КЛАСИФІКАЦІЯ ТА РЕКОМЕНДАЦІЇ ЗАХИСТУ ВІД MITM АТАК

УДК 004.056.53

DOI: https://doi.org/10.35546/2313-0687.2019.25.58-65

Козел Віктор
к.т.н., доцент кафедри інформаційних технологій, Херсонський національний технічний університет,
Херсон, Україна, ORCID ID: 0000-0002-2627-2499, **E-mail:** k_vic@ukr.net

Анотація. Сьогодні особлива актуальність набуває захист персональних даних та методи захисту інформації від несанкціонованого доступу. Найголовнішим для користувача є уважне користування мережею, та не ризикувати при підозрілий роботі мережі або будь яких дій де вас просять вводити особисті дані, завжди потрібно бути впевненим у тому, що це не зловмисник запрошує у вас дані, а саме система з якою ви працюєте.

Методи дослідження. У статті розглядається загальна класифікація типів атак у вигляді схеми для більш зручного використання. Проведено аналіз поведінки зловмисника у разі застосування MITM атак, а також розроблені рекомендації налаштування Wi-Fi роутерів, щодо підвищення безпеки комп'ютерної мережі.

Основні результати дослідження. Забезпечення безпеки протоколу зв'язку з використанням Wi-Fi роутерів при повсякденному застосуванні з використанням рекомендацій. Виявлено що, безпечний протокол зв'язку повинен мати кожне з наступних властивостей: конфіденційність, цілісність. В якості основних рекомендацій, що до захисту від атак виділено наступні: зробити мережу прихованою, створювати декілька мереж для використання IoT, створити окрему підмережу для дітей та гостей. Наведені рекомендації налаштування кількох параметрів значно поліпшують загальну безпеку домашньої мережі.

Наукова новизна. Запропонована класифікація атак дозволяє виявити рівень моделі OSI на якому відбувається втручання в комп'ютерну мережу, що дозволяє обрати найбільш зручний засіб забезпечення безпеки комп'ютерної мережі. Рекомендації налаштування роутерів розроблені виходячи з сучасних потреб та вмінь простих користувачів.

Практична значимість. У наш час поширення комп'ютеризації усіх галузей життєдіяльності людини забезпечення конфіденційності інформації набуває особливої актуальності для простого користувача мереж.

Ключові слова: *безпека, роутер, атака, комп'ютерні мережі.*

Постановка проблеми.

Сьогодні дуже багато інформації передається в інтернеті та дуже велика частина цієї інформації передається через технологію Wi-Fi, але якщо канал не є закритим та захищений додатково (з використанням спеціально навчених людей – системних адміністрато-

рів або спеціалістів з інформаційної безпеки) або це не передача за допомогою кабелю, то інформація може бути перехоплена зловмисником. Справа у тому, що коли використовується кабель, то комп'ютер користувача вже під'єднаний до мережі і зловмиснику для під'єднання до такої мережі потрібно під'єднати кабель до свого комп'ютеру, тобто потрібен фізичний контакт, що далеко не завжди є можливим, а коли використовується бездротова точка доступу, то користувач повинен під'єднатись до неї та відправити пароль на цю точку доступу, тобто зловмисник також може під'єднатись до цієї точки доступу тобто до цієї ж мережі знаючи пароль, який він може перехопити у момент коли користувач відправляє його на точку доступу, а подалі почати перехоплювати усю інформацію що використовує користувач у мережі. Таким чином класифікація атак та рекомендації що до захисту сучасних комп'ютерних мереж є актуальною на даний час.

Аналіз останніх досліджень і публікацій

Для обмеження і блокування збору інформації о системі з боку неавторизованого об'єкта розробляються різні методи протидії мережевому скануванню: від реалізації прихованих каналів дослідження до використання підходу до ідентифікації аномалій а також налаштування мережевого обладнання для запобігання неавторизованого проникнення[1-5]. Але ці методи не дають однозначного результату в разі застосування кіберзлочинцем комбінування різних загроз. Таким чином, розроблення простих рекомендацій для звичайного користувача є актуальною оскільки запропоновані методи та рекомендації впершу чергу рекомендовані для системних адміністраторів і є важкими для звичайних користувачів.

Мета дослідження. Метою даної статті є розробка та дослідження сучасних комп'ютерних атак. Розробка класифікації загроз та розробка рекомендацій що до захисту комп'ютерних мереж від MITM атак.

Виклад матеріалу дослідження.

У неоднорідній мережі для передачі інформації застосовуються набір протоколів TCP/IP, які забезпечують сумісність між комп'ютерами різних типів. Цей набір протоколів став відомим завдяки сумісності та можливості надання доступу до ресурсів глобальної мережі Інтернет, та став стандартом міжмережевої взаємодії. Однак з розповсюдженням стека протоколів TCP/IP проявились його слабкі сторони, що призвело до можливості віддалених атак на розподілені системи, оскільки їх частини (компоненти) зазвичай використовують відкриті канали передачі даних. При атаках порушник може не тільки прослуховувати канал зв'язку але і модифікувати інформацію що передається.

Надлишкова функціональність в сучасних системах є великим недоліком в контексті віддалених атак, в результаті цього тяжкість виявлення процесу проведення віддаленої атаки та відносна простота проведення виводить цей вид неправомірних дій на перше місце за ступеню небезпеки, а також перешкоджає своєчасному реагуванню на відповідну загрозу. Все це підвищує шанси вдалої атаки.

Мережеві атаки на розподільні обчислювальні системи (РОС) можна класифікувати наступним чином (рис. 1):

- За характером впливу:
- За ціллю впливу:
- За початком дії впливу:
- За розташуванням суб'єкта атаки відносно об'єкта атаки:
- За наявності зворотнього зв'язку з об'єктом атаки:
- За рівнем моделі ISO/OSI.

Технологія MITM атаки. Атака посередника, або атака «людина посередині» (англ. Man in the middle (MITM)) – вид атаки в криптографії, коли зловмисник таємно ретранслює і при необхідності змінює зв'язок між двома сторонами, які вважають, що вони безпосередньо спілкуються один з одним, схема МА (рис. 2). Є методом компрометації каналу зв'язку, при якому зломщик, підключившись до каналу між контрагентами, здійснює втручання в протокол передачі, видаляючи або спотворюючи інформацію.[6]

Щоб зрозуміти принцип атаки посередника, варто спочатку розібратися з тим, як працює сам інтернет. Основні точки взаємодії: клієнти, маршрутизатори, сервери. Найбільш поширений протокол взаємодії між клієнтом і сервером – Hypertext Transfer Protocol (HTTP). Серфінг в інтернеті за допомогою браузера, електронна пошта, обмін миттєвими повідомленнями – все це здійснюється через HTTP. Коли ви вводите http://www.сайт.com в адресному рядку вашого браузера, то клієнт (ви) відправляє 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.

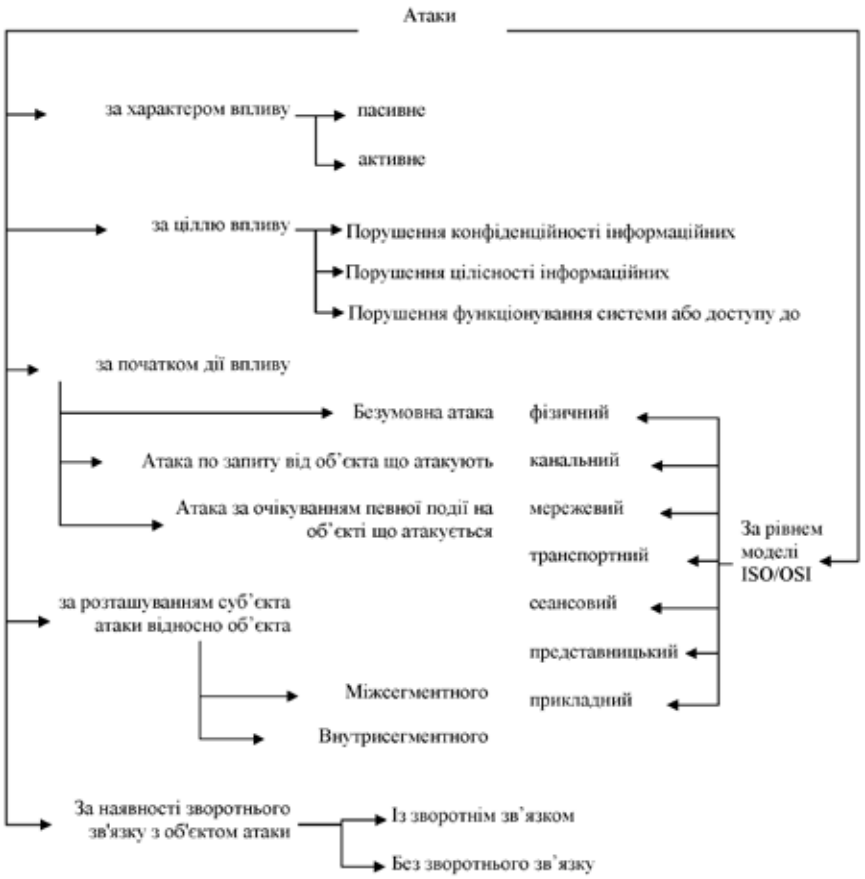

Рис. 1. Класифікація атак

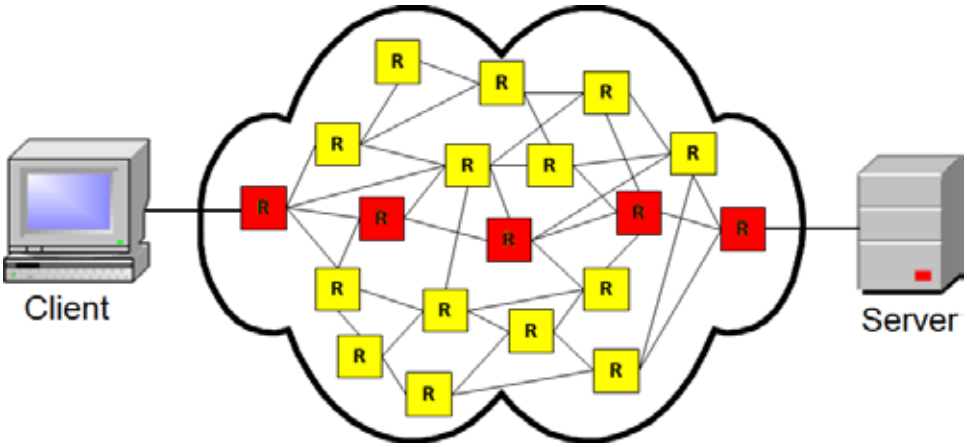

Рис. 2. Взаємодія клієнт-сервер

Забезпечення безпеки протоколу зв'язку. Безпечний протокол зв'язку повинен мати кожне з наступних властивостей:

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

Якщо хоч одна з цих правил не дотримано, весь протокол скомпрометований.

Одним із прикладів атак типу «людина посередині» є активне прослуховування, при якому зловмисник встановлює незалежні зв'язку з жертвами і передає повідомлення між ними. Тим самим він змушує жертв повірити, що вони розмовляють безпосередньо один з одним через приватну зв'язок, фактично ж вся розмова управляється зловмисником. Зловмисник повинен вміти перехоплювати всі передані між двома жертвами повідомлення, а також вводити нові. У більшості випадків це досить просто, наприклад, зловмисник може вести себе як «людина посередині» в межах діапазону прийому бездротової точки доступу (Wi-Fi).

Дана атака спрямована на обхід взаємної аутентифікації або відсутність такої і може увінчатися успіхом тільки тоді, коли зловмисник має можливість видати себе за кожну кінцеву точку або залишатися непоміченим в якості проміжного вузла. Більшість криптографічних протоколів включає в себе деяку форму аутентифікації кінцевої точки спеціально для запобігання MITM-атак.

Атака «людини посередині» дозволяє підмінити необхідні дані при передачі, атакуючий посилає команду переадресації на HTTP протокол. За допомогою даного методу вся інформація передається знову у незашифрованому вигляді. Існує два основні методи вирішення проблеми несанкціонованої переадресації:

- примусовий розрив HTTP сесій;
- примусова переадресація з HTTP на HTTPS вебсервісом.

У першому випадку користувач не зможе отримати доступ до сайту, якщо він використовує HTTP протокол при з'єднанні. Даний спосіб діє на шкоду власникові веб-сайту, так як людина, що не знає таких тонкощів, краще відмовиться від послуг компанії через недоступність сайту. Звичайному користувачеві не зробить самостійний протокол HTTPS. У другому випадку відбувається непомітна переадресація за допомогою скриптів сервісу на протокол HTTPS. Даний спосіб є найбільш ефективним як для клієнта, так і для власника сайту. В даному випадку, якщо проводиться атака MITM, то сайт не дасть перейти на протокол HTTP. А пізніше виступають у дію сертифікати SSL.[6]

Також існує проблема підміни сертифікатів SSL атакуючим. Для цього атакуючому необхідно отримати SSL сертифікат від одного з ліцензіатів. Але цього не досить, так як ліцензіати дорожать своєю репутацією і правом на видачу сертифікатів, в результаті чого за підозрілою активністю сертифікат блокується. Таким чином, атака можлива тільки, якщо використовується HTTP протокол. У зв'язку з масовим переходом на HTTPS протокол, складно знайти сайт, який би не мав SSL сертифікат. Веб сервіси, де існує авторизація через логін і пароль або електронні платежі, зобов'язані мати SSL сертифікат. На сьогоднішній день неможливо знайти веб-сайт такого типу на HTTP протоколі. У зв'язку з цим дана атака не є актуальною, але все одно продовжує використовуватися та атакуючі максимально змінюють стандартні алгоритми цієї атаки.

MITMf – це фреймворк для атак людина-посередині. Цей інструмент базується на sergio-proxy. Метою MITMf – бути інструментом «все в одному» для мережевих атак і атак «людина по середині», при цьому оновлюючи і вдосконалюючи існуючі атаки і техніки. Спочатку створений для виправлення значних недоліків інших інструментів (наприклад, Ettercap, Mallory), програма була практично повністю переписана з нуля для забезпечення модульного і легко маштабуємого фреймворка, який кожен може використовувати для реалізації своїх власних атак MITM. Особливості:

- Цей фреймворк містить вбудовані сервера SMB, HTTP і DNS, які можуть управлятися і використовуватися безліччю плагінів, він також містить модифіковану версію SSLStrip proxy, яка дозволяє HTTP модифікацію і частковий обхід HSTS.
- Починаючи з версії 0.9.8, MITMf підтримує активну фільтрацію пакетів і маніпуляцію (в основному те, що робили etterfilters, тільки краще), дозволяючи користувачам модифікувати будь-який вид трафіку або протоколу.

- Конфігураційний файл може бути відредагований на льоту в той час коли MITMf запущений, зміни будуть передані у фреймворк: це дозволяє вам робити тонке налаштування плагінів і сервера під час виконання атаки.
- MITMf буде захоплювати FTP, IRC, POP, IMAP, Telnet, SMTP, SNMP (community strings), NTLMv1 / v2 (всі підтримувані протоколи на зразок HTTP, SMB, LDAP і т.д.) і облікові дані Kerberos з використанням Net-Creds, який запускається при старті програми.
- Інтеграція з Responder дозволяє LLMNR, NBT-NS і MDNS poisoning, а також підтримку шахрайського сервера WPAD.

Узагальнюючи усі типи, види, технології та методи атак, розглянуті у розділах 1 та 3, розглянемо загальні рекомендації для виявлення атак і більшого захисту мережі від них та конкретні рекомендації для виявлення та запобігання від конкретних атак.

Виявлення та захист від MITM атак. Перевірка затримки за часом може потенційно виявити атаку в певних ситуаціях. Наприклад, при тривалих обчисленнях хеш-функцій, які виконуються протягом десятка секунд. Щоб виявити потенційні атаки, сторони перевіряють розбіжності в часі відповіді. Припустимо, що дві сторони зазвичай витрачають певну кількість часу для виконання конкретної транзакції. Однак, якщо одна транзакція займає аномальний період часу для досягнення іншої сторони, це може свідчити про втручання третьої сторони, що вносить додаткову затримку в транзакцію.

Для виявлення атаки «людина посередині» також необхідно проаналізувати мережевий трафік. Наприклад, для детектування атаки по SSL слід звернути увагу на наступні параметри:

- IP-адреса сервера.
- DNS-сервер.
- X.509-сертифікат сервера.
- Чи підписано сертифікат самостійно.
- Чи підписано сертифікат центром сертифікації.
- Чи був сертифікат анульований.
- Чи змінювався сертифікат недавно.
- Чи отримували інші клієнти в інтернеті такий же сертифікат.
- Захист від атак «людина по середині».

Для запобігання MITM атак потрібно бути уважними при користуванням мережею, використовувати https протокол замість http, якщо вас веб-сторінка перенаправляє на http протокол краще не відкривати її, усі сучасні ресурси використовують захищений протокол.

Використовувати статичні записи у arp-таблиці, для уникнення від типу атаки arp-спуфінгу, тепер атакуючий не зможе змінити записи у таблиці оскільки вони задані жорстко (статично). Перевага такого захисту у простоті її реалізації для звичайного користувача без належних знань. Але у використання у крупних мережах таких підхід є важким. Але у місцях де використовуються великі мережах зазвичай роботають спеціально обучені люди для вирішення цих питань.

Використовування VPN з шифруванням та/або https, у такому випадку усі дані, що перехоплює атакуючий є зашифрованими.

За можливістю відмовитись від передачі важливих даних через відкриті wifi мережі. Використання закритих wifi мереж значно знижує ймовірність присутність атакуючого, а MITM атака є безуспішною.

Рекомендаційні дії для захисту Wi-Fi для звичайного користувача. Для того щоб покращити захист роутеру необхідно правильно його налаштувати. З усіх налаштувань за замовчуванням пароль для доступу до інтерфейсу адміністратора роутера повинен бути змінений в першу чергу. Зокрема, для надійного захисту роутера підберіть сильну і унікальну ключову фразу замість стандартного імені користувача на приклад «admin», «administrator», «root», «user». Крім зниження витрат для виробників, ці та інші настройки за замовчуванням призначені для полегшення віддаленого усунення несправностей. Однак якщо не змінити їх, можна зіткнутися з рядом проблем. Наприклад, реєстраційні дані часто очевидні і загальні для окремих моделей і навіть цілих брендів. Тому облікові дані можна легко знайти в Інтернеті або відгадати, спробувавши найбільш поширені комбінації, наприклад, «admin / password».[7]

Крім цього, часто назвою бездротової мережі є бренд і модель. Змініть це ім'я, а саме Service Set Identifier (SSID), на те, що не ідентифікує Вас або Ваше місце розташування.

Також за замовчуванням часто включена функція під назвою Wi-Fi Protected Setup (WPS), яка призначена

для допомоги в підключенні нових пристроїв. Однак у зв'язку з недоліками впровадження, WPS може бути легко використаний для шкідливих цілей, зокрема для здійснення атак на пароль.

Іншою особливістю, яка часто використовується за умовчанням у роутерах і пов'язане зі значним ризиком для безпеки, є Universal Plug and Play (UPnP). У разі відсутності потреби в UPnP, який призначений для забезпечення безперешкодної зв'язку між пристроями, краще його вимкнути. Також для запобігання потенційних атак і захисту роутера варто вимкнути всі протоколи і порти, які не використовуються.

Для забезпечення захисту роутера від атак зловмисників необхідно забезпечити захист Wi-Fi за допомогою налаштування складного і надійного пароля. Комбінація повинна відрізнятися від усіх інших реєстраційних даних користувача, в тому числі і пароля для доступу до консолі адміністратора роутера. Крім цього, необхідно вказати протокол безпеки для бездротового з'єднання. Єдиним варіантом, який можна порекомендувати, є WPA2. Для домашніх користувачів кращий варіант – персональний режим (WPA2-Personal або WPA2-PSK) WPA2, який доповнений шифруванням AES. Надійне шифрування захищає всі дані при передачі між підключеним до Wi-Fi комп'ютером або мобільним пристроєм і роутером. Таким чином, зловмисники не зможуть переглянути інформацію, навіть якщо вона потрапила в руки кіберзлочинців. На роутерах все ще можуть бути доступні два старих режиму безпеки Wi-Fi – WPA і WEP. Однак, їх не варто використовувати, особливо останній. Оскільки WPA2 був обов'язковим для всіх сертифікованих апаратних засобів Wi-Fi ще в 2006 році.

Вбудоване програмне забезпечення роутерів, як і програмне забезпечення комп'ютерів, вимагає регулярного оновлення. Пристрої можуть містити уразливості через відсутність оновлень програмно-апаратних засобів. Це дозволяє зловмисникам легко проникнути всередину мережі, тоді як відомі проблеми безпеки можна запобігти за допомогою простого сканування на наявність відомих вразливостей.

Для перевірки актуальності оновлень перейдіть до адміністративної панелі роутера. Сучасні моделі оновлюються автоматично або повідомляють про нові версії прошивки, тоді як для застосування виправлення на застарілих моделях потрібно відвідати сайт постачальника і перевірити наявність новішої. Такі дії необхідно робити регулярно, принаймні, кілька разів на рік, щоб забезпечити захист роутера від нових вразливостей.

Цілком можливо, що виробник припинив випускати оновлення для Вашої моделі, тому на неї не може бути встановлено ніяких оновлень. Крім виправлення вразливостей, нова версія програмно-апаратних засобів може також мати кращою продуктивністю і новими функціями, включаючи ті, які пов'язані з механізмами безпеки.

Деякі роутери дозволяють створювати кілька мереж, що особливо зручно при використанні Інтернету речей (IoT). У разі використання технологій смарт-будинку потрібно винести всі пристрої Інтернету речей в окрему підмережу, щоб їх уразливості не могли бути використані для доступу до даних на комп'ютері, смартфоні або інших гаджетів для зберігання даних. Для додаткового захисту роутера також необхідно створити окрему підмережу для дітей та гостей. Таким чином, можливо запобігти ризику доступу шкідливого програмного забезпечення до ваших цифровим файлам.

Також рекомендується вимкнути віддалене управління роутером, щоб зменшити шанси злочинців отримати доступ до нього з будь-якої точки світу, наприклад, шляхом використання вразливостей. Таким чином, для внесення будь-яких змін в налаштування потрібен фізичний доступ до роутера.

Висновки. Розглянуті методи захисту Wi-Fi користувача дозволяють застосовувати ці методи для звичайного користувача, що не має спеціальних знань в області мереж, інформаційної безпеки та подібного, саме такі користувачі найчастіше піддаються вдалим атакам. В якості основних рекомендацій, що до захисту від атак виділимо наступні: зробити мережу прихованою, тобто у переліку доступних wifi мереж SSID даної корпоративної мережі не буде видно, для атакуючого це ускладнює злом даної мережі, створювати декілька мереж для використання IoT, створити окрему підмережу для дітей та гостей. Насправді засобів забезпечення захисту роутера значно більше, ніж було розглянуто. Однак навіть налаштування кількох параметрів значно поліпшить загальну безпеку домашньої мережі.

СПИСОК ЛІТЕРАТУРИ:

1. Бахарева Н. Ф., Тарасов В. Н., Шухман А. Е., Полежаев П. Н., Ушаков Ю. А., Матвеев А. А. Выявление атак в корпоративных сетях с помощью методов машинного обучения/ Современные информационные технологии и ИТ-образование. 2018. №3. С.626-632. URL: https://cyberleninka.ru/article/n/vyyavlenie-atak-v-korporativnyh-setyah-s-pomoschyu-metodov-mashinnogo-obucheniya (дата обращения: 01.12.2019).
2. Гаврилова Е. А. Исследование методов обнаружения сетевых атак. *Научные записки молодых исследователей.* 2017. №4. С.55-58. URL: https://cyberleninka.ru/article/n/issledovanie-metodov-obnaruzheniya-setevyh-atak (дата обращения: 11.12.2019).
3. Thing V.L.L. IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach // 2017 IEEE Wireless Communications and Networking *Conference (WCNC). San Francisco*, CA, 2017. Pp. 1-6. DOI: 10.1109/ WCNC.2017.7925567
4. Bodström T., Hämäläinen T. State of the Art Literature Review on Network Anomaly Detection with Deep Learning / O. Galinina, S. Andreev, S. Balandin, Y. Koucheryavy (Eds.) // *Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN 2018, ruSMART 2018. Lecture Notes in Computer Science*. Vol. 11118. Springer, Cham, 2018. Pp. 64-76. DOI: 10.1007/978-3-030-01168-0_7
5. Aygun R.C., Yavuz A.G. Network Anomaly Detection with Stochastically Improved Autoencoder Based Models. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). New York, NY,* 2017. Pp. 193-198. DOI: 10.1109/CSCloud.2017.39
6. M. Ramilli, W. Cerroni and F. Callegati, "Man-in-the-Middle Attack to the HTTPS Protocol" in *IEEE Security & Privacy*, vol. 7, no. 01, pp. 78-81, 2009. doi: 10.1109/MSP.2009.12.
7. Безпека домашньої мережі: як забезпечити захист роутера від атак. eset: веб-сайт. [Електронний ресурс] URL: https://eset.ua/ua/news/view/655/bezopasnost-domashney-seti-kak-obespechit-zashchitu-routera-ot-atak (дата звернення: 11.12.2019).
8. Wi-Fi to carry up to 60% of mobile data traffic by 2019 [Електронний ресурс] URL: http://www.juniperresearch.com/press/press-releases/Wi-Fi-to-carry-60pc-of -mobile-datatraffic-by-2019

MITM ATTACK PROTECTION CLASSIFICATION AND RECOMMENDATIONS

Viktor Kozel

Candidate of Engineering Sciences (PhD), Associate Professor of the Information Technologies, Kherson National Technical University, Kherson, Ukraine, ORCID ID: 0000-0002-2627-2499, **E-mail:** k_vic@ukr.net

Abstract. Today, the protection of personal data and methods of protecting information from unauthorized access become particularly relevant. The most important thing for the user is the bladed use of the computer network, and not to risk suspicious operation of the network or any actions where you are asked to enter personal data, it is always necessary to be sure that it is not the attacker who invites you to enter data, namely the system with which you work.

Research methods. The article discusses the general classification of attack types in the form of a diagram for more convenient use. An analysis of the behavior of the attacker in case of MITM attacks has been carried out, as well as recommendations for setting up Wi-Fi routers, to improve the security of the computer network have been developed.

The main results of research. Secure the communication protocol using a Wi-Fi router for everyday use using the suggested recommendations. It is revealed that a secure communication protocol should have any of the following properties: confidentiality, integrity. As the main recommendations, to protection against the attacks it is allocated the following: to make network hidden, to create several networks for use IoT, to create a separate subnet for children and guests. The following recommendations for configuring individual settings significantly improve overall home network security.

Scientific novelty. The proposed classification of attacks allows to identify the level of OSI model on which interference in the computer network takes place, which allows to choose the most convenient way to ensure security of the computer network. Router configuration recommendations designed to meet today 's needs and skills of simple users.

Practical significance. Today, widespread computerization in all spheres of human activity, ensuring the confidentiality of information becomes particularly relevant for a simple user of networks.

***Keywords**: security, router, attack, computer networks.*

КЛАССИФИКАЦИЯ И РЕКОМЕНДАЦИИ ЗАЩИТЫ ОТ MITM АТАК

Виктор Козел
к.т.н., доцент кафедры информационных технологий, Херсонский национальный технический университет,
Херсон, Украина, **ORCID ID:** 0000-0002-2627-2499, e-mail: k_vic@ukr.net

Аннотация. Сегодня особую актуальность приобретает защита персональных данных и методы защиты информации от несанкционированного доступа. Самым главным для пользователя является безлопастное использование компьютерной сетью, и не рисковать при подозрительной работе сети или каких-либо действий где вас просят ввести личные данные, всегда нужно быть уверенным в том, что это не злоумышленник приглашает вас ввести данные, а именно система с которой вы работаете.

Методы исследования. В статье рассматривается общая классификация типов атак в виде схемы для более удобного использования. Проведен анализ поведения злоумышленника в случае применения MITM атак, а также разработаны рекомендации настройки Wi-Fi роутеров, по повышению безопасности компьютерной сети.

Основные результаты исследования. Обеспечение безопасности протокола связи используя Wi-Fi роутер при повседневном применении с использованием предложенных рекомендаций. Выявлено что, безопасный протокол связи должен иметь любое из следующих свойств: конфиденциальность, целостность. В качестве основных рекомендаций, к защите от атак выделено следующие: сделать сеть скрытой, создавать несколько сетей для использования IoT, создать отдельную подсеть для детей и гостей. Приведенные рекомендации настройки отдельных параметров значительно повышают общую безопасность домашней сети.

Научная новизна. Предложенная классификация атак позволяет выявить уровень модели OSI на котором происходит вмешательство в компьютерную сеть, что позволяет выбрать наиболее удобный способ обеспечения безопасности компьютерной сети. Рекомендации настройки роутеров разработаны исходя из современных потребностей и умений простых пользователей.

Практическая значимость. В наше время повсеместная компьютеризация во всех сферах жизнедеятельности человека обеспечение конфиденциальности информации приобретает особую актуальность для простого пользователя сетей.

Ключевые слова: *безопасность, роутер, атака, компьютерные сети.*

REFERENCES:

1. Bakhareva N. F., Tarasov V. N., Shukhman A. E., Polezhaev P. N., Ushakov Yu. A.., & Matveev A. A. (2018). Vy`yavlenie atak v korporativny`kh setyakh s pomoshh`yu metodov mashinnogo obucheniya. *Sovremenny`e informaczionny`e tekhnologii i IT-obrazovanie*, 14 (3), 626-632.
2. Gavrilova E. A. (2017). Issledovanie metodov obnaruzheniya setevy`kh atak. *Nauchny`e zapiski molody`kh issledovatelej*, (4), 55-58.
3. Thing V.L.L. (2017). IEEE 802.11 Network Anomaly Detection and Attack Classification: A Deep Learning Approach. *IEEE Wireless Communications and Networking Conference (WCNC). San Francisco, CA*, 1-6. DOI: 10.1109/ WCNC.2017.7925567
4. Bodström T. & Hämäläinen T. (2018). State of the Art Literature Review on Network Anomaly Detection with Deep Learning. *Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN 2018, ruSMART. Lecture Notes in Computer Science*. Vol. 11118. Springer, Cham,. 64-76. DOI: 10.1007/978-3-030-01168-0_7
5. Aygun R.C. & Yavuz A.G. (2017). Network Anomaly Detection with Stochastically Improved Autoencoder Based Models. *IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). New York, NY*, 193- 198. DOI: 10.1109/CSCloud.2017.39
6. Callegati, Franco & Cerroni, Walter & Ramilli, Marco. (2009). Man-in-the-middle attack to the HTTPS protocol. *Security & Privacy, IEEE*. 7. 78-81. 10.1109/MSP.2009.12..
7. Eset (2019). Bezpeka domashn`oyi merezhi`: yak zabezpechiti zakhist routera vi`d atak. URL: https://eset.ua/ua/news/view/655/bezopasnost-domashney-seti-kak-obespechit-zashchitu-routera-ot-atak
8. Wi-Fi to carry up to 60% of mobile data traffic by (2019). URL: http://www.juniperresearch.com/press/press-releases/Wi-Fi-to-carry-60pc-of -mobile-datatraffic-by-2019