Уязвимости протокола WEP шифрования на базе беспроводных технологий

А.Р. Мухаметьянова

Студент 3 курса

направление «Прикладная информатика»

факультета Физики и математики

Россия, Бирск, БФ УУНиТ

Всемирная сеть интернет стала для человечества настоящим прорывом, благодаря которому человек имеет безграничный доступ к информации, а также широкие возможн

ости и удобства для личного пользования. Один из самых популярных на сегодня способов доступа в интернет - подключение к Wi-Fi сети. Ведь именно данная сеть позволяет осуществлять одновременный доступ в сеть интернет и с телефона, и с компьютера. Но ее используют и в системы видеонаблюдения, построенные на базе беспроводных технологий. Данная система более уязвима.

На сегодняшний день очень широко используется беспроводные технологии в качестве средств обеспечения охраны периметра здания, также внутренние помещения используют камеры видеонаблюдения. Владелец дома, либо охранник может в режиме онлайн наблюдать все, что происходит в помещениях здания, используя камеры видеонаблюдения. Также система видеонаблюдения имеет свои существенные ошибки, так как злоумышленник даже, находясь на расстоянии без физического доступа к самой системе способен подменить изображение на мониторе. Один из способов выглядит примерно так. Опасность подобных ошибок проектной команды заключается в том, что простое нажатие кнопки сброса настроек (RESET) вернет маршрутизатор к заводским настройкам и, тем самым, позволит обойти любые меры безопасности, которые вы ранее на нем установили.

Защита беспроводной сети – важнейший аспект безопасности. Подключение к интернету с использованием небезопасных ссылок или сетей угрожает безопасности системы и может привести к потере информации, утечке учетных данных и установке в вашей сети вредоносных программ . Очень важно применять надлежащие меры защиты Wi-Fi, рассмотрим одни из самых распространенных это - WEP, WPA.

Беспроводные сети передают данные посредством радиоволн, поэтому, если не

приняты меры безопасности, данные могут быть с легкостью перехвачены. WEP (Wired Equivalent Privacy) — это алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения защиты, передаваемых данных. Также имеются 64, 128, 256 и 512-битное WEP шифрование. Чтоб, была высокая стойкость сети к взлому используют больше бит для хранения ключа, тем самым имея больше возможных комбинацийключа. Одна из основных задач технологии WEP – предотвращение атак , с которой она успешно справлялась в течение определенного времени. Однако, несмотря на изменения протокола и увеличение размера ключа, со временем в стандарте WEP были обнаружены различные недостатки. По мере роста вычислительных мощностей злоумышленникам стало проще использовать эти недостатки. Одна часть ключа WEP является статической т.е., 40бит в случае 64 битного шифрования. Вторая часть является динамической, которая изменяется в процессе работы сети. Для полной защиты данных, соответственно, будет недостаточно 24 бит динамически меняющихся данных ключа. Также в иной раз в беспроводных сетях используют протокол WPA. WPA является более стойким протоколом шифрования, чем протокол WEP.

В WPA также используется алгоритм RC4. Более стойким он является из-за использования динамических ключей сети и протокола проверки целостности пакетов.

Как происходит взлом протоколов WEP? В первую очередь, злоумышленнику необходимо обнаружить сеть, которая охватывает здание. В принципе это легко выполнить с использованием программ сканирования сети. Например, Kismet. Так как WEP зашифровывает только часть фреймов данных, данные находятся в открытом доступе.

Если же WEP не используется в здании, злоумышленник может установить SSID. Злоумышленник может также обойти защиты каналов передачи данных, если они защищены WEP протоколом.

В WEP протоколе ключевой поток зависит от вектора инициализации v и k.k, т.е., фиксированного ключа, не изменяющийся для простоты эксплуатации. Сам ключевой поток зависит только от вектора инициализации, пересылаемый по сети в открытом виде. Из этого следует, что злоумышленник может перехватить пакет с использованным вектором инициализации. После примерно 16 млн. пакетов вектор инициализации обязательно будет повторяться, так как вектор инициализации имеется всего лишь длину 24 бита. А вот длина фиксированного ключа в данном случае совсем не имеет никакой роли.

Ситуация также усложняется тем, что не описано в протоколе алгоритм изменения вектора инициализации. Указывается лишь только его необходимость изменения.

Большинство беспроводных сетевых карт сбрасывают вектор инициализации на 0 при каждом включении и для каждого последующего пакета линейно увеличивают на 1. Т.е., каждая беспроводная сессия начинается с повторного использования пакета ключа.

WPA (Wi-Fi Protected Access) – это протокол, которым объединение Wi-Fi заменило протокол WEP. WPA похож на WEP, однако в нем усовершенствована обработка ключей безопасности и авторизации пользователей.

WEP предоставляет всем авторизованным системам один ключ, а WPA использует протокол целостности временного ключа, динамически изменяющий ключ, используемый системами. Это не позволяет злоумышленникам создать собственный ключ шифрования, соответствующий используемому в защищенной сети.

Кроме того, протокол WPA включает проверку целостности сообщений, чтобы определить, имел ли место захват или изменение пакетов данных злоумышленником. Протокол WPA использует 256-битные ключи, что значительно надежнее 64 и 128-битных ключей, используемых протоколом WEP.

При работе над статьей в качестве теоритического материала использовались следующие источники информации [1, 2, 3].

Таким образом, WEP протокол для защиты от атаки на системы видеонаблюдения, построенные на базе беспроводных технологий, следует использовать более надежные и менее уязвимые протоколы, такой как -WPA.

Литература

1.Редакция. THG. Взламываем. WEP, 2011: [Электронныйресурс].URL: http://www.thg.ru/
network
/20110806/
print
.
html
.(Дата обращения 11.03.2023)

2. Service Set Identifiers. CiscoSystems, Inc. 2011: [Электронныйресурс]
URL:http://www.cisco.com/en/US/docs/routers/access/3200/software/wireless/ServiceSetID.pdf(
Датаобращения
11.03.2023

3. Технологии WEP иWPA: [Электронныйресурс] URL:
https://www.kaspersky.ru/resource-center/definitions/wep-vs-wpa (Дата обращения
11.03.2023)