МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

“ На правах рукопису”
УДК

До захисту допущено
Завідувач кафедри СІКЗ
_____ Шуклін Г.В.
“____” _____2021 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека

на тему: **МЕТОД ЗАХИСТУ ІНФОРМАЦІЇ «СИСТЕМИ РОЗУМНИЙ ДІМ» НА БАЗІ НОВОГО ПРОТОКОЛУ ОБМІНУ ДАНИХ**

Виконав: студент 6 курсу, групи СЗДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Технічні системи інформаційного та кібернетичного захисту»
(шифр і назва спеціальності)
Овчинік С.О.
(прізвище та ініціали)
Керівник Лаптєв О.А.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Гребенніков А.Б.

Київ – 2021

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
к.т.н. Шуклін Г.В
“__” _____ 2020р.

ЗАВДАННЯ

на магістерську кваліфікаційну роботу

студенту Овчиннік Сергій Олександрович

1. **Тема роботи**: Метод захисту інформації «системи розумний дім» на базі нового протоколу обміну даних.
   Затверджено наказом по університету від « » 2020р. №
2. **Термін здачі:** студентом оформленої роботи «21» грудня 2020р.
3. **Предмет дослідження:** метод захисту інформації у процесі передачі від Господара до «системи розумний дім».
4. **Об’єкт дослідження:** процес передачі інформації між Господарем та «системою розумний дім»
5. **Мета роботи:** розробка методів захисту передачі інформації між Господарем та «системою розумний дім» на базі нового протоколу обміну даних.
6. **Перелік питань, які мають бути розроблені:**
   1.Огляд загроз інформації та підходів до «системи розумний дім».
   2.Аналіз існуючих методів захисту інформації «системи розумний дім».
   3.На основі проведених аналізів розробити метод захисту інформації «системи розумний дім» на базі нового протоколу обміну даних
7. **Перелік публікацій:**
   1.Овчиннік С.О., Лаптєв О.А., Гребенніков А.Б. Метод захисту інформації «СИСТЕМИ РОЗУМНИЙ ДІМ» на базі нового протоколу обміну даних. Інтернет конференція «Актуальні проблеми кібербезпеки». Тези доповідей 22 жовтня 2020. Київ. ДУТ с.35-49
   2.Овчиннік С. О. (Ovchynnik S. O.), Лаптєв О. А. (Laptiev O. A.), Зозуля С. А. (Zozulya S. A.), Правдивий А. М. (Pravdyvyy A. M.). Метод захисту інформації системи «розумний дім» на базі нового протоколу обміну даних. Сучасний захист інформації №3(43), 2020
8. **Перелік ілюстративного матеріалу:**
   Презентація виконана на 15 слайдах для подання за допомогою оверхедів (світлопроекторів) та комп’ютерних засобів.
9. **Дата видачі завдання** “___”_____ 2020 р.

Керівник: Лаптєв Олександр Анатолійович _____

Завдання прийняв до виконання: Овчиннік Сергій Олександрович_____

КАЛЕНДАРНИЙ ПЛАН

№ З\П	Назва етапів магістерської роботи	Строк виконання етапів	Примітка
1	Уточнення постановки завдання	до 07.09.2020р.	виконано
2	Аналіз літератури	до 10.09.2020р.	виконано
3	Обґрунтування вибору рішення	до 24.09.2020р.	виконано
4	Збір даних	до 30.09.2020р.	виконано
5	Написання першого розділу роботи	до 23.10.2020р.	виконано
6	Написання другого розділу роботи	до 15.11.2020р.	виконано
7	Написання третього розділу роботи	до 29.11.2020р.	виконано
8	Підготовка ілюстративного матеріалу	до 17.12.2020р.	виконано
9	Отримання рецензій	до 28.12.2020р.	виконано
10	Захист в ДЕК	до 18.01.2021р.	виконано

Студент С.О. Овчиннік

Науковий керівник О.А. Лаптєв

РЕФЕРАТ

Дипломна робота містить 81 сторінку, 12 малюнків, 1 таблицю та 20 джерел літератури.

У роботі розроблено метод захисту інформації «системи розумний дім» на базі нового протоколу обміну даних.

Досліджено склад «системи розумний дім» та її роль. Детально розглянуто існуючі протоколи у мережах систем розумного дому.

Ґрунтуючись на проведеному дослідженні розроблені рекомендації по застосуванню нового протоколу обміну даними у мережах систем розумного дому.

Мета роботи. Розробка методів захисту передачі інформації між Господарем та «системою розумний дім» на базі нового протоколу обміну даних.

Завдання дослідження:

1.Огляд загроз інформації та підходів до «системи розумний дім».

2.Аналіз існуючих методів захисту інформації «системи розумний дім».

3.На основі проведених аналізів розробити метод захисту інформації «системи розумний дім» на базі нового протоколу обміну даних.

Об’єкт дослідження. процес передачі інформації між Господарем та «системою розумний дім».

Предмет дослідження. метод захисту інформації у процесі передачі від Господара до «системи розумний дім».

Методи дослідження. Для досягнення поставленої мети в роботі використано методи дослідження на основі системного підходу. Використані методи теорії ймовірностей, аналітичного моделювання.

Таким чином, на даний час в практиці і теорії передачі інформацій від Господара до «СИСТЕМИ РОЗУМНИЙ ДІМ» загострилося протиріччя між

швидкою й гарантованою передачею інформації та достовірного розпізнання інформації «СИСТЕМОЮ РОЗУМНИЙ ДІМ» з метою точного виконання отриманої команди.

Для розв’язання вказаного протиріччя в роботі сформульовано актуальну науково-прикладну задачу щодо розробки МЕТОДУ ЗАХИСТУ ІНФОРМАЦІЇ «СИСТЕМИ РОЗУМНИЙ ДІМ» НА БАЗІ НОВОГО ПРОТОКОЛУ ОБМІНУ ДАНИХ.

ANNOTATION

Thes is contains 81 pages, 12 drawings, 1 tables and 20 sources of literature.

When working with the method of information protection "smart home system" based on a new data exchange protocol.

The composition of the "smart smoke system" and its role are studied. Existing protocols in smart home networks are considered in detail.

Based on the research, the developed recommendations for the application of a new data exchange protocol in smart home networks.

The purpose of the work. The security methods section transmits information between the Host and the "smart home system" based on a new data exchange protocol.

Objectives of the study:

1.Review of information threats and approaches to the "smart smoke system".

2.Analysis of existing methods of information protection "smart smoke system".

3.On the basis of the conducted analyzes to develop a method of information protection "smart home system" on the basis of a new protocol of data exchange.

Object of study. the process of transmitting information between the Lord and the "system of intelligent action."

Subject of study. the method of protecting information in the process of transmission from the Master to the "smart smoke system".

Research methods. To achieve this goal in the use of methodological research based on a systems approach. Use methods of probability theory, analytical modeling.

Thus, at present in the practice and theory of information transfer from the Owner to the "SMART HOUSE" SYSTEM the contradiction has intensified due to fast

and guaranteed information transfer and reliable recognition of information by the "SMART HOUSE SYSTEM" due to the fact that the command is executed.

To resolve this contradiction in the work with the formulated current scientific and applied problem for the development of the INFORMATION PROTECTION METHOD "SMART HOUSE SYSTEM" ON THE BASIS OF A NEW DATA EXCHANGE PROTOCOL.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ 10
ВСТУП 11
РОЗДІЛ 1 СИСТЕМА «РОЗУМНИЙ ДІМ». ОСНОВНІ ПОНЯТТЯ І ФУНКЦІЇ 13
1.1 Концепція розумного будинку 13
1.1.1 Що таке «Розумний дім?» 13
1.1.2 Основні елементи «Розумного дому» 14
1.2 Основні особливості розумного будинку 16
1.2.1 Доступність 16
1.2.2 Соціальна інтеграція 17
1.2.3 Зручність 18
1.2.4 Стійкість 18
1.3 Продуктизація 19
1.3.1 Чому – клієнту потрібні стимули для виходу на ринок при розробці продукту? 20
1.3.2 Як виробляти - процес розробки нового продукту (NPD) 21
1.3.3 Що слід враховувати під час виробництва - управління проектним портфелем 24
Висновки до 1 розділу 25
РОЗДІЛ 2 ОГЛЯД ТЕХНОЛОГІЙ ПЕРЕДАВАННЯ ДАНИХ В СИСТЕМІ РОЗУМНИЙ БУДИНОК 27
2.1 Протоколи автоматизації будинку для Інтернету речей 27
2.1.1 Домашня автоматизація X10 29
2.1.2 Автоматизація будинку Zigbee 30
2.1.3 Автоматизація будинку Insteon 32
2.1.4 Автоматизація дому Wi-Fi 33
2.1.5 Домашня автоматизація Bluetooth 35
2.1.6 Домашня автоматизація 6LoWPAN 37
2.1.7 Thread протокол для IoT 37
2.1.8 Автоматизація будинку ANT 38
2.1.9 Домашня автоматизація EnOcean 38
2.2 Найкращі протоколи домашньої автоматизації 39

2.3 Розумний будинок: Загрози і заходи протидії 41
2.3.1 Загрози розумних будинків..... 41
2.3.2 Захист розумних будинків 43
Висновок до 2 розділу..... 45
РОЗДІЛ 3 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ В СИСТЕМІ «РОЗУМНИЙ БУДИНОК» 46
3.1 Ключові проблеми в кібербезпеці та конфіденційності..... 47
3.2 Домени додатків IoT 48
3.4 Загальний характер загроз безпеці – як аналогія доменних загроз 50
3.4.1 Загрози 50
3.4.2 Вразливості..... 51
3.4.3 Приклади вразливостей..... 53
3.5 Деяка існуюча підтримка безпеки для IoT 54
3.5.1 6LoWPAN та безпека..... 56
3.5.2 RPL та безпека..... 57
3.5.3 CoAP та безпека 57
3.5.4 Майбутні вказівки щодо безпеки IoT 58
3.6 Майбутні проблеми безпеки розумного дому..... 59
3.6.1 Підтримка автоконфігурації 59
3.6.2 Оновлення програмного забезпечення та прошивки IoT 61
3.7 Підходяща архітектура розумного дому для забезпечення безпеки..... 64
3.7.1 Архітектура проміжного програмного забезпечення та безпека..... 64
3.7.2 Хмарні архітектури та безпека 66
3.7.3 Архітектура шлюзів..... 67
3.8 Метод захисту інформації «Системи розумний дім» на базі нового протоколу обміну даних 69
Висновки до 3 розділу 77
ВИСНОВКИ..... 79
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 80

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

IoT (Internet of Things) – Інтернет речей

IPSec (Internet Protocol Security) – протокол захисту мережевого трафіку на IP-рівні

6LoWPAN (IP version 6 Low power Wireless Personal Area Network protocol) – стандарт взаємодії по протоколу IPv6 поверх малопотужних бездротових персональних мереж стандарту IEEE 802.15.4

GITAR (Generic extension for Internet-of-Things ARchitectures) – агальне розширення для архітектур Internet-of-Things, що забезпечує динамічне оновлення мережевих та прикладних модулів

IEEE (Institute of Electrical and Electronics Engineers) – Інститут інженерів з електротехніки та електроніки

RPL (Routing Protocol for Low-Power and Lossy Networks) – протокол маршрутизації для мереж з низьким енергоспоживанням і з втратами

TLS (Transport Layer Security) – захист на транспортному рівні

ВСТУП

Ми живемо у світі, що швидко змінюється, де найбільш помітними світовими тенденціями є, наприклад, велика кількість інформації, технологічний прогрес та зростаюча середня тривалість життя населення. Це революціонізувало розробку нових концептуальних продуктів, які стають все більш поширеними та важливими для ділового життя. У цьому дослідженні розумний дім як приклад цих нових продуктів був обраний об'єктом з метою вивчити, як створити розумний дім.

Хоча концепція розумного дому використовується в основному для домашньої автоматизації та допоміжних технологій, може застосовуватися до всіх ситуацій, де існують її ключові особливості. При розробці розумних будинків для різних потреб важливе значення мали нові процеси розробки продуктів у поєднанні з управлінням портфелем продуктів. Тому чином, «Воронка розвитку» (Von Stamm 2008) була використана як теоретична основа для пошуку основних проблем та рішень в області виробництва розумного дому.

Для емпіричної частини дослідження застосовано якісний підхід до дослідження. Поглиблені інтерв'ю з напівструктурованими запитаннями проводились із двома респондентами: підприємцем розумного будинку та дизайнером. Позиціонування товару, визначення замовника, збалансування швидкості витрат у НДДКР (Науково-дослідні та дослідно-конструкторські роботи) були визнані найбільш складними аспектами, в той час як основне рішення було розглянуто як сегментацію споживачів, цілісний досвід користувачів із інтегрованими системними схемами та встановлення кінцевої мети як «бути розумнішим».

Отримані результати передбачають вимогу щодо прийняття підходу «продукція, що керує потребами ринку», та впровадження промислових стандартів для розумних будинків та їх розвитку. Однак через широкий обсяг досліджень та лише декілька первинних джерел даних дослідження мало свої

обмеження. Для подальших досліджень можна використати більше інтерв'ю або вивчити ефективність розробки нового продукту з точки зору "ринкової" та "технологічної" перспективи.

РОЗДІЛ 1 СИСТЕМА «РОЗУМНИЙ ДІМ». ОСНОВНІ ПОНЯТТЯ І ФУНКЦІЇ

1.1 Концепція розумного будинку

1.1.1 Що таке «Розумний дім?»

Визначення розумного будинку варіюється залежно від контексту, де він використовується. В основному є два різні способи вираження або вузьким, або узагальненим.

У вузькому розумінні, розумний дім більше описується як автоматизація будинку або допоміжний домотик (Домотика - це безліч систем, які автоматизують будинок, надаючи послуги з управління енергією, безпеки, комфорту та зв'язку, які можуть бути інтегровані з допомогою внутрішніх та зовнішніх мереж зв'язку, дротового або бездротового, і контроль над якими можна проводити зсередини і зовні будинку). Це стосується використання комп’ютера та інформаційних технологій для управління пристроями та функціями в домашньому середовищі, таких як освітлення, розважальні системи, температура тощо. Розумні будинки використовують електронну мережеву технологію для інтеграції різних пристроїв та приладів, що знаходяться майже у всіх будинках, щоб усім будинком можна було управляти централізовано або віддалено як єдину машину. Усередині кожної з цих машин інтеграція всіх пристроїв та приладів дозволяє їм спілкуватися між собою та між собою за допомогою домашнього контролера, тим самим одночасно дозволяючи керувати різними машинами в запрограмованих сценаріях або режимах роботи.

У загальному розумінні, розумний будинок може бути будь-яким з “середовищ”, що розгорнуте за допомогою взаємозв’язаних пристроїв людина-машина та/або машина-машина, з можливістю моніторингу та керування автоматично або віддалено, а також можливістю зв’язку з іншими подібними “середовищами” або система моніторингу та контролю. Прикладом може бути використання сенсорної системи для моніторингу клімату: розгортання різних датчиків / детекторів температури, вологи, ґрунту, повітря, води тощо, а також періодична відправка отриманих даних на сервер. Досягнення бездротового зв'язку дозволило багатьом сенсорним пристроям надсилати та отримувати дані на великі відстані, що сприяє постійному моніторингу клімату, а також управлінню навколишнім середовищем, що реалізується в будь-якому місці в будь-який час.

Підводячи підсумок як вузьких, так і узагальнених розумінь, розумний дім може використовувати загальне визначення: середовище з незалежними пристроями, що функціонують в інтегрованій системі під централізованим управлінням віддалено або автоматично, і здатністю спілкуватися з іншими подібними середовищами або системами команд за допомогою спільних протоколів.

1.1.2 Основні елементи «Розумного дому»

З обговорення визначення розумного будинку, а також Ларсена К. (2010) , розробленого у його роботі «Технологія розумного будинку», чітко видно, що середовище розумного будинку складається з наступних трьох елементів: по-перше, окремі працюючі пристрої, які працюють незалежно один від одного та контролюють кожну із своїх функцій, наприклад температуру, вологу, безпеку, освітлення, екранування, енергію, розваги, стан повітря, якість ґрунту, якість води ... тощо. Це можуть бути різні датчики, сповіщувачі, вимірювачі, вимикачі

тощо, які можуть експлуатуватися під дистанційним або автоматичним управлінням.

По-друге, централізований блок управління середовищем, такий як панелі управління або інтелектуальні мобільні пристрої (телефони, планшети або інші із додатком відносного управління), які можуть керувати всіма окремими функціонуючими пристроями, розміщеними в одному середовищі, таким чином, «внутрішнім» блоком зв'язку. Управління здійснюється за допомогою віддаленого (Bluetooth, інфрачервоного або іншого радіочастотного підходу), переважно через бездротову мережу (Wi-Fi) в якості першого пріоритетного вибору.

По-третє, спільні протоколи, що взаємодіють між одним середовищем та «сторонніми», наприклад інші осередки розумного будинку або командні системи (центри управління, центри обробки даних тощо), за допомогою яких одне середовище може обмінюватися повідомленнями / даними між собою та центром сумісно, таким чином, створюючи “між” спосіб зв'язку. За допомогою цього налаштування, розумне домашнє середовище та інші подібні осередки можуть складати запрограмовану керовану мережу і використовуватися в будь-якому місці в будь-який час будь-якими способами, якими керує один центр. Іншими словами, налаштування протоколу стає одним із обов’язкових елементів розумного дому, який використовується широко і розумно, наприклад, в контексті Інтернету речей (IoT). Ці протоколи потрібно узгодити та запрограмувати до обміну даними, якщо тільки одне середовище розумного дому не призначене для роботи в ізольованому режимі.

Виходячи з вищевикладеного, саме час спробувати схематизувати системний вигляд, який демонструє розумне домашнє середовище, а також внутрішні та міжмережеві взаємозв’язки, див. Рисунок 1. У цьому вигляді окремі функціонуючі пристрої одного середовища демонструються кольоровими полями, серед яких централізований блок управління показаний посередині. Внутрішня комунікація всередині осередка представлена чорними стрілками, тоді як взаємодія з іншими середовищами та командним центром - синіми стрілками двостороннього напрямку.

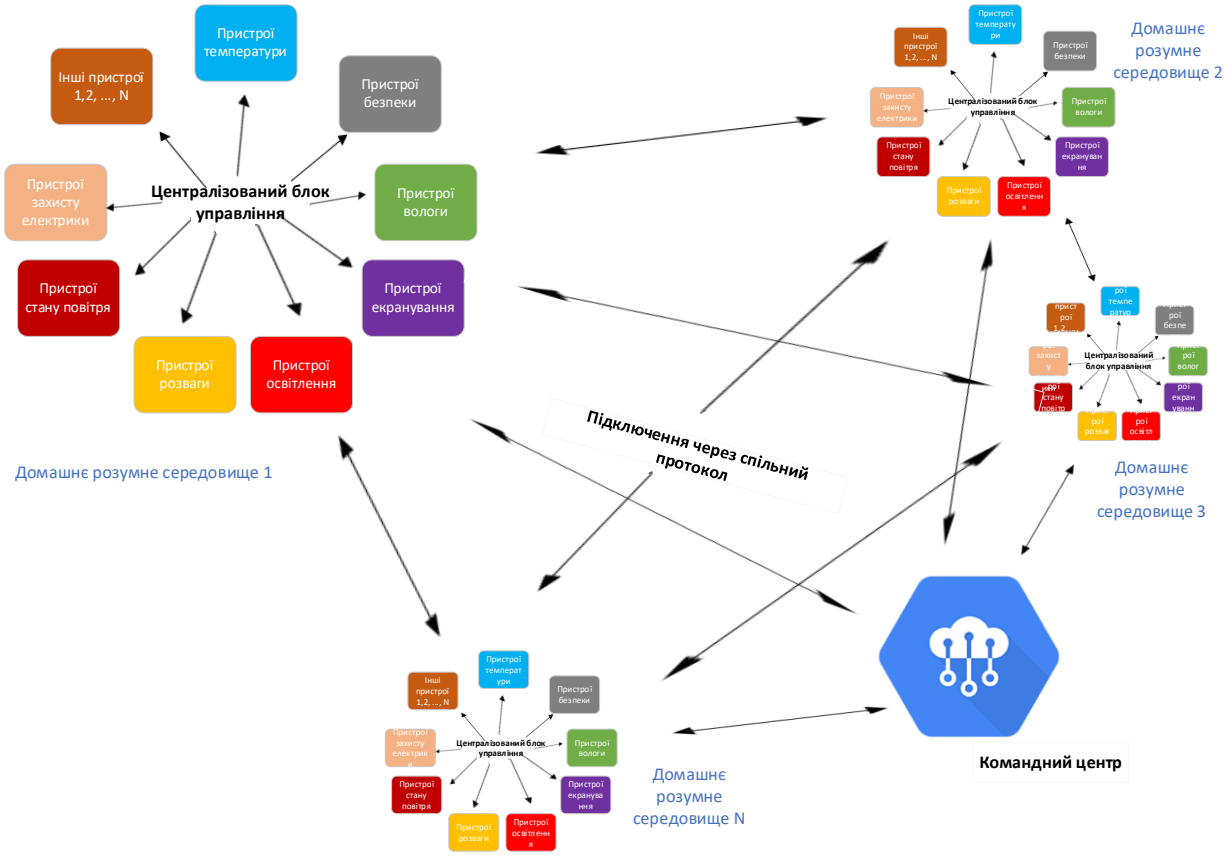


Рис. 1.1. Система розумних домашніх середовищ та командного центру

1.2 Основні особливості розумного будинку

Визначення та основні елементи розумного будинку дають уявлення про основні особливості з чотирьох наступних уявлень:

1.2.1 Доступність

Уявлення про доступність: до розумного будинку легко отримати доступ та використовувати всі пристрої з дистанційним або автоматичним управлінням. Навіть якщо один кінцевий користувач не може керувати ним сам, існує

допоміжне керування, контроль допомоги якого може підтримуватися іншими середовищами або, швидше за все, командним центром.

Багато випадків використання переваг доступності можна виявити в тих професійних організаціях, які сприяють безпеці та функціональним нормам для мешканців за допомогою технологій розумного будинку. Подібно до спільного досвіду у Великобританії (Gentry, Dewsbury & Linskell 2011), випадок проілюстрував, як проектувальник розумного будинку оцінював потреби мешканців та впроваджував інфраструктури та обладнання з технологічним пристосуванням, так що кінцевий результат розумного будинку міг допомагати людям з неврологічними станами.

1.2.2 Соціальна інтеграція

Уявлення про соціальну інтеграцію: немає обмежень щодо використання розумного будинку. Вік, стать та рухові здібності кінцевих споживачів не мають значення, якщо хтось може користуватися блоком управління середовища або хтось інший, хто може допомогти (віддалено) керувати всіма пристроями середовища.

Типовим використання є сфера охорони здоров’я та соціальних служб: розумні домашні камери обладнані для будинків для людей похилого віку та інвалідів, яким складно працювати у звичайній діяльності у повсякденному житті. У цих будинках є, наприклад, вхід та доступ для інвалідних візків, меблі з регулюванням висоти, датчик падіння, автоматичний пристрій оповіщення про аварії, аудіопристрої, система нагадування про ліки ... і віддалений комунікатор, що надсилає / отримує дані до / з центрального диспетчерського управління.

На додаток до всього вищезазначеного, концепція розумного будинку також допомагає лікарям / медичним працівникам віддалено відстежувати симптоми людини, даючи вказівки щодо реабілітації та виносити базові клінічні

судження в надзвичайних випадках, навіть якщо ця людина не перебуває у лікарнях / клініках. За допомогою інтелектуальних будинків ці люди можуть жити самостійно без шкоди для якості життя.

1.2.3 Зручність

З точки зору зручності: завжди доступний та гнучкий, коли/де/як потрібно. З вищенаведених двох прикладів моніторингу навколишнього середовища та охорони здоров’я та соціальних послуг можна легко визначити перевагу зручності.

Прикладом використання в цьому варіанті є застосування концепції розумного будинку в області управління нерухомістю: коли і як обігрівати / охолодити будівлю, заблокувати / розблокувати вхід, увімкнути / вимкнути освітлення, зрошувати сад / трав'яні поля ... все це можна керувати окремо в одній будівлі та контролювати / додатково контролюватися командним центром.

Концепцію «розумного будинку» можна навіть використовувати як соціальне, технологічне і віртуальне навчально-розробницьке середовище Heimovaara-Kotonen E. (2014), складена в Університет прикладних наук JAMK, Фінляндія. Коли потрібні різні навчальні ситуації, розумна домашня лабораторія буде налаштована на відповідні ситуації, такі як приміщення для навчання навичок для занять фізіотерапією, стаціонар для практик медсестр тощо.

1.2.4 Стійкість

В результаті такого використання в моніторингу навколишнього середовища (доступність), автоматичної допомоги у сфері здоров’я та соціальних

послуг (соціальна інтеграція) та управління енергоспоживанням (зручність), розумний дім має переваги з точки зору розвитку стійкості. На думку Мелвіна К.Хендрікса (2014), стійкість - це практика резервування ресурсів для майбутнього покоління без шкоди для природи та інших її компонентів. Порівнюючи цю термінологію з визначенням «розумного дому», ключовими елементами та функціями, можна знайти очевидні спільні речі.

Одним із цікавих випадків використання переваг стійкості є використання технологій розумного будинку для контролю споживання енергії (Dütschke, Fichtner & Paetz 2011), в ході якого було вивчено сприйняття споживачами використання розумного будинку. У дослідженні вивчалася реакція споживачів на систему управління енергоспоживанням, яка оптимізує споживання електроенергії на основі різних рішень для розумного будинку. Споживачі самі побачили багато переваг, особливо можливість заощадити. Тому розумні прилади і розумні лічильники, обладнані в їх будинках, вважалися необхідними елементами.

Концепція розумного дому ідеально впишеться в контекст розумного міста, якщо розглядати її в широкому соціальному масштабі. В цьому контексті, як було досліджено в «Дослідження розумного дому» (Комітет міст цифрових технологій та міст, заснованих на знаннях, UCLG 2012) місто можна визначити «розумним», якщо воно позитивно працює в шести сферах (економіка, мобільність, навколишнє середовище, громадянство , якість життя та управління), побудованих на основі розумного поєднання елементів (комунікації, інфраструктура, економічний розвиток) та цілеспрямованої та незалежної діяльності громадян (участь, освіта), що забезпечують раціональне управління природними ресурсами.

1.3 Продуктизація

На даний момент концепція розумного будинку (визначення, ключові елементи та особливості) була обговорена. Щоб відповісти на питання про те, як перетворити концепцію на продукт, слід вивчити ключове слово “виробництво”. Далі в наступних пунктах буде розглянуто „виробництво” з трьох аспектів: чому, як і що.

1.3.1 Чому – клієнту потрібні стимули для виходу на ринок при розробці продукту?

По-перше, цей світ вступив у період нових концепцій, що створювалися настільки швидко на відміну від будь-яких інших епох після промислової революції, але успішний новий продукт, перенесений з НДДКР (Науково-дослідні та дослідно-конструкторські роботи) у виробництво, є загальною і серйозною проблемою для організацій будь-яких розмірів (Бретхауер 2002). На успішну розробку нового продукту впливає багато факторів, у тому числі ефективний процес розробки, більш швидке і правильне позиціонування на ринку, а також знання клієнта і ринку. Подібно до того, як Барретт (1996) говорив два десятиліття тому, що статистично 80 відсотків нещодавно представлених продуктів не змогли вийти на ринок через два роки. Традиційно, з позиції бізнес-літератури, маркетингові дослідження засновані на ринкових поглядах, які полягають у з'ясуванні того, що клієнт хотів би, а потім в реалізації цього, а саме як «ринковий підхід» до інновацій та продуктивності (Trott 2005).

По-друге, з точки зору концепції «розумного дому», визначення найбільш підходящого процесу для розробки продукту і визначення «правильного» ринку та споживачів може бути зародком. Беручи до уваги його ключові особливості, розумний дім не тільки робить повсякденне життя зручним та економить час, але також забезпечує енергоефективність та раціональне використання природних

ресурсів для суспільства, переваги розумного будинку можуть бути безмежними. Тому розумні будинки вже почали залучати зацікавлені сторони на ринку, включаючи архітекторів, розробників, виробників пристроїв, постачальників послуг та будівельників інфраструктури.

Для подальшої розробки цієї теми використовується окремий приклад на європейському ринку. Згідно з європейським звітом про ринок розумних будинків (2014 р.), очікується, що конкретний ринок розумного будинку в області автоматизації будинків буде рости пристойними темпами протягом багатьох років. У цій галузі технологія розумного будинку пропонує перспективи значного поліпшення рівня життя людей похилого віку, немічних та інвалідів, які в даний час не мають автоматизованої демотичної діяльності, що в іншому випадку можуть повністю залежати від домашньої допомоги. Ці переваги можуть бути реалізовані лише в тому випадку, якщо технологія стане доступною та доступною для тих, хто її найбільше потребує. Таким чином, глибоке розуміння цієї частини споживачів та їхніх точних потреб, а також доступність може стати вирішальним рушієм цього ринку, сегментації продукції, а потім відповідного процесу розробки продукту.

1.3.2 Як виробляти - процес розробки нового продукту (NPD)

За останні 30 років в управлінських літературах приділяється велика увага та обговорюються теорії, що стосуються концепції розробки нових продуктів (NPD). На думку Тротта (2005, ст.383), фактична розробка нових продуктів - це процес перетворення бізнес можливостей у матеріальні продукти.

Зазвичай представлений лінійний процес NPD серед великої кількості теорій можна описати як цю модель:

Генерація ідей => Перегляд ідей => Тестування концепції => Бізнес-аналіз => Розробка продукту => Тестовий маркетинг => Комерціалізація => Моніторинг та оцінка.

Однак, думаючи про те, «чому», як обговорювалося в попередньому пункті, потреби покупців як основний ринковий фактор повинні мати пріоритет при виборі відповідного процесу NPD для розробки продукту розумного будинку, а це, по суті, процес, орієнтований на ринок / клієнта.

За словами Бретхауера (2002, ст.35), новий продукт, що надходить на ринок із помітною перевагою над конкуренцією, незабаром погіршиться, більше не являючись продуктом. Щоб максимізувати якість продукції, продуктивність та прибутковість для захисту від погіршення, був розроблений процес “Надійна конструкція та продукт” шляхом впровадження прогресивних інструментів з двох аспектів: фокусування на конструкції товару та фокусі на передачі товару. Далі автор повинен інтерпретувати ці два набори інструментів стислим резюме:

• Набір інструментів А. Зосереджуючись на надійній конструкції продукту.

Рис. 1.2. Інструменти надійного проектування продукту для NPD

Дотримуючись вищеописаних інструментів, поетапно можна охарактеризувати «повний» продукт і бути готовим до наступних кроків, щоб пройти процес передачі.

• Набір інструментів В. Зосереджуючись на надійному процесі передачі

Рис. 1.3. Інструменти надійного процесу передачі для NPD.

Як тільки вищезазначені інструменти виконуються поступово, цілий процес від проектування до передачі продукту теоретично визнається надійним.

Однак ця розробка може вказувати на те, що завдяки використанню успішного процесу розробки нового продукту можна очікувати таких переваг:

1.Конкурентна перевага;

2.Здатність реагувати на потреби клієнтів;

3.Збільшення ймовірності прибутковості та загальної якості;

4.Зменшення часу циклу виведення нового продукту на ринок;

5.Постійно вдосконалюється команда розробників продуктів.

1.3.3 Що слід враховувати під час виробництва - управління проектним портфелем

Після обговорення причини та процесу / засобів виробництва, наступний крок, відповідно, переходить до " **Що слід враховувати під час виробництва** "?

Беручи до уваги аспект структури товару, як визначити різні рівні товарних позицій - компоненти, версії апаратного забезпечення, випуски програмного забезпечення, сімейство продуктів, конфігурація, складання та упаковка?

Розглядаючи аспект цілого життєвого циклу, як визначити дорожню карту товару, керувати варіантами, розробити технічне обслуговування та термін гарантії?

Щоб охопити всі необхідні елементи виробництва, тобто централізоване управління процесами, методами, технологіями, ресурсами, фінансами, ризиками і навіть змінами, сюди має бути включено управління товарним портфелем (PPM - product portfolio management).

Постійно переслідуючи точку зору вигідного продуктового рішення, Толонен, Харконен та Хаапасало (2014) зазначили, що управління товарним портфелем можна розглядати як платформу, що приводить до стратегічних доріг щодо продукту та випуску, щоб забезпечити успішні та постійні додаткові та архітектурні рішення. PPM націлений на економічно ефективне оновлення товарних портфелів шляхом додавання нових продуктів до портфоліо,

вдосконалення та модифікації існуючих продуктів, одночасно усуваючи неконкурентоспроможні.

Візуалізована модель (див. Рис.4.) чітко окреслює рамки пропонованого управління PPM: весь PPM побудований за допомогою вертикальних та горизонтальних субпортфоліо, через які вертикальний портфель представляє рівні структури продукції в комерційних та технічних частинах, тоді як горизонтальний представляє чотири фази життєвого циклу товару. Оновлення товарного портфеля вимагає стратегічних PPM порівняно з вертикальними та горизонтальними субпортфоліоми. В ідеалі горизонтальне та вертикальне оновлення портфеля відбуватиметься в рівновазі та синхронно із впровадженням нових продуктів, а також зі зниженням старого продукту.

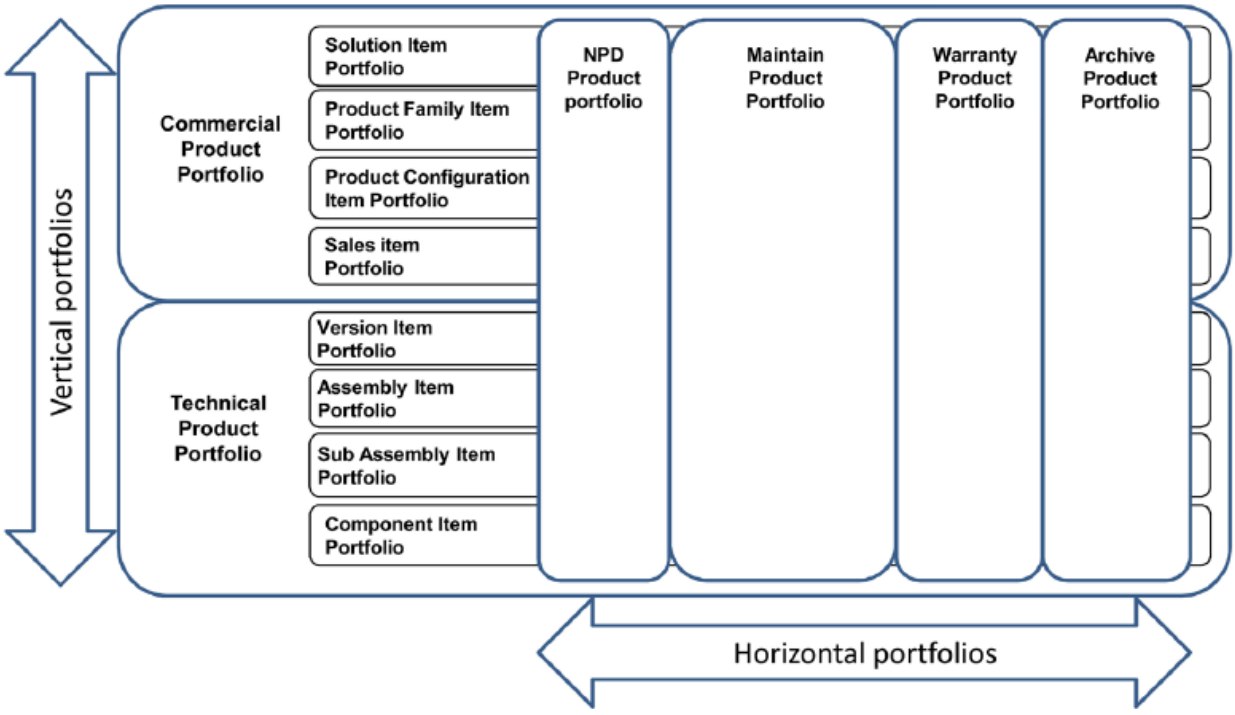


Рис. 1.4. Ідеальна основа для управління товарним портфелем

Висновки до 1 розділу

В даному розділі розглянуто концепцію, можливості, економічні аспекти, а також особливості проектів «розумного будинку».

Система «розумний будинок» - це практично повна автоматизація управління девайсами, пристроями у всіх кімнатах і приміщеннях будинку, а також офісах, квартирах і т.д. Система управляє як окремими блоками, так і всім в цілому. Можлива передача команд на місці або дистанційно за допомогою телефонів. Під «розумним» будинком слід розуміти систему, яка забезпечує безпеку і ресурсозбереження (в тому числі і комфорт) для всіх користувачів. У найпростішому випадку вона повинна вміти розпізнавати конкретні ситуації, що відбуваються в будинку, і відповідним чином на них реагувати: одна з систем може управляти поведінкою інших по заздалегідь виробленим алгоритмам. Крім того, від автоматизації декількох підсистем забезпечується синергетичний ефект для всього комплексу.

РОЗДІЛ 2 ОГЛЯД ТЕХНОЛОГІЙ ПЕРЕДАВАННЯ ДАНИХ В СИСТЕМІ РОЗУМНИЙ БУДИНОК

2.1 Протоколи автоматизації будинку для Інтернету речей

Що ми маємо на увазі під протоколом? З точки зору мережі, протокол - це заздалегідь визначений набір правил та стандартів між пристроями. Це те, як ваші розумні прилади простягають руку та розмовляють між собою. Це може включати спектр, мову, порти та відповідні відповіді. Пристрій може використовувати кілька протоколів, але певні дії можуть потребувати певного протоколу. Вам потрібно підтвердити сумісність між вашими пристроями, особливо контролерами.

Ознайомимося із списком популярних протоколів домашньої автоматизації для Інтернету речей, тобто X10, Zigbee, Insteon, Wi-Fi, Bluetooth, Insteon, 6LoWPAN та EnOcean. Порівняння цих протоколів та наш досвід свідчить, що Zigbee, 6LoWPAN, Thread та Bluetooth LE пропонують найбільш перспективні результати для домашньої автоматизації, керованої IoT.

Домашня автоматизація означає використання Інтернету речей (IoT) для підключення та управління побутовими пристроями та побутовою технікою. Протоколи домашньої автоматизації, навпаки, - це способи передачі цієї інформації на інші пристрої, як дротовим, так і бездротовим. Ось гарне введення деяких протоколів домашньої автоматизації, які можна використовувати для створення вашого наступного розумного будинку.

Хоча концепція не нова - оскільки розумні ліхтарі та прилади на основі таймера існують вже деякий час - поява IoT та штучного інтелекту додало автоматизації дому абсолютно новий вимір. У наші дні розумні будинки можна контролювати та контролювати дистанційно з мінімальним наглядом

користувачів. Більше того, розробка цифрових продуктів паралельних технологій, таких як програми для смартфонів та протоколи віддаленого доступу, значно покращила сценарії використання домашньої автоматизації, забезпечуючи зручність, контроль та безпеку для розумних домашніх користувачів.

В іншому контексті, автоматизація будинків також призвела до економії коштів і виявилася корисною для навколишнього середовища, зменшивши мінімальне споживання енергії в житлових та комерційних будівлях.

Ось хороший прогноз того, як ви можете розробляти продукти IoT для домашньої автоматизації.

У минулому році технологія автоматизації будинків стала свідком величезного стрибка вперед. Такі продукти, як Amazon Echo та Google Home, нарешті змогли проникнути в основний споживчий простір та розпочати галузеву тенденцію. Отже, 2020 рік, як очікується, продовжить цю тенденцію за допомогою таких технологій, як розпізнавання обличчя, голосові команди та біометрія, які знайдуть ширше застосування в рішеннях розумного будинку.

Провідні технологічні компанії інвестують величезні суми в НДДКР, щоб створити власні пов'язані екосистеми для дому та офісу. Кінцевим баченням є створення повністю автоматизованих систем, які можуть розпізнавати та реагувати на обраних осіб чи групи користувачів у домашньому або офісному середовищі.

Тут ми розглянемо популярні сьогодні протоколи автоматизації будинку:

- Zigbee
- WiFi
- Bluetooth
- 6LoWPAN
- Thread
- ANT and EnOcean
- Comparison of Protocols

2.1.1 Домашня автоматизація X10

Одна з перших впроваджених технологій управління будинком, x10 існує з 1975 року. X10 використовує існуючі лінії електропередач для управління лампами, приладами та контролю дверей та вікон. Технічно X10 трохи відстає від свого часу, і затримки між дією та реакцією відчутні через використання РЧ-сигналів. Протоколи X10 також сприйнятливі до збоїв, пов'язаних із лінійним шумом, і вимагають додаткової установки фільтрів, з'єднувачів та повторювачів, щоб мінімізувати такі випадки.

У 1999 році було запроваджено оновлення під назвою Universal Powerline Bus (UPB), яке усуває більшість недоліків X10. UPB використовує більш складну установку, що включає унікальні ідентифікатори пристроїв, спільний доступ до мережі та індивідуальні паролі мережі, щоб забезпечити більш реалістичну та настроювану реалізацію розумного будинку.

Нижче розглянутий рисунок-схема функцій протоколу X10.

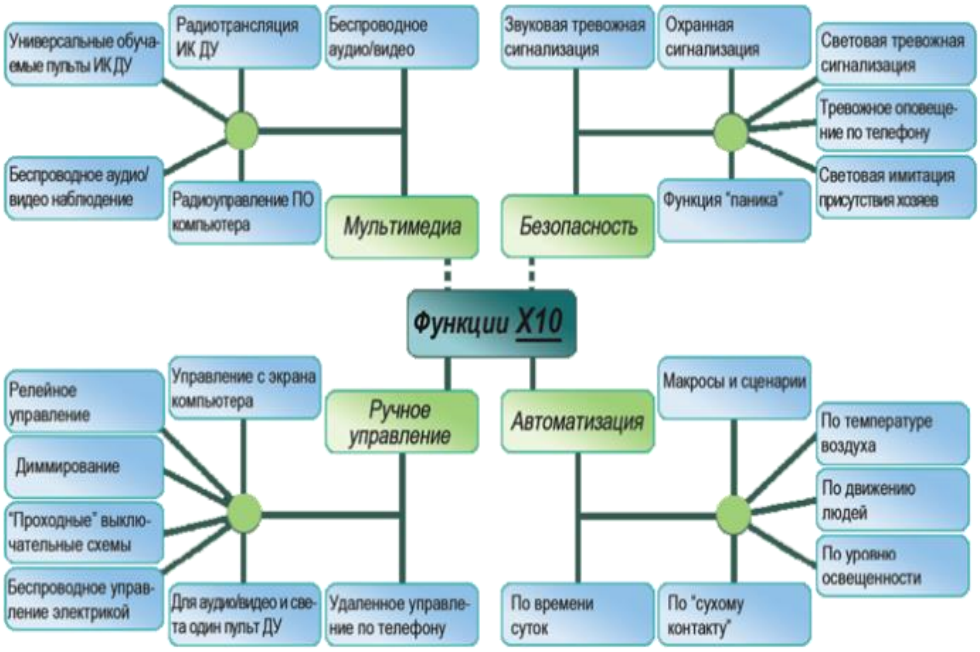


Рис. 2.1. Схема функції протоколу X10

2.1.2 Автоматизація будинку Zigbee

Провідна назва технологій розумного будинку, протокол Zigbee відомий своєю зручною роботою та сумісністю зі старими версіями. Протокол стверджує, що додає майже сім років автономної роботи до розумних датчиків безпеки - забезпечуючи довгострокове рішення для домашньої безпеки. Оскільки він використовує стандартизовані вимоги до сполучення, Zigbee також сумісний з більшістю сучасних пристроїв та приладів, що зменшує загальні витрати на розробку для власників продуктів та розробників.

Домашня автоматизація Zigbee також поставляється з конфігураціями "зроби сам", що дозволяє збільшити можливості налаштування як для розробників продуктів, так і для кінцевих користувачів. Ось кілька основних особливостей Zigbee –

- Віддалений доступ з контрольованим Інтернетом управління розумним будинком.
- Підтримка програми для смартфонів для модуляції розумних побутових приладів та пристроїв.
- Розумне управління живленням та контроль для підтримуваних продуктів.
- Підтримує встановлення додаткових сертифікованих пристроїв безпеки та протоколів для підвищення рівня домашньої безпеки.
- Дозволяє освітлювальним виробам використовувати динамічні елементи керування освітленням, які часто використовуються для створення унікальних домашніх та офісних умов.

Zigbee - один з небагатьох протоколів розумного будинку, який пропонує більші можливості налаштування для продуктових планувальників. Компанія має програму сертифікації та дотримання вимог НА, щоб гарантувати, що

сертифікована продукція безперешкодно інтегрується з протоколами домашньої автоматизації Zigbee.

Завдяки надзвичайно масштабованому характеру, бездротовій працездатності та використанню 128-бітового шифрування AES для захисту персональних даних, протокол може використовуватися також для офісних та ділових середовищ.

Плюси

- Пристрої Zigbee, як правило, дешевші, ніж Z-Wave.
- Як і Z-Wave, пристрої Zigbee можуть утворювати сітчасту мережу, щоб розширити свій діапазон.
- Підходить для пристроїв, які потребують безпечного зв’язку на короткий діапазон, оскільки можуть використовувати шифрування.
- Zigbee завжди був майже однаковим, незважаючи на деякі доопрацювання, тому питань сумісності щодо цього немає.
- Не існує реального обмеження кількості пристроїв, які може мати одна мережа Zigbee.

Мінуси

- Незважаючи на те, що це технічно відкритий стандарт, деяким виробникам вдається закрити свої пристрої Zigbee. Це створює тип «огородженого саду»;
- Пристрої Zigbee потребують такої можливості з’єднання, оскільки кожен пристрій має максимальний радіус дії 20 метрів;
- Як і Z-Wave, пристрої Zigbee потребують концентратора для управління;
- Перебування в спектрі 2,4 ГГц може спричинити проблеми з перевантаженнями пристроїв WiFi.

2.1.3 Автоматизація будинку Insteon

Технологія Insteon domotics використовує як лінії електропередачі, так і радіочастотний зв’язок для розумного домашнього підключення. Протокол вимагає перевірки всіх повідомлень - отриманих сумісним пристроєм - на наявність помилок та впровадження виправлень, що підвищує надійність функцій.

Однак протокол Insteon та підтримувані ним продукти в минулому зазнавали певних випадків злому білих шапок. У багатьох випадках хакери могли отримати доступ до розумних будинків та особистої інформації користувачів Insteon. З тих пір ці протоколи були скасовані.

Плюси:

- Керуйте своїм освітленням і термостатом зі свого смартфона або планшета;
- Автоматичне увімкнення світла при заході сонця;
- DIY система безпеки. *«Не впевнені, чи це для вас? Перегляньте наш посібник із безпеки “зроби сам”»;*
- Керуйте домашньою автоматизацією з будь-якої точки світу;
- Початковий набір містить все необхідне для налаштування.

Мінуси:

- Їм потрібно пройти довгий шлях, щоб ефективно інтегрувати свою колекцію пристроїв з додатками Insteon для смартфонів і веб-порталом, який керую нею;
- Користувачі стверджують, що обладнання трохи незграбне і потребує модернізації;
- Якщо ви купуєте стартовий набір, вам точно потрібно придбати додаткове обладнання;

- Порівняно з іншими системами домашньої автоматизації, для запуску та роботи датчика руху потрібно більше роботи, ніж слід.

2.1.4 Автоматизація дому Wi-Fi

Враховуючи проникнення мереж Wi-Fi у локальні мережі, це один із найбільш зручних протоколів для роботи з розробниками систем домашньої автоматизації. Протоколи Wi-Fi забезпечують готову інфраструктуру, яка має властивість керувати великими обсягами даних. Ще однією перевагою використання протоколу Wi-Fi для автоматизації дому та офісу є вбудоване 256-бітове шифрування AES. Однак низька швидкість Wi-Fi та потужність сигналу можуть бути вузьким місцем у більших настройках домотики. Крім того, більшість будинків та підприємств використовують стандарт Wi-Fi 802.11n, який занадто енергоємний для більшості програм IoT.

Нещодавно Wi-Fi Alliance оголосив про новий стандарт 802.11ah. Протокол, який Альянс називає Wi-Fi HaLow, може працювати на більші відстані, ніж існуючі діапазони 2,4 ГГц та 5 ГГц - нібито до 1 кілометра в ідеальних умовах - і був спеціально розроблений для впровадження IoT та автоматизації.

Хоча реальне застосування цього протоколу все ще потрібно ретельно перевірити, схильність діапазону 900 МГц до роботи серед різних перешкод добре відома. Функція Wi-Fi 802.11ah, що працює на гігагерцах, дозволяє покращити розміщення розумного будинку, підключеного автомобіля та цифрового медичного обслуговування. Таким чином, теоретично продукти, що використовують смугу HaLow, матимуть значно кращу зону покриття. Також смуга HaLow може передавати з мінімальною частотою 150 Кбіт / с через канали до 2 ГГц. Це означає, що підключені пристрої IoT можуть швидко відновити свій пасивний стан після пробудження для отримання вказівок - економить більше енергії - і, отже, подолати одне з властивих обмежень поточних мереж Wi-Fi.

Однак обмежуючим фактором діапазону HaLow є його швидкості передачі, які залишаються на низьких десятках мегабіт в секунду і можуть не задовольнити розробників продуктів, які потребують більшої пропускної здатності.

Плюси:

- Через високу пропускну здатність у двох спектрах, які він може використовувати, WiFi, як правило, є найшвидшою точкою між пристроями;
- Якщо у вас є маршрутизатор WiFi, ви можете використовувати пристрої WiFi. Це найбільш сумісний із стандартів тут;
- Завдяки сумісності та великій частці ринку, WiFi також є найбільш легко масштабованим;
- Пристрої WiFi також, як правило, є найбільш доступними по ціні, оскільки ця технологія є доступною для виробників;
- Пристрої WiFi, особливо на частоті 5 ГГц, можуть передавати найбільший обсяг даних. Це працює особливо добре, якщо ви намагаєтеся транслювати високоякісне відео;
- Пристрої WiFi також, як правило, найпростіші у впровадженні. Просто додайте їх у свою мережу WiFi і увійдіть у свій обліковий запис для отримання відповідної послуги.

Мінуси:

- Пристрої WiFi мають потужний радіоприймач і роблять більше обробки на самому пристрої, що вимагає більших витрат енергії;
- Навіть незважаючи на те, що доступ до більш високого спектру надає їм більшу пропускну здатність, наявність занадто великої кількості пристроїв може спричинити затори та повільність;
- Більш висока пропускна здатність також має менший діапазон, якщо ви не придбаєте окремий пристрій для розширення діапазону.

Wi-Fi також має проблеми з контролем якості. Оскільки технологія настільки дешева і легко доступна, існує дуже низький рівень її впровадження у

пристрої. Деякі виробники просто задумуються про це, або просто намагаються вивести на ринок "розумні пристрої" з WiFi якомога швидше, щоб заробити на цьому. Немає жодної організації, яка б стежила за впровадженням WiFi, як для інших стандартів;

Пристрої WiFi також потребують реєстрації в деяких хмарних послугах. Це не тільки поширюється на згадану раніше проблему безпеки, але зв’язок із хмарним сервером через Інтернет також додає відставання у вашому пристрої.

2.1.5 Домашня автоматизація Bluetooth

Мережі Bluetooth іноді використовуються розробниками розумних будинків як протокол домашньої автоматизації, хоча існуюча технологія залишається обмеженою своїм діапазоном та якістю сигналу. Тим не менш, деякі розумні домашні пристрої можуть використовувати сигнали Bluetooth для підключення та виконання основних завдань (залежно від рівня підтримки).

Проблеми безпеки: Основна проблема власників продуктів, які використовують мережі Bluetooth для домашньої автоматизації, - це безпека. Існуюча технологія Bluetooth з низьким енергоспоживанням (LE) схильна до саботажу через багаторазові випробування безпеки, такі як:

- Пасивне прослуховування, яке дозволяє третьому пристрою перехоплювати дані, якими обмінюються два спарених пристрої. Хоча BLE використовує 128-бітове шифрування AES для забезпечення передачі даних, все ще існують деякі недоліки протоколу, які хакери можуть використати для перехоплення та дешифрування персональних даних;
- Атаки "людина посередині" або MITM, які дозволяють стороннім пристроям вставити себе між двома законними пристроями, створюючи їм ілюзію взаємозв'язку. Перехоплення дозволяє зловмисному пристрою обдурити Gap Central та Gap Peripheral та втручатися в обмін інформацією;

- Відстеження особистості, коли третя сторона може відстежувати конкретного користувача, пов’язуючи адресу пристрою BLE з його пристроєм. У цьому випадку BLE має механізм періодичної зміни адреси пристрою для подолання цього недоліку.

Bluetooth 5 і Bluetooth Mesh: майбутній запуск технології Bluetooth 5 і Mesh являє собою найбільше вдосконалення технології Bluetooth з моменту її запуску. Bluetooth Mesh перетворить поточну технологію з топології мережі "точка-точка" на основі зірок у справжню топологію мережевих мереж. Це розширить діапазон підтримуваних пристроїв Bluetooth за межі типових персональних мереж, які ми маємо сьогодні. Крім того, сітка дозволить розширити покриття Bluetooth за допомогою додаткових вузлів, відкриваючи можливості для продуктів розумного будинку, які не пов'язані з підключенням до Інтернету. Новіші стандарти Bluetooth також використовуватимуть новіші заходи шифрування та безпеки для подолання існуючих недоліків безпеки.

Плюси

- Ви, мабуть, уже маєте пристрої Bluetooth;
- Додавати до пристрою порівняно дешево;
- Низьке споживання енергії означає менше заміни батареї;
- Він має мережеві можливості.

Мінуси

- Оскільки це новіший стандарт, важче знайти пристрої, що використовують його;
- Нижня пропускна здатність обмежує кількість даних, які Bluetooth Low Energy може передавати одночасно;
- Це також відкриває Bluetooth для проблем із безпекою порівняно із такими стандартами, як Zigbee та WiFi.

2.1.6 Домашня автоматизація 6LoWPAN

Акронім 6LoWPAN - це поєднання останньої версії протоколу IPv6 та малопотужних безпровідних персональних мереж (LoWPAN). 6LoWPAN може передавати інформацію бездротово за допомогою Інтернет-протоколу і особливо призначений для підключення найменших пристроїв до Інтернету речей.

6LoWPAN пропонує міжмашинну взаємодію та додатки Інтернет речей:

- 6LoWPAN Інтелектуальні вимірювачі;
- Розумні побутові прилади (освітлення, термостати тощо);
- Всі агрегати низької потужності, які можуть працювати поблизу сусіднього приймача.

2.1.7 Thread протокол для IoT

Запропонована Google спочатку, Thread - це відкритий набір протоколів для рішень для розумного будинку. Thread працює бездротово з використанням протоколів IP-адрес, як і 6LoWPAN, і означає підключити ще більш малопотужні пристрої в системі домашньої автоматизації. Thread використовує ряд модифікацій та функцій, щоб виправити існуючі вузькі місця в домашній інтеграції:

- Протокол відкритого стандарту, що передає пакети IPv6 через 6LoWPAN;
- Спрощений користувальницький інтерфейс та підтримка смартфонів та комп’ютерів для управління домотиками;

- Захищена та зашифрована AES мережа для мінімізації порушення даних;
- Багато менше енергії від підключених пристроїв - подовжує термін служби батареї підключених датчиків;
- Незалежна активація вузла, тобто немає жодної точки відмови для пристроїв у сітці;
- Універсальна підтримка різноманітних пристроїв та побутової техніки.

2.1.8 Автоматизація будинку ANT

Ця система домашньої автоматизації, що продається ANT Wireless, використовує стек протоколів бездротового зв'язку. ANT дозволяє апаратному забезпеченню, що працює в діапазоні ISM 2,4 ГГц, спілкуватися за допомогою правил співпраці.

Вузли ANT можуть одночасно виступати як підлеглі або ведучі в бездротовій сенсорній мережі. Це означає, що вузли можуть діяти як передавачі, приймачі або приймачі-передавачі для маршрутизації трафіку до інших вузлів. Також вузли можуть автоматично визначати час передачі на основі активності сусідніх вузлів.

2.1.9 Домашня автоматизація EnOcean

Ця технологія використовується для систем автоматизації будівель, які покладаються на бездротову технологію збору енергії. Модулі EnOcean - це комбінація електроніки та перетворювачів енергії наднизького енергоспоживання,

що забезпечує зв’язок між датчиками, перемикачами / контролерами та шлюзами без заряду акумулятора.

EnOcean пропонує ліцензії на свої запатентовані функції в закритому рамках EnOcean Alliance і знайшов багато інших застосувань (у транспорті та логістиці), крім автоматизації будинку.

2.2 Найкращі протоколи домашньої автоматизації

Серед перерахованих методів домашньої автоматизації Zigbee, 6LoWPAN, Thread та Bluetooth LE пропонують найбільш перспективні результати для домашньої автоматизації IoT. Там, де Zigbee та 6LoWPAN широко використовуються завдяки їх простоті встановлення та сумісності - Bluetooth та Thread обіцяють кращу інтеграцію найближчим часом. Ось як менеджери продуктів та розробники можуть отримати вигоду від інтеграції цих протоколів у свої рішення для розумного будинку,

Zigbee: Дозволяє велику кількість налаштувань продукту та масштабованості. Процес інтеграції та сертифікації простий, а Zigbee також забезпечує зворотну сумісність для старих продуктів. Крім того, протокол має вбудовані заходи безпеки, усуваючи необхідність додаткових кроків від розробників продуктів.

6LoWPAN: Ідеально підходить для батарейних датчиків, таких як температура, дим тощо, а також для управління побутовими приладами, такими як пральні машини. Ультранизьке використання енергії цієї технології зробило її однією з найкращих технологій розумного будинку.

Bluetooth: Незважаючи на те, що в теперішній формі він не настільки придатний для використання, система домашньої автоматизації Bluetooth знайде

широке застосування після випуску функціональних можливостей сітки. Планувальники продуктів зможуть розробляти та застосовувати інтелектуальні рішення для дому з незалежним та взаємозалежним функціонуванням у локальних приватних мережах.

Thread: Ініціатива підтримується великою кількістю постачальників обладнання та програмного забезпечення для спільної розробки розумного будинку. Його універсальне прийняття означає швидше оновлення фреймворку, кращий рівень безпеки та менше споживання енергії для розробників розумних будинків.

Протоколи автоматизації будинку – Порівняння

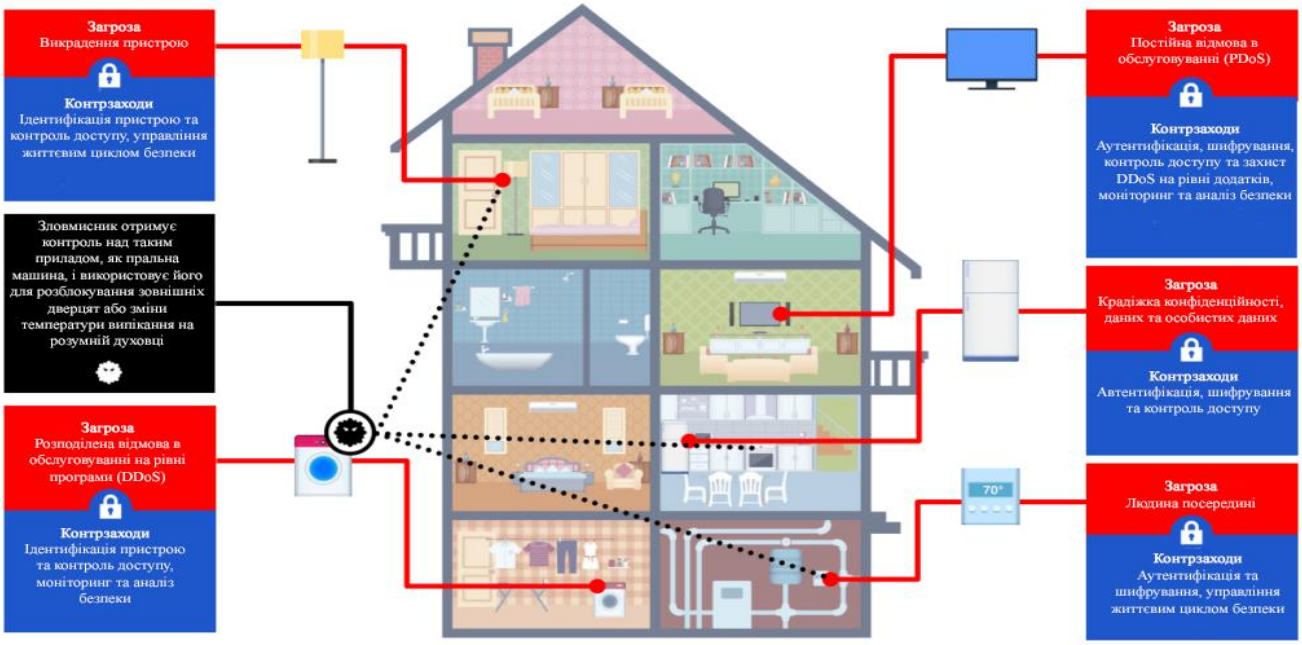
	Wi-Fi	**Z-Wave**	**Zigbee**	**Thread**	**BLE**
Площа покриття	широка	широка	широка	широка	широка
Енергоефективний	Ні	Так	Так	Так	Так
Пропускна здатність даних	висока	низька	низька	низька	висока*
Діапазон частот	2.4GHz	900MHz	2.4GHz	2.4GHz	2.4GHz
Топологія	зірка	сітка	сітка	сітка	скаттернет
Об’єднання	Wi-Fi Alliance	Z-Wave Alliance	Zigbee Alliance	Thread Group	Bluetooth SIG

Табл. 2.1. Порівняння протоколів автоматизації будинку

Хоча Wi-Fi фактично є стандартом для бездротових локальних мереж, його використання в якості протоколу домашньої автоматизації залишається затьмареним низькою енергоефективністю. З іншого боку, Z-хвилі, Zigbee і Thread пропонують меншу пропускну здатність даних, що ідеально підходить лише для роботи з наднизьким енергоспоживанням та підтримки тривалого часу автономної роботи датчиків. Саме Bluetooth LE може запропонувати як більшу швидкість передачі даних, так і низьке споживання енергії (в ідеальних умовах), але знову ж не відповідає безпеці.

2.3 Розумний будинок: Загрози і заходи протидії

Безпека є важливою проблемою в середовищі розумного будинку. Особливо в ситуаціях, коли розумні будинки можуть зберігати та передавати конфіденційні дані третім особам, що робить дані, зібрані в розумних



середовищах, вразливими до серйозних порушень безпеки та конфіденційності. Отже, виявлення цих проблем безпеки має вирішальне значення для вжиття відповідних заходів щодо їх пом’якшення та підвищення безпеки зібраних даних у цих будинках. Ця робота зосереджує свою увагу на аналізі можливих проблем безпеки в розумних домашніх середовищах, виявленні різних атак та вразливостей з можливими рекомендаціями та контрзаходи для пом'якшення цих загроз.

Рис. 2.2. Типова схема загроз-контрзаходів в «розумному домі»

2.3.1 Загрози розумних будинків

За оцінками, 80% пристроїв IoT вразливі до широкого кола атак. Очевидно, що підключення традиційно «самостійних» розумних пристроїв, таких як світильники, прилади та замки, створює численні ризики для кібербезпеки. Навіть підключені радіо-няні вразливі для цифрових вторгнень, оскільки низка жахливих батьків із запізненням виявили, коли хакери розмовляли зі своїми маленькими дітьми через скомпрометовані пристрої. Поширені загрози кібербезпеки та атаки на розумні домашні пристрої включають:

Людина посередині (Man-in-the-middle): Зловмисник порушує, перериває або підробляє зв'язок між двома системами. Наприклад, підроблені дані про температуру, «генеровані» пристроєм моніторингу навколишнього середовища, можуть бути підроблені та передані в хмару. Подібним чином зловмисник може вимкнути вразливі системи HVAC під час теплової хвилі, створюючи катастрофічний сценарій для постачальників послуг із зазначеними моделями.

Викрадення даних та особистих даних (Data and identity theft): Дані, отримані незахищеними пристроями, що носяться та розумними пристроями, надають кібер-зловмисникам велику кількість цільової особистої інформації, яка потенційно може бути використана для шахрайських транзакцій та виявлення крадіжок.

Викрадення пристрою (Device hijacking): Зловмисник викрадає і фактично бере на себе контроль над пристроєм. Ці атаки досить складно виявити, оскільки зловмисник не змінює основних функціональних можливостей пристрою. Більше того, потрібен лише один пристрій, щоб потенційно заразити всі розумні пристрої вдома. Наприклад, зловмисник, який спочатку компрометує термостат, може теоретично отримати доступ до всієї мережі та дистанційно відімкнути двері або змінити PIN-код клавіатури, щоб обмежити вхід.

Розподілена відмова в обслуговуванні (Distributed Denial of Service, DDoS): атака відмови в обслуговуванні (DoS-атака) намагається зробити машину або мережевий ресурс недоступними для призначених користувачів тимчасовим або невизначеним відключенням служб хоста, підключеного до Інтернету. У випадку розподіленої атаки відмови в обслуговуванні (DDoS), вхідний трафік, що

затоплює ціль, походить з декількох джерел, що ускладнює зупинку кібернаступу просто блокуючи одне джерело. Насправді DDoS-атаки швидко зростають, в першу чергу через брак безпеки в пристроях IoT. Ботнет-атака Mirai була масовою розподіленою DDoS-атакою, через яку більша частина Інтернету стала недоступною на східному узбережжі США.

Постійна відмова в обслуговуванні (Permanent Denial of Service, PDoS): Постійні атаки відмови в обслуговуванні (PDoS), також відомі як флешинг, - це атака, яка наносить шкоду пристрою настільки сильно, що вимагає заміни або перевстановлення обладнання. Одним із таких прикладів є BrickerBot, кодований для використання жорстко закодованих паролів на пристроях IoT та спричинення постійної відмови в обслуговуванні. Ще один приклад може бачити фальшиві дані, подані на термостати, намагаючись завдати непоправної шкоди через сильний перегрів.

2.3.2 Захист розумних будинків

Підключені розумні домашні пристрої повинні бути захищені комплексним рішенням безпеки IoT (від пристрою до хмари), яке не порушує прибутковість постачальника послуг або виробників обладнання та час виходу на ринок. Комплексне рішення безпеки IoT має включати такі можливості:

Безпечне завантаження (Secure boot)

Безпечне завантаження використовує методи підписання криптографічного коду, гарантуючи, що пристрій виконує лише код, згенерований OEM-пристроєм або іншою довіреною стороною. Використання технології безпечного завантаження перешкоджає хакерам замінювати прошивку шкідливими версіями, тим самим запобігаючи атакам.

Взаємна автентифікація (Mutual authentication)

Кожного разу, коли розумний домашній пристрій підключається до мережі, його слід аутентифікувати перед отриманням або передачею даних. Це гарантує, що дані надходять із законного пристрою, а не з шахрайських джерел. Криптографічні алгоритми, що включають симетричні ключі або асиметричні ключі, можуть бути використані для двосторонньої автентифікації. Це гарантує, що дані надходять із законного пристрою, а не з шахрайських джерел. Криптографічні алгоритми, що включають симетричні ключі або асиметричні ключі, можуть бути використані для двосторонньої автентифікації. Наприклад, алгоритм безпечного хешу (SHA-x) можна використовувати для симетричних ключів, а алгоритм цифрового підпису еліптичної кривої (ECDSA) для асиметричних ключів.

Безпечне спілкування (Encryption)

Захист даних під час передачі між пристроєм та його сервісною інфраструктурою (хмара). Шифрування забезпечує доступ до переданих даних лише тим, хто має секретний ключ дешифрування. Наприклад, розумний термостат, який надсилає дані про використання оператору послуг, повинен мати можливість захистити інформацію від цифрового прослуховування.

Моніторинг та аналіз безпеки (Security monitoring and analysis)

Збирає дані про загальний стан системи, включаючи пристрої кінцевих точок та трафік підключення. Потім ці дані аналізуються для виявлення можливих порушень безпеки або потенційних системних загроз. Після виявлення слід виконати широкий спектр дій, сформульованих у контексті загальної політики безпеки системи, наприклад, карантинних пристроїв на основі аномальної поведінки. Цей цикл моніторинг-аналіз-дія може виконуватися в режимі реального часу або пізніше для виявлення моделей використання та виявлення потенційних сценаріїв атак. Дуже важливо забезпечити захист пристроїв кінцевих точок від можливого втручання та обробки даних, що може призвести до неправильного повідомлення про події.

Управління життєвим циклом безпеки (Security lifecycle management)

Функція управління життєвим циклом дозволяє постачальникам послуг та виробникам обладнання контролювати аспекти безпеки пристроїв IoT під час роботи. Швидка бездротова (OTA) заміна ключів пристрою під час відновлення після кібер-катастрофи забезпечує мінімальне порушення роботи служби. Крім того, безпечне виведення з експлуатації пристрою гарантує, що браковані пристрої не будуть перероблені та використані для підключення до служби без дозволу.

Висновок до 2 розділу

На сьогодні автоматизація залишається основною сферою діяльності майже у всіх сферах, і більшість технологій IoT зосереджені на посиленні контролю M2M над ручними завданнями. Розумні будинки становлять значну частину цього плану, пропонуючи власникам розумних продуктів та розробникам розумних будинків вікно можливостей адаптуватися та розвиватися якомога раніше.

РОЗДІЛ 3 ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ В СИСТЕМІ «РОЗУМНИЙ БУДИНОК»

Сьогодні, завдяки нестримному розвитку мікроелектроніки, каналів зв'язку, Інтернет-технологій і Штучного Інтелекту, тема «розумних будинків» стає все більш і більш актуальною. Людське житло зазнало істотних змін з часів кам'яного віку і в епоху Промислової Революції 4.0 і Інтернету Речей стало зручним, функціональним і безпечним. Розумний будинок включає в себе величезну кількість IoT-пристроїв, які збирають і обробляють дані. Вони дають користувачам певні можливості по контролю за апартаментами як в ручному, так і автоматичному режимі. У «розумному середовищі» пристрої періодично обмінюються даними по мережі. Це відбувається або безпосередньо від пристрою до пристрою, або через хмару. Тому захист передачі інформації клієнт-«розумний будинок» є дуже актуальним на сьогоднішній день.

Особливістю роботи - «розумного будинка» є те, що більшість команд на пристрої проходять через мережи передачі даних. В цілому всі елементи ланцюжка мають доступ в Інтернет. Це робить їх уразливими до атак ззовні і наражає на небезпеку не тільки інформацію користувача, але також його здоров'я. Все це змінює парадигму мислення, в якій мовиться: «Мій будинок - острівець безпеки».

Однак безпека, особливо безпека протоколів обміну даними між клієнтом та «розумний будинок» - це 100% вимога для розумного будинку. До складу системи безпеки можуть входити системи спостереження, системи моніторингу (в тому числі здоров'я) і системи безпеки, до яких можна отримати віддалений доступ.

3.1 Ключові проблеми в кібербезпеці та конфіденційності

Інтернет перетворився з корисного науково-дослідного інструменту у фундаментальну корисну систему, таку ж важливу, як електроенергія, вода та газ. Скрізь, де є цінний ресурс, існує також злочин, який прагне отримати користь від незаконного використання цієї технології або відмовити у використанні цього ресурсу іншим. Взаємозв'язаний характер Інтернету означає, що на інтернет-ресурси можна атакувати з будь-якої точки світу, і це робить кібербезпеку ключовою проблемою. Кібербезпека обертається навколо трьох основних тем.

Конфіденційність полягає у збереженні конфіденційності даних, щоб лише авторизовані користувачі (як люди, так і машини) мали доступ до цих даних. Криптографія - ключова технологія досягнення конфіденційності.

Аутентифікація полягає у тому, щоб перевірити, чи не було фальсифіковано дані, і що дані можуть бути підтверджені, що їх було надіслано заявленим автором. Фіксація відмови від авторства (тобто уникнення відмови відправника в тому, що він насправді надіслав повідомлення) іноді розглядається окремо, але ми включаємо його сюди як підмножину автентифікації.

Доступ стосується лише надання належним чином уповноваженим користувачам доступу до даних, комунікаційної інфраструктури та обчислювальних ресурсів, а також гарантування, що цим авторизованим користувачам не заборонений такий доступ.

Огляд порушень інформаційної безпеки - це щорічний звіт про кіберзагрози, замовлений Департаментом бізнесу, інновацій та професійних навичок Великобританії та проведений PriceWaterhouseCoopers (міжнародна мережа компаній, що пропонують послуги в області консалтингу та аудиту). Останнє опитування 2015 [7] року показує, що порушення безпеки посилюються; 90% великих організацій зазнали кібер-порушень у 2015 році проти 81% у 2014 році, а 74% малого бізнесу також зазнали порушень безпеки, що свідчить про двозначний темп приросту в річному обчисленні 14%.

Зараз, коли Інтернет став критично важливим компонентом сучасного бізнесу, кібербезпека стала необхідним компонентом інформаційних систем. Однак із посиленням кібербезпеки кіберзлочинність стає все більш масштабною, деструктивнішою та більш досконалою. У Smart Homes здатність домовласників безпечно управляти своїми системами вимагає надійних та інтуїтивно зрозумілих автоматизованих систем для допомоги в управлінні мережею. Без таких систем загроза безпеці та конфіденційності розумного будинку, ймовірно, перевищує переваги.

3.2 Домени додатків IoT

Деякі домени додатків особливо піддаються підвищенню продуктивності завдяки впровадженню технології IoT. Програми автоматизації заводів та заводів часто групуються під заголовком «Industrial Internet of Things». Надійність, в тому числі через резервування, безпеку та придатність для суворих умов - є одними з ключових питань.

Мережа біомедичних інструментів та баз даних у лікарнях може суттєво покращити кількість та доступність рішень щодо діагностики та лікування [9]. Це також має значні наслідки для сільських та віддалених клінік, забезпечуючи готовий доступ до висновків спеціалістів [10]. Поширення медичних інструментів в домашніх умовах покращило якість життя та скоротило госпіталізацію [11].

Останні два десятиліття спостерігається сплеск використання електроніки в автомобілях на основі десятків мережевих мікропроцесорів [12]. Наступним етапом розвитку буде зв'язок між транспортними засобами, а також між транспортними засобами та інфраструктурою [13]. Стандартизація, безпека та вартість є головними рушіями.

Транспорт та логістика вже є великими користувачами RFID-міток (англ. Radio Frequency IDentification, радіочастотна ідентифікація) для відстеження

вантажів, піддонів і навіть окремих предметів [14]. Напрямок дослідження тут полягає в розумних тегах, які можуть реєструвати та повідомляти транспортні умови, такі як удар, нахил, температура, вологість та тиск [15]. Тут ключовим фактором є низька вартість, а також впорядковане спілкування до сотень або тисяч тегів одночасно.

Технологія IoT чинить руйнівний вплив на дуже широкий спектр галузей, включаючи розваги, харчування, громадський транспорт, спорт та фітнес, телекомунікації, виробництво, готелі, освіту, екологію, робототехніку та роздрібну торгівлю. У багатьох із цих галузей IoT стає ключовим фактором, що сприяє інноваціям та успіху, і галузі готові інвестувати в нові технології. Спеціальна IT-підтримка може надаватися співробітникам або від зовнішніх постачальників, щоб гарантувати, що безпека та доступність їхніх систем є достатніми для їхніх бізнес-потреб.

IoT та розумний дім

Ця робота стосується зовсім іншого середовища - розумного будинку. Професійне проектування, встановлення та налаштування системи може бути доступним, коли розумна електроніка буде включена до складу нового будинку. Однак у більшості випадків технологія розумного дому IoT, швидше за все, буде модернізована до існуючого будинку поштучно по мірі виникнення потреб. Часто не існує постійної професійної підтримки як на етапах проектування, так і на етапі розгортання IoT у Розумному домі. Незважаючи на те, що існують деякі досить широко розповсюджені спеціалізовані стандарти розумного будинку, такі як зв’язок між лініями електропередач X.10, вони не мають будь-якого типу безпеки і були розроблені до підключення цих мереж домашнього управління до Інтернету [16]. Зараз існує безліч мережевих стандартів, які можна використовувати вдома (Zwave, Insteon, Bluetooth, Zigbee, Ethernet, Wifi, RS232, RS485, C-bus, UPB, KNX, EnOcean, Thread) [17]. Кожен з них має свої сильні та слабкі сторони, і очікування, що гетерогенна мережа з безліччю різних протоколів буде ефективно та безпечно управляти не експертом, представляє значні проблеми.

Розумний дім потенційно забезпечує додатковий комфорт та безпеку, а також покращує екологічну стійкість. Наприклад, інтелектуальна система кондиціонування може використовувати широкий спектр побутових датчиків та веб-джерел даних для прийняття інтелектуальних робочих рішень, а не простих схем управління вручну або за фіксованим графіком. Розумна система кондиціонування може передбачити очікувану наповненість будинку, відстежуючи дані про місцезнаходження, щоб забезпечити, щоб кондиціонер досяг бажаного рівня комфорту, коли будинок зайнятий, та економить енергію, коли цього немає.

На додаток до поліпшеного комфорту, Розумний дім може допомогти в самостійному житті для людей похилого віку. Розумний дім може допомогти у виконанні щоденних завдань, таких як прибирання, приготування їжі, покупки та прання одягу. Падіння когнітивних функцій низького рівня можна підтримати за допомогою інтелектуальних домашніх систем, які забезпечують своєчасне нагадування про ліки. Моніторинг стану здоров’я вдома може сигналізувати вихователям реагувати до того, як буде потрібна дорога та руйнівна госпіталізація [11]. Однак жодна з цих переваг, швидше за все, не буде використана, якщо система Розумний дім не буде захищена та надійна.

3.4 Загальний характер загроз безпеці – як аналогія доменних загроз

3.4.1 Загрози

Хоча Розумний дім - це зовсім інше середовище, загальний характер загроз безпеці аналогічний іншим доменам.

Загрози конфіденційності - це загроза, які приводять до небажаного розголошенню конфіденційної інформації. Наприклад, порушення

конфіденційності в системах домашнього спостереження може призвести до ненавмисного оприлюднення конфіденційних медичних даних. Навіть, здавалося б, нешкідливі дані, такі як внутрішня температура будинку, а також знання параметрів роботи системи кондиціонування, можуть бути використані для визначення того, зайнятий будинок чи ні, що є передвісником крадіжки зі зломом. Втрата конфіденційності в таких речах, як ключі та паролі, призведе до несанкціонованого доступу до системи.

Загрози автентифікації можуть призводити до фальсифікації або контролю інформації. Наприклад, неавторизовані попередження про стан системи можуть ввести в оману контролера будинку, який вважає, що існує надзвичайна ситуація, і відкриває двері та вікна, щоб забезпечити аварійний вихід, а насправді дозволяє незаконний вхід. Одне питання, яке буде розглянуто пізніше, - це автоматичне оновлення програмного забезпечення - якщо вони не пройшли належну перевірку автентичності, можуть виникнути проблеми.

Загрози доступу - це, мабуть, найбільші загрози. Несанкціонований доступ до системного контролера, особливо на рівні адміністратора, робить всю систему небезпечною. Це може відбуватися через невідповідний пароль та управління ключами, або через неавторизовані пристрої, що підключаються до мережі. Навіть якщо контроль неможливий, несанкціоноване підключення до мережі може вкрасти пропускну здатність мережі або призвести до відмови в обслуговуванні законних користувачів. Оскільки багато пристроїв Smart Home можуть працювати від акумулятора та бездротового зв'язку з низьким робочим циклом, заповнення мережею запитів може призвести до атаки виснаження енергії - форми відмови в обслуговуванні.

3.4.2 Вразливості

Істотна вразливість - доступність мережної системи. Оскільки сучасні системи Smart Home підключені до Інтернету, атаки можна проводити віддалено, або шляхом прямого доступу до мережевих інтерфейсів управління, або шляхом завантаження шкідливого програмного забезпечення на пристрої.

Проблемою є також фізична доступність системи. Як для бездротових, так і для технологій несучих ліній електропередач, до мереж можна отримати фізичний доступ ззовні будинку, навіть якщо сам будинок надійно заблокований.

Наступною вразливістю є обмежені системні ресурси. Контролери пристроїв традиційно являють собою невеликі 8-розрядні мікроконтролери з дуже обмеженими обчислювальними ресурсами та ресурсами зберігання, що обмежує їх здатність реалізовувати складні алгоритми безпеки.

Неоднорідність системи - це вразливість. Пристрої надходять від багатьох виробників з різними мережевими стандартами та різними можливостями оновлення програмного забезпечення. Часто пристрої мають мало або взагалі не мають документації про своє внутрішнє програмне забезпечення, операційні системи та встановлені механізми захисту.

Інша проблема - виправлена прошивка. Дуже мало розумних побутових приладів, які надають будь-які регулярні послуги оновлення програмного забезпечення для виправлення уразливих місць безпеки. Хтось підозрює, що в даний час існує небагато стимулів постійно виправляти програмне забезпечення, щоб випереджати вразливі місця для пристроїв вартістю кілька доларів.

Повільне використання стандартів є вразливістю. Хоча деякі власні системи, такі як підсистема моніторингу стану здоров'я, можуть мати добре розроблену безпеку, що відповідає стандартам, більшість сучасних пристроїв Smart Home реалізують мало підходів, якщо такі взагалі існують.

Ми вважаємо найбільшою вразливістю відсутність спеціальних спеціалістів з безпеки, які можуть управляти складностями мережі Розумний дім. Небагато домовласників можуть дозволити собі професійну постійну допомогу в управлінні домашньою мережею. Натомість домовласники-любителі повинні

мати можливість самостійно управляти своїми системами просто, безпечно та надійно.

3.4.3 Приклади вразливостей

Як приклад, власник дому може припустити, що їх веб-камера доступна лише тим користувачам, яким було надано її ім’я хосту та номер порту. Однак за допомогою пошукових систем, що сканують пристрої в Інтернеті, таких як Shodan (https://www.shodan.io) [18] та Censys (https://censys.io) [19], які законно шукають доступні датчики, багато пристроїв раптом стають відомими і видно.

Звичайні пошукові системи, такі як Google і Bing, сканують в Інтернеті, отримуючи веб-сторінки та переходячи за гіперпосиланнями на цих сторінках, щоб індексувати веб-сторінки, зображення або деякі популярні типи файлів. З іншого боку, пошукові системи, що сканують Інтернет-пристрій, працюють як мережевий сканер, скануючи відкриті порти Інтернет-вузлів та індексуючи інформацію заголовка або банера, що повертається підключеними пристроями; заголовки або банери відповіді часто включають тип пристрою, модель, постачальника, версію мікропрограми та іншу інформацію. Окрім протоколів HTTP і HTTPS, пошукові системи, що сканують пристрої в Інтернеті, використовують різні протоколи (FTP, SSH, DNS, SIP та RTSP тощо) для підключення до відкритих портів вузлів. Для полегшення доступу ці пошукові системи також надають інтерфейс прикладного програмування (API) для програмного доступу до результатів пошуку. Зловмисники можуть скористатися цими пошуковими системами, щоб знайти вразливі пристрої в Інтернеті. Наприклад, використання ключових слів пошуку “port:554 has_screenshot:true” у Shodan поверне список камер домашнього спостереження з їхніми IP-адресами, географічним розташуванням та знімками екрана, як показано на рис. 3.1.

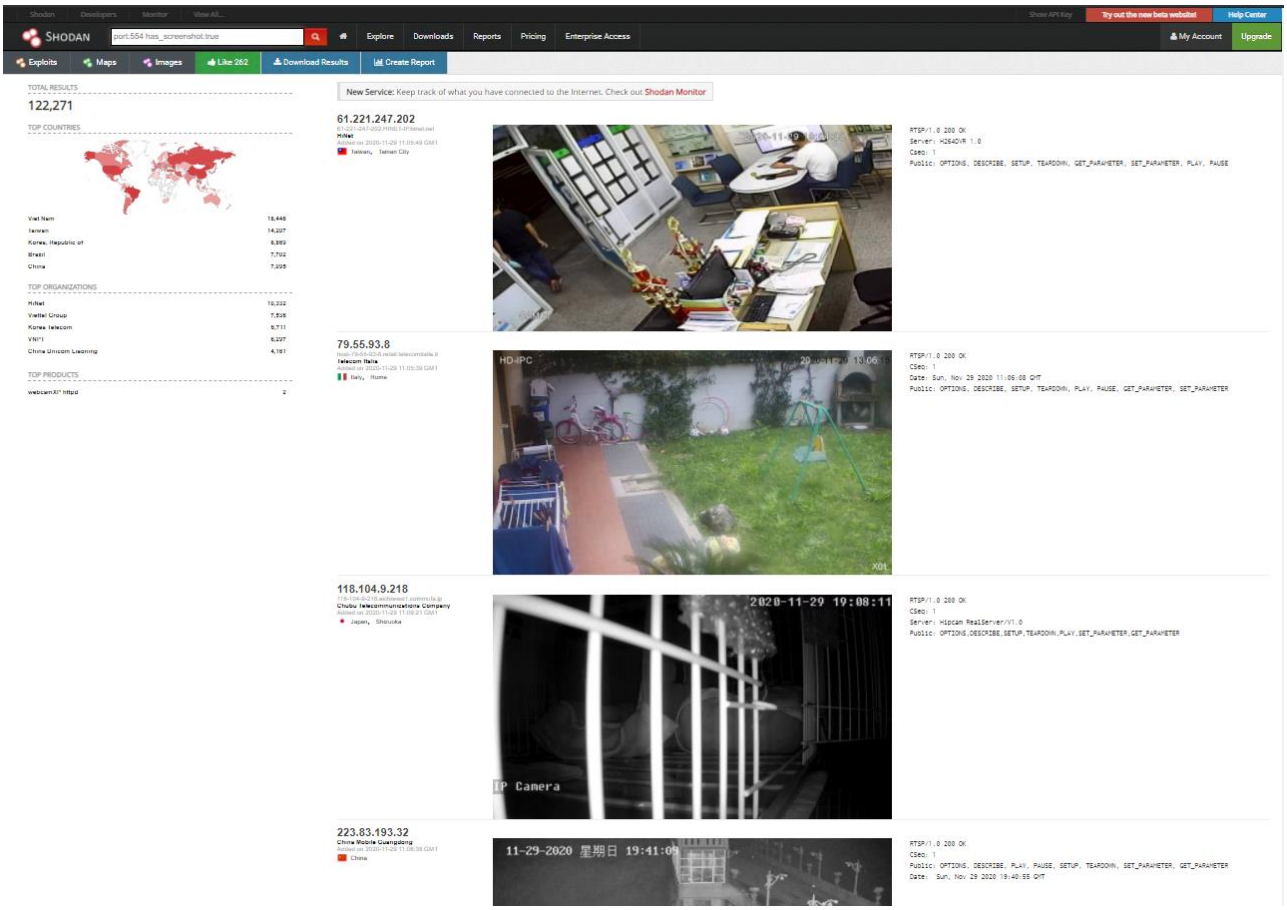


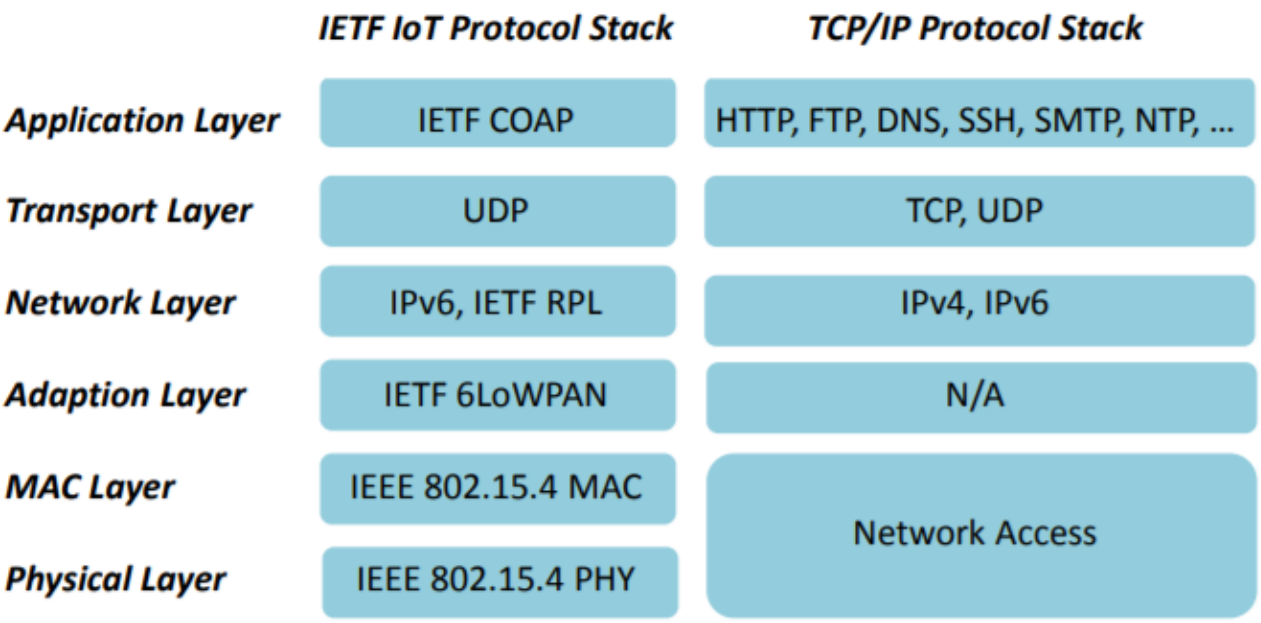
Рис. 3.1. Список камер домашнього спостереження з пошукової системи сканування пристроїв Інтернету Shodan

3.5 Деяка існуюча підтримка безпеки для IoT

Через низьку вартість обчислювальні пристрої IoT, як правило, не настільки потужні, як традиційні настільні та портативні комп'ютери. Більшість пристроїв IoT мають низьку енергію, використовують мікроконтролер низького класу та мають обмежену пам'ять. Такі контролери добре відповідають вимогам окремих контролерів у пральній машині або кондиціонері.

Однак ці характеристики ускладнили перехід до мережевих контролерів, оскільки існуючі протоколи Інтернету, як правило, не призначені для цих вбудованих пристроїв. Для вирішення цих проблем було створено декілька

робочих груп Internet Engineering Task Force (*Інженерна рада інтернету*, IETF - відкрите міжнародне співтовариство проектувальників, учених, мережевих операторів і провайдерів, створене IAB в 1986 році, яке займається розвитком протоколів і архітектури Інтернету.). Робота стандартизації IETF щодо IoT відіграла життєво важливу роль у створенні необхідних полегшених протоколів зв'язку для обмежених середовищ у існуючій мережі IP. Сюди входять IPv6 через малопотужні бездротові персональні мережі (6LoWPAN: RFC 6282) [20], протокол маршрутизації IPv6 для малопотужних та мереж зі втратами (RPL: RFC 6550) [21] та протокол обмежених додатків (CoAP: RFC 7252) [22]. На рис. 3.2. показано порівняння між IETF IoT та стеками протоколів TCP / IP. Після підключення пристроїв до Інтернету будь-яка загроза безпеці в Інтернеті може також порушити безпеку та конфіденційність IoT. У наступних розділах ми розглядаємо поточні впровадження системи безпеки для цих стандартних



протоколів IoT.

Рис. 3.2. Порівняння між IETF IoT та стеками протоколів TCP/IP

3.5.1 6LoWPAN та безпека

Інститут інженерів з електротехніки та електроніки (IEEE) визначив стандарт 802.15.4 для бездротових персональних мереж (WPAN). IEEE 802.15.4 визначає, як фізичні та медіа-рівні управління доступом повинні працювати в умовах низької пропускної здатності, недорогих, низьких швидкостей та низької енергії, характерних для цих мереж. Таким чином, 6LoWPAN [23] - це легкий протокол, розроблений IETF, що дозволяє передавати пакети IPv6 через бездротові мережі IEEE 802.15.4.

Набір Internet Protocol Security (IPsec) визначив заголовки автентифікації (AH) та інкапсуляцію корисних навантажень безпеки (ESP), щоб забезпечити цілісність даних, конфіденційність, автентифікацію джерела та захист від повторного відтворення пакетів IPv6. Автори [24] запропонували стислі функції AH та ESP для 6LoWPAN для реалізації IPsec і, таким чином, забезпечують наскрізний захищений зв'язок між бездротовими пристроями.

Покращена схема автентифікації та встановлення ключів для мереж 6LoWPAN (EAKES6Lo) була запропонована авторами у матеріалах Міжнародної конференції IEEE 2015 року з питань комунікаційного семінару (ICCW), Лондон, Великобританія, 8–12 червня 2015 р. [25]. EAKES6Lo розділений на два етапи для підвищення безпеки мереж 6LoWPAN. Дві фази: (1) налаштування системи; та (2) автентифікація та встановлення ключа. На фазі 1 для шифрування передачі даних у мережі використовується симетричний механізм криптографії Advanced Encryption Standard (AES). Для перевірки цілісності даних використовується хеш-функція Алгоритм дайджесту повідомлень 5 (MD5) або Алгоритм безпечного хешу (SHA). На етапі 2 відбудеться обмін шістьма повідомленнями для завершення процесу автентифікації та встановлення ключів та встановлення взаємної автентифікації.

Таким чином, 6lowPAN забезпечує шаблон для безпечного бездротового зв'язку, навіть для обмежених ресурсів пристроїв.

3.5.2 RPL та безпека

Протоколи маршрутизації є основним компонентом звичайних мереж, і це також стосується мереж 6LoWPAN. RPL [21] - це оптимізований протокол маршрутизації IPv6, розроблений IETF, спеціально для мереж з низьким енергоспоживанням та втрат (LLN) і в основному використовується мережами 6LoWPAN. RPL - це протокол маршрутизації з віддаленим вектором, і його топологія відображення базується на структурі орієнтованого на цільову спрямованість ациклічного графіка (DODAG). Загальна схема аутентифікації топології, яка називається Trust Anchor Interconnection Loop (TRAIL) для RPL, представлена в [26]. TRAIL може запобігти атакам топологічної невідповідності з боку фальшивих вузлів, виявляючи та ізолюючи ковані вузли. Повідомлення в обидва кінці було використано TRAIL для перевірки цілісності висхідного шляху до кореневого вузла та допомоги вузлам у дереві отримати справжню інформацію про рейтинг. Інновація TRAIL полягає в тому, що кожен вузол у дереві може перевірити свій висхідний шлях до кореня та виявити будь-які підроблені атаки рангу.

Отже, існуючі рішення можуть забезпечити безпечне створення таблиці маршрутизації в мережах Smart Home.

3.5.3 CoAP та безпека

CoAP [22] - це протокол HTTP-подібного прикладного рівня, призначений для обмежених мереж пристроїв. Оскільки існують деякі особливі вимоги, такі як груповий зв'язок у мережах IoT, CoAP надає підтримку багатоадресної передачі,

якої HTTP не має. Для кращої відповідності з'єднанням із низькою пропускною здатністю та середовищам пристроїв із низькою обчислювальною потужністю CoAP приймає протокол User Datagram Protocol (UDP). UDP - простіший протокол транспортного рівня з низькою затримкою та без зв'язку в порівнянні з відповідним протоколом управління передачею (TCP). CoAP - це протокол без статусу і заснований на моделі архітектури клієнт-сервер. Він використовує операції стилю запит / відповідь для обміну повідомленнями між клієнтом та сервером. Подібно до HTTP, CoAP також базується на репрезентативній моделі передачі стану (REST), де кожен ресурс на сервері має власний єдиний ідентифікатор ресурсу (URI), клієнт може отримати доступ до ресурсу, зробивши запит на сервер, і запит може бути одним із цих чотирьох методів: GET, POST, PUT та DELETE.

На сьогодні захист транспортного рівня (TLS: RFC 5246) [28] є переважним протоколом шифрування для HTTP, але реалізація TLS є надто складною для обмежених ресурсами пристроїв IoT. Для захисту комунікацій CoAP використовує Datagram Transport Layer Security (DTLS: RFC 6347) [29] як протокол безпеки. DTLS пропонує ті самі послуги безпеки, що і TLS. Основна відмінність між TLS і DTLS полягає в тому, що TLS базується на протоколі TCP, а DTLS базується на протоколі UDP. Специфікація CoAP визначила чотири різні режими безпеки. Пристрій може знаходитися в одному з чотирьох режимів безпеки: NoSec, PreSharedKey, RawPublicKey та Certificate.

Знову ж таки, стандарти IETF забезпечують безпечні механізми для безпечного веб-спілкування в обмежених мережах.

3.5.4 Майбутні вказівки щодо безпеки IoT

Як вказують вищезазначені три приклади, вже проводиться значна робота щодо забезпечення критично важливих програм IoT. Багато зусиль було

спрямовано на розробку IP-сумісних захищених комунікаційних мереж, які підходять для пристроїв з обмеженими ресурсами і використовують сучасні методи безпеки. Однак багато з цих методів вимагають ретельного, уніфікованого загальносистемного проектування та досвідчених мережевих інженерів, щоб спроектувати та підтримувати безпечну систему IoT. Основна увага в нашій роботі не на цьому стилі «технічної» безпеки, а на аспекті управління системою безпеки Smart Home, тобто на тому, як правильно встановити та підтримувати безпеку, увімкнену цими потужними інструментами.

3.6 Майбутні проблеми безпеки розумного дому

Було багато різних пропозицій щодо архітектур розумного будинку, кожна з яких має певні проблеми безпеки. Три найважливіші та найпопулярніші архітектури - це архітектури проміжного програмного забезпечення, хмари та шлюзу. Наступні розділи досліджують проблеми безпеки та труднощі реалізації для цих стилів архітектури.

3.6.1 Підтримка автоконфігурації

Очікується, що все більше розумних побутових приладів буде підключено до мереж Smart Home. Відсутність технічної підтримки є найбільшим викликом у домашньому середовищі. Домогосподарства будуть обтяжені виснажливими, повторюваними та схильними до помилок ручними завданнями щодо додавання та управління цими розумними пристроями у своїй домашній мережі, що може становити серйозний ризик для безпеки. Отже, для успішного впровадження

розумного будинку слід додатково вивчити підхід безпечної автоматичної конфігурації не лише для спрощення інсталяції та обслуговування пристрою Smart Home, але й для підвищення безпеки в процесі автоматичної конфігурації.

Наш підхід вимагає функціональності шлюзу та хмарних служб. Коли новий пристрій приєднано до мережі, шлюз буде використовувати ідентифікатор пристрою для опитування довіреної веб-служби, щоб виявити деталі пристрою - яка його функціональність, які команди, які шифрувальні та мережеві протоколи він розуміє, і будь-які важливі оновлення мікропрограми, які зараз доступні. Це інший підхід до більшості підходів до автоматичної конфігурації, що вимагає збереження великої кількості цієї інформації на самих пристроях, а також для того, щоб пристрої могли вже реалізувати глибокий стек протоколів. З нашим підходом простий ідентифікатор пристрою та веб-служба забезпечують легку доступність цієї інформації та її актуальність.

На рис. 3.3 показано типову архітектуру мережі та ряд кроків, необхідних для ініціації цієї автоматичної конфігурації

Рис. 3.3. Архітектура автоконфігурації

3.6.2 Оновлення програмного забезпечення та прошивки IoT

Настільні операційні системи регулярно та автоматично оновлюються в міру виявлення та виправлення вразливих місць безпеки. Мобільні пристрої, такі як смартфони, також регулярно отримують оновлення програмного забезпечення, включаючи механізми перевірки справжності змін. Такі системи економічно життєздатні, оскільки кількість варіантів операційних систем та виробників операційних систем невелика, а розгорнутих пристроїв мільйони. Подібна послуга регулярного оновлення недоступна для сотень різних пристроїв IoT.

Пристрій IoT - це поєднання апаратного та програмного забезпечення для виконання конкретних, спеціальних завдань. Прошивка - це тип програмного забезпечення, яке програмується в енергонезалежну пам’ять смарт-пристрою. Це є важливою частиною будь-якої системи IoT, оскільки прошивка - це програма, яка безпосередньо взаємодіє з апаратним забезпеченням, контролюючи роботу та функції системи, починаючи від ініціалізації пристрою, взаємодії з користувачами, обробки запитів та виконання завдань. Як наслідок, життєво важливим є оновлення програмного забезпечення смарт-пристрою для усунення вразливостей системи безпеки, покращення функціональності, додавання нових функцій та виправлення інших помилок. На відміну від корпоративного середовища, яке має власний IT-відділ або технічну групу для управління та розгортання оновлень програмного забезпечення, середовище Розумний дім зазвичай не має технічної підтримки. Пристрої IoT для Smart Homes повинні мати механізми автоматичного впровадження безпечних та надійних оновлень мікропрограми, практично без втручання користувача. Такою функціональністю може керувати домашній шлюз.

Для забезпечення цілісності та автентичності оновлень та запобігання можливим підробкам програмного забезпечення, таким як введення зловмисного програмного забезпечення, до оновлень слід застосовувати цифрові підписи на основі сертифікатів. Перед оновленням кожне оновлення має бути перевірене на відповідність його цифровому підпису, а цифровий сертифікат має бути перевіреним, щоб переконатися, що він дійсний та виданий продавцем або довіреною третьою стороною. Методології, що використовуються для завантаження нових оновлень, також вимагають ретельного продумування. Якщо механізми перевірки оновлень порушені, хакер може заблокувати встановлення нових оновлень та здійснити атаку на незмінену прошивку. Зловмисники також можуть замаскувати легітимну стару версію прошивки з уразливими місцями безпеки як останню версію, в результаті чого прошивка повернеться до несправної версії. Тому постачальник пристрою або виробник повинен зашифрувати та цифрово підписати оновлену інформацію про випуск, не надаючи кіберзлочинцям можливості втручатися в процес обслуговування версії оновлення. Через низьку пропускну здатність та обмеженість ресурсів багатьох інтелектуальних пристроїв, дельта-оновлення значно покращують ефективність та скорочують час завдання, оскільки оновлення дельти містять лише ті дані, які змінилися. Це може значно зменшити можливість помилки оновлення, особливо для пристроїв, що працюють від акумуляторів, через перезарядку акумулятора під час трудомісткого процесу оновлення мікропрограми.

Автори [36] запропонували новий механізм оновлення програмного забезпечення для пристроїв IoT з обмеженими ресурсами, який називається Generic extension for Internet-of-Things ARchitectures (GITAR), який можна застосувати до існуючих операційних систем IoT. На думку авторів, ця архітектура здатна використовувати стандартні файлові структури, інструменти та методи для застосування часткових оновлень коду (дельта-оновлення) для протоколів та програм під час виконання. Ця архітектура складається з трьох рівнів: статичного системного рівня, рівня динамічного компонента та рівня ядра.

Основні компоненти операційної системи та драйвери апаратного забезпечення реалізовані на системному рівні. З метою підвищення портативності програмного забезпечення системний рівень поділяється на апаратну абстракцію (HAL) та рівень апаратного інтерфейсу (HIL). Статичний код на системному рівні можна оновити лише оновивши всю прошивку. На відміну від системного рівня, програми та компоненти мережевого протоколу працюють на рівні компонентів, а код на рівні компонентів є гнучким, а це означає, що цей код можна динамічно оновлювати замість заміни всієї прошивки. Рівень ядра - це інтерфейс між системним та компонентним рівнями. Він пов'язує динамічні компоненти між собою та з функціями системи. Автори продемонстрували свій підхід за допомогою популярної операційної системи IoT з відкритим кодом Contiki, не вимагаючи значних змін у вихідному коді в існуючих мережевих протоколах та додатках.

Запропонований нами підхід, подібний до автоматичної конфігурації, спирається на два ключові компоненти. Перший реалізований як веб-сервіс. Виробник або довірена третя сторона (як зазначено під час автоматичної конфігурації) підтримує найновіші версії програмного забезпечення та мікропрограми, які можна перенести на шлюзи, визначені під час процесу автоматичної конфігурації. Веб-служба може розрізняти вразливості в операційній системі або конкретному коді програми пристрою, а також може завантажувати виправлення для обох. Шлюз управляє процесом оновлення локально. Шлюз може автоматично планувати ці оновлення в зручний для місцевого часу час. Шлюз може також керувати оновленням інформації про відкат, якщо установка оновлення призводить до несподіваної втрати функціональності, коли шлюз проводить автоматичне тестування оновленого програмного забезпечення. Шлюз може також автоматично реагувати на критичні вразливості, наприклад, блокуючи мережевий доступ до незахищеного пристрою, доки не з’явиться патч.

3.7 Підходяща архітектура розумного дому для забезпечення безпеки

Було багато різних пропозицій щодо архітектур розумного будинку, кожна з яких має певні проблеми безпеки. Три найважливіші та найпопулярніші архітектури - це архітектури проміжного програмного забезпечення, хмари та шлюзу. Наступні розділи досліджують проблеми безпеки та труднощі реалізації для цих стилів архітектури.

3.7.1 Архітектура проміжного програмного забезпечення та безпека

Проміжне програмне забезпечення - це програмний рівень, який розміщується між низькорівневим рівнем пристроїв та високорівневим прикладним рівнем. Зазвичай він забезпечує загальний інтерфейс та стандартну структуру обміну даними для абстрактних складних та різноманітних деталей апаратного забезпечення нижчого рівня. Коли проміжне програмне забезпечення отримує запит від додатку вищого рівня, воно перетворює високий рівень стандартизованого запиту доступу до ресурсів до відповідних методів, специфічних для пристрою. Коли пристрій відповідає назад на додаток, проміжне програмне забезпечення обробляє низькорівневі методи та перетворення даних, а потім надсилає відповідні абстрактні команди та дані назад до програми. Додатку не потрібно знати основні деталі різних реалізацій обладнання, він може просто викликати команди та функції, що надаються проміжним програмним забезпеченням. Безпеку та захист конфіденційності слід розглядати на всіх рівнях

проміжного програмного забезпечення, від нижчого рівня взаємодії апаратного забезпечення до вищого рівня загального інтерфейсу.

VIRTUS Middleware [30] - це проміжне рішення, засноване на відкритому протоколі розширюваного обміну повідомленнями та присутності (XMPP). Він приймає протокол SASL (Simple Authentication and Security Layer) для автентифікації та Transport Layer Security (TLS) для захисту даних та конфіденційності.

Безпечне проміжне програмне забезпечення для вбудованих однорангових систем (SMEPP) [31] - це проміжне програмне забезпечення, яке зосереджується на забезпеченні однорангового зв'язку між розумними вузлами. Перш ніж пристрій зможе спілкуватися з іншими, йому потрібно приєднатися до групи, надавши дійсні облікові дані. Існує три різні рівні безпеки, але лише рівень 1 і рівень 2 використовують механізми безпеки. Немає реалізації безпеки під рівнем 0. SMEPP реалізує криптографію із загальнодоступним ключем на рівні 1 та криптографію з відкритим ключем на рівні 2 для групового прийому. З іншого боку, SMEPP застосовує аутентифікацію на рівні 1 та автентифікацію разом із підходом шифрування на рівні 2 для захисту безпеки даних.

Хоча проміжне програмне забезпечення широко застосовується в корпоративних системах з машинами настільного класу для управління складними різнорідними мережами, пропоновані в даний час рішення проміжного програмного забезпечення IoT вимагають значних додаткових складних програмних рівнів і криптографічних процедур, які повинні бути реалізовані на пристроях, які не мають ні пам'яті, ні обчислювальної потужності для розміщення. їх. Окрім проблем із продуктивністю, ще одна проблема архітектури проміжного програмного забезпечення полягає в тому, що дефекти кодування в проміжному програмному забезпеченні, ненавмисно введені розробниками, можуть потенційно загрожувати безпеці пристроїв IoT. Тож ми відкидаємо рішення проміжного програмного забезпечення як на сьогодні неможливі для багатьох пристроїв класу IoT.

3.7.2 Хмарні архітектури та безпека

Співпраця між пристроями є важливим аспектом IoT. Такі сумісні функції вимагають високої обчислювальної потужності, на яку не здатні більшість пристроїв IoT. Для вирішення проблеми продуктивності пристроїв IoT дослідники запропонували хмарні рішення для IoT. Хмара має ресурси для моніторингу, збору, зберігання та обробки даних з пристроїв IoT. Аналізуючи ці дані, хмара може ініціювати дії відповідно до визначених користувачем політик для досягнення складного управління розумним будинком. Хмарна архітектура IoT також відома як Cloud of Things (CoT).

Автори [32] пропонують хмарну архітектуру IoT, засновану на протоколі CoAP IETF [22]. Архітектура складається з трьох розділених етапів, які є етапами мережі, протоколу та бізнес-логіки. Кожен етап включає чергу вхідних подій, пул потоків та обробник подій, який обробляє логіку етапу. Легкий DTLS [29] використовується цією архітектурою як протокол безпеки для автентифікації та зв'язку.

Безпечна схема для домашньої мережі (HAN), заснована на хмарних обчисленнях, була представлена в [33]. Система управління домом (HMS) управляє пристроями та політиками та забезпечує точку доступу для користувачів. У статті автори реалізують функції HMS у хмарі та інтерфейси HMS із хмарними службами. Ця схема використовує симетричне шифрування ключів для застосування конфіденційності між наскрізними зв’язками, і кожному розумному об’єкту присвоюється унікальний ключ.

Хмарне рішення усуває потребу в окремому домашньому контролері та забезпечує хороший спосіб для IoT підключатися та співпрацювати; однак він замінює потребу в локальних обчисленнях потребою в значному Інтернет-зв'язку. Через обмежений ресурс IoT, великі обсяги необроблених даних, що генеруються

пристроями IoT, повинні передаватися в хмару без попередньої обробки; тому домашні пристрої потребують високошвидкісного підключення до Інтернету, що постійно працює, з низькою затримкою, але такі постійні з’єднання з високошвидкісним Інтернетом не завжди доступні, особливо у сільській або віддаленій місцевості. Затримка контролю збільшується, особливо якщо сервери закордонні або мережа перевантажена.

Усі пристрої повинні бути доступні через Інтернет, що має широку поверхню атаки, і кожен пристрій повинен мати достатньо ресурсів для реалізації повних протоколів мережевої безпеки. Атаки відмови в обслуговуванні, засновані на обмеженні доступу до більш широкого Інтернету, або випадкові перебої в роботі мережі можуть спричинити збої критично важливих завдань, таких як охорона здоров'я вдома та системи фізичної безпеки. Окрім того, оскільки користувачі не мають повного контролю над своїми хмарними службами, їм доводиться довіряти хмарним провайдерам впровадити відповідні та достатні заходи безпеки для своїх даних, але це не завжди так.

Оскільки хмарні системи виходять з ладу без постійного підключення до мережі, ми не віримо, що вони можуть забезпечити безпечну та доступну систему Smart Home самі по собі, а також піддають всі мережеві пристрої мережевим атакам.

3.7.3 Архітектура шлюзів

Шлюз IoT - це відносно багатий на ресурси мережевий процесор, що працює в одній локальній мережі з іншими кінцевими точками IoT. Це може бути не лише центральним пунктом управління, який займається координацією

пристроїв IoT, але також може покращити взаємозв'язок та взаємодію між смарт-пристроями різних виробників. Крім того, він може виступати в якості моста для підключення локальної інфраструктури IoT до хмари. Оскільки шлюз має більше обчислювальної потужності та ресурсів, великі обчислювальні завдання та багато пам’яті можуть бути завантажені з пристроїв IoT на шлюз. З точки зору безпеки, шлюз може централізувати аутентифікацію користувача та застосовувати контроль доступу для захисту від несанкціонованого доступу або модифікації обмежених даних. Він також діє як брандмауер для захисту смарт-пристроїв та конфіденційності від кіберзагроз та зменшення поверхні атаки.

У роботі [34] автори представляють архітектуру інтегрованого шлюзу доступу (IAGW) для підтримки різних вузлів додатків через стандартні інтерфейси для середовищ Smart Home. Архітектура включає всюдисущий сенсорний мережевий рівень, мережевий рівень та рівень послуг. IAGW включає модуль безпеки для реалізації аутентифікації, авторизації та шифрування. Однією з переваг цієї архітектури є те, що вона має модуль якості обслуговування (QoS) для пріоритетності трафіку та гарантування ресурсів для критично важливих операцій.

Систематична концепція, яка називається серверною архітектурою Internet-of-Things (SBIOTA) [35], є запропонованим сервером шлюзу для забезпечення ефективного, ефективного, безпечного та спільного інтеграційного рішення для IoT. Ця концептуальна архітектура включає нову послугу автоматичної конфігурації на шлюзі, що полегшує процес розгортання та управління пристроєм, щоб пристрій можна було підключити до мережі та бути повністю функціональним у цій мережі з мінімальним ручним налаштуванням. Його початковий підхід полягає в тому, що автентифікація та зв’язок між шлюзом та пристроями здійснюються через окремий мережевий порт або антену короткого діапазону, фізично прилеглу до сервера. Перш ніж підключати пристрої до мережі, користувачеві потрібно розмістити їх у фізичній близькості від шлюзу для

автентифікації та обмінюватися відповідною інформацією, щоб забезпечити підключення до мережі лише законним пристроям.

Шлюз може реалізовувати складні алгоритми управління на досить потужному процесорі та може керувати критичними функціями розумного будинку. Навіть за тимчасової відсутності підключення до Інтернету, він може забезпечити складний брандмауер та підтримку проксі для пристроїв IoT, щоб вони мали мінімальний вплив прямих мережевих атак, і він може працювати з обмеженими ресурсами пристроями IoT без складного проміжного програмного забезпечення. Отже, це наша улюблена архітектура розумного будинку.

3.8 Метод захисту інформації «Системи розумний дім» на базі нового протоколу обміну даних

У міру того, як все більше підключених пристроїв приєднується до екосистемі Інтернету речей, дослідники проводять ряд тестів безпеки, щоб виявити уразливості Інтернету речей і розповісти світу про потенційні проблеми безпеки при підключенні пристроїв без належних заходів безпеки. Ключові вектори загроз:

1) Загроза, що виходить від зламаних пристроїв. Оскільки багато пристроїв мають власні цінності в силу їх конструкції і характеру функцій, підключений пристрій являє собою потенційну ціль для використання зловмисником. Підключена камера відеоспостереження може розкрити особисту інформацію, наприклад місцезнаходження користувача, при зломі. Це може бути щось настільки ж просте, як управління освітленням в будинку або службовому приміщенні, або щось настільки ж зловмисне, як керування автомобілем або медичним пристроєм, який може заподіяти фізичну шкоду.

2) Загроза по каналу зв'язку. Загроза по каналу зв'язку включає в себе моніторинг і перехоплення повідомлень під час сеансу зв'язку. Через обсяг і чутливості даних, що проходять через екосистеми IoT, атаки з метою націлювання на канал зв'язку особливо небезпечні, оскільки повідомлення і дані можуть бути перехоплені, захоплені або ними можна маніпулювати під час передачі. Наприклад, зловмисник може відслідковувати споживання енергії, щоб дізнатися час простою або час безвідмовної роботи системи (наприклад, службових приміщень), щоб спланувати атаку на всі основні системи управління і контролю розумних міст; інший зловмисник може маніпулювати даними, переданими комунальною компанією, і змінювати інформацію. Успішні порушення, такі як ці приклади, можуть поставити під загрозу довіру до інформації та даних, що передаються через інфраструктуру IoT.

3) Основні загрози для виробників пристроїв Інтернету речей і постачальників хмарних послуг можуть поставити під загрозу всю екосистему Інтернету речей, оскільки виробникові і хмари Інтернету речей довірено розміщувати трильйони даних, деякі з яких є дуже конфіденційними за своєю природою. Ці дані важливі, тому що вони являють собою аналітику, яка є основним стратегічним активом, це значний обсяг конкурентної інформації в очах підпільної APT-групи, якщо вона розкрита. Якщо майстер скомпрометований, це дасть зловмисникові можливість маніпулювати безліччю пристроїв одночасно, деякі з яких, можливо, вже були розгорнуті в польових умовах. Наприклад, якщо у постачальника, який часто випускає вбудоване програмне забезпечення / програмне забезпечення, механізм скомпрометований, на пристрої може бути впроваджений шкідливий код.

Тому пропонується метод захисту інформації «Системи розумний дім» на базі нового протоколу обміну даних. Він заснований на модифікації відомого алгоритму (OFM) S-box ГОСТ 34.12-2015, що забезпечує "усунення" можливих криптографічних закладок та підвищення криптостійкості в постквантовий період (поява повномасштабного квантового комп'ютер, що дозволяє зламати на основі алгоритмів Гровера та Шора сучасні симетричні та асиметричні криптосистеми).

Крім того, комерційне впровадження забезпечить "протидію" можливих криптодепозитів спецслужбами, що зменшить ризик злому шляхом виявлення "слабких" (вразливих) місць на основі криптографічних закладок.

В алгоритмі блок, що шифрується (довжина 64 біта), розділений на дві рівні частини (32 біти) - праву та ліву. Далі тридцять дві ітерації виконуються з використанням ітераційних ключів, отриманих з вихідного 256-бітного ключа шифрування. Під час кожної ітерації здійснюється одне перетворення на основі мережі Фейстела з правою та лівою половиною зашифрованого блоку. Спочатку права частина складається в модуль 232 з поточним ітераційним ключем, потім отримане 32-бітове число ділиться на вісім 4-бітових і кожен з них, використовуючи таблицю перестановок, перетворюється в інший 4-бітний номер. Після цього перетворення отримане число крутиться вліво на одинадцять розрядів. Далі XOR трансформується з лівою половиною блоку. Отримане 32-бітове число записується в правій половині блоку, а старий вміст правої половини переноситься в ліву половину блоку. Діаграма основного кроку крипто-перетворення алгоритму показана на рис. 3.4.

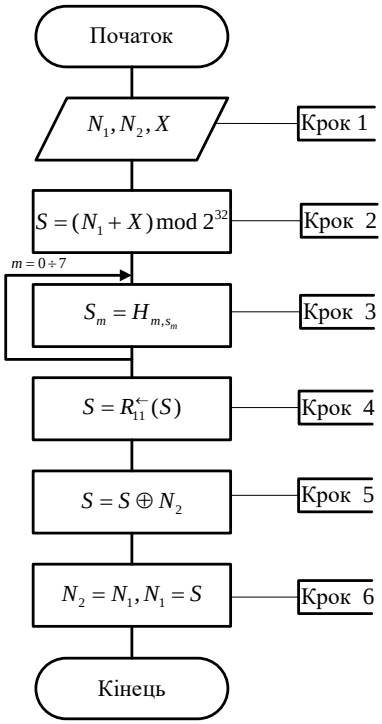


Рис. 3.4. Схема основного кроку криптоперетворення алгоритму ГОСТ 34.12-2015

Основний крок криптотрансформації алгоритму складається з наступних етапів:

Крок1. Введення вихідних даних для основного кроку криптоперетворення N - 64-розрядний блок введення перетворюється на два 32-розрядних цілих числа (молодшу (N_1) і найстаршу (N_2) частини);

Крок2. Додавання до ключа. Молодша частина перетвореного блоку складається в модуль із ключовим елементом, що використовується на кроці.

Крок3. Заміна блоку. Отримане на попередньому кроці 32-бітове значення інтерпретується як масив із чотирьох 4-бітових блоків коду: $S_m = (S_0, S_1, S_2, \ldots S_{15})$.

Крок4. Циклічний зсув на 11 біт вліво.

Крок5. Додане побиття: значення, отримане на кроці 3, порушується модулем 2 із старшою половиною перетвореного блоку.

Крок6. Зсув по ланцюжку: Молодша частина перетвореного блоку зміщується на місце старшого, а на його місце розміщується результат попереднього кроку.

Тоді структура алгоритму може описати діаграму, представлену на рис. 3.5.

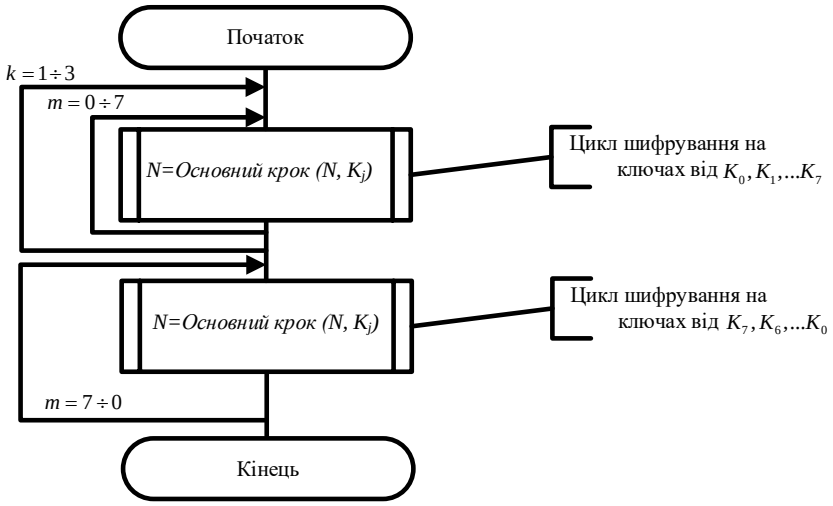


Рис. 3.5. Цикл шифрування ГОСТ 34.12-2015

Щоб створити вдосконалення алгоритму ГОСТ 34.12-2015, ми змінимо основний крок криптоперетворення алгоритму (рис. 3.6) в режимі OFM.

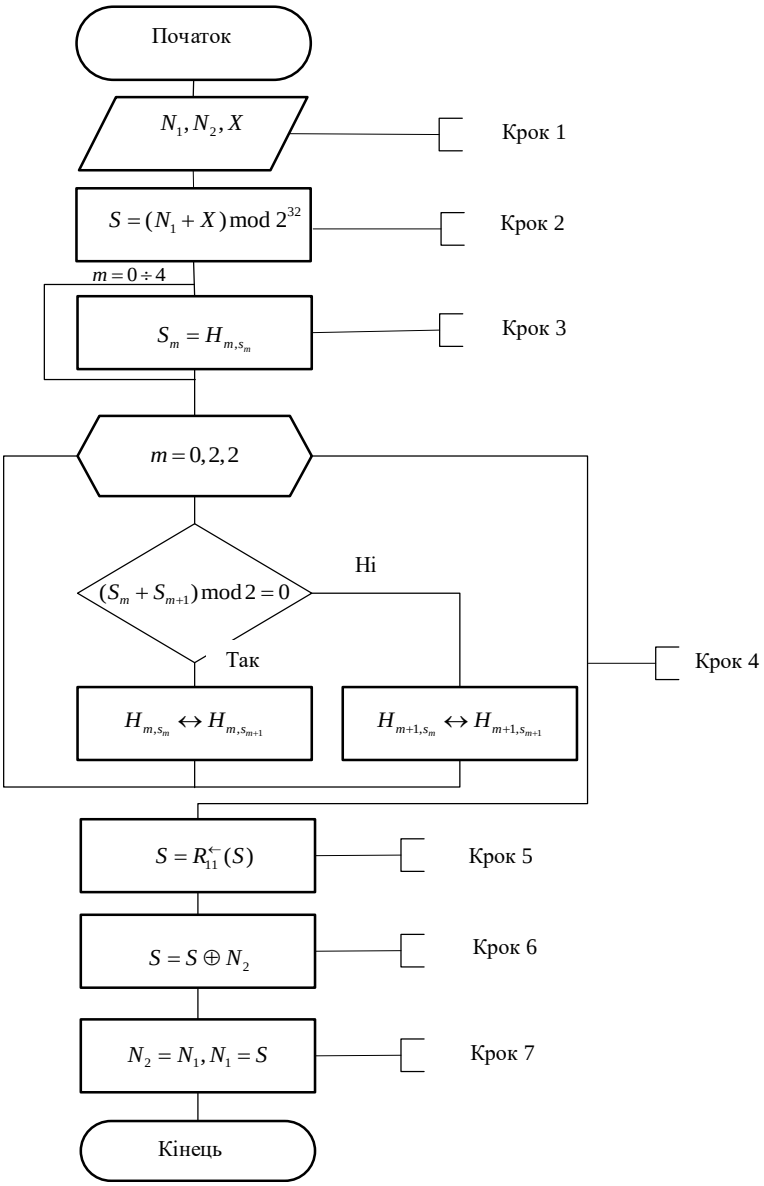


Рис. 3.6. Схема вдосконаленого основного кроку криптоперетворення алгоритму ГОСТ 34.12-2015

Візьміть за основу порядок змін значень у блоці S алгоритму потокового шифрування RC 4. RC4, алгоритм потокового шифрування, був запропонований в 1987 році Рональдом Лінном Рівестом, відомим американським фахівцем з криптографії. З 1994 року він широко використовується в ряді криптографічних додатків, включаючи відомі, такі як SSL та TLS, для шифрування даних, переданих через мережі передачі даних, які не забезпечують захист даних

користувачів, WPA та WEP для захисту бездротових з'єднань. В алгоритмі шифрування потокового передавання два значення S-блоку міняються місцями, коли формується псевдо-ключова послідовність.

Основний крок криптоперетворення алгоритму складається з наступних етапів:

Крок1. Введення вихідних даних для основного кроку криптоперетворення N - 64-розрядний блок введення перетворюється на два 32-розрядних цілих числа (молодшу (N_1)) та найстаршу (N_2)) частини);

Крок2. Додавання до ключа. Молодша частина перетвореного блоку складається в модуль з ключовим елементом, що використовується на сходинці.

Крок3. Заміна блоку. 32-бітове значення, отримане на попередньому кроці, інтерпретується як масив із чотирьох 8-бітових блоків коду: $S_m = (S_0, S_1, S_2, \ldots S_{255})$.

Потім значення кожного з чотирьох блоків замінюється новим, яке вибирається таблицею заміщення наступним чином: значення блоку S_i змінюється на елемент порядку S_i (нумерація від нуля) і вузол підстановок (тобто і рядок таблиці заміщення, нумерація також від нуля). Іншими словами, як заміна значення блоку, елемент вибирається із таблиці замін із числом, рівним номеру блоку, що замінюється, і номером стовпця, рівним 8-бітовому значенню цілого невід'ємного номер.

Крок4. Динамічна зміна таблиці заміщення виглядає наступним чином: якщо сума $S_0 + S_1$ парне число, то міняються місцями значення $S_0 \leftrightarrow S_1$ таблиць H_0, інакше $S_0 \leftrightarrow S_1$ таблиць H_1. Якщо сума $S_2 + S_3$ парне число, то поміняйте місцями значення $S_2 \leftrightarrow S_3$ таблиць H_2, інакше $S_0 \leftrightarrow S_1$ таблиць H_3.

Крок5. Циклічний зсув на 11 біт вліво.

Крок6. Додане побиття: значення, отримане на кроці 3, порушується модулем 2 зі старшою половиною перетвореного блоку.

Крок7. Зсув по ланцюжку: Молодша частина перетвореного блоку зміщується на місце старшого, а на його місце розміщується результат попереднього кроку.

Крок6. Отримане значення перетвореного блоку повертається в результаті виконання алгоритму основного кроку крипто-перетворення.

Використання цього перетворення дозволяє динамічно (на основі простого генератора послідовностей псевдо-ключів) формувати режим OFM та забезпечувати необхідний рівень криптостійкості.

Розрахунки та практичні рекомендації:

Підсумовуючи етапи захищеності, знайдемо «Підвищення ймовірності захищеності»:

У звітах зарубіжних компаніях наведені наступні дані: P1=0,4 – це стандартний захист «розумного дому». Але, як виявилося, алгоритми шифрування і конфіденційність даних була на проблематичному рівні. Постає питання покращити безпеку, розробивши бездротовий мережевий стандарт, ймовірність якого P2=0,25. Тепер існує ймовірність захищеності P1+P2=0,4+0,25=0.65. Згадавши, що в системах «Розумний дім» відсутнє шифрування, запропонуємо модифікацію відомого алгоритму (OFM) S-box ГОСТ 34.12-2015, що забезпечує "усунення" можливих криптографічних закладок та підвищення криптостійкості в постквантовий період, ймовірність захищеності якого P3=0.3. У зв’язку з тим, що у нас система послідовна, ми отримаємо P1+P2+P3=0,95=P. Розрахуємо наскільки наша нова система має більшу захищеності:

$$(P-(P1+P2))/(P1+P2)\times 100\%=(0,95-0,65)/(0,65)\times 100\%\approx 46\%$$

Отже, наша нова система на 46% має більшу захищеність, ніж існуючий до цього метод.

Окрім математично технічних засобів розроблені практичні рекомендації щодо захисту пристроїв IoT у своїх розумних будинках. Заходи безпеки, які користувачі можуть прийняти для захисту своїх розумних будинків від атак на пристрої Інтернету речей:

1) Зрівняйте всі підключені пристрої. Всі пристрої, підключені до мережі, наприклад, вдома чи на рівні підприємства, повинні бути добре враховані. Слід зазначити їх налаштування, облікові дані, версії прошивки і останні виправлення.

Цей крок може допомогти оцінити, які заходи безпеки слід вжити користувачам, і визначити, які пристрої, можливо, доведеться замінити або оновити.

2) Змініть паролі та налаштування за замовчуванням. Переконайтеся, що установки, що використовуються кожним пристроєм, відповідають більш високої безпеки, і поміняйте налаштування, якщо це не так. Змініть паролі за замовчуванням і слабкі паролі, щоб уникнути атак, таких як груба сила і небажаний доступ.

3) Патч вразливостей. Установка виправлень може виявитися складним завданням, особливо для підприємств. Але обов'язково застосовувати виправлення відразу після їх випуску. Для деяких користувачів виправлення можуть порушити їх звичайні процеси, для чого можна використовувати віртуальне виправлення.

4) Застосовуйте сегментацію мережі. Використовуйте сегментацію мережі, щоб запобігти поширенню атак і ізолювати потенційно проблемні пристрої, які не можна відразу відключити.

Загальні рекомендації з безпеки Інтернету речей

1) Традиційні параметри, такі як справжність, конфіденційність, цілісність і доступність, можуть використовуватися для захисту екосистеми Інтернету речей.

2) Для управління безпекою взаємопов'язаних пристроїв нам потрібна дійсно відкрита екосистема зі стандартизованими інтерфейсами прикладного програмування, які забезпечують взаємодію з надійною і автоматичною системою виправлень. Криптографічні механізми - більш надійний спосіб захисту зв'язку від підробки, підробки прошивки і незаконного доступу.

3) Багаторівнева безпека з високим рівнем захисту для захисту даних від атак шкідливих програм, вразливостей в мережах і програмних додатках.

4) Апаратна безпека може бути реалізована шляхом впровадження захисту мікросхеми у вигляді TPM (Trusted Perception Module), довіреного термінального модуля і довіреного мережевого модуля. Безпечне завантаження можна

використовувати, щоб гарантувати, що на пристрої буде працювати тільки перевірене програмне забезпечення.

5) Мережева безпека може бути досягнута за допомогою рішень безпеки, орієнтованих на дані, які забезпечують безпеку шифрування даних при передачі або зберіганні. Для виявлення небажаних вторгнень і запобігання зловмисних дій можуть використовуватися брандмауери і системи запобігання вторгнень.

6) Безпека на рівні додатків відноситься до методів захисту веб-додатків від зловмисних атак, які можуть розкрити конфіденційну інформацію. Це можна зробити за допомогою брандмауера веб-додатків, контролера доставки додатків, безпечного веб-шлюзу і т. д.

7) Повинні бути національні сертифікати або політики, що засвідчують безпеку електронної ланцюга поставок.

Напрямки подальших досліджень

Подальші дослідження доцільно спрямувати на удосконалення програмних засобів для ліквідування загроз, що виходять від зламаних пристроїв. Оскільки багато пристроїв мають власні цінності в силу їх конструкції і характеру функцій, підключений пристрій являє собою потенційну ціль для використання зловмисником. Підключена камера відеоспостереження може розкрити особисту інформацію, наприклад місцезнаходження користувача, при зломі. Це може бути щось настільки ж просте, як управління освітленням в будинку або службовому приміщенні, або щось настільки ж зловмисне, як керування автомобілем або медичним пристроєм, який може заподіяти фізичну шкоду.

Висновки до 3 розділу

Проведений аналіз проблем безпеки обміну даними між клієнт - «розумний будинок». Визначені пріоритети захисту інформації на етапі передачі інформації.

Проведений аналіз запропонованого нового бездротового мережевого стандарту Thread. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а основним його достоїнством є безпека. Одночасно в мережі можуть знаходитися до 250 пристроїв, які захищаються шифруванням рівня банківської системи. Але цього недостатньо для забезпечення цілісності інформації.

Запропоновано використання нового алгоритму шифрування на основі поточного алгоритму шифрування, заснованого на алгоритмі блокчейну, завдяки використанню динамічно змінюваного нелінійного бієктивного перетворення (S-блоки) дозволяє уникнути значних проблем інформаційної безпеки.

Цей алгоритм використовуються для забезпечення конфіденційності (безпеки під час передачі), цілісності (безпеки при зберіганні та модифікації лише для авторизованих користувачів) та автентичності (достовірність джерела повідомлення). Та забезпечує надійний захист інформації. Дозволяє підвищити захист протоколу передачі даних «Системи розумний дім» на 46 %

ВИСНОВКИ

Проведений аналіз проблем безпеки обміну даними між клієнт - «розумний будинок». Визначені пріоритети захисту інформації на етапі передачі інформації. Проведений аналіз запропонованого нового бездротового мережевого стандарту Thread. Thread використовує IPv6 і побудований на стандарті IEEE 802.15.4, а основним його достоїнством є безпека. Одночасно в мережі можуть знаходитися до 250 пристроїв, які захищаються шифруванням рівня банківської системи. Але цього недостатньо для забезпечення цілісності інформації.

Запропоновано використання нового алгоритму шифрування на основі поточного алгоритму шифрування, заснованого на алгоритмі блокчейну, завдяки використанню динамічно змінюваного нелінійного бієктивного перетворення (S-блоки) дозволяє уникнути значних проблем інформаційної безпеки.

Цей алгоритм використовуються для забезпечення конфіденційності (безпеки під час передачі), цілісності (безпеки при зберіганні та модифікації лише для авторизованих користувачів) та автентичності (достовірність джерела повідомлення). Та забезпечує надійний захист інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

Книги

1. Thubert, P. Compression Format for Ipv6 Datagrams over IEEE 802.15.4-Based Networks; RFC 6282; Hui, J., Ed.; Internet Engineering Task Force: Fremont, CA, USA, 2011.

2. Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks; RFC 6550; Winter, T., Thubert, P., Eds.; Internet Engineering Task Force: Fremont, CA, USA, 2012.

3. Shelby, Z.; Hartke, K.; Bormann, C. The Constrained Application Protocol (Coap); RFC 7252; Internet Engineering Task Force: Fremont, CA, USA, 2014.

4. Shelby, Z.; Bormann, C. 6lowpan: The Wireless Embedded Internet; John Wiley & Sons: New York, NY, USA, 2011; Volume 43.

5. Raza, S.; Duquennoy, S.; Chung, T.; Yazar, D.; Voigt, T.; Roedig, U. Securing Communication in 6lowpan with Compressed Ipsec. In Proceedings of the 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barcelona, Spain, 27–29 June 2011; pp. 1–8.

6. Yue, Q.; Maode, M. An authentication and key establishment scheme to enhance security for m2m in 6lowpans. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 2671–2676.

7. Perrey, H.; Landsmann, M.; Ugus, O.; Schmidt, T.C.; Wahlisch, M. Trail: Topology Authentication in RPL. 2013, arXiv:1312.0984v2.

8. Xiang He "SMART HOME" - FROM A CONCEPT TO A LIVING PRODUCT

9. Athina Lazakidou, Konstantinos Siassiakos, Konstantinos Ioannou. Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications

10. Olexander Belej, Lohutova Tamara. БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

11. H. C. Keong, M. R. Yuce, “UWB-WBAN sensor node design,” IEEE Trans., Boston, MA, pp. 2176-2179, 2011

12. F. Wu, C. Rüdiger, M.R. Yuce, “Real-Time Performance of a Self-Powered Environmental IoT Sensor Network System,” Sensors, 17:282, pp. 184-253, 2017

13. S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, “An experimental study of security and privacy risks with emerging household appliances,” in Communications and Network Security (CNS), 2014 IEEE Conference he. IEEE, 2014

14. Monastyrsky, L., Petryshyn, O. Features of data collection and processing for smart object management / L. Monastyrsky, O., Petryshyn // Electronics and Information Technologies. - 2017. - Issue 7. - P. 86–92

Наукові статті

15. Белей О.І., Логутова Т.Г. БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ

16. Білова А.О., Онищенко В.В. МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РОЗУМНОГО БУДИНКУ

Електронні ресурси

17. IoT Privacy and Security Challenges for Smart Home Environments URL: https://www.mdpi.com/2078-2489/7/3/44

18. БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ URL: https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/107

19. A Review on Security in Smart Home Development URL:https://www.researchgate.net/publication/228416463_A_Review_on_Security_in_Smart_Home_Development

20. A Study of Smart Home Environment and it’s Security Threats

URL:https://www.researchgate.net/publication/303089918_A_Study_of_Smart_Home_Environment_and_it's_Security_Threats