УДК 004.056

Какабьян К.С.,
студент
4 курс, факультет №1 Кибербезопасности и управления
Поволжский государственный университет
телекоммуникаций и информатики
Россия, г. Самара

БЕЗОПАСНОСТЬ WI-FI СЕТЕЙ: РИСКИ И МЕТОДЫ ЗАЩИТЫ

Аннотация: *В статье рассматривается важность обеспечения безопасности Wi-Fi сетей в современном мире, описываются основные угрозы, с которыми может столкнуться беспроводная сеть, такие как перехват трафика, взлом паролей, атаки MITM и атаки на MAC-адреса. Также приводятся основные методы защиты беспроводных сетей, включая использование сильных паролей, шифрования и методов аутентификации, мер безопасности на устройствах, образующих сеть, регулярное обновление программного обеспечения, использование механизмов мониторинга и обнаружения, использование гостевых сетей и физическая защита устройств.*

Ключевые слова: *Wi-Fi, уязвимости, атаки, защита, шифрование, аутентификация, мониторинг.*

WI-FI NETWORK SECURITY: RISKS AND PROTECTION METHODS

Abstract: *This article discusses the importance of ensuring Wi-Fi network security in the modern world, describing the main threats that a wireless network*

may face, such as traffic interception, password cracking, MITM attacks, and MAC address attacks. The article also provides the main methods of protecting wireless networks, including using strong passwords, encryption and authentication methods, security measures on network devices, regular software updates, using monitoring and detection mechanisms, using guest networks, and physical device protection.

Keywords: *Wi-Fi, vulnerabilities, attacks, protection, encryption, authentication, monitoring.*

Защита беспроводных сетей

В сегодняшнем мире беспроводные технологии используются повсеместно, начиная от домашних сетей Wi-Fi и заканчивая сетями мобильной связи. Однако беспроводные сети являются уязвимыми для различных атак, таких как перехват сетевых пакетов, взлом, подмена записей в таблице маршрутизации и многих других. Поэтому защита беспроводных сетей является критически важной для обеспечения безопасности и конфиденциальности данных.

Основные угрозы в беспроводных сетях

Основными угрозами для беспроводных сетей являются следующие:

1. Перехват трафика

Перехват трафика является одной из самых распространенных атак на беспроводные сети. Атакующий может использовать различные инструменты для перехвата трафика, например, программное обеспечение для отслеживания пакетов, чтобы захватить и анализировать передаваемые данные. Это может привести к утечке конфиденциальной информации, такой как логины, пароли, данные банковских карт и т. д.

2. Взлом паролей

Взлом паролей является другой распространенной угрозой для беспроводных сетей. Атакующие могут использовать различные методы для взлома паролей, такие как атака по словарю, атака методом подбора пароля с учетом всех возможных комбинаций символов. Если пароль слабый или используется устаревший протокол шифрования, то взлом пароля может быть относительно легкой задачей.

3. Атаки Man-in-the-Middle (MITM)

Атаки Man-in-the-Middle (MITM) - это атаки, подразумевающие перехват трафика злоумышленником между двумя устройствами, и последующая манипуляция передаваемыми данными. Это может привести к утечке конфиденциальной информации.

4. Атаки на MAC-адреса

MAC-адреса используются для идентификации устройств в беспроводной сети. Атакующие могут использовать различные методы для подделки MAC-адресов. Манипуляции с MAC-адресами являются еще одной распространенной атакой на беспроводные сети. Злоумышленник может подделать MAC-адрес устройства, чтобы получить доступ к защищенной сети или скрыть свой MAC-адрес, чтобы избежать идентификации. Это может позволить злоумышленнику получить несанкционированный доступ к сети или скрыть свою активность в сети.

Основные методы защиты беспроводных сетей

Для защиты беспроводных сетей от угроз можно использовать различные методы, в том числе:

1. Использование сильных паролей

Сильные пароли - это пароли, которые длиннее 12 символов и содержат несколько типов символов (буквы, цифры, символы). Использование таких

паролей значительно затрудняет взлом, особенно при использовании протоколов шифрования WPA2 и WPA3.

2. Использование протоколов шифрования

Протоколы шифрования используются для защиты данных, передаваемых по беспроводной сети. Протоколы шифрования, такие как WPA2 и WPA3, обеспечивают более надежную защиту, чем устаревший протокол WEP. Кроме того, можно использовать виртуальные частные сети (VPN) для создания дополнительного слоя защиты передаваемых данных.

3. Использование методов аутентификации

Методы аутентификации используются для проверки подлинности пользователей, пытающихся получить доступ к беспроводной сети. Методы аутентификации, такие как WPA2-Enterprise и IEEE 802.1X, обеспечивают более надежную защиту, чем методы, основанные на предоставлении пароля.

4. Использование мер безопасности на устройствах, образующих сеть

Меры безопасности на уровне устройств могут включать в себя использование антивирусного программного обеспечения и программного обеспечения, предназначенного для обнаружения взломов. Эти меры могут помочь защитить устройства в беспроводной сети от вредоносного программного обеспечения и других типов атак.

5. Регулярное обновление программного обеспечения

Регулярное обновление программного обеспечения на устройствах в беспроводной сети является важным аспектом защиты от угроз. Обновления программного обеспечения содержат исправления уязвимостей и другие улучшения, которые помогают защитить устройства от новых видов атак.

6. Использование механизмов мониторинга и обнаружения

Механизмы мониторинга и обнаружения могут использоваться для обнаружения и пресечения атак на беспроводные сети. Эти механизмы могут включать в себя системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS). IDS и IPS могут быть использованы для

мониторинга трафика в беспроводной сети и обнаружения аномальных действий, которые могут указывать на атаку.

7. Использование гостевых сетей

Гостевые сети могут быть использованы для отделения гостевых устройств от основной сети и предотвращения распространения угроз на основную сеть. Гостевые сети могут быть созданы с помощью специального программного обеспечения, такого как гостевые порталы, которые могут быть настроены для требования аутентификации устройств входящих в сеть.

8. Физическая защита устройств

Физическая защита устройств является важным аспектом защиты от угроз в беспроводных сетях. Это включает в себя защиту устройств от физического доступа и установку устройств в безопасных местах.

Заключение

Беспроводные сети стали неотъемлемой частью нашей повседневной жизни, но они также представляют угрозы для безопасности информации. Угрозы могут быть вызваны различными факторами, такими как уязвимости протоколов, отсутствие шифрования, атаки на MAC-адреса и другие.

Для защиты беспроводных сетей необходимо использовать меры безопасности, такие как установка паролей и шифрование, использование механизмов аутентификации и авторизации, мониторинг трафика и обнаружение угроз, регулярное обновление программного обеспечения. Кроме того, физическая защита устройств также является важным аспектом защиты беспроводных сетей. Однако, ни одна из мер безопасности не является полностью надежной. Всегда есть вероятность возникновения новых уязвимостей, которые могут быть использованы для атаки. Поэтому необходимо постоянно мониторить беспроводные сети и обновлять меры безопасности для защиты от новых угроз.

В целом, защита беспроводных сетей является сложной задачей, но это крайне важно для обеспечения безопасности информации и предотвращения утечек данных. Следование основным мерам безопасности и постоянное обновление мер защиты помогут защитить беспроводные сети от угроз.

Использованные источники:

1. Гордейчик С.В., В.В. Дубровин. В.В. Безопасность беспроводных сетей - Москва: Горячая линия-Телеком, 2008. – 287 с.
2. Варлатая С.К. Анализ методов защиты беспроводной сети Wi-Fi от известных способов взлома злоумышленником / С.К. Варлатая, О.С. Рогова, Д.Р. Юрьев // Молодой ученый.—2015. — № 1(81). — С. 36–37.
3. Александрова Е.С., Иванов Г.Н., Ковцур М.М. Анализ механизмов защиты Wi-Fi сетей. // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). С 47-51.
4. Пролетарский А.В. Беспроводные сети Wi-Fi: учебное пособие / А.В. Пролетарский, И.Ф. Баскаков. — 2-е изд. — Москва: ИНТУИТ, 2016. — 284 с.