



SECTION: COMPUTER TECHNOLOGY.

SEKCJA: TECHNOLOGIA KOMPUTEROWA.

How to cite: Skopen, M., & Budya, O. (2024). Strengthening the Security of Wireless Surveillance System Networks. *Horizons of Innovation: Conference on Multidisciplinary Trends in Science 2024*. (pp. 76-81). Futurity Research Publishing. <https://futuraity-publishing.com/horizons-of-innovation-conference-on-multidisciplinary-trends-in-science-2024-2/>

Strengthening the Security of Wireless Surveillance System Networks

Микола Скопень¹, Олександр Будя²

¹кандидат економічних наук, доцент, викладач-методист кафедри загальнотеоретичної та прикладної підготовки Київського фахового коледжу туризму та готельного господарства, Україна, м. Київ, Україна

²кандидат технічних наук доцент, викладач-методист кафедри загальнотеоретичної та прикладної підготовки Київського фахового коледжу туризму та готельного господарства, м. Київ, Україна

Accepted: January 17, 2024 | **Published:** February 4, 2024 | **Language:** Ukrainian

Abstract: This study explores the enhancement of the security of a wireless network for a home surveillance system through the use of MCU (Microcontroller Unit) devices and Meraki within the Cisco Packet Tracer 8.2.1 network emulation system platform. The microcontroller facilitates the integration of actuators (e.g., LEDs) into the wireless network and controls them upon the activation of the surveillance system. The Meraki server and the Meraki-MX65W Security Appliance improve the security of wireless networks by refining their architecture and enabling remote administration

via cloud technologies. The technology presented is recommended for inclusion in educational processes, as well as for the simulation-based control of IoT (Internet of Things) devices during the design phase.

Keywords: Wireless networks, security enhancement, IoT device management, MCU and Meraki device interaction, surveillance systems.

Вступ

У літературних джерелах достатньо добре розглянуто принципи організації, побудови та захисту мереж (Жураковський & Зенів, 2020), налаштування мікроконтролера MCU (Скопєнь, Любима, 2022) та технологію використання пристроїв Meraki у бездротових мереж (Скопєнь, Будя, 2023). Втім, не розкрито, яким чином можна налаштувати взаємодію мікроконтролера MCU та пристроїв Meraki при посиленні безпеки бездротової мережі. В даному випадку мікроконтролер виконує функцію керування LED при спрацюванні системи спостереження, а пристрої Meraki виконують функції централізованого контролю за доступом до мережі та налаштування технології шифрування даних. Саме це і пропонується авторами нижче для розгляду.

Результати дослідження

Розглянемо необхідність посилення безпеки бездротової мережі системи відеоспостереження, яка моніторить територію навколо приватного будинку, з використанням платформи мікроконтролера UMC та обладнання Meraki. Визначено послідовність дій, яка включає наступні етапи: моделювання та налаштування топології мережі; конфігурація роутера для підключення безпекового пристрою Meraki-MX65W до сервера Meraki; налаштування параметрів безпекового пристрою Meraki-MX65W; встановлення через хмарний сервер Meraki бездротового зв'язку між користувачами та шифрування передаваних даних; програмування мікроконтролера MCU; інтеграція пристроїв IoT та розробка програмної логіки реагування сирени та світлодіодів на детектування руху.

Моделювання та конфігурування топології системи спостереження

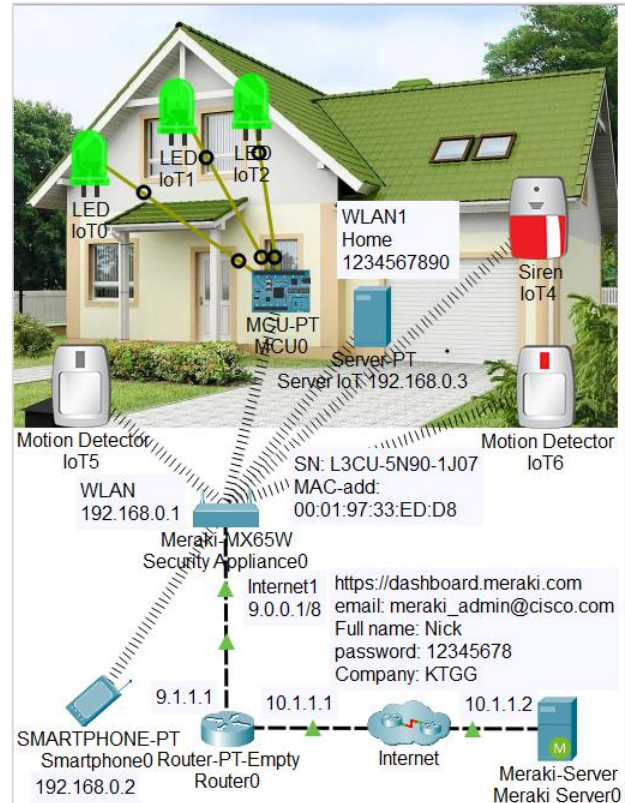
здійснюється на платформі системи Cisco Packet Tracer 8.2.1, яка регламентує вибір типу Meraki – сервера та пристрою безпеки Meraki-MX65W [Рисунок 1]. Встановлюються пристрої, а саме: Meraki – сервер з картою PT-HOST-NM-1CGE (DNS Server – 10.1.1.2); роутер з двома мережевими картами PT-ROUTER-NM-1CGE; пристрій безпеки Meraki-MX65W (встановити POWER-ADAPTER); смартфон (IP-адреса 192.168.0.2 від Meraki-MX65W); сервер IoT з мережевою картою WMP300N (IP-адреса 192.168.0.3 від Meraki-MX65W); пристрої IoT Siren, Motion Detector, MCU, LED. Роутер підключається до порту Internet1 Meraki-MX65W, а на сервері IoT (вкладка Services) вмикається режим IoT і створюється аккаунт (вкладка Desktop). Для цього у вікно Web Browser вводиться 192.168.0.3 і натискається Sign up now. Далі здійснюється введення у вікно Registration Server Account Creation: admin, admin і натискання кнопки Create.

Налаштування роутера. Здійснюється встановлення IP-адреси порту *Internet1* *i-MX65W* – 9.0.0.1. В даному випадку пристрої будуть мати зв'язок з Meraki – сервером. Їхньою метою треба на вкладці роутера *CLI* ввести програмний код [Рисунок 2].

Для налаштування параметрів **Security Appliance Meraki-MX65W** треба увімкнути на смартфоні режим *DHCP* для власного конфігурування (*IP-адреса* – 192.168.0.2 та ін.). Копіюється у *Meraki-MX65W* на вкладці *Config* серійний номер пристрою (*A28D-W3NA-NRG1*). Далі на смартфоні у вікно *Web Browser* вводиться IP-адреса 192.168.0.1, а у поле *User Name* вставляється серійний номер. При відкритті пристрою на вкладці *Connection* копіюється MAC-адреса пристрою для подальшої реєстрації на Meraki – сервері (*Hardware address* 00:01:97:33:ED:D8), а на вкладці *Configure* для Internet1 вибирається у списку режим: *IP assignment – DHCP* та натискається нижче кнопка *Save*.

Рисунок 1

Топологія системи спостереження на платформі мікроконтролеру UMC та пристроїв Meraki



Джерело: власна розробка авторів

Рисунок 2

Програмний код увімкнення служби
DHCP

```
Router(config)#ip dhcp pool Nick
Router(dhcp-config)#network 9.0.0.0 255.0.0.0
Router(dhcp-config)#default-router 9.1.1.1
Router(dhcp-config)#dns-server 10.1.1.2
```

Для **налаштування через хмарний сервер Meraki бездротового зв'язку користувачів та шифрування даних** у вікні *Web Browser* смартфона вводиться <https://dashboard.meraki.com>, а при відкритті сервера, натискається *Create an account* для реєстрації. При цьому і діалогове вікно вводяться наступні параметри: *Email*: meraki_admin@cisco.com; *Full name*: Nick; *Password*: 12345678; *Confirm Password*: 12345678; *Company*: KTGG. Натискається кнопка *Create Account*. Далі з метою створення мережі WLAN1 та реєстрації пристрою безпеки натискається вгорі посилання *here (mym)* і ліворуч - *Create a network*. У поле *Network name* вводиться WLAN1 і натискається кнопка *Create network*. Нижче у відповідні поля вводяться параметри реєстрації пристрою безпеки (серійний номер, MAC-адреса, назва мережі) та натискається кнопка *Add devices*. За посиланням *Security Appliance/ Wireless Setting* здійснюється шифрування доступу вузлів до WLAN1, тобто встановлення параметрів: *Status* – *Enabled*, *SSID Name* – *Home*, *Security* – *WPA2-PSK*, *WPA Key* – 1234567890, *WPA encryption mode* – *WPA2 only*. Натискається кнопка *Save Changes*. Після цього можна до WLAN1 підключати пристрої.

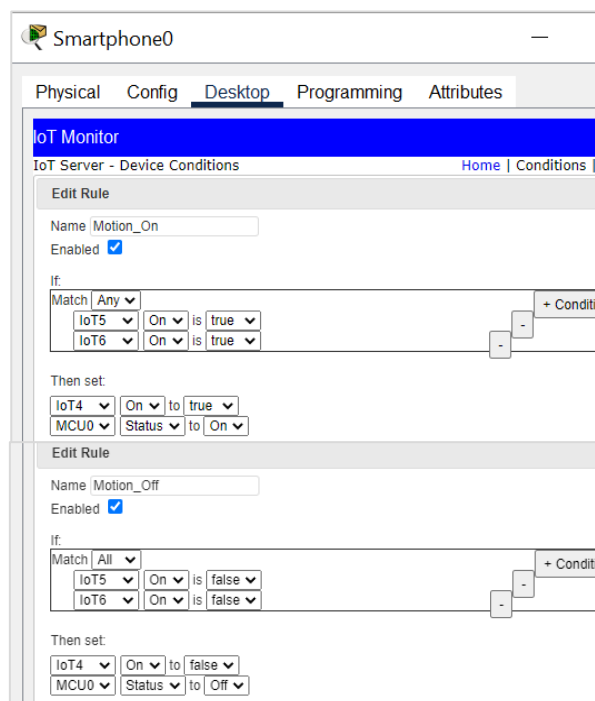
Для **налаштування та програмування мікроконтролера MCU** на вкладці *Physical* вимикається живлення і вставляється плата PT-IOT-NM-1W-AC, а на вкладці *Config/ Wireless* (при відновленні живлення) встановлюється: *SSID* – *Home*, перемикач - *WPA2-PSK*. У поле *PSK Pass Phrase* вводиться ключ: 1234567890. На вкладці *Config/Setting* встановлюється перемикач *Remote Server*, *Server Address* – 192.168.0.3, *User Name* – admin і *Password* – admin. При натисканні кнопки *Connect* мікроконтролер MCU буде зареєстрований на сервері IoT. Здійснення керування LED мікроконтролером MCU вимагає підготовки відповідної програми. Для цього на вкладці *Programming* натискається кнопка *New* і вводиться ім'я *MotionSensor*. У полі зі списком вид програми повинен бути *Empty* – *JavaScript*. Натискається кнопка *Create*. Далі треба клацнути курсором на *main.js* і ввести наступні рядки програми [Рисунок 3]. Здійснити запуск програми кнопкою *Run*. Смартфон в режимі *IoT Monitor* повинен показувати стан LED.

Підключення пристроїв IoT та програмування реакції Siren та LED на рух. Для цього на кожному пристрою IoT активізується вкладка *Config/ Wireless0* і у поле *SSID* вводиться: *Home*. Встановлюється перемикач *WPA2-PSK* і у вікно *PSK Pass Phrase* вводиться ключ шифрування 1234567890. На вкладці *Config/Setting* встановлюється перемикач *Remote Server*, *Server Address* – 192.168.0.3, *User Name* – admin і *Password* – admin. Натискається

кнопка *Connect* (при успішній реєстрації на сервері перетворюється на *Refresh*). В даному випадку відповідний пристрій буде підключено до *Meraki-MX65W* та отримає в режимі *DHCP* IP-адресу, а також буде зареєстрований на сервері *IoT*. Для програмування реакції пристроїв *Siren* та *LED* на рух активізується на смартфоні режим *IoT Monitor* та вкладка *Conditions*, натискається кнопка *Add* і формуються два програмних модулі *Motion_On* та *Motion_Off* [Рисунок 4].

Рисунок 4

Програмування реакції Siren та LED на спрацювання Motion Detector



Джерело: власна розробка авторів

Трасер версії 8.2.1. Незважаючи на зазначені обмеження, розроблену методику можна рекомендувати для застосування у навчальних процесах, а також для моделювання бездротових мереж на етапі їх проектування. Також, запропонована технологія відкриває перспективи для подальших досліджень у сфері забезпечення безпеки мережевих комплексів за допомогою обладнання Meraki.

Список використаних джерел:

Жураковський, Б.Ю., & Зенів І.О.(2020) *Комп'ютерні мережі. Частина 1: навч. посіб. для студ. спеціальності 121 "Інженерія програмного забезпечення" та 126 "Інформаційні системи та технології", спеціалізації "Інженерія програмного забезпечення інформаційно*

Рисунок 3

Програма взаємодії сервера IoT та мікроконтролера при керуванні LED (Скопень, Любима, 2022)

```
var state = "0";
function setup() {
  IoEClient.setup({ // Реєстрація на IoT&RADIUS сервері
    type: "LED",
    states: [{
      name: "Status",
      type: "options",
      options: {
        "0": "Off",
        "1": "On"
      }
    }],
    controllable: true
  });
  IoEClient.onInputReceive = function(input) { // Реакція на зміну стану
    setState(input);
  };
  setState(state);
}
function setState(newState) { // Відпрацювання зміни стану
  var stateValue = 0;
  if (newState === "1") {
    stateValue = 1023;
    state = "1";
  } else if (newState === "0") {
    state = "0";
    stateValue = 0;
  } else {
    return;
  }
  digitalWrite(A0, stateValue);
  digitalWrite(A1, stateValue);
  digitalWrite(A2, stateValue);
  IoEClient.reportStates(state);
  setDeviceProperty(getName(), "state", state);
}
```

Висновки

Отже, запропонована методика підвищення безпеки бездротових мереж систем відеоспостереження, яка базується на використанні платформи MCU та обладнання Meraki, сприяє вдосконаленню якості освітнього процесу в галузі Інтернету речей. Варто зазначити, що обсяг цього дослідження був обмежений можливостями обладнання безпеки, доступного в системі Cisco Packet

управляющих систем" та "Інформаційне забезпечення робототехнічних систем". Київ: КПІ ім. Ігоря Сікорського.

Скопень, М., & Любима, А. (2022). Моделювання топології мережі взаємодії radius-сервера та мікроконтролера mcu при керуванні пристроями інтернету речей. *InterConf : with the Proceedings of the 6th International Scientific and Practical Conference "Scientific Community: Interdisciplinary Research"* (January 26-28, 2022) (p.1074-1081), Hamburg, Busse Verlag GmbH, 96. <https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/18311>

Скопень М.М., & Будя О.П. (2023). Посилення безпеки локальної мережі IoT з використанням пристроїв Meraki. *Економічний розвиток держави та регіонів в контексті сучасних інтеграційних процесів: Матеріали доповідей міжнародної науково-практичної конференції* (19-20 травня 2023 р. м. Ужгород) (с. 119-122). Львів-Торунь : Liha-Pres. <http://surl.li/hpikd>.