Дослідження безпеки системи розумного будинку

Войтович О. П., Вишньовський В. В., Савченко К. В.
кафедра захисту інформації,
Вінницький національний технічний університет
Вінниця, Україна
e-mail: voytovych.olesya@vntu.edu.ua

Investegation of smart house security

Olesya Voitovych, Vladislav Vyshnovskyi, Kateryna Savchenko
Vinnytsia National Technical University
Vinnytsia, Ukraine
e-mail: voytovych.olesya@vntu.edu.ua

***Анотація* — Із стрімким розвитком інформаційного суспільства з'являються нові технології, які все більше інтегруються в життя людей та отримують доступ до величезної кількості інформації. Відповідно все гострішим постає питання забезпечення безпеки інформації у кіберпросторі. В даному дослідженні проведено аналіз літературних джерел, в результаті якого, було виділено вразливості технології Інтернет речей загалом, та розумного будинку. Крім того, запропоновано систему захисту розумного будинку й сформульовано рекомендації щодо покращення безпеки.**

Ключові слова— Інтернет речей, Розумний будинок, Система захисту, безпека, загрози, атаки, вразливості, протоколи.

***Abstract*— With the advent of the information society, new technologies are emerging that are increasingly integrated into people's lives and access to a huge amount of information. Accordingly, the issue of information security in cyberspace is becoming more acute. The author analyzes deferent sources in which the main concepts of one of the spheres of modern industry, namely the Internet of Things (IoT). Modern systems of "smart home", the system of home automation, the basic elements and systems of a reasonable house were considered. In addition, the main aspects of security of the system, the vulnerability of IoT technology in general are highlighted. It was found that a smart home system is based on three types of devices, namely: controllers (hubs), sensors (sensors) and actuators. These main devices include motion sensors, presence, vibration, glass breakdown, door opening (windows), video surveillance systems, video doorphones, electronic locks, sirens, and so on. Such elements base allows you to construct the necessary security system of varying complexity. The block diagram is based on the hardware and software platform Arduino, namely Arduino Uno (Robotdyn uno ch340 / atmega328pa) and Arduino Nano (V3.0 AVR Atmega328 P - 20AU) boards. To extend the functionality and features of the system, the following expansion schemes are used: Bluetooth HC - 06, RFID rc522, GSM SIM800L, motion detector HC - SR501, distance sensor HC - SR04 and two channel relay. The main feature of the proposed implementation is that due to remote control of the system and monitoring, a notification will be received about any penetration into the house. In addition, tips to improve the security of a smart house system are formulated.**

Keywords— Internet of Things, Smart house, system of protection, security, threats, attacks, vulnerabilities, protocols

I. ВСТУП

Поява Інтернету значно полегшила життя людини. З'явилася можливість миттєвого доступу до будь-якої інформації. На початку доступ до мережі був можливий лише за допомогою комп'ютерів, згодом смартфони надали можливість доступу до мобільного Інтернету. В даний час відбувається перехід до Інтернет речей (Internet of Things, IoT) [1]. Цей термін застосовується до пристроїв, які мають можливість доступу до мережі Інтернет, тобто сучасні автомобілі, побутові пристрої, фітнес-трекери тощо, якими можна керувати за допомогою смартфону або іншого пристрою [1] через віддалений доступ. IoT надає широкий спектр можливостей споживачам та організаціям різних галузей, наприклад: медицина, логістика тощо. Розумні об'єкти здатними бачити, чути, думати і виконувати роботу, обмінюючись інформацією та координуючи рішення. У зв'язку з популяризацією IoT, розробники отримують нові задачі з гарантування безпеки IoT-додатків, оскільки останні мають доступ до великої кількості конфіденційних даних та керуючих систем [2].

Яскравим прикладом технології IoT є розумний будинок – система, яка повністю аналізує та оптимізує процес управління житловим простором [1]. Важливим аспектом як IoT, так і розумного будинку є захист даних та каналів зв'язку.

IoT – це технологія, яка включає в себе мережу інтелектуальних механізмів, машин, електронних компонентів, програмного забезпечення, датчиків, які надають можливість підключення до мережі.

Таким чином IoT-пристрої та додатки мають доступ до конфіденційних даних і надають можливість управління через мережу [2]. Постає важливе питання забезпечення безпеки даних та каналів зв'язку. Отже IoT-додатки повинні відповідати ряду таких вимог, як [2]:

- запобігання зломів та компрометації даних;
- підтримка неперервного моніторингу;
- забезпечення стабільності.

Такий підхід зумовлений великою кількістю атак, що можуть бути реалізовані на технологію IoT [3]. Методологія оцінки ризиків повинна охоплювати питання забезпечення конфіденційності безпеки, унеможливлення шахрайських дій, кібератак та викрадання інтелектуальної власності. Ключовим моментом є те, що безпека пристрою повинна враховуватися на етапі проектування [4]. Сюди відноситься безпека в кінцевих вузлах і профілактичні заходи. Одним з можливих способів підвищення стійкості IoT і в тому числі розумного будинку є створення та використання стійкого до атак програмного та апаратного забезпечення.

II.Опис спроектованої системи

Для експериментального дослідження безпеки IoT було розроблено систему типу «Розумний будинок», яка об'єднує усі електроприлади в домі єдиним «розумом», що дозволяє керувати ними віддалено або з використанням пульта, як одним цілим і їх можна розділити на 5 підгруп: керуючі пристрої, керовані пристрої, датчики, шлюзи зв'язку та логічні пристрої.

Дозволяється виконувати керування простими електроприладами, наприклад: лампами, розетками, побутовими нагрівачами. Розумний дім буде виконувати керування просто вмикаючи або вимикаючи їх за допомогою реле, з більш складними приладами він впорається підключившись до їхнього "мозку".

До однієї з основних підсистем розумного будинку відносяться системи безпеки. Складовими системи безпеки є датчики руху, присутності, вібрації, розбиття скла, відкриття вікон або дверей, відеоспостереження, електронні замки (розумні замки), модулі керування воротами та сирени [5].

Різноманітні пристрої безпеки дозволяють сконструювати оптимальну систему безпеки, від порівняно простої до достатньо складної.

Система сигналізації є основною системою безпеки, професійні пристрої сигналізації дозволяють моментально відреагувати на вторгнення у будинок, при цьому спрацює звукова сирена, яка сповістить сусідів про вторгнення, а також система зробить сповіщення за допомогою дзвінка або СМС на телефон або в службу позавідомчої охорони.

Спроектована система (рис.1) містить в собі дві апаратно-програмні платформи Arduino Uno та Arduino Nano а також включає ряд модулів таких, як [6]:

- GSM-модуль;
- датчик руху;
- двоканальне реле;
- Bluetooth-модуль;
- RFID-модуль;
- датчик відстані;
- освітлення.

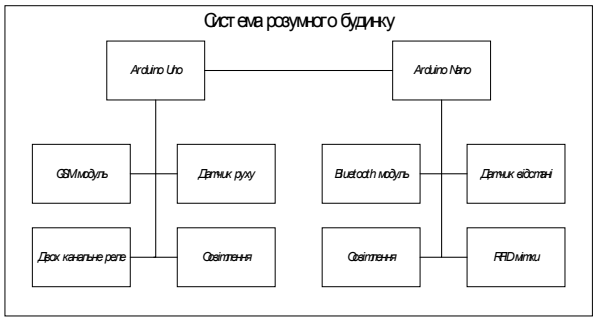

Рис. 1 – Структурна схема розумного будинку

Спроектована система повинна працювати таким чином: при запуску системи сигналізації розумного будинку, надається можливість отримання попередження про проникнення шляхом спрацювання всіх вище перерахованих датчиків, зокрема GSM-модуля. В свою чергу після спрацювання будь-якого з датчиків GSM-модуль зателефонує на вказаний номер або відправить повідомлення [7]. Також завдяки Bluetooth-модулю, надається можливість моніторингу системи з написаного мобільного додатку та віддаленого керування всією системою в цілому. При виявлені будь якого руху датчиком руху (HC-SR501), вмикається освітлення (двоканальне реле), а також Arduino Uno вмикає GSM модуль передавши власнику системи інформацію про проникнення. Модуль RFID з'єднується з Arduino Nano та дозволяє проводити автентифікацію в системі [8].

III.Атаки на складові системи

Пристрої, які отримують доступ до мережі Інтернет можуть захоплюватися в ботнети і використовуватися для розподілених атак, цим самим ускладнюючи відслідковування джерел атаки і полегшуючи «злам» пристроїв [11]. Наприклад атаки з використанням Simple Network Management Protocol (SNMP), як особлива форма DoS-атак, дозволяють зловмиснику отримати доступ до незахищених мережевих пристроїв (датчики, камери, роутери), які потім використовують як ботів для подальших атак.

За результатами дослідження "Доктор Web" [9] за минулий рік кількість шкідливого ПЗ для IoT

пристроїв стрімко зросла, серед такого шкідливого ПЗ можна виділити Linux.ProxyM.

Також не обійшлось без зламу RFID технології, основним методом з яких залишається і досі є підслуховування каналу зв'язку. Також при отриманні незаконного доступу до RFID, зловмисник може змінити дані, записати шкідливий код, виконати SQL ін'єкцію та переповнення буфера, дія яких дасть доступ до системи третім особам [10]. RFID-мітка може бути заражена вірусом, який потім вразить серверну базу даних, яка використовується програмним забезпеченням RFID [10].

За попередній рік покращилось програмне забезпечення, яке є спрямоване суто на злам Bluetooth. До таких програм можна віднести BlueZ. hciconfig, hcitool та hcidump. Основною їх метою є дослідження точки доступу, зібрати як найбільше інформації яка в подальшому знадобиться для зламу.

Також є можливість атаки «грубою силою» (метод повного перебору, brute force), яке може бути критичним.

Фізичні атаки можуть пошкоджувати, знищити чи викрасти апаратні складові системи захисту. Можуть застосовуватися як фізична сила, так і специфічні методи порушення цілісності, наприклад нагрівання [11].

IV. Пропозиції по підвищенню рівня захисту

Задля забезпечення безпеки необхідно притримуватись таких основних правил, а саме:

- забезпечення конфіденційності (дані та канали заявку повинні бути надійно зашифровані);
- забезпечення цілісності (дані гарантовано не повинні бути змінені третьою особою, а трафік повинен іти правильним шляхом);
- забезпечення доступності (дані та послуги будуть отримані за прийнятний час);
- забезпечення автентичності (надійна перевірка того, що дані отримані від правильного джерела);
- забезпечення неможливості відмови від виконаних дій (відслідковування подій в системі та логування).

Для захисту інформації, яка зберігається на пристроях та в момент її передачі, повинна використовуватися строга автентифікація, шифрування і безпечне управління ключами шифрування. Одним з можливих способів підвищення стійкості IoT і в тому числі розумного будинку є створення не тільки стійкого програмного забезпечення, а й перенесення частини цієї задачі на апаратне забезпечення.

Крім того, необхідно постійно проводити моніторинг появи нових вразливостей та оновлювати існуючу систему безпеки відповідно до результатів моніторингу. Оскільки найнадійніше на сьогоднішній день програмне забезпечення, в майбутньому може бути зламане.

Для забезпечення (гарантії) безпеки даних в RFID необхідно підтримувати три основні функції: захист переданих або збережених в пам'яті даних від несанкціонованого доступу, забезпечення цілісності даних та автентифікація тегів і рідерів при встановленні з'єднання [12]. Для захисту конфіденційності даних від пасивних і активних атак використовуються криптографічні процедури [12]. Незмінне число-ідентифікатор, що привласнюється мітці при виробництві, гарантує захист міток від підробки. Дані на мітці легко шифруються. Як цифровий пристрій, радіочастотна мітка при необхідності захищається паролем, і зашифровується. В одній мітці можна одночасно зберігати відкриті і закриті дані. Також є можливе екранування при розміщенні на металевих поверхнях.

Для захисту від DoS-атак потрібно забезпечувати ідентифікацію всіх пристроїв, які можуть бути доступними через свою мережу і є вразливими до зламу.

Для підвищення рівня захищеності даних, які циркулюють в GSM-мережах, можна застосовувати різноманітні механізми захисту. Один з таких методів використання PIN-коду, одного з найбільш простих методів автентифікації. Він дає дуже низький рівень захисту в умовах використання радіозв'язку.

Криптографічні методи дають можливість за допомогою відносно простих засобів домогтися високого рівня безпеки. Шифрування є досить ефективним для захисту конфіденційності в GSM, але не може використовуватися для захисту кожного окремо взятого обміну інформацією по радіоканалу.

Захистом від негласної активації мобільного телефону є акустичне зашумлення мікрофона, що дозволяє захистити мобільний телефон при виявленні факту його несанкціонованої активації.

Захист Bluetooth базується на трьох основних процесах: автентифікація, авторизація та шифрування [13]. Служба Bluetooth-шифрування має три режими: режим 1, в якому немає шифрування; режим 2, в якому шифрується зв'язок з пристроями, а трансляції трафіку немає; в режимі 3 шифруються всі види зв'язку. Основою, на якій базується безпека Bluetooth, є генерація ключів, яка виробляється на основі PIN-коду [13]. Сучасна Bluetooth-технологія не пропонує ніякого засобу автентифікації користувача, що робить Bluetooth-пристрої особливо уразливими до так званих spoofing атак та неправильного застосування розпізнавальних пристроїв. Особливо слабким

аспектом Bluetooth є процес «синхронізації» пристроїв, при якому відбувається обмін ключами в незакодованих каналах.

Також причиною вразливості є можливість використання коротких, слабких, а також поширених паролів. Такі паролі значно спрощують ініціалізацію. Саме це робить ключі зв'язку дуже простими для вилучення з перехоплених спарених передач.

Виділяють наступні методи захисту [13]:

- відключення discoverable-режиму;
- включення аутентифікації на основі PIN-ключів;
- антивірусне ПЗ;
- використання додаткового ПЗ (Blooover, Blooover II, BT Audit).

В даний час забезпечення безпеки відбувається, в основному, шляхом використання комплексного захисту.

V. Висновки

Таким чином було проаналізовано IoT, який надає широкий спектр можливостей споживачам та організаціям різних галузей, наприклад: медицина, логістика тощо. У зв'язку з популяризацією IoT, розробники отримують нові задачі з гарантування безпеки IoT-додатків, оскільки останні мають доступ до великої кількості конфіденційних даних.

Також розроблено систему захисту розумного будинку, яка базується на основі двох апаратно-програмних платформ: Arduino Uno та Arduino Nano. До скаладу системи також входять різного роду модулі, а саме: Bluetooth, RFID, GSM, датчики руху та відстані.

Виконано дослідження Інтернет речей, яке показало велику проблему в забезпечені безпеки. Яскравим прикладом технології IoT є розумний будинок – система, яка повністю аналізує та оптимізує процес управління житловим простором. Важливим аспектом як IoT, так і розумного будинку є захист даних. Так як практично, будь який пристрій може бути зламаний.

Рекомендовано в подальшій роботі використовувати складні паролі для Bluetooth. Для захисту інформації, яка зберігається на пристроях та в момент її передачі, використовувати строгу автентифікацію, шифрування і безпечне управління ключами шифрування. Одним з можливих способів підвищення стійкості Інтернет речей і в тому ж числі розумного будинку є створення не тільки стійкого програмного забезпечення, а й перенесення частини цієї задачі на апаратне забезпечення.

Для забезпечення безпеки даних в RFID, буде застосовано захист даних, які збережених в пам'яті від несанкціонованого доступу, а також забезпечення цілісності даних та автентифікація.

Література References

[1] Интернет вещей: как изменится вся наша жизнь на очередном этапе развития Сети. [Електронний ресурс]. – Режим доступу: URL http://www.cisco.com/c/ru_ru/about/press/press-releases/2011/062711d.html- Назва з екрану

[2] Защита IoT-устройств и шдюзов [Електронний ресурс]. – Режим доступу: URL https://www.ibm.com/developerworks/ru/library/iot-trs-secure-iot-solutions1/index.html– Назва з екрану

[3] Mouaatamid O., Lahmer M., Belkasmi M. Internet of Things Security: Layered classification of attacks and possible Countermeasures. Electronic Journal Of Information Technology, 2016, 9.

[4] Что такое интернет вещей (Internet of Things, IoT) [Електронний ресурс]. – Режим доступу: URL http://www.tadviser.ru/index.php/B9_(Internet_of_Things,_IoT)# – Назва з екрану

[5] Центральні елементи розумного будинку [Електронний ресурс]. – Режим доступу: URL http://sutem.com.ua/021%20inels.php-Назва з екрану

[6] Савченко К. В., Войтович О. П. Структурна схема системи захисту розумного будинку // Матеріали конференції XLVI Науково – технічна конференція факультету інформаційних технологій та комп'ютерної інженерії(2017) [Електронний ресурс]–Режим доступу: https://conferences.vntu.edu.ua/index.php/all – fitki/all – fitki – 2017/paper/view/2736 – Назва з екрану

[7] Вишньовський В. В., Войтович О. П. Структурна схема системи захисту розумного будинку // Матеріали конференції XLVI Науково – технічна конференція факультету інформаційних технологій та комп'ютерної інженерії(2017) [Електронний ресурс]–Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/view/2639/2009 – Назва з екрану

[8] Savchenko K., Vyshnovskiy V. System bezpieczeństwa inteligentnego domu // Materiały konferencyjne. 54. Konferencja studenckich kół naukowych Pionu Hutniczego [Електронний ресурс] – Режим доступу: http://www.kolanaukowe.agh.edu.pl/ph/dzialalnosc/sesje/54.%20Konferencja%20SKNPH%20 – %20zeszyt.pdf – Назва з екрану

[9] Интернет Вещей [Електронний ресурс]. – Режим доступу: URL https://www.anti-malware.ru/companies/drweb – Назва з екрану

[10] Проблемы и их решения в RFID технологии [Електронний ресурс]. – Режим доступу: URL http://www.itsec.ru/articles2/Inf_security/problemy-i-resheniya-rfid/– Назва з екрану

[11] Интернет вещей: особенности, проблемы и уязвимости [Електронний ресурс]. – Режим доступу: URL http://json.tv/tech_trend_find/internet-veschey-osobennosti-problemy-i-uyazvimosti-20160321115428– Назва з екрану

[12] Проблемы защиты информации в RFID – системах высокого уровня сложности, построенных на принципах EPCGLOBAL [Електронний ресурс]. – Режим доступу:_URL http://cyberleninka.ru/article/n/problemy – zaschity – informatsii – v – rfid – sistemah – vysokogo – urovnya – slozhnosti – postroennyh – na – printsipah – epcglobal – Назва з екрану

[13] Обзор безопасности протокола передачи данных Bluetooth [Електронний ресурс]. – Режим доступу:_URL http://cyberleninka.ru/article/n/obzor – bezopasnosti – protokola – peredachi – dannyh – Bluetooth – Назва з екрану