Vol. 5, No. 1, 2023

Юрій Гасюк[1], Андріанна Йовбак[2], Михайло Мельник[3], Роман Винарович [4] Іван Попович[5]

[1]Кафедра систем автоматизованого проектування, Національний університет Львівська політехніка, вул. Степана Бандери 12, Львів, Україна, E-mail: yurii.l.hasiuk@lpnu.ua
[2]Кафедра систем автоматизованого проектування, Національний університет Львівська політехніка, вул. Степана Бандери 12, Львів, Україна, E-mail: andrianna.v.yovbak@lpnu.ua
[3]Кафедра систем автоматизованого проектування, Національний університет Львівська політехніка, вул. Степана Бандери 12, Львів, Україна, E-mail: mykhaylo.r.melnyk@lpnu.ua, ORCID 0000-0002-8593-8799
[4]Кафедра систем автоматизованого проектування, Національний університет Львівська політехніка, вул. Степана Бандери 12, Львів, Україна, E-mail: roman.i.vynarovych@lpnu.ua
[5]Кафедра систем автоматизованого проектування, Національний університет Львівська політехніка, вул. Степана Бандери 12, Львів, Україна, E-mail: popovych.i.p@gmail.com

ПРОБЛЕМИ БЕЗПЕКИ В СИСТЕМАХ РОЗУМНОГО ДОМУ

Отримано: Вересень 12, 2023 / Переглянуто: Жовтень 10, 2023 / Прийнято: жовтень 24, 2023

https://doi.org/

Анотація. У статті проведено дослідження вразливості протоколів передачі даних, які використовуються у системах керування "розумного будинку", з особливим акцентом на аналізі комунікаційних протоколів, що використовуються в цих системах. Поширення взаємопов'язаних пристроїв та Інтернету речей (IoT) призвело до зростання занепокоєння щодо конфіденційності даних, несанкціонованого доступу та потенційних кібератак. Проведений поглиблений аналіз різних комунікаційних протоколів, що використовуються в середовищі "розумного будинку", що дало змогу виявити їхні переваги та недоліків з точки зору безпеки. На основі проведеного аналізу надані рекомендації щодо вибору протоколів зв'язку, які відповідають принципам безпеки і конфіденційності в середовищі "розумного будинку".

Ключові слова: системи розумного будинку, безпека, уразливості, автентифікація, шифрування, сегментація мережі

Вступ

Стрімкий розвиток технологій призвів до появи та широкого розповсюдження систем "розумного дому", які революціонізували спосіб взаємодії людей зі своїм житловим простором [1]. Ці системи охоплюють мережу взаємопов'язаних пристроїв і приладів, які спілкуються, співпрацюють і автоматизують завдання для підвищення комфорту, зручності та енергоефективності [2]. Розумні будинки охоплюють широкий спектр застосувань, починаючи від автоматизованого освітлення і клімат-контролю до моніторингу безпеки і розважальних систем.

Хоча концепція "розумних будинків" обіцяє численні переваги, такі як підвищення енергоефективності, зручності та якості життя, вона також створює низку проблем у сфері безпеки, які не можна залишати поза увагою [3]. Взаємопов'язана природа цих пристроїв, яку часто називають Інтернетом речей (IoT), наражає їх на потенційні вразливості, якими можуть скористатися зловмисники [4]. Зі збільшенням кількості взаємопов'язаних пристроїв у середовищі "розумного будинку" зростає і потенційна область для атак кіберзлочинців.

Основне побоювання, пов'язане з системами "розумного дому", - це їхня вразливість до порушень безпеки та несанкціонованого доступу. Компрометація одного пристрою в мережі може призвести до ланцюгової реакції, витоку конфіденційних персональних даних і навіть надання несанкціонованого контролю над критично важливими системами. Більше того, дані, зібрані цими

пристроями, які часто включають особисті звички, розпорядок дня та вподобання, викликають значні ризики для приватності.

У цій статті розглядаються проблеми безпеки, які виникають в результаті інтеграції різних пристроїв в середовище "розумного будинку", з особливим акцентом на протоколах зв'язку. Протоколи зв'язку слугують основою для обміну інформацією між цими пристроями, а їхня безпека має вирішальне значення для захисту всієї екосистеми [5]. Аналізуючи переваги та недоліки різних протоколів зв'язку, які зазвичай використовуються в системах "розумного будинку", ця стаття має на меті надати інформацію для прийняття обґрунтованих рішень, що забезпечують баланс між зручністю та безпекою.

Наступні розділи цієї статті присвячені всебічному дослідженню протоколів зв'язку в системах "розумного будинку", аналізу їхніх аспектів безпеки, а також практичним рекомендаціям щодо зменшення вразливостей і створення безпечного середовища "розумного будинку". Оскільки технологічний ландшафт продовжує розвиватися, розуміння тонкощів безпеки протоколів зв'язку "розумних" будинків набуває першорядного значення для забезпечення захисту приватного життя людей і цілісності їхнього житлового простору.

Огляд літературних джерел за темою публікації

Впровадження систем "розумного будинку" стрімко зросло в останні роки завдяки перспективам зручності, енергоефективності та покращення якості життя [6]. Однак це зростання супроводжується збільшенням кількості досліджень, що висвітлюють проблеми безпеки, притаманні цим взаємопов'язаним середовищам .

Порушення безпеки, пов'язані з пристроями "розумного дому", підкреслили нагальність усунення вразливостей. Помітним інцидентом стала атака ботнету Mirai у 2016 році, який скористався слабкою захищеністю пристроїв Інтернет речей, щоб запустити масштабну розподілену атаку типу "розподілена відмова в обслуговуванні" (DDoS). Цей інцидент виявив потенційну можливість викрадення цих пристроїв і використання їх в якості інструментів кіберзлочинців, що ілюструє гостру потребу в удосконаленні заходів безпеки [7,8].

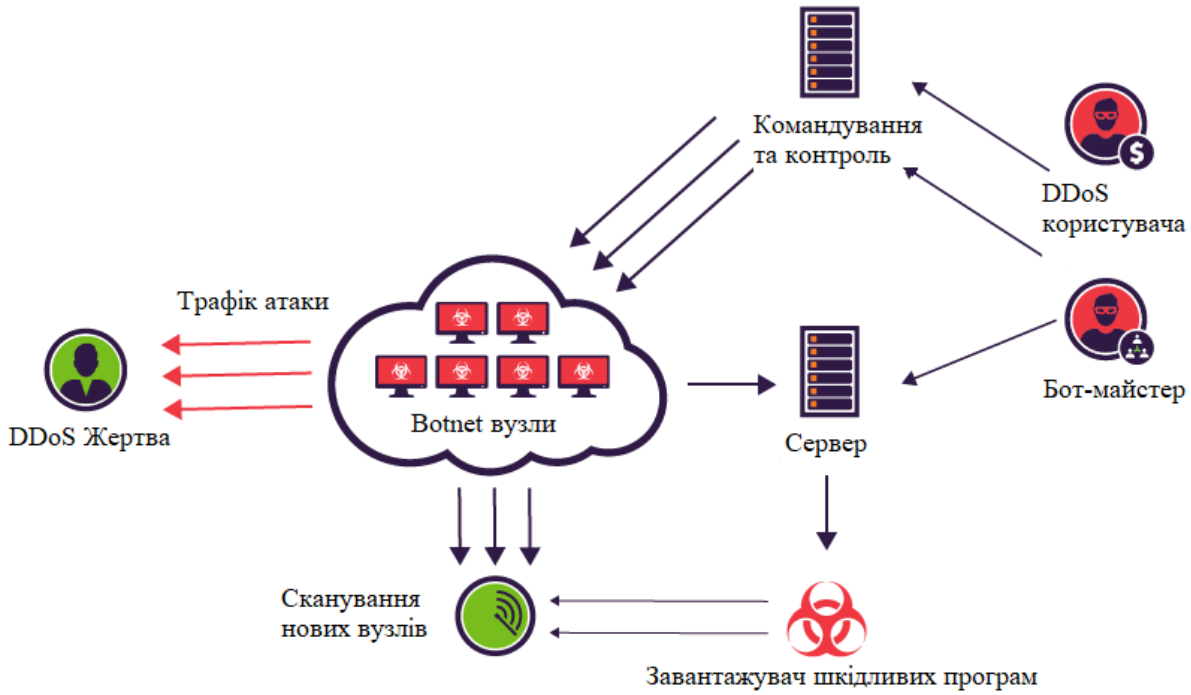

Рис. 1. Пояснення атаки ботнету Mirai

Дослідники широко вивчають протоколи зв'язку як потенційну вразливість. Такі протоколи, як

Wi-Fi та Bluetooth, хоч і є зручними, але можуть бути вразливими до перехоплення інформації та несанкціонованого доступу через їхнє широке використання та звичність. Zigbee і Z-Wave, з іншого боку, рекламуються за їхнє низьке енергоспоживання і можливості великого радіусу дії, але стикаються з критикою за відносно слабку реалізацію безпеки[9].

Дослідження також вивчали концепцію "агностицизму протоколів", припускаючи, що гібридні підходи, які використовують кілька протоколів, можуть забезпечити більш безпечну основу для систем "розумного будинку". Крім того, прогрес у криптографічних технологіях, таких як полегшені протоколи шифрування і автентифікації, показав свою перспективність у підвищенні безпеки каналів зв'язку [10].

Хоча дослідження пролили світло на проблеми безпеки в розумних будинках, залишається потреба у всебічному аналізі протоколів зв'язку з точки зору їх впливу на безпеку. Ця стаття має на меті заповнити цю прогалину шляхом проведення поглибленого аналізу поширених протоколів зв'язку, їхніх сильних і слабких сторін, а також їхньої придатності для різних сценаріїв "розумних" будинків.

Синтез існуючих досліджень з оригінальним аналізом сприятиме цілісному розумінню ландшафту безпеки в протоколах зв'язку розумних будинків. Спираючись на висновки попередніх досліджень, ця стаття має на меті надати практичні рекомендації для приватних осіб, виробників і розробників політики для прийняття обґрунтованих рішень, що підвищують рівень безпеки систем "розумного будинку".

Постановка проблеми

Системи розумного будинку побудовані на мережі взаємопов'язаних пристроїв, які обмінюються даними для забезпечення безперебійної автоматизації та управління. Вибір протоколу зв'язку відіграє ключову роль у визначенні того, наскільки ефективно ці пристрої взаємодіють, обмінюються даними та співпрацюють для виконання різних завдань. У середовищі розумного будинку зазвичай використовується кілька протоколів зв'язку, кожен з яких має свої особливості та вплив на безпеку.

протокол Wi-Fi

Wi-Fi (Wireless Fidelity) - це широко розповсюджений протокол зв'язку, який забезпечує високу швидкість передачі даних і широку сумісність. Він дозволяє пристроям підключатися до інтернету та один до одного в межах певного діапазону. Хоча Wi-Fi пропонує зручність і високошвидкісне з'єднання, його широке використання робить його першочерговою мішенню для кібератак. Потенційними проблемами безпеки, пов'язаними з мережами Wi-Fi, є перехоплення інформації, несанкціонований доступ та злам паролів [13].

Безпека Wi-Fi є критично важливим аспектом бездротових мереж, враховуючи потенційні ризики, пов'язані з несанкціонованим доступом і витоком даних. Для захисту мереж Wi-Fi існують різні протоколи та механізми безпеки.

Ось деякі ключові аспекти:

- протокол WEP (Wired Equivalent Privacy): Одна з найперших схем шифрування, яка зараз вважається застарілою та небезпечною через вразливості, що дозволяють її легко зламати.
- протокол WPA (Wi-Fi Protected Access): Покращений варіант WEP, який використовує для шифрування протокол TKIP (Temporal Key Integrity Protocol - протокол тимчасової цілісності ключа). Він більш безпечний, ніж WEP, але все ще має деякі вразливості.
- протокол WPA2 і WPA3: це найновіші та найбезпечніші протоколи шифрування Wi-Fi, які використовують AES (Advanced Encryption Standard) для шифрування і пропонують надійні функції безпеки.
- Корпоративна безпека. У корпоративних умовах часто використовуються додаткові рівні безпеки, такі як автентифікація RADIUS і цифрові сертифікати.
- Фільтрація MAC-адрес: Дозволяє підключатися до мережі Wi-Fi лише пристроям з певними

MAC-адресами.

• VPN (віртуальна приватна мережа). Часто використовується для додаткового рівня безпеки, особливо в публічних мережах Wi-Fi.

• Брандмауери та системи виявлення вторгнень. Використовуються для моніторингу та контролю мережевого трафіку на основі попередньо встановлених організацією політик безпеки.

протокол Bluetooth

Bluetooth - ще один поширений протокол, який забезпечує бездротовий зв'язок між пристроями на невеликій відстані. Він зазвичай використовується для підключення смартфонів, колонок і переносних пристроїв до центрального хабу. Обмежений радіус дії Bluetooth знижує ризик зовнішніх атак, але в старих версіях протоколу були виявлені вразливості при сполученні пристроїв та аутентифікації [12].

Ключові аспекти безпеки Bluetooth:

• Механізми сполучення. Пристрої Bluetooth використовують такі механізми створення пари, як PIN-код, Just Works і Secure Simple Pairing (SSP) для встановлення безпечного з'єднання.

• Шифрування. Після створення пари Bluetooth-пристрої використовують алгоритми шифрування для захисту даних, що передаються.

• Аутентифікація. Пристрої автентифікують один одного за допомогою механізму "запит-відповідь", щоб переконатися, що обидва є тими, за кого себе видають.

• Захист від підслуховування: Bluetooth використовує частотно-скачкоподібну модуляцію спектра, щоб мінімізувати ризик перехоплення сигналу.

• Підміна пристрою. Зловмисники можуть видавати себе за легальні пристрої Bluetooth, і для протидії цьому використовуються такі заходи безпеки, як автентифікація та авторизація.

• Атаки "людина посередині". Ці атаки передбачають перехоплення несанкціонованим пристроєм зв'язку між двома спареними пристроями.

• Блюджекінг і блюнарфінг: Це специфічні типи атак, коли зловмисник надсилає небажані повідомлення або викрадає інформацію з пристрою з підтримкою Bluetooth..

Zigbee

Zigbee розроблений спеціально для додатків з низьким енергоспоживанням і низькою швидкістю передачі даних. Він працює на частоті 2,4 ГГц і утворює комірчасту мережу, що дозволяє пристроям ретранслювати дані для розширення зони дії мережі. Хоча Zigbee пропонує енергоефективність і надійність, його механізми безпеки критикують за слабкість. Використання криптографії з симетричним ключем і відсутність надійних методів автентифікації можуть зробити його вразливим до атак.

Ключові аспекти Zigbee:

• Шифрування. Zigbee використовує шифрування AES-128 для захисту передачі даних між пристроями.

• Створення пари та встановлення ключів. Zigbee використовує протокол встановлення ключів для безпечного підключення пристроїв, гарантуючи, що тільки авторизовані пристрої можуть приєднатися до мережі.

• Аутентифікація пристрою. Мережі Zigbee часто використовують ідентифікатори пристроїв і ключі для автентифікації, гарантуючи, що тільки авторизовані пристрої можуть отримати доступ до мережі.

• Лічильник кадрів. Використовується для запобігання повторним атакам, коли зловмисник перехоплює і ретранслює пакети даних.

• Оновлення мережевих ключів. Періодичне оновлення мережевих ключів підвищує безпеку, ускладнюючи зловмисникам злам шифрування.

• Вразливості: Zigbee вразливий до різних атак, таких як перехоплення, атаки "зловмисника посередині" та підміна пристроїв..

Протокол Z-Wave

Z-Wave - це ще один протокол бездротового зв'язку з низьким енергоспоживанням, який працює на іншій частоті, ніж Wi-Fi і Bluetooth. Він пропонує відмінний радіус дії та стійкість до перешкод, що робить його придатним для розгортання великих систем "розумного будинку". Z-Wave використовує стандартизовану систему безпеки, яка включає механізми шифрування та автентифікації, що робить його більш безпечним у порівнянні з деякими іншими протоколами [14].

Ключові протоколи безпеки:

- Шифрування. Z-Wave використовує шифрування AES-128 для захисту передачі даних, як і Zigbee.
- Мережеві ключі. Z-Wave використовує мережеві ключі для безпечного зв'язку між пристроями, і ці ключі можна оновлювати для підвищення безпеки.
- Аутентифікація пристрою. Пристрої в мережі Z-Wave аутентифікуються за допомогою унікальних ідентифікаторів, гарантуючи, що тільки авторизовані пристрої можуть приєднатися до мережі.
- Безпечне включення. Z-Wave має безпечний процес включення, який гарантує, що нові пристрої, які приєднуються до мережі, будуть автентифіковані та захищені.
- S2 Security Framework. Новітня система безпеки Z-Wave, відома як S2, пропонує розширені функції безпеки, включаючи ECDH для обміну ключами.
- Вразливості. Z-Wave вразливий до різних типів атак, включаючи атаки "зловмисника посередині", атаки повторного відтворення та підміну пристроїв..

Thread

Це бездротовий протокол на основі IPv6, розроблений для пристроїв Інтернету речей. Він працює на частоті 2,4 ГГц і підтримує mesh-мережі. Thread включає такі функції безпеки, як безпечне завантаження, наскрізне шифрування та авторизація пристроїв. Зосередженість на безпеці та низькому енергоспоживанні робить його потенційним претендентом на розгортання безпечного розумного будинку [15]. Однак, як і будь-який інший бездротовий протокол, Thread має свій власний набір проблем і особливостей безпеки.

Ключові аспекти Thread:

- Шифрування. Thread використовує шифрування AES-128 для захисту пакетів даних під час передачі.
- Аутентифікація пристрою. Мережі Thread використовують унікальні ідентифікатори пристроїв та попередньо надані ключі для автентифікації пристроїв.
- Безпечне введення в експлуатацію. Thread має безпечний процес введення в експлуатацію, який включає в себе шифрування QR-кодів та додаткові рівні автентифікації.
- Атаки на вичерпання енергії. Мережі Thread чутливі до атак на вичерпання енергії, коли зловмисник намагається вичерпати ресурси мережі.
- Атаки на підбір паролів. Потокові мережі також можуть бути вразливими до атак на підбір паролів, особливо на етапі введення в експлуатацію.
- Розширення діапазону мережі. Мережа Thread може бути інтегрована в безпілотні літальні апарати (БПЛА) для збільшення радіусу дії мережі, що також створює нові виклики для безпеки.

Кожен з цих протоколів зв'язку має свій власний набір переваг і міркувань щодо безпеки.

У наступних розділах ми заглибимося в детальний аналіз аспектів безпеки цих протоколів, проливаючи світло на вразливості, контрзаходи та їхню придатність для створення безпечного середовища розумного будинку. Цей огляд має на меті надати інформацію для прийняття обґрунтованих рішень при виборі протоколів зв'язку для системи "розумний дім".

Виклад основного матеріалу

У контексті систем "розумного будинку" забезпечення надійної безпеки має першорядне значення через делікатний характер даних і потенційні наслідки несанкціонованого доступу [11]. У цьому розділі представлено поглиблений аналіз вразливостей безпеки, пов'язаних з кожним

протоколом зв'язку, який зазвичай використовується в середовищі "розумного будинку".

Табл.1.

ПОРІВНЯННЯ ПРОТОКОЛІВ ЗВ'ЯЗКУ

Протокол	***Переваги***	***Недоліки***
Wi-Fi	• Висока швидкість передачі даних підходить для додатків з інтенсивним використанням даних. • Широко розповсюджений і сумісний з широким спектром пристроїв. • Звичний для користувачів, вимагає мінімального налаштування.	• Схильність до перехоплення та несанкціонованого доступу, якщо не захищена належним чином. • Високе енергоспоживання порівняно з малопотужними альтернативами. • Обмежений радіус дії в деяких випадках
Bluetooth	• Зв'язок на невеликій відстані знижує ризик зовнішніх атак. • Спрощений процес створення пари для зручності користувача. • Підходить для персональних мереж	• Вразливий до загроз при створенні пари та автентифікації. • Обмежений радіус дії може вимагати наявності центрального вузла
Zigbee	• Зв'язок з низьким енергоспоживанням, що підходить для пристроїв, які працюють від батареї. • Топологія комірчастої мережі збільшує радіус дії та покриття. • Добре підходить для сценаріїв домашньої автоматизації.	• Слабкі механізми безпеки та вразливості. • Проблеми сумісності між різними профілями Zigbee.
Z-Wave	• Сильніші механізми безпеки в порівнянні з деякими іншими протоколами. • Надійний зв'язок та перешкодостійкість. • Розроблено спеціально для домашньої автоматизації.	• Закритий характер протоколу може обмежити вибір постачальників. • Потенційні проблеми сумісності між різними поколіннями пристроїв Z-Wave
Thread	• Наголос на безпеці завдяки наскрізному шифруванню та безпечному завантаженню.	• Все ще розвивається і не так широко розповсюджений, як інші протоколи. • Проблеми інтеграції можуть вплинути на

Протокол	***Переваги***	***Недоліки***
	• Підтримка IPv6 забезпечує інтеграцію з існуючою інтернет-інфраструктурою. • Зв'язок з низьким енергоспоживанням підходить для пристроїв, що працюють від батареї.	безпеку

Вибір правильного протоколу зв'язку для системи розумного будинку передбачає ретельне вивчення переваг і недоліків кожного протоколу з точки зору безпеки, сумісності, масштабованості і простоти використання.

Вибір найбільш підходящого протоколу залежить від конкретних вимог системи розумного будинку. Наприклад, система, орієнтована на безпеку, може віддати перевагу Z-Wave або Thread через їхній акцент на механізми безпеки. Система з поєднанням застарілих і сучасних пристроїв може отримати вигоду від Wi-Fi і Bluetooth для сумісності. Однак, враховуючи еволюційний характер технологій, важливо не тільки оцінити поточний стан цих протоколів, але й передбачити майбутні оновлення та вдосконалення.

У наступному розділі ми надамо практичні рекомендації, засновані на проведеному аналізі, які допоможуть у виборі протоколів зв'язку, що відповідають принципам безпеки в середовищі розумного будинку.

Результати та обговорення

Рекомендації щодо безпечного використання систем розумного дому

На основі аналізу протоколів зв'язку та їх впливу на безпеку можна виділити практичні рекомендації щодо створення безпечної системи розумного будинку.

1) Оцінка ризиків і міркування щодо конфіденційності

a) Провести ретельну оцінку ризиків, щоб виявити потенційні загрози безпеці та вразливості, характерні для вашого середовища розумного будинку.

b) Враховувати чутливість даних, зібраних пристроями, і надавати перевагу протоколам, які пропонують надійні механізми шифрування та автентифікації.

c) Надавати пріоритет конфіденційності користувачів, обираючи протоколи, які мінімізують ризик витоку даних і забезпечують контроль над їхнім спільним використанням.

2) Гібридні підходи

a) Розглянути можливість впровадження гібридних комунікаційних підходів, які використовують сильні сторони декількох протоколів, пом'якшуючи при цьому їхні слабкі сторони.

b) Використовувати Wi-Fi або Ethernet для високошвидкісних додатків, таких як потокове передавання даних, а протоколи Zigbee або Z-Wave - для пристроїв з низьким енергоспоживанням і підвищеною безпекою.

3) Часті оновлення програмного забезпечення

a) Регулярно оновлювати прошивку та програмне забезпечення на всіх пристроях, щоб забезпечити застосування найновіших виправлень безпеки.

b) Оптимально підходить для пристроїв і виробників, які мають досвід оперативного усунення вразливостей безпеки.

4) Надійна автентифікація та шифрування

a) Надавати перевагу протоколам, які пропонують надійні механізми автентифікації (наприклад, обмін публічними та приватними ключами), щоб запобігти несанкціонованому доступу.

б) Обирати протоколи, які використовують надійні методи шифрування для захисту даних під

час передачі та у стані спокою [16].

5) Репутація та підтримка постачальника

а) Обирати пристрої та протоколи від відомих виробників, які мають репутацію розробників, що дбають про безпеку.

b) Переконатися, що вибрані пристрої отримують постійну підтримку та оновлення для вирішення нових проблем безпеки.

6) Сегментація мережі

а) Сегментувати мережу розумного дому, щоб ізолювати критичні пристрої та обмежити потенційні шляхи атак.

б) Використовувати окремі віртуальні локальні мережі для пристроїв розумного дому та інших компонентів мережі, щоб підвищити безпеку.

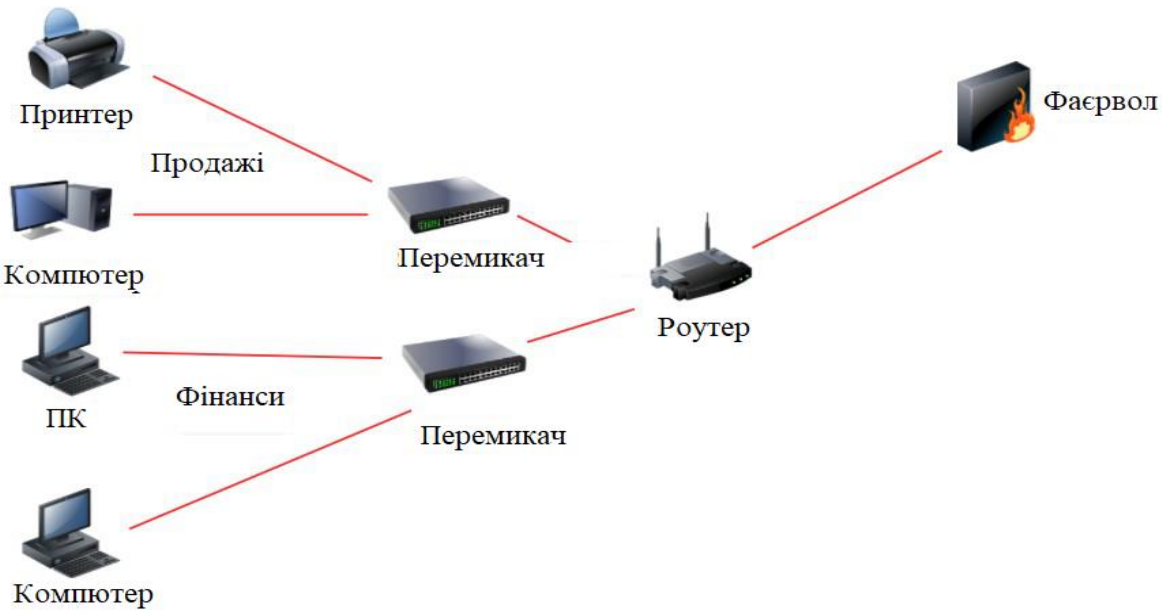

Рис. 2. Загальна схема сегментації мережі

7) Навчання користувачів

а) Навчити усіх користувачів системи "розумний дім" найкращим практикам підтримки безпеки та конфіденційності.

б) Заохочувати використання надійних, унікальних паролів та активацію двофакторної автентифікації, де це можливо.

8) Регулярний аудит безпеки

а) Періодично проводити аудит безпеки, щоб виявити вразливі місця та оцінити загальний стан безпеки системи розумного будинку.

б) Звернутися до фахівців або служб безпеки для проведення ретельних оцінок.

9) Захист на майбутнє

а) Обирати протоколи, які демонструють підтримку постійного вдосконалення безпеки та адаптації до нових загроз.

10) Відповідність нормативним вимогам

а) Ознайомитись з місцевими нормами і стандартами, що стосуються конфіденційності даних і безпеки Інтернету речей.

б) Переконатися, що обрані протоколи зв'язку відповідають нормативним вимогам.

Дотримуючись цих рекомендацій, приватні особи та виробники можуть створити безпечніше

середовище розумного будинку, яке поєднує в собі зручність і надійні заходи безпеки. Оскільки технології Інтернету речей і розумного будинку продовжують розвиватися, підтримка проактивного і адаптивного підходу до безпеки залишається вкрай важливою.

Майбутні напрямки та нові протоколи

З розвитком технологій розвиваються і протоколи зв'язку, які лежать в основі систем розумного будинку. У цьому розділі ви дізнаєтеся про нові тенденції та протоколи, які можуть вплинути на майбутнє безпечного середовища "розумного будинку".

• 5G і периферійні обчислення

Розгортання мереж 5G відкриває потенціал для більш швидкого і надійного зв'язку, зменшуючи затримки і забезпечуючи взаємодію в режимі реального часу [19]. Граничні обчислення, які обробляють дані ближче до джерела, можуть підвищити безпеку, зменшуючи необхідність передачі даних через зовнішні мережі.

• Блокчейн і децентралізовані протоколи

Технологія блокчейн пропонує розподілені і захищені від несанкціонованого доступу реєстри, які можуть підвищити безпеку і цілісність даних розумного будинку [17][18]. Децентралізовані протоколи зв'язку можуть зменшити залежність від централізованих серверів і зменшити кількість точок відмови.

• Вдосконалення методів автентифікації

Біометрична автентифікація (відбитки пальців, розпізнавання обличчя) може підвищити безпеку і зручність користувачів, зменшивши залежність від паролів [21]. Багатофакторна автентифікація може стати більш поширеною для забезпечення ідентифікації користувачів.

• Вдосконалені методи шифрування

Удосконалення алгоритмів шифрування та полегшена криптографія можуть забезпечити більший рівень безпеки з мінімальними обчислювальними витратами [20].

• Стандартизація та інтероперабельність

Зусилля, спрямовані на стандартизацію та інтероперабельність між різними протоколами зв'язку, можуть спростити інтеграцію та підвищити безпеку.

• Машинне навчання та безпека на основі штучного інтелекту

Алгоритми машинного навчання можуть аналізувати моделі поведінки пристроїв для виявлення аномалій і потенційних порушень безпеки. Безпекові рішення на основі ШІ можуть забезпечити виявлення загроз і реагування на них у реальному часі.

• Пост-квантова криптографія

Поява квантових комп'ютерів зумовлює необхідність розробки постквантової криптографії для забезпечення довгострокової безпеки.

• Постійне вдосконалення протоколів:

Існуючі протоколи, такі як Zigbee, Z-Wave і Thread, ймовірно, будуть вдосконалюватися для усунення поточних вразливостей безпеки і нових загроз.

• Рішення безпеки, орієнтовані на користувача:

Майбутні протоколи та системи можуть надавати пріоритет безпеці, орієнтованій на користувача, пропонуючи детальний контроль над обміном даними та згодою користувача [18].

• Розвиток нормативно-правової бази:

Очікується, що правила і стандарти, пов'язані з IoT і безпекою "розумного будинку", будуть розвиватися, формуючи дизайн і реалізацію комунікаційних протоколів.

Сфера протоколів зв'язку розумного будинку динамічно розвивається, а постійні дослідження і розробки формують майбутнє безпечних середовищ Інтернету речей. Інформованість про ці нові тенденції та протоколи має вирішальне значення для приватних осіб, виробників і представників влади, оскільки вони працюють разом, щоб забезпечити постійну безпеку і конфіденційність систем "розумного будинку".

Висновки

Еволюція систем розумного будинку відкрила еру зручності, автоматизації та підключення. Однак цей прогрес супроводжується низкою проблем безпеки, які потребують ретельного розгляду. У роботі проведено комплексний аналіз комунікаційних протоколів, які зазвичай використовуються в середовищі "розумного будинку", з оцінкою їхніх аспектів безпеки, переваг і недоліків.

Цей аналіз показав, що жоден протокол зв'язку не захищений від вразливостей безпеки. Кожен протокол має свій власний набір сильних і слабких сторін, і при виборі протоколу необхідно керуватися конкретними вимогами системи розумного будинку, чутливістю даних, що передаються, і бажаним рівнем зручності.

Технологічний світ, що швидко змінюється, вимагає проактивного та адаптивного підходу до безпеки. Рекомендації, надані в цій статті, слугують орієнтиром для навігації в складних протоколах зв'язку розумного будинку, але вони не є вичерпними. Залишатися пильними щодо нових загроз, йти в ногу з прогресом в області шифрування і автентифікації, а також розвивати культуру обізнаності про безпеку - ось основні практики для забезпечення довгострокової безпеки систем "розумного будинку".

Оскільки технології продовжують розвиватися і з'являються нові протоколи, співпраця між виробниками, дослідниками, політиками і користувачами буде відігравати вирішальну роль у формуванні майбутнього безпечних розумних будинків. Надаючи пріоритет безпеці, конфіденційності та дизайну, орієнтованому на користувача, можна реалізувати бачення безпечного і безперебійного використання розумного будинку, пропонуючи людям переваги автоматизації, захищаючи при цьому їхнє цифрове життя.

Список використаних джерел

1. S. Türkyılmaz and E. Altindag, “Analysis of Smart Home Systems in the Context of the Internet of Things in Terms of Consumer Experience,” EconJournals, vol. 12, no. 1, 2022.

2. M. H. Kabir, and M. T. Ahmed, "IoT-based low-cost smart home automation and security system using wireless technology," Aust. J. Eng. Innov. Technol., vol. 5, no. 3, pp. 101–112, 2023.

3.A. M. Yang, C. Zhang, Y. Chen, Y. Zhuansun, and H. Liu, "Security and Privacy of Smart Home Systems Based on the Internet of Things and Stereo Matching Algorithms," IEEE Internet Things J., vol. 7, no. 4, pp. 2521–2530, 2020.

4. A. T. Kouanou, C. T. Tchapga, M. S. Ekonde, V. Monthe, B. A. Mezatio, J. Manga, G. R. Simo, and Y. Muhozam, "Securing Data in an Internet of Things Network Using Blockchain Technology: Smart Home Case," SN Comput. Sci., vol. 3, no. 2, p. 167, 2022.

5. G. Goyal, P. Liu, and S. Sural, "Securing Smart Home IoT Systems with Attribute-Based Access Control," SAT-CPS@CODASPY, pp. 37–46, 2022.

6. K. Taghizad-Tavana, M. Ghanbari-Ghalehjoughi, N. Razzaghi-Asl, S. Nojavan, and A. Alizadeh, «An Overview of the Architecture of Home Energy Management System as Microgrids, Automation Systems, Communication Protocols, Security, and Cyber Challenges,» Sustainability, vol. 14, p. 15938, 2022.

7. M. A. N. Abrishamchi, A. H. Abdullah, A. D. Cheok, and K. S. Bielawski, "Side channel attacks on smart home systems: A short overview," IECON, pp. 8144–8149, 2017.

8. G. Kaur and K. S. Saini, "Securing Network Communication Between Motes Using Hierarchical Group Key Management Scheme Using Threshold Cryptography in Smart Home Using Internet of Things," in Computing and Network Sustainability, H. Vishwakarma and S. Akashe, Eds., vol. 12, Springer, Singapore, 2017.

9. M. Mamdouh, A. I. Awad, H. F. A. Hamed, and A. A. M. Khalaf, "Outlook on Security and Privacy in IoHT: Key Challenges and Future Vision," AICV, pp. 721–730, 2020.

10. Y. Wan, K. Xu, G. Xue, and F. Wang, «IoTArgos: A Multi-Layer Security Monitoring System for Internet-of-Things in Smart Homes,» INFOCOM, pp. 874–883, 2020.

11. F. Hussain and M. Qi, "Integrated Privacy-Preserving Framework for Smart Home," ICNC-FSKD, pp. 1246–1253, 2018.

12. S. J. Danbatta and A. Varol, «Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation,» ISDFS, pp. 1–5, 2019.

13. M. Tahir, et al., "Wi-Fi Aided Home Energy Management System and AC Prediction through Temperature and Humidity Sensors," in Proc. 2022 Int. Conf. on Cyber Resilience (ICCR), Dubai, UAE, 2022, pp. 1-9, doi: 10.1109/ICCR56254.2022.9995822.

14. S. Rohini and K. Venkatasubramanian, «Z-Wave based Zoning Sensor for Smart Thermostats,» Indian J. Sci. Technol., vol. 8, no. 20, Aug. 2015, doi: 10.17485/ijst/2015/v8i20/79081.

15. Z. Zhao, K. Agbossou, and A. Cardenas, «Connectivity for Home Energy Management applications,» in Proc. 2016 IEEE PES Asia-Pacific Power and Energy Eng. Conf. (APPEEC), Xi'an, 2016, pp. 2175-2180, doi: 10.1109/APPEEC.2016.7779872.

16. B. Mbarek, B. Buhnova, and T. Pitner, «SeMLAS: An Efficient Secure Multi-Level Authentication Scheme for IoT-Based Smart Home Systems,» IWCMC, pp. 1373–1378, 2019.

17. S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, «Blockchain smart contracts: Applications, challenges, and future trends,» Peer-to-Peer Networking and Applications, vol. 14, pp. 2901–2925, 2021.

18. J. Xue, C. Xu, and Y. Zhang, «Private Blockchain-Based Secure Access Control for Smart Home Systems,» KSII Trans. Internet Inf. Syst., vol. 12, pp. 6057–6078, 2018, doi: 10.3837/tiis.2018.12.024.

19. D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Smart Manufacturing and Tactile Internet Based on 5G in Industry 4.0: Challenges, Applications, and New Trends," Electronics, vol. 10, 2021, doi: 10.3390/electronics10243175.

20. D. Shin, K. Yun, J. Kim, P. V. Astillo, J.-N. Kim, and I. You, "A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks," in IEEE Access, vol. 7, pp. 142531-142550, 2019, doi: 10.1109/ACCESS.2019.2943929

Yurii Hasiuk[1] , Andrianna Yovbak[2] , Mykhaylo Melnyk[3] , Roman Vynarovych[4] , Ivan Popovych[5]

[1]Computer Aided Design Systems Department Lviv Polytechnic National University,
S. Bandery str. 12, Lviv, Ukraine, E-mail: yurii.l.hasiuk@lpnu.ua
[2] Computer Aided Design Systems Department Lviv Polytechnic National University,
S. Bandery str. 12, Lviv, Ukraine,, E-mail: andrianna.v.yovbak@lpnu.ua
[3] Computer Aided Design Systems Department Lviv Polytechnic National University,
S. Bandery str. 12, Lviv, Ukraine, E-mail: mykhaylo.r.melnyk@lpnu.ua, ORCID 0000-0002-8593-8799
[4] Computer Aided Design Systems Department Lviv Polytechnic National University,
S. Bandery str. 12, Lviv, Ukraine, E-mail: roman.i.vynarovych@lpnu.ua
[5] Computer Aided Design Systems Department Lviv Polytechnic National University,
S. Bandery str. 12, Lviv, Ukraine, E-mail: popovych.i.p@gmail.com

SECURITY PROBLEMS IN SMART HOME SYSTEMS

Recieved: September 12, 2023 / Revised: October 10, 2023 / Accepted: October 24, 2023

Abstract. This paper investigates the vulnerability of data transmission protocols used in smart home control systems, focusing on analyzing the communication protocols used in these systems. The spread of interconnected devices and the Internet of Things (IoT) has led to growing concerns about data privacy, unauthorized access, and potential cyberattacks. An in-depth analysis of various communication protocols used in the smart home environment was conducted, which allowed us to identify their advantages and disadvantages from a security perspective. Based on the analysis, recommendations are made for selecting communication protocols that meet the principles of security and confidentiality in the "Smart Home" environment.

Keywords: smart home systems, security, vulnerabilities, authentication, encryption, network