КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2021.13.2938
УДК 004.056.53

**Крівенко Сергій Вікторович**
д.т.н., доцент кафедри системного аналізу та інформаційних технологій
Маріупольський державний університет, м. Маріуполь, Україна
ORCID ID: 0000-0002-0319-7174
s.krivenko@mdu.in.ua

**Ротаньова Наталія Юріївна**
к.пед.н., доцент кафедри системного аналізу та інформаційних технологій
Маріупольський державний університет, м. Маріуполь, Україна
ORCID ID: 0000-0001-8437-7566
rotanevan@gmail.com

**Лазаревська Юліанна Артурівна**
асистент кафедри системного аналізу та інформаційних технологій
Маріупольський державний університет, м. Маріуполь, Україна
ORCID ID: 0000-0001-8318-5861
lazarevskayulianna@gmail.com

**Карпенко Уляна Олександрівна**
здобувач вищої освіти ОС «Бакалавр» ОП Кібербезпека
Маріупольський державний університет, м. Маріуполь, Україна
ORCID ID: 0000-0002-8634-0457
kulana131@gmail.com

# ДОСЛІДЖЕННЯ СИСТЕМИ НА УРАЗЛИВІСТЬ ДО MITM - АТАКИ ЗА ДОПОМОГОЮ СТВОРЕННЯ FAKE AP

**Анотація.** Проблеми кібербезпеки стають щоденною загрозою для бізнеса та користувачів Інтернету. Сфера кібербезпеки постійно змінюється, але очевидно, що кіберзагрози стають все більш серйозними і відбуваються все частіше. Статистичні дані про кількість здійснених кібератак за результатом 2020 року показав різкий сплеск кіберзлочинності. Останнім часом в галузі інформаційної безпеки переважна кількість інцидентів пов'язана в атаками на різні розподілені інформаційні системи. При цьому значну кількість успішних атак складають атаки, проведені за допомогою атак типу «Man in the middle» (MITM). MITM – атаки небезпечні тим, що за їх допомогою зловмисники отримують доступ до конфіденційної інформації, не тільки компаній але і звичайних користувачів. Тому метою цієї статті є дослідження видів MITM – атак, а також розробка рекомендації щодо протидії такими видам атак. Дослідження проведено з використанням методів аналізу та опису. Об'єктом дослідження є MITM-атаки. Предметом дослідження є визначення способів протидії атакам типу MITM. В результаті проведеного дослідження розглянуто основні типи та описано методику проведення MITM – атак. Результатом проведеного дослідження стала розробка рекомендації для протидії MITM – атакам. Запропоновані методи попередження атак «Людина посередині» можуть забезпечити високий рівень безпеки комп'ютерної мережі. Дане дослідження буде корисно запропонованими способами запобігання здійснення MITM – атак, не тільки для адміністраторів безпеки, а також користувачам мережі Wi-Fi, які намагаються захистити свої персональні данні. Також результати дослідження можуть бути використані для розробки більш досконалого програмного забезпечення, яке може підвищити рівень безпеки комп'ютерної мережі.

**Ключові слова:** кібератака; MITM-атака; точка доступу; Fake AP; SSL; WPA; SSID; попередження MITM-атак.

## ВСТУП

У сучасному світі широкого поширення набули Wi-Fi мережі. Сьогодні їх можна зустріти практично скрізь, будь то магазин, кафе, кінотеатр і т.д. І люди активно використовують можливість безкоштовного і доступного Інтернету. Це дійсно дуже зручно, проте існує висока ймовірність піддатися атакам хакерів.

Особливістю Wi-Fi мереж є те, що це відкрита, громадська мережа. Саме тому, вона найчастіше буде схильна до атаки «перехоплення сеансу». Будь-яка атака, яка включає використання сеансу між пристроями, є перехопленням сеансу. Коли ми розмірковуємо про сеанс, ми говоримо про з'єднання між пристроями, стан якого можна вважати задовільним. Тобто мова йде про ситуацію, де є організований діалог, в якому формально встановлено з'єднання, воно підтримується, і для його завершення повинен використовуватися певний процес [1].

Однією з типів атак «перехоплення сеансу» є атака «людина посередині» або «Man in the middle» (MITM). MITM - атаки це вид криптографічної атаки, де зловмисник перехоплює і підміняє повідомлення, якими обмінюються користувачі мережі [1]. Такий вид атаки є практично повністю прозорою для користувачів, оскільки жоден з них здогадується про присутність третього користувача між ними.

Найбільш схильні до MITM є атакам Wi-Fi мережі. Люди не замислюючись підключаються до мереж, які не захищені паролем, в той час як зловмиснику досить просто розгорнути Fake AP, не обтяжуючи себе примусовим відключенням клієнта від оригінальної мережі. Незважаючи на те, що цільові ОС з моменту появи MITM - атаки вже сотні разів оновилися і системи стали захищеними, ця атака жива і становить загрозу для користувачів. І, на жаль, не доводиться очікувати того, що найближчим часом стандарт буде виправлений або дописаний.

**Постановка проблеми.** MITM – атаки продовжують бути популярними вже багато років, за рахунок того, що засновані не на слабких місцях програмного забезпечення точок доступу або клієнтів, а на особливостях повсюдно використовуваного стандарту 802.11, а точніше, на особливостях роботи його протоколу аутентифікації. Хоча стандарт і визначає, як користувач приєднується до точки доступу, спосіб вибору цієї точки не визначений, немає згадки про те, чи повинна базова станція проходити перевірку автентичності або вона довірена за замовчуванням. Вирішення цієї проблеми було залишено на розсуд постачальників обладнання та програмного забезпечення операційної системи.

З часом кількість способів реалізації MITM - атак збільшилася. Так, наприклад, атаки на сайти з протоколом HTTP вдосконалили до атак на сайти з протоколом HTTPS шляхом підміни сертифікатів і обходу HSTS. Атака зі створенням Rogue AP переросла в Ewil Twin. І навіть не дивлячись на захист від підміни сертифікатів з боку браузерів, такі атаки досі дієві, оскільки можна обійти і цей захист.

**Аналіз останніх досліджень і публікацій.**

Аналіз досліджень зарубіжних вчених, що займаються питанням вивченняматак «людина посередині» показав, що найчастіше в них розглядаються методи і схеми виявлення MITM-атак. Так, в роботі В. Валліваара, М. Сайліо та К. Халунен [2, с 131-133] був запропонований метод виявлення MITM - атак з використанням тимчасових відміток заголовків пакетів TCP. У дослідженні Д. Ал-Абрі [3, с 1857-1862] представлена схема виявлення, яка зосереджена на виявленні MITM незалежно від схеми, що використовується для переадресації трафіку. Дослідження таких авторів, як А. Маллік, А. Ахсан та Дж.-Ч. Цу [4, с 77-92] носить лише ознайомчий характер і розкриває питання

самого терміна атаки «людина посередині». В працях [5-9] мова іде про методи протидії мережевому скануванню: від реалізації прихованих каналів дослідження до використання підходу до ідентифікації аномалій а також налаштування мережевого обладнання для запобігання неавторизованого проникнення. Отже, проблеми уразливості до MITM – атаки потребують подальшого вирішення і є актуальними.

**Мета статті.** Використання зловмисниками MITM-атак краде конфіденційні данні, що завдає великі збитки компаніям, їх клієнтам та простим користувачам**.** Отже, метою дослідження є демонстрація уразливості WI-FI з'єднання, щодо атак MITM та аналіз видів атаки «Людина посередині», а також розробка рекомендації щодо протидії MITM-атакам.

## ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Основними точками взаємодії у Інтернет-мережі є клієнти, маршрутизатори, сервери. Найбільш поширений протокол взаємодії між клієнтом і сервером - Hypertext Transfer Protocol (HTTP). Серфінг в Інтернеті здійснюється через HTTP за допомогою браузера, електронної пошти, обміну миттєвими повідомленнями. При введені адресу веб-сторінки в адресному рядку браузера користувачам відправляється запит на відображення веб-сторінки сервера. Пакет (HTTP GET-запит) передається через кілька маршрутизаторів на сервер. Після цього сервер відповідає веб-сторінкою, яка відправляється клієнту і відображається на його моніторі. HTTP-повідомлення повинні передаватися в безпечному режимі, щоб забезпечити конфіденційність і анонімність.

Щоб протокол зв'язку був безпечними, він мусить мати кожне з наступних властивостей [10]:

- Конфіденційність - тільки передбачуваний одержувач може прочитати повідомлення.
- Автентичність - особистість взаємодіючих сторін доведена.
- Цілісність - підтвердження того, що повідомлення не було змінено в дорозі.

Зауважимо, що коли одне з цих правил не дотримано, весь протокол є скомпрометованими.

Для запобігання атак, які використовують недосконаліть APR, була створена захищена версія протоколу HTTP. Transport Layer Security (TLS) і його попередник, Secure Socket Layer (SSL) формує криптографічні протоколи, які забезпечують безпеку передачі даних по мережі. Отже, захищений протокол буде називатися HTTPS [10].

З розвитком інформаційних технологій MITM - атаки удосконалювалися, знаходячи нові способи реалізації в залежності від атакованих об'єктів (сайти, локальні мережі і обладнання), загальною метою яких є моніторинг і зміна вихідного трафіку, тому доцільним є розгляд питання щодо основних атак.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

*Атаки, засновані на вразливості ARP*

Значна деформація протоколу дозволу адрес (Address Resolution Protocol, ARP) - включає відправку підроблених повідомлень ARP по локальній мережі. Це також відомо, як підміна ARP, деформація (отруєння) ARP-маршрутизації і деформація (отруєння) кеша ARP.

Такі атаки намагаються перенаправити трафік зловмисникові замість спочатку наміченого хоста. Отруєння ARP робить це, пов'язуючи адресу управління доступом до середовища (Media Access Control, MAC) зловмисника з IP-адресою мети. Даний принцип працює тільки проти мереж, що використовують ARP.

Отруєння ARP є це різновидом атаки типу Man-in-the-Middle, яку можна використовувати для зупинки мережевого трафіку, його зміни або перехоплення. Метод часто використовується для ініціювання подальших атак, таких як захоплення сеансу або відмову в обслуговуванні.

ARP - це протокол, який пов'язує цей IP-адреса з адресою канального рівня відповідної фізичної машини. Оскільки IPv4 і раніше є найбільш часто використовуваних Інтернет-протоколом, ARP зазвичай усуває розрив між 32-бітними IPv4-адресами і 48-бітними MAC-адресами та працює в обох напрямках.

Зв'язок між заданим MAC-адресою і його IP-адресою зберігається в кеш-таблиці ARP. Коли пакет, що прямує до вузла в локальній мережі, потрапляє в шлюз, використовується ARP для зв’язку MAC або фізичну адресу вузла з його корреліруючим IP-адресою.

Потім хост переглядає свій кеш ARP. Якщо він знаходить відповідну адресу, то така адреса використовується для перетворення формату і довжини пакету. Якщо правильна адреса не знаходиться, ARP відправляє пакет запиту, який запитує інші машини в локальній мережі. Якщо машина відповідає за адресою, кеш ARP оновлюється на випадок, коли в майбутньому з'являться запити з того ж джерела [11].

*Атаки, засновані на вразливості mDNS*

Існує імовірність, що зловмисники при кожній нагоді можуть проникнути в будь-яку мережу і зловжити її протоколами за допомогою атак перенаправлення мережі, які відомі як «атаки отруєння». Існують протоколи особливо уразливі для зловживань.

Один з таких протоколів - це mDNS. DNS-сервери перетворюють імена веб-сайтів що читає людина (наприклад, www..com) в числові IP-адреси (наприклад 23.92.23.113) що читаються комп'ютером. Транзакція пошуку DNS зазвичай є одноадресною, тобто один комп'ютер запитує у одного сервера перетворення імені в IP-адресу.

Замість того, щоб питати один сервер, mDNS, протокол, пов'язаний з DNS, відправляє пакет іншим хостам навколо нього, щоб отримати відповідь на запит: «Де це знаходиться?». Крім того, mDNS використовується разом з виявленням служб DNS, що допомагає виявляти списки доступних служб через DNS. Ці функції корисні в домашніх мережах, де локальні DNS-сервери не існують, а комп'ютерам необхідно знайти інші локальні ресурси, такі як принтери. Одним з послідовних користувачів протоколу mDNS є служба Apple Bonjour, а це означає, що mDNS активно використовується в мережах, що містять пристрої MacOS і iOS.

Подібно до того, як зловмисники мають намір зловживати NetBIOS і LLMNR, mDNS може бути використаний зловмисником, при відповіді на запит mDNS за рахунок підміни собою законного ресурсу або комп'ютера в мережі. В результаті зловмисник може змусити пристрій відправляти конфіденційну інформацію безпосередньо на свою машину [12].

*DNS імітація, підміна (деформація, отруєння кеша DNS)*

DNS є одиним з найбільш важливих інфраструктурних протоколів Інтернету, який призначений, для сприяння контактам і позбавлення людей від проблеми запам'ятовування IP-адреси кожного сервера, з яким вони спілкуються. При введенні адреси домену в браузері, запит на дозвіл імені відправляється на DNS-сервер, який потім шукає доменне ім'я в своєму каталозі і повертає IP-адресу відповідного серверу.

ISSN 2663 - 4023

Підміна DNS (імітація) є типом атаки, при якій зловмисник перехоплює DNS-запит і повертає адресу, яка веде до його власного сервера, замість реальної адреси. Хакери можуть використовувати так званий спуфинг (spoofing) DNS для запуску атаки Man-in-the-Middle і направлення жертви на підроблений сайт, який виглядає як справжній, або вони можуть просто перенаправити трафік на справжній сайт і непомітно вкрасти інформацію [13].

Що стосується DNS, то до найбільш серйозних загроз можна віднести спуфінг DNS та отруєння кеша DNS.

Спуфінг DNS виникає в результаті старань (дій) зловмисників, яка імітує законні сервери, що призначенні для перенаправлення трафіку домену. Нічого не підозрюючи «жертви» потрапляють на шкідливі веб-сайти, що є результатом різних методів атак з підміною DNS.

Отруєння кеша DNS - це метод підміни DNS на стороні (території) користувача, при якому система реєструє шахрайський IP-адреса в кеші локальної пам'яті. Це змушує DNS викликати з пам'яті поганий сайт, навіть коли проблема буде вирішена або ніколи не існувала на стороні сервера [14].

Існують методи DNS-спуфинга, або атак з отруєнням кешу, наприклад, обман в рамках атаки Man-in-the-middle, захоплення сервера DNS, отруєння кеша DNS через спам. Розглянемо метод спуфінга DNS, як такий що може надати злочинцям більш тривалий доступ до конфіденційних даних користувача.

У випадку появи зловмисника між веб-браузером і DNS-сервером, відбувається зараження їх обох. Інструмент використовується для одночасного зараження кешу на локальному пристрої і зараження серверу на DNS-сервері. В результаті відбувається перенаправлення на шкідливий сайт, що розміщений на власному локальному сервері зловмисника. [14].

Небезпека таких атак полягає у великих збитках, які вони породжують.

Крадіжка даних може бути особливо прибутковою для зловмисників з підміною DNS. Банківські веб-сайти і популярні інтернет-магазини легко підроблюються, що означає, що будь-який пароль, кредитна карта або особиста інформація можуть бути скомпрометовані. Перенаправлення будуть фішинговими веб-сайтами, призначеними для збору інформації користувача.

Зараження шкідливим ПЗ - ще одна поширена загроз, що пов'язана з підміною DNS. Якщо виникає пере направлення облудної інформації, адресатом може виявитися сайт, заражений шкідливими завантаженнями. Управління через завантаження (Drive by downloads) - простий спосіб автоматизувати зараження будь-якої системи. В кінцевому підсумку, якщо не використовувати безпеку в Інтернеті, існує ризик впливу шпигунського ПЗ, реєстраторів ключів або черв'яків.

Зупинка оновлень безпеки може бути результатом підробки DNS. Якщо на підроблених сайтах є постачальники послуг Інтернет-безпеки, законні оновлення безпеки виконуватися не будуть. В результаті комп'ютер може піддатися додатковим загрозам, таким як віруси або Трояни.

Цензура в Інтернеті - це ризик, який насправді є звичайним явищем в деяких частинах світу. Наприклад, Китай використовує модифікації DNS, щоб гарантувати, що всі веб-сайти, що переглядаються в країні, схвалені. Цей блок на національному рівні отримав назву Великого брандмауера, і є одним із прикладів того, наскільки потужною може бути підміна DNS.

Зауважимо що, важко усунути отруєння кеша DNS. Оскільки очищення зараженого сервера не усуває проблему з настільного або мобільного пристрою, пристрій

повернеться на підроблений сайт. Більш того, чисті робочі столи, що підключаються до зараженого серверу, знову будуть скомпрометовані [14].

*Шахрайська (підроблена) точка доступу (Rogue (Fake) AP) і Evil Twin (Злий Близнюк)*

Шахрайська точка доступу є точкою бездротового доступу, яка була встановлена в захищеній мережі без явної авторизації адміністратора локальної мережі, незалежно від того, додана вона співробітником або зловмисником.

Технічно будь-яким добромисним співробітником легко встановити «програмну точку доступу», або недорогий бездротовий маршрутизатор, для полегшення доступу з мобільних пристроїв. Ймовірно, що подібна точка буде налаштована як «відкрита» або зі слабким рівнем безпеки, що потенційно дозволить доступ неавторизованимсторонам.

Якщо зловмисник встановлює точку доступу, він може запускати різні типи сканерів вразливостей і замість того, щоб фізично знаходитися всередині організації, може атакувати віддалено [15].

Evil Twin є більш просунута версія атаки Fake AP. Rogue AP можна використовувати в громадських місцях, де люди можуть легко підключатися до точок доступу без пароля. Зловмисник в цей час пропускає весь трафік через себе, маючи можливість його розшифрувати і прочитати.

Атака Evil Twin передбачає, що зловмисником встановлюється шахрайська точка бездротового доступу, також відома як «злий близнюк», яка імітує характеристики (включаючи SSID) законної точки доступу. Користувачі можуть автоматично підключатися до «злого близнюка» або робити це, думаючи, що шахрайська точка доступу є частиною надійної мережі WI-FI. Зловмисники можуть прискорювати цей процес, вплинувши на з'єднання з легальної точкою доступу, яку імітує їх пристрій. Після підключення користувачем до «злого близнюка», їм поступає запит на введення імені користувача та паролю, для отримання доступу через шахрайську форму, яка відправляється зловмисникові. Або зловмисник може отримати незахищену інформацію через підслуховування [16 ].

Щоб ця атака спрацювала, необхідно виконати кілька ключових вимог. По-перше, ця атака спонукає користувача до деяких неосвіченим дій. У випадку з досвідченим користувачем, ця атака може не спрацювати. По-друге, жертва повинна бути успішно аутинтифікована в своїй мережі і помітно неуважна, щоб приєднатися до невідомої відкритої мережі, яка з'явилася з нізвідки. Крім того, спроба підключитися до цієї мережі (в macOS) видає попередження про те, що в останній раз, коли мережа була підключена, у неї був інший тип шифрування [17].

Отже з результатів дослідження зрозуміло, що процес виявлення MITM – атак досить складний. Тому доцільним є попередження здійснення таких атак. За результатами проведеного дослідження можемо скласти список рекомендації для протидії MITM – атакам:

- Використання між мережевого екрану. Для Windows це вбудований Windows Defender Firewall.
- Для роботі в Інтернеті не використовувати протокол зв’язку HTTP.
- Використовувати для підключення до публічних мереж VPN сервіси.
- Обов’язкове встановлення антивірусних програм.
- Для входу в облікові записи використовувати двофактрну аутентифікацію та після завершення роботи виходити з облікових записів.
- Використання менеджера паролів для уникнення авто заповнення паролів.
- Постійне оновлення програмного забезпечення.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Man in the Middle є видом атак, спрямованих на порушення конфіденційності і, в деяких випадках, цілісності інформації. Методи здійснення MITM-атак продовжують удосконалюються і доповнюються, йдучи в обхід нових протоколів захисту. WI-FI є однією з найбільш уразливих систем. В роботі проведено аналіз методів здійснення MITM-атак. На основі цього дослідження розроблено рекомендації для протидії MITM-атакам. Моніторинг трафіку мережі не може надійно захистити користувачів від здійснення MITM-атак. У подальших дослідженнях доцільно розробити програмне забезпечення для виявлення таких атак як для домашніх, так і для корпоративних мереж.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 *Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking*. TechGenix. https://techgenix.com/understanding-man-in-the-middle-attacks-arp-part3/

2 Vallivaara, V. (2014). Detecting Man-in-the-Middle Attacks on Non-Mobile Systems. ACM conference on data and application security and privacy : Proceedings of the 4th, San Antonio, 3 March 2014 / ed. by M. Sailio, K. Halunen. San Antonio Texas, 130–133

3 Al Abri, D. (2015). Detection of MITM attack in LAN environment using payload matching. У *2015 IEEE International Conference on Industrial Technology (ICIT)*. IEEE. https://doi.org/10.1109/icit.2015.7125367

4 Mallik, A. (2019). MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109. https://doi.org/10.22373/cj.v2i2.3453

5 Бахарева, Н. Ф., Тарасов, В. Н., Шухман, А. Е., Полежаев, П. Н., Ушаков, Ю. А., Матвеев, А. А. (2018). Выявление атак в корпоративных сетях с помощью методов машинного обучения. *Современные информационные технологии и ИТ-образовани, (3),* 626-632. https://cyberleninka.ru/article/n/vyyavlenie-atak-v-korporativnyh-setyah-s-pomoschyu-metodov-mashinnogo-obucheniya

6 Гаврилова, Е. А. (2017). Исследование методов обнаружения сетевых атак. *Научные записки молодых исследователей*, *(4),* 55-58. https://cyberleninka.ru/article/n/issledovanie-metodov-obnaruzheniya-setevyh-atak

7 Thing, V. L. L. (2017). IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach. У *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE. https://doi.org/10.1109/wcnc.2017.7925567

8 Bodström, T., & Hämäläinen, T. (2018). State of the Art Literature Review on Network Anomaly Detection with Deep Learning. У *Lecture Notes in Computer Science* (с. 64–76). Springer International Publishing. https://doi.org/10.1007/978-3-030-01168-0_7

9 Aygun, R. C., & Yavuz, A. G. (2017). Network Anomaly Detection with Stochastically Improved Autoencoder Based Models. У *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE. https://doi.org/10.1109/cscloud.2017.39

10 Иванов, О. Все об атаке "Человек посередине" (Man in the Middle, MitM). https://www.antimalware.ru/analytics/Threats_Analysis/man-in-the-middle-attack

11 Lake, J. ARP poisoning/spoofing: How to detect & prevent it. Comparitech. https://www.comparitech.com/blog/vpn-privacy/arp-poisoning-spoofing-detect-prevent

12 Salihoglu M. Poisoning Attacks, Round 2: Beyond NetBIOS and LLMNR. https://www.crowe.com/cybersecurity-watch/poisoning-attacks-round-2-beyond-netbios-llmnr

13 What is DNS spoofing Man in The Middle Attack?| Security Wiki. Secret Double Octopus. https://doubleoctopus.com/security-wiki/threats-and-tools/dns-spoofing

14 What is DNS Cache Poisoning and DNS Spoofing? https://www.kaspersky.com/resource-center/definitions/dns

15 Contributors to Wikimedia projects. Rogue access point - Wikipedia. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Rogue_access_point

16 Baxter, K. Evil Twin Attack - Firewalls.com. https://www.firewalls.com/blog/security-terms/evil-twin-attack

17 How to Hack Wi-Fi: Stealing Wi-Fi Passwords with an Evil Twin Attack. WonderHowTo. https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (13), 2021
ISSN 2663 - 4023

**Krivenko Serhii**
Doctor of Technical Sciences, Associate Professor of Systems Analysis and Information Technology
Mariupol State University, Mariupol, Ukraine
ORCID ID: 0000-0002-0319-7174
s.krivenko@mdu.in.ua

**Rotaniova Natalya**
Candidate of Sciences in Pedagogy, Associate Professor of Systems Analysis and Information Technology
Mariupol State University, Mariupol, Ukraine
ORCID ID: 0000-0001-8437-7566
rotanevan@gmail.com

**Lazarevska Yulianna**
Assistant of the Systems Analysis and Information Technologies Department
Mariupol State University, Mariupol, Ukraine
ORCID ID: 0000-0001-8318-5861
lazarevskayulianna@gmail.com

**Karpenko Ulyana**
Educational level "Bachelor"student of Educational Progam Cybersecurity
Mariupol State University, Mariupol, Ukraine
ORCID ID: 0000-0002-8634-0457
kulana131@gmail.com

# RESEARCH OF THE SYSTEM FOR VULNERABILITY TO MITM – ATTACKS USING THE CREATION OF FAKE AP

**Annotation.** The problems of the cybersecurity are becoming a daily threat to the business sphere and the Internet users. The field of the cybersecurity is constantly changing, but it is obviously that the cyber threats are becoming more serious and occur more often. The statistics on the number of cyber attacks in 2020 showed a sharp surge in the cybercrime. In the field of the information security, the majority of incidents has been related to attacks on the various distributed information systems recently. At the same time, a significant amount number of the successful attacks are those that carried out using such attacks as "Man in the middle" (MITM). MITM - attacks are dangerous because with their help attackers gain access to the confidential information, not only the companies but also the ordinary users. Therefore, the purpose of this article is to study the types of MITM - attacks, as well as to develop the recommendations for combating such types of attacks. The study was conducted using methods of analysis and description. The object of the study is MITM attacks. The subject of the study is to determine ways to counter attacks such as MITM. As a result of the conducted research the basic types and the technique of carrying out MITM - attacks are considered. The result of the study was the development of the recommendations for the countering MITM attacks. The proposed methods of preventing "Man in the middle" attacks can ensure a certain high level of the computer network security. This study will be useful in ways suggested to prevent MITM attacks, not only for security administrators, but also for Wi-Fi users trying to protect their personal data. The results of the study can also be used to develop better software that can increase the security of any computer network.

**Keywords**: cyber attack, MITM-attack; access point; Fake AP; SSL; WPA; SSID; MITM-attack prevention.

## REFERENCES

1 *Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking*. TechGenix. https://techgenix.com/understanding-man-in-the-middle-attacks-arp-part3/

2 Vallivaara, V. (2014). Detecting Man-in-the-Middle Attacks on Non-Mobile Systems. ACM conference on data and application security and privacy : Proceedings of the 4th, San Antonio, 3 March 2014 / ed. by M. Sailio, K. Halunen. San Antonio Texas, 130–133

3 Al Abri, D. (2015). Detection of MITM attack in LAN environment using payload matching. У *2015 IEEE International Conference on Industrial Technology (ICIT)*. IEEE. https://doi.org/10.1109/icit.2015.7125367

4 Mallik, A. (2019). MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109. https://doi.org/10.22373/cj.v2i2.3453

5 Bakhareva, N. F., Tarasov, V. N., Shukhman, A. E., Polezhaev, P. N., Ushakov, Yu. A., Matveev, A. A. (2018). Vыiavlenye atak v korporatyvnыkh setiakh s pomoshchiu metodov mashynnoho obuchenyia. Sovremennыe ynformatsyonnыe tekhnolohyy y YT-obrazovany, *(3),* 626-632. https://cyberleninka.ru/article/n/vyyavlenie-atak-v-korporativnyh-setyah-s-pomoschyu-metodov-mashinnogo-obucheniya

6 Havrylova, E. A. (2017). Yssledovanye metodov obnaruzhenyia setevыkh atak. Nauchnыe zapysky molodыkh yssledovatelei, *(4),* 55-58. https://cyberleninka.ru/article/n/issledovanie-metodov-obnaruzheniya-setevyh-atak

7 Thing, V. L. L. (2017). IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach. У *2017 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE. https://doi.org/10.1109/wcnc.2017.7925567

8 Bodström, T., & Hämäläinen, T. (2018). State of the Art Literature Review on Network Anomaly Detection with Deep Learning. У *Lecture Notes in Computer Science* (с. 64–76). Springer International Publishing. https://doi.org/10.1007/978-3-030-01168-0_7

9 Aygun, R. C., & Yavuz, A. G. (2017). Network Anomaly Detection with Stochastically Improved Autoencoder Based Models. У *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE. https://doi.org/10.1109/cscloud.2017.39

10 Yvanov, O. Vse ob atake "Chelovek poseredyne" (Man in the Middle, MitM). https://www.antimalware.ru/analytics/Threats_Analysis/man-in-the-middle-attack

11 Lake, J. ARP poisoning/spoofing: How to detect & prevent it. Comparitech. https://www.comparitech.com/blog/vpn-privacy/arp-poisoning-spoofing-detect-prevent

12 Salihoglu M. Poisoning Attacks, Round 2: Beyond NetBIOS and LLMNR. https://www.crowe.com/cybersecurity-watch/poisoning-attacks-round-2-beyond-netbios-llmnr

13 What is DNS spoofing Man in The Middle Attack?| Security Wiki. Secret Double Octopus. https://doubleoctopus.com/security-wiki/threats-and-tools/dns-spoofing

14 What is DNS Cache Poisoning and DNS Spoofing? https://www.kaspersky.com/resource-center/definitions/dns

15 Contributors to Wikimedia projects. Rogue access point - Wikipedia. Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Rogue_access_point

16 Baxter, K. Evil Twin Attack - Firewalls.com. https://www.firewalls.com/blog/security-terms/evil-twin-attack

17 How to Hack Wi-Fi: Stealing Wi-Fi Passwords with an Evil Twin Attack. WonderHowTo. https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880