ВИДИ АТАК НА IOT SMART HOUSE

Куля Ю.Е., Квашенко В.Р.

V.V. Popovsky Departanent Infocommunication Engineering,
Kharkiv National University of Radio Electronics, Ukraine

E-mail: yuliia.kulia@nure.ua,
vladyslav.kvashenko@nure.ua

Abstract

Internet of Things is a rapidly evolving technology in which interconnected computing devices, sensors share data to detect and act accordingly to situation and deliver smart services like temperature monitoring, automatic light control, smart locks, smoke detection, etc. But it also opens the door to new set of security and privacy issues, such as personal and private data of users. In this paper, we discuss multilayer structure of IoT, and what security challenges faces each layer.

SmartHouse – це застосування середовища IoT, яке складається з фізичних компонентів і Інтернет складової. Ці пристрої обмінюються даними один з одним і надають інноваційні розумні послуги користувачам. Розумні обігрівачі, розумні холодильники, розумні телевізори, розумні годинники, мобільні пристрої та розумні замки – це розумна побутова техніка на основі Internet of Things, яка робить життя людини комфортнішим. За допомогою програмно-апаратного комплексу автоматизації Smart House ми можемо спостерігати та контролювати побутові прилади, освітлення, температуру в кімнаті, клімат у домі, двері та вікна.

Незважаючи на те, що розумні будинки зручніші у використанні та керуванні всією побутовою технікою, через підключення до Інтернету, а також динамічний розвиток IT інфраструктури, Smart House стикаються з різними проблемами безпеки. В середовищі Smart House, безліч розумних пристроїв взаємопов'язані та постійно обмінюються інформацією, архітектура середовища Internet of Things стала різносторонньою, і через цю різносторонність. ці пристрої вразливі до атак безпеки. ISO 27005 визначив атаку як незаконну діяльність, яку виконує зловмисник проти мережі та отримати доступ до мережі для внесення змін, які можуть призвести до втрати конфіденційних даних користувачів [1].

Зловмисник може спостерігати та збирати дані про різні дії користувача, за допомогою інформації, зібраної пристроями Smart House. Крім того, зловмисник може отримати контроль над пристроями Smart House віддалено і може використовувати пристрої для своїх цілей, завдаючи збитків власнику технології Smart House.

Ці атаки не тільки гіпотетичні, так, було виявлено, що у 2014 році більше 73,000 Smart House відеокамер транслювали відео з камер спостереження в Інтернет. Згідно з [2], майже 70% розумних пристроїв мають вразливості у захисті, також, дослідження показує, що 90% пристроїв збирали приватну інформацію користувачів на етапі тестування. Ці дані можуть бути використані зловмисником у своїх цілях, або як для атаки на скомпрометований пристрій.

Види атак на технологію Smart House

Можливість адаптації та розгортання технологій Internet of Things зростає з кожним днем, отже, все більше розумних пристроїв підключаються до мережі Інтернет. Як відомо, середовище Internet of Things складається з чотирьох рівнів: прикладний, фізичний, мережевий та сприйняття. Таким чином, для убезпечення розумного будинку потрібно розгорнути захист на кожному з рівнів.

Програма може бути зупинена, або використана не за призначенням у зв'язку з вразливістю в безпеці, як результат атаки прикладний рівень може створювати помилки. Найпопулярніші атаки на технологію Smart House на прикладному рівні наведені в таблиці 1.

Таблиця 1. Види атак на технологію Smart House на прикладному рівні [3, 4]

Вид атаки	Методики проведення атаки	Методи захисту
Фішинг атака	Візуальна схожість і збір даних про ціль	Дослідження та збагачення знань про технології фішингу
Переконфігурація з віддалених пристроїв	Доступ з віддалених мереж	Оновлення програми, зміна початкових паролів, відключення непотрібних функцій
Вламання до мережі Smart House	Криптосистема Рабіна	Квантовий розподіл ключів
Атака шкідливим кодом	Виявлення моменту для атаки на основі стану роботи пристрою	Виявлення шкідливого коду за відстеженням стану роботи пристрою

Хакери, націлені на рівень сприйняття, оскільки там знаходиться велика кількість програмних датчиків, які вони використовують вони використовують, щоб замінити програмне забезпечення пристрою своїм власним. Здебільшого загрози надходять від зовнішніх об'єктів. В таблиці 2 наведені найпопулярніші атаки на рівень сприйняття.

Таблиця 2. Види атак на технологію Smart House на рівень сприйняття [5]

Вид атаки	Методики проведення атаки	Методи захисту
Атаки підслуховування	Зчитування даних з датчиків	Екранування мережі IoT від мережі Інтернет
Атаки з побічного каналу	Атака на фізичні процеси пристрою	Фізичне екранування пристрою дає можливість знизити побічні канали витоку інформації
Booting attacks	Під час запуску пристрою, поки не запущені програми захисту, пристрій вразливий до атак	Програмована користувачем вентильна матриця
Зашумлення даних	Під час збору даних і процесу обробки в набір даних може бути введений шум, у результаті якого погіршується якість даних.	Автоматичне шумозаглушення ANR

Мережний рівень відповідає за обмін інформацією між пристроями. У результаті, на цьому рівні виникає великий обмін даними. Основними проблемами безпеки цього рівня є цілісність і автентифікація даних, якими обмінюються пристрої. В таблиці 3 наведені найпопулярніші атаки на мережний рівень.

Таблиця 3. Види атак на технологію Smart House на мережний рівень

Вид атаки	Методики проведення атаки	Методи захисту
DoS атака	Посилання великої кількості запитів до пристрою з метою викликання його нетипової роботи	Використання фреймворку IDS, фільтрування кількості запитів від одного пристрою
Неавторизований доступ	Автентифікація до системи в профіль з необмеженим рівнем доступу, підключення до пристроїв без паролю	Авторизація по ролях в мережі з відповідним рівнем доступу
Людина посередині	Використання незахищеного мережевого зв'язку для доступу до даних	Використання firewall або VPN, використання захищених каналів зв'язку. IDS IPS системи
Атака на шлюз мережі IoT	Атака на шлюз з метою унеможливити доступ пристроїв до мережі Інтернет	Використання фреймворку IDS, фільтрування кількості запитів від одного пристрою

Джерела живлення є основою розумних домашніх пристроїв. Таким чином потрібен механізм забезпечення безперебійної роботи під час відсутності електропостачання. На цьому рівні пристрої повинні бути захищені від погодних умов та впливу інших людей . В таблиці 4 наведені найпопулярніші атаки на фізичний рівень.

Таблиця 4. Види атак на технологію Smart House на фізичний рівень

Вид атаки	Методики проведення атаки	Методи захисту
Фізичне ушкодження	Нанесення фізичної шкоди пристрою	Встановлення решіток, захисних пристроїв
Погодні умови	Довгий контакт з різними типами природних факторів	Використання захищених пристроїв, або унеможливлювання контакту з природними чинниками
Втрата електроживлення	Відключення пристрою від електромережі	Встановлення автономних точок живлення або використання пристроїв з вбудованими резервними точками живлення
Копіювання пристрою	Створення повного клону пристрою і маніпулювання станом інших мережевих пристроїв	Захист від фізичної заміни пристрою

Висновки

Розумний дім — це нова програма IoT, у якій пристрої спілкуються та діляться конфіденційною інформацією. У такому середовищі кілька компонентів об’єднуються, щоб досягти налагодженої безперебійної роботи. Оскільки IoT є відносно новим на ринку, виробники пристроїв зазвичай віддають перевагу простоті пристрою аніж його безпеці. Виробники розумних пристроїв здебільшого зосереджуються на пристроях з меншим обчислювальним ресурсом і низьким енергоспоживанням, отже, не приділяючи потрібної уваги безпеці пристроїв. Оскільки IOT складається з безлічі пристроїв, коли ці численні пристрої підключаються, вони стикаються з різними проблемами безпеки та конфіденційності Ця робота показує багаторівневу структуру IoT досліджує можливі атаки на кожний з рівнів. Крім того наведені найрозповсюдженіші вирішення для розглянуних в роботі атак.

Література

1. ISO/IEC. ISO/IEC 27005:2018 [Електронний ресурс] / ISO/IEC. – 2018. – Режим доступу до ресурсу: https://www.iso.org/standard/75281.html.

2. 70 Percent of IoT Devices Vulnerable to Cyberattacks: HP [Електронний ресурс] – Режим доступу до ресурсу: https://www.securityweek.com/70-iot-devices-vulnerable-cyberattacks-hp.

3. Kaur M. Security in IoT-based smart grid through quantum key distribution. In: Advances in computer and computa-tional sciences [Електронний ресурс] / M. Kaur, S. Karla // 2018 – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-981-10-3773-3_51.

4. Wei D. Status-based detection of malicious code in internet of things (IoT) devices. In: 2018 IEEE Conference on Communications and Network Security [Електронний ресурс] / D. Wei, X. Qiu. – 2018. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8433183.

5. Study of secure boot with a fpga-based IoT device [Електронний ресурс] / Y.Liu, J. Briones, R. Zhou, N. Magotra. – 2017. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8053108.