**Національний технічний університет України**

**«Київський політехнчний інститут імені Ігоря Сікорського»**

**Навчально-науковий інститут атомної та теплової енергетики**

**Кафедра цифрових технологій в енергетиці**

**ЗВІТ**

**з лабораторної роботи №3**

**з дисципліни «Основи технології Інтернету речей (ІоТ)»**

Виконав:

студент групи ТР-23

Ровний Г.О.

Дата здачі 4.11.2024

КИЇВ - 2024

Тема 3. «Дослідження особливостей функціонування «Розумного» будинку середовищі Cisco Packet Tracer»

**Мета роботи:**

ознайомити студентів з принципами функціонування систем «розумний» будинок, їх основними компонентами та технологіями, а також провести дослідження типів атак на IoT-пристрої, оцінити їх вплив на безпеку та працездатність системи.

**Частина 1**

**Поставлене завдання:**

1. Виконати дослідження системи «розумний» будинок.
2. Провзаємодіяти із системою «розумний» будинок.

**Результат виконання роботи**

**Крок 1. Аналіз пристроїв, що входять до складу «розумного» будинку.**

**Дати відповідь на запитання:**

1. Два коаксіальні кабелі залишають коаксіальний спліттер у відображеній топології. Які пристрої підключаються до коаксіального кабелю?

До коаксіального кабелю підключено лише два пристрої: телевізор (**TV**) та кабельний модем (**CableModem0**).

1. Кабельний модем - це інтерфейс між мережею Інтернет-провайдера та домашньою мережею. До яких пристроїв підключається кабельний модем?

У відображеній топології кабельний модем підключено до Домашнього шлюзу (**Home Gateway**) та до Коаксіального спріттера (розгалужувач) (**Coaxial Splitter**).

1. Які домашні пристрої, підключені до домашнього шлюзу?

До домашнього шлюзу підключено більшість пристроїв Розумного будинку:

Розумна сонячна панель (Smart Solar Panel), коаксіальний спріттер (Coax Splitter0), Кабельний модем (Cable Modem), Розумну батарею (Smart Battery), розумне вікно (Smart Window), Розумну лампу (Smart Lamp), Розумний вентилятор (Smart Fan), смартфон (Smartphone), Розумний будильник (Smart alarm), Планшет (Tablet), датчики руху, диму, температури та води, кавомашина (Smart Coffee Maker), а також Розумні двері (Smart door) та Двері гаража (Garage door).

**Крок 2. Взаємодія із системою «розумний» будинок.**

Натиснемо на планшет, що знаходиться в ліжку спальні.

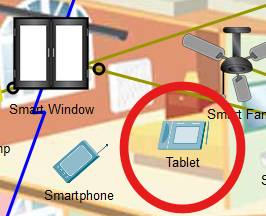


Рис. 1. Планшет в розумному будинку

Перейдемо до Робочого столу і далі – до веб-браузера. В адресному рядку зазначимо ІР адресу 192.168.25.1 (адреса домашнього шлюзу). А для входу домашній шлюз введемо admin/admin як ім’я користувача та пароль.

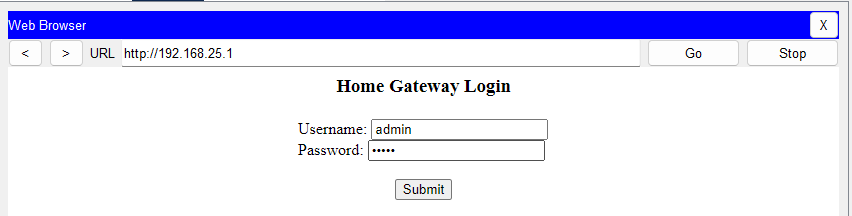


Рис. 2. Вхід в домашній шлюз

В результаті бачимо всі пристрої які підключені до домашнього шлюзу:

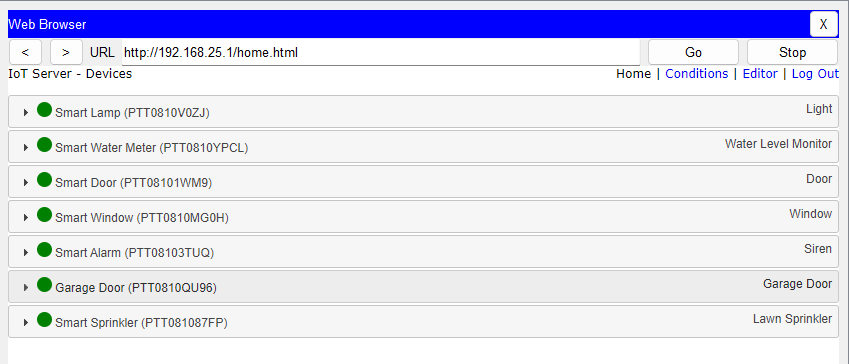


Рис. 3. Список підключених пристроїв до домашнього шлюзу

Наразі «розумні» двері відчинені (зелене світло на ручці дверей), але спробуємо заблокувати їх віддалено. Для цього натиснемо на іконку «розумних» дверей в браузері, щоб розгорнути цю опцію. Та написнемо Lock для їх блокування. На це вказує червоне світло на ручці дверей.

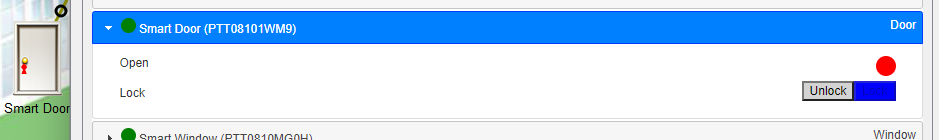


Рис. 4. Віддалене блокування дверей

Натиснемо на детектор диму в браузері. Можемо спостерігати нульовий рівень диму (оскільки його зараз немає). Але датчик диму ніяк не можна контролювати, окрім фізичної взаємодії. Лише моніторити показники.

**Крок 3. Туманні обчислення в «розумному» будинку.**

Запуск автомобіля

Сценарієм передбачено розміщення автомобіля в гаражі. В загальному випадку, автомобіль виробляє монооксид вуглецю, який підвищує рівень диму в приміщенні.

Знову перейдемо до налаштувань домашнього шлюзу через планшет. Відкриємо вікно датчику диму, яке залишимо відкритим, а також запустимо двигун автомобіля клацнувши за допомогою клавіші ALT по ньому.

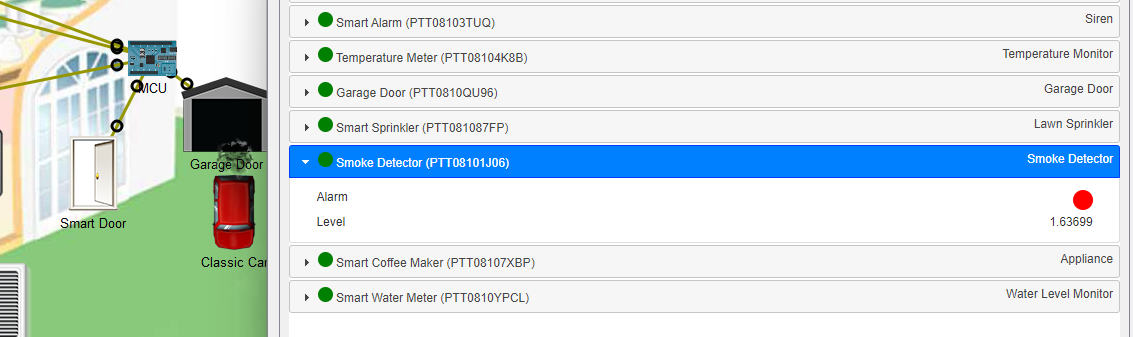


Рис. 5. Реагування датчика диму на дим в гаражі

Можемо спостерігати що після того, як датчик диму завіксував високий вміст вуглецю, автоматично спрауювала система яка відкрила розумні двері і запустила систему вентиляції а також відкрила вікно, що дозволило знизити показники диму в будинку. Після того, як двигун вимикається, датчик диму перестеє фіксувати шкідливі викиди газу, і до MCU подається сигнал про необхідність закриття дверей, вікон та зупинки системи вентиляції всередині будинку.

**Частина 2.**

**Поставлене завдання:**

1. Дослідити найпоширеніші типи атак на IoT.
2. Дослідити методи, засоби чи механізми захисту від атак на ІоТ.

**Результат виконання роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| Назва та тип атаки | IoT-Dyn | Mirai | Kaiten |
| Час, коли відбулася атака, кількість  постраждалих пристроїв | 21 жовтня 2016 рік | 2016 | 2001 |
| Вектор атаки (на що було здійснено  вплив/на що вплинула атака) | відбулася масова атака типу DDoS на компанію Dyn, яка обслуговує значну частину інфраструктури DNS (Domain Name System) Інтернету. | Ботнет, утворений зламаними (скомпрометованими) пристроями типу «інтернет речей» (відеопрогравачі, «розумні» вебкамери, тощо). Всього шкідливе ПЗ мало відомості про 61 різних комбінацій логін-пароль для отримання доступу до облікового запису методом перебору[3]. Дослідження показали, що значна частина вразливих пристроїв була виготовлена з використанням складових виробництва фірми XiongMai Technologies з офісом в Ханчжоу | шкідливе програмне забезпечення, яке функціонує як троянський кінь. Воно відкриває “чорний хід” на зараженому комп’ютері, дозволяючи зловмисникам виконувати інші шкідливі дії1. Kaiten не створює копій самого себе, а потрапляє на систему як файл, завантажений іншими шкідливими програмами або користувачами, які відвідують шкідливі сайти |
| Наслідки для системи | Вважається, що ця діяльність використовувала ботнет координовану через велику кількість пристроїв під'єднаних до інтернету — таких як принтери, камери, які були інфіковані Mirai. З оціненим навантаженням в 1,2 Тбіт/с, згідно з експертною думкою, атака стала найбільшою із зафіксованих | На початку листопада 2016 року створений на основі Mirai ботнет (Botnet 14) розпочав DDoS-атаку проти Ліберії. Країна отримувала доступ до Інтернету завдяки єдиному оптоволоконному каналу ACE, прокладеному в 2011 році. Даний канал надає зв'язок для всього західного узбережжя Африки та має пропускну здатність до 5.1 ТБ/c. Нападникам вдалось тимчасово розірвати доступ цілої країни до Інтернету.  В жовтні 17 року інженери компанії Check Point оприлюднили доповідь про виявленого ними хробака, що атакує пристрої класу «інтернет речей» та утворює на їх основі ботнет. Новий хробак отримав назву IoTroop або Reaper. На відміну від Mirai, новий хробак покладається на щонайменше 9 відомих вразливостей у пристроях різних виробників. За оцінкою дослідників, новий хробак вразив пристрої у понад 1 млн організацій по всьому світу | Kaiten націлювався на невеликі системи та досить часто використовувався локально для ураження невеликих систем. |

Таблиця 1. Дослідження атак і загроз для ІоТ

|  |  |  |  |
| --- | --- | --- | --- |
| Назва інструменту/ розробник: | Microsoft Azure IoT Hub | AES (Advanced Encryption Standard) | ‘Шифрування TLS (Transport Layer Security) |
| Алгоритм використання (опис роботи  інструменту): | хмарна служба, яка забезпечує безпечне та масштабоване двостороннє спілкування між IoT-пристроями та хмарними рішеннями. Іншими словами це як центральний хаб, де мільйони пристроїв можуть підключатися, надсилати дані та отримувати команди. | симетричний блоковий шифр, що означає, що для шифрування та дешифрування даних використовується один і той же ключ. Він працює над блоками даних фіксованого розміру (128 біт) і використовує ключі різної довжини (128, 192 або 256 біт). Процес шифрування складається з кількох раундів, під час яких дані піддаються різним трансформаціям, включаючи підстановки, перестановки та змішування з ключем. Чим довший ключ, тим більше раундів і тим вища стійкість до злому. | TLS забезпечує захищений канал зв’язку між пристроями шляхом шифрування даних, що передаються. Це досягається за допомогою симетричного шифрування для конфіденційності даних і асиметричного шифрування для обміну ключами. |
| Основні характеристики та можливості  (включно з ефективністю захисту): | 1. Обслуговує мільйони пристроїв.  Забезпечує безпечний зв'язок між пристроями та хмарою.  2. Підтримує різні протоколи (MQTT, AMQP, HTTP) та ОС.  3. Дозволяє віддалено керувати пристроями, оновлювати програмне забезпечення та отримувати діагностичні дані.  4. Легко інтегрується з іншими службами Azure, такими як Azure Stream Analytics, Azure Machine Learning та Azure Cosmos DB. | 1. Ефективно дозволяє шифрувати великі обсяги даних.  2 Відносно проста реалізація  3. Сумісність із протоколами HTTPS та SSH  4. AES використовують у багатьох додатках, включаючи бездротові (Wi-Fi, Bluetooth), банківські системи, email, жорсткі диски.  5. Пропонує три рівні безпеки в залежності від довжини ключа (128, 192, 256) | 1. Аутентифікація  2. Цілісність  3.Конфіденційність |

Таблиця 2. Дослідження методів (засобів чи механізмів) захисту від атак на ІоТ

**Висновок:**

У результаті виконання лабораторної роботи було опрацьовано та на практиці закріплено основні функціональні можливості системи розумного будинку. На основі побудованої топології smart home було досліджено взаємодію між різними так званими розумними пристроями які скаладють систему розумного будинку. А також було вивчено найпоширеніші типи атак на IoT системи та деякі способи протидії їм.