження широко використовували варіації метрик, заснованих на теорії інформації, Ентропії Шеннона, Узагальненої Ентропії та Дивергенції, таких як дивергенція Куллбека-Лейблера для виявлення DDoS-атак та FE.

Пропонується використовувати нову узагальнену метрику Di–Divergence, розбіжності на основі теорії інформації для розподіленого виявлення та пом'якшення різних типів DDoS–атак та FE. Запропонована метрика виявлення обчислюється у всіх точках проникнення, званих PoP, і надсилається центральному координатору, розташованому в приміщенні мережі жертв, який потім об'єднує метрику виявлення.

Тому запропонован розподілений підхід на основі метрики gence–розбіжність для розподілу сховища та обчислювальних накладних витрат на розгортання захисту жертви. Це також призвело до захисту пропонованого розподіленого рішення від великого обсягу мережевих пакетів, що генеруються під час DDoS–атак та FE.

Результати звітування показують, що система захисту від D–FAC на основі розбіжностей ефективніше виявляє різні типи DDoS–атак; і перевершив існуючі системи, засновані на ентропії Шеннона, узагальненій ентропії та інших заходах дивергенції. Ця ефективність вимірювалася за допомогою різних показників оцінки системи виявлення, таких як точність виявлення, FPR, F–міра, швидкість класифікації та точність.

Конструкція системи захисту D–FAC є надійною та стійкою до несправностей, оскільки вона може продовжувати свою роботу навіть у тому випадку, якщо деякі з PoP не надсилають обчислену метрику виявлення вчасно.

Запропонований розподілений алгоритм виявлення не залежить від будь–якого конкретного інструменту атаки DDoS або шаблону атаки. Отже, його можна використовувати для виявлення DDoS–атак і в майбутньому.

Запропонована система захисту D–FAC була перевірена з використанням реального мережевого трафіку, що генерується за допомогою набору інструментів базових атак та генераторів трафіку, а також модельованого відстеженням

моделювання помітно використовуваних реальних наборів даних при перевірки DDoS.

Модель системи D–FAC. Як DDoS–атаки, так і FE викликають значні відхилення у розподілі мережевого трафіку. Показники виявлення, засновані на теорії інформації, такі як Ентропія або Розбіжність, можуть швидко фіксувати такі зміни в мережевому трафіку. З безлічі метрик, заснованих на теорії інформації, використана нова метрику ϕ- Divergence для виявлення DDoS–атак та IP, оскільки вона є більш ефективною та сприйнятливою для вимірювання навіть помірних варіацій, невизначеності чи випадковості розподілу ймовірностей[15].

Існує безліч метрик розбіжностей, заснованих на теорії інформації, які можна використовувати для кількісної оцінки різниці між набором розподілів ймовірностей.

Для будь–яких двох дискретних ймовірностей розподіли

$P = (p1, p2, \ldots\ldots, pN)$ *ma* $Q = (q1, q2, \ldots\ldots, qN)$ *з* $\sum i = 1Npi = \sum i = 1Nqi = 1$, $i = 1,2,\ldots, N$, узагальнена інформаційна дивергенція (GID) визначається як:

$$n\, D\alpha\,(P\|Q) = 1/1\text{-}\alpha log\sum piαqi1\text{-}\alpha,\ \alpha \geqslant 0.\ i = 1\ , \qquad (4.12)$$

де N – загальна кількість мережевих потоків, отриманих у часовому вікні. Тут $D\alpha$ представляє значення розбіжності, обчислене за допомогою метрики GID для параметра ентропійного індексу α. Коли $\alpha \rightarrow 1$, розбіжність Куллбека-Лейблера (KL) виводиться наступним чином:

$$D1\,(P\|Q) = \sum i = 1Npilogpiqi. \qquad (4.13)$$

Далі пропонується використовувати ϕ–Divergence, яка базується на f–Divergence. ϕ–Divergence визначається як:

$$D\alpha\,'\,(P\|Q) = \sum i = 1Npisinh\,(\alpha logpiqi)\,sinh\,(\alpha),\ \alpha \rightarrow 1. \qquad (4.14)$$

Тут $D\alpha\ '$ представляє значення розбіжності, обчислене за допомогою метрики ϕ- Divergence на параметр ентропійного індексу α. Запропонований вище показник розбіжності має несиметричний характер.

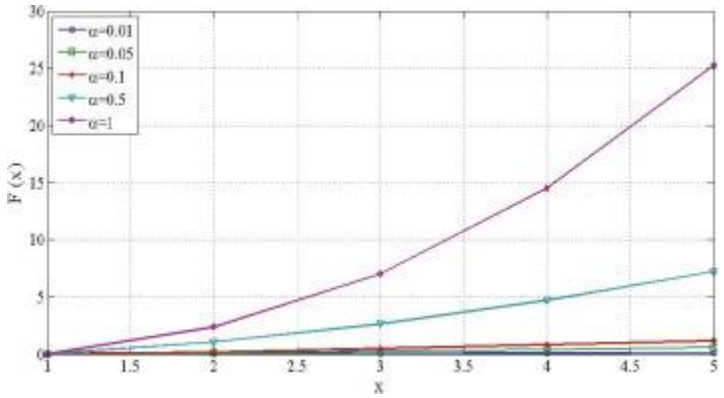
Симетрична версія ϕ- Divergence дається за формулою:

$$DJ\alpha = D\alpha\,'(P, Q) + D\alpha\,'(Q, P) \quad (4.15)$$

Визначальна функція ϕ- Divergence подана як:

$$F(x) = x\sinh(\alpha \log(x) / \sinh(\alpha), \alpha > 0 \quad (4.16)$$

Поведінка $F(x)$ на різних α-порядку показано на графіках рис. 4.5.



1. Завантаження: Завантаження зображення високої роздільної здатності (77 КБ)
2. Завантаження: Завантаження зображення в повному розмірі

Рисунок 4.5 – Графіки залежності поведінки F (x) від збільшення α-порядку

Очевидно, що значення $F(x)$ зростає експоненціально з незначним збільшенням α-порядку.

Аналіз графіків показує, що використання властивісті для збільшення інформаційної відстані між двома потоками мережевого трафіку, призвело до більшої ефективності виявлення метрики Di–Divergence.

Таким чином, метрика ϕ–Divergence має вищу швидкість збіжності для досягнення конкретного рішення, і вона дала кращі результати в порівнянні з іншими метриками на основі ентропії. Це пояснюється тим, що метрика розбіжності обчислюється з використанням окремих значень розподілу ймовірностей з у часовому вікні, тоді як метрика ентропії просто узагальнює варіації розподілу ймовірностей до одного значення. Отже, метрики розбіжності краще підходять для прогнозування моделі змін розподілу ймовірностей порівняно з метриками, заснованими на ентропії, які можуть бути легко обмануті

досвідченими зловмисниками. Тому набагато кращі результати можна отримати за допомогою метрики ϕ–Divergence порівняно з іншими існуючими широко використовуваними метриками теорії інформації.

ВИСНОВКИ

В атестаційній роботі магістра на тему: «Захист інформації «Інтернет речей в локальних мережах» виконано завдання у повному обсязі.

В першому розділі представлені аналіз перспектив розвитку концепції Internet of Things.

Розглянуто технології та стандарти для комутації та конвергенції інфраструктури Інтернету речей. Досліджені варіанти підключення IoT до існуючих мереж.

Інтернет речей або, як його ще називають, мережа мереж є мережею різноманітних підключених до Інтернету пристроїв, що реалізують різні моделі взаємодії - «Річ - Річ» (Thing-Thing), «Річ - Користувач» (Thing-User) і «Річ - Web - Об'єкт »(Thing-Web Object). З'єднання «розумних речей» (від англ .: Smart Things) в єдину мережу надає критично важливі якісні зміни для розвитку людської життєдіяльності Наприклад, в сучасних автомобілях працюють відразу кілька мереж: одна управляє роботою двигуна, інша - системами безпеки, третя підтримує зв'язок і т.д.

Досліджені моделі комутації споживачів PAN до LAN, WAN та Інтернету. Представлені інфраструктура та безпека IoT–платформ.

В офісних і житлових будівлях також встановлюється безліч мереж для управління опаленням, вентиляцією, кондиціюванням, телефонним зв'язком, безпекою, освітленням. У міру розвитку Інтернету речей та багато інших мереж будуть підключатися один до одного і набувати все більш широкі можливості в сфері безпеки, аналітики та управління. В результаті Інтернет речей придбає ще більше можливостей відкрити людству нові, більш широкі перспективи.

В другому розділі проведені дослідження основних методів захисту інформації послуг Інтернет-речей в локальних мережах

Проведено аналіз безпеки Інтернету речей локальних мереж, яка будується на фундаменті з чотирьох напрямів:

- безпека зв'язку;
- захист пристроїв;
- контроль пристроїв;

– контроль взаємодій в мережі.

Таким чином, безпека IoT повинна бути комплексною. Всі вектори загроз повинні придушуватися. Іноді такі атаки відбуваються через локальну мережу, які підключені до промислової мережі або до локальної мережі IoT, в інших випадках атака відбувається через Інтернет або через прямий фізичний доступ до пристрою.

Однак, найбільш простий вид атак, який може бути реалізований на рівні доступу, є відправка даних від Інтернет-речей в альтернативний хмарний сервіс, який буде далі розглянуто в роботі - «хибна хмара»[28].

Для захисту даних, що надходять від Інтернету-речей до віддаленого хмарного сервера через мережі зв'язку загального доступу пропонується використовувати такі методи захисту на основі алгорітмів:

– Метод захисту на базі використання алгоритмів гібридного шифрування;

– Метод захисту на базі створення унікальних патернів мережевого трафіку.

В роботі розглянуто такий вид уразливості Інтернет-речей, як перехват і відправка даних в хибні хмари, і запропоновані методи захисту. Найбільш ефективним є метод створення унікальних паттернів при захистї мережевого трафіку Інтернет-речей, відповідний як для малопотужних Інтернет-речей на базі мікроконтролера, так і для більш потужних речей на базі мікропроцесорів, включаючи малопотужні 8-й розрядні мікроконтролери.

В третьому розділі представлені методи тестування елементів локальних мереж та особливості вимог нормативного забезпечення.

Запропонована методологія тестування та сканування елементів локальної мережі на базі сканеру Nmap, що входить до ОС Kali Linux. Nmap ("Network Mapper").

Проведен детальний аналіз результатів тестування відкритих портів та сканування запущених служб на web-сервері, сценаріїв встановлення типу операційної системи, контролю сервісів та їх версій та різних типів ін'єкцій.

Заходи щодо забезпечення безпеки можна умовно розділити за чотирма напрямками - підключення, ідентифікація, шифрування трафіку і безпеки додатків.

Збереження цілісності та конфіденційності даних досягається застосуванням шифрування для аутентифікації і збереження цілісності повідомлень. Процедура передбачає підтвердження даних користувача і ліквідності використовуваних сертифікатів, що досить складно реалізувати в глобальних масштабах, тому виробники часто жорстко вбудовують облікові дані в програмно-апаратний комплекс. Ця інформація дозволяє чітко ідентифікувати пристрій, але не годиться для забезпечення цілісності даних. На транспортному рівні питання безпеки передачі даних вирішується в рамках протоколів Transport Layer Security (TLS) і Datagram TLS (DTLS) шляхом створення захищеного тунелю для додатків.

Але незважаючи на це, додатки є найбільш вразливою частиною рішення. Їх безконтрольне поширення становить серйозну загрозу. Надання розподіленої платформи для обробки даних різними додатками - одна з особливостей архітектури Інтернету речей, і основні тенденції в удосконаленні протоколу їх безпечного підключення OAuth 2.0 Internet of Things - виявлення розумних речей і їх аутентифікація, використання цифрових ідентифікаторів і централізоване управління доступом до ресурсів.

В четвертому розділі представлена методика розрахунку, аналізу та оцінка методів захисту інформації локальних мереж нових поколінь

Проведен аналіз системи забезпечення безпеки локальних мереж нових поколінь та схеми захисту трафіку локальної мережі на основі брандмауера web–додатків WAF.

Запрпонована та описана схема блокування ненормального трафіку з Інтернету.

Приведена діаграма детального порівняння обох варіантів систем захисту інформації WAF та IPS в локальних мережах нових поколінь (НП).

Ефективність механізму захисту в значній мірі залежить від реалізації ряду принципів. По–перше, механізми захисту слід проектувати з урахуванням розподілу ресурсів між кордонами і можливістю їх перерозподілу.

По–друге, питання захисту слід розглядати комплексно в рамках єдиної системи захисту. Системний підхід забезпечує адекватний багаторівневий та багаторубіжний ЗІ, що розглядається як комплекс організаційно-правових та технічних заходів.

Розроблена математична модель на прикладі комплексної системи ЗІ, яка

характеризується великою кількістю рубежів в локальної мережі НП.

Дана математична модель транспортної задачі має $n+m+1$ змінних. Для її вирішення може бути використана одна з модифікацій симплекс–методу (метод потенціалів).

Запрпонована методика захисту транспортних ресурсів локальної мережи від DDoS (Distributed Denial of Service) –атак[16].

Побудовані графіки залежності поведінки F (x) від збільшення α-порядку. Аналіз графіків показує, що використання властивості для збільшення інформаційної відстані між двома потоками мережевого трафіку, призвело до більшої ефективності виявлення метрики Di–Divergence.

Таким чином, метрика ϕ–Divergence має вищу швидкість збіжності для досягнення конкретного рішення, і вона дала кращі результати в порівнянні з іншими метриками на основі ентропії.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Основи криптографічного захисту інформації в телекомунікаційних системах. Навчальний посібник. Частина 1 / В. В. Поповський, А. В. Персіков. – Харків: СМИТ, 2010. – 352 с.

2. Koucheryavy A.State of the Art and Research Challenges for USN Traffic Flow Models / A. Koucheryavy // 16th International Conference on Advanced Communication Technology (ICACT), IEEE, 2014. - PP. 336-340.

3. Koucheryavy A. The Mobile Sensor Network Life-Time under Different Spurious Flows Intrusion / A. Koucheryavy, I. Bogdanov, A. Paramonov // Lecture Notes in Computer Science. - 2013. - Vol. 8121. - PP. 312-317.

4. Bhattasali T.Sleep Deprivation Attack Detection in Wireless Sensor Networks /T. Bhattassali, R. Chaki, S. Sanyal // International Journal of Computer Applications. - 2012. - Vol. 40, Iss. 15. - PP. 19-25.

5. Iera A.The Internet of Things / A. Iera, C. Floerkemeier, J. Mitsugi, G. Morabito // IEEE Wireless Communications. - Vol. 17. Iss. 6. - PP. 8-9.

6. Рибас К. В., Скалозуб В.В., Методи забезпечення захисту трафіку Інтернет–речей, Шоста Міжнародна науково-технічна конференція: «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв'язку (ЕМС-2020)» –ХНУРЕ:Харьків,48-53с.

7. Рибас К. В., Скалозуб В.В., Реалізація методів захисту інфраструктури web-додатків хмарних сервісів, The 1-st International scientific and practical conference «European scientific discussions» (November 28–30, 2020) Potere della ragione Editore, Rome, Italy. 2020. – 776 p., 230 – 236p. ISBN 978-88-32934-02-1

8. Рибас К. В., Скалозуб В.В., Методи захисту послуг хмари, IV Международная научно-практическая конференция «PRIORITY DIRECTIONS OF SCIENCE AND TECHNOLOGY DEVELOPMENT», 20-22 декабря 2020 года Киев, Украина, 1-7с.

9. ISO/IEC 27000:2018 - an overview and introduction to the ISO27k standards plus a glossary for the specialist vocabulary.

10. ISO/IEC 27003:2017 provides pragmatic guidance on how to implement ISO/IEC 27001.

11. ISO/IEC 27034:2011+ provides guidance for application security (in 7½ parts).

12. Защита веб-приложений, Богдан Тоболь, [Електроний ресурс]-доступ до ресурсу: https://www.anti-alware.ru/analytics/Technology_Analysis/web-security-myths-and-reality-2018.

13. Latest DDoS attack trends Report, [Електроний ресурс] - доступ до ресурсу: http://www.darkreading.com/vulnerabilities- and-threats/ddos-attack-trends-by-the-numbers/d/d-id/1326754- 2016.

14. Ma, X., Chen, Y., DDoS detection method based on chaos analysis of network traffic entropy. Commun. Lett., IEEE 18 (1), 2014-114–117pp.

15. Monosek Network analysis tool, [Електроний ресурс]- доступ до ресурсу:http://www.ncs-in.com, 2016.

16. Ozcelik, Brooks, R.R., 2015. Deceiving entropy based DoS detection. Comput. Secur.48, 234–245 pp.

17. Ranjan, S., Swaminathan, R., Uysal, M., Nucci, A., Knightly, E., DDoS-shield: DDoS-resilient scheduling to counter application layer attacks. IEEE/ACM Trans. Netw. 17 (1), 2009 – 26–39pp.

18. Recent DDoS Attacks Report, [Електроний ресурс] – доступ до ресурсу: https://www.ddosattacks.net/twitter-amazon-other- top-websites-shut-in-cyber-attack/, 2016.

19. Sachdeva, M., Singh, G., Kumar, K., Singh, K.,. Measuring the impact of DDoS attacks on web services, Citeseer – 2010.

20. Sachdeva, M., Kumar, K., Singh, G., A comprehensive approach to discriminate DDoS attacks from flash events. J. Inf. Secur. Appl. 26. 2016. 8–22 pp.

21. Saravanan, R., Shanmuganathan, S., Palanichamy, Y., Behavior-based detection of application layer distributed denial of service attacks during flash events. Turk. J. Electr. Eng. Comput. Sci. 24 (2), 2016 -510–523 pp.

22. Singh, K., Singh, P., Kumar, K.,. Application layer http-get flood DDoS attacks: research landscape and challenges. Comput. Secur. 65, 2017- 344–372 pp.

23. Singh, K., Singh, P., Kumar, K., Impact analysis of application layer ddos attacks on web services: a simulation study. Int. J. Intell. Eng. Inf. 5 (1), 2017- 80–100 pp.

24. Wang, F., Wang, H., Wang, X., Su, J., A new multistage approach to detect subtle DDoS attacks. Math. Comput. Modell. 55 (1), 2012-198–213pp.

25. Wang, C., Miu, T.T., Luo, X., Wang, J., 2018. Skyshield: A sketch-based defense system against application layer DDoS attacks. IEEE Trans. Inf. Forensics Secur. 13 (3), 559–573pp.

26. Xiang, Y., Li, K., Zhou, W., 2011. Low-rate DDoS attacks detection and traceback by using new information metrics. IEEE Trans. Inf. Forensics Secur. 6 (2), 426–437pp.

27. Yu, S., Zhou, W., 2008. Entropy-based collaborative detection of DDoS attacks on community networks, Pervasive Computing and Communications, 2008. Sixth Annual IEEE International Conference on PerCom 2008. IEEE, 566–571 pp.

28. Yu, S., Thapngam, T., Liu, J., Wei, S., Zhou, W., 2009. Discriminating DDoS flows from flash crowds using information distance, NSS'09. Third International Conference on Network and System Security, 2009. IEEE, 351–356 pp.

29. Васильєв А.Б.Тестування мереж зв'язку наступного покоління. А. Б. Васильєв, Д.В. Тарасов, Д.В. Андрєєв, А. Е. Кучерявий. - М.: ФГУП ЦНІІС, 2008. - 140 с.

30. Богданов І. А. Характеристики життєвого циклу мобільного сенсорної мережі при різних потоках помилкових подій / І. А. Богданов, А. І. Парамонов, А. Е. Кучерявий // Електрозв'язок. - 2013. - № 1. - С. 32-33.

31. Stankovich J.A Vision of a Smart City in the Future / J. Stankovich // Smart Cit- ies. - 2013. - Vol. 1, Iss. 10.

32. Доценко С. М.Системи виявлення вторгнень на основі вбудованих мікропроцесорних систем / С. М. Доценко, А. Г. Владико, І. Д. Летенко // телеком комунікація. - 2013. - № S7. - С. 15-18.

33. Локальные вычислительные сети. Справочник. Под ред. С.В. Назароваю М.: "Финансы и статистика",2004. – 238с.

34. В.С.Барсуков «Безопасность: технологии, средства, услуги» М. Кудиц - образ 2001.- 236с.

35. Основи локальних мереж [Електроний ресурс]-2016 – Доступ до ресурсу: ресурсу:http://www.intuit.ru/department/network/baslocnet/9/.