УДК 004.056.53

БЕЗОПАСНОСТЬ ПЕРЕДАЧИ ДАННЫХ ПО БЕСПРОВОДНЫМ СЕТЯМ

Пичугина Е.Ю., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *информационная безопасность, перехват трафика, MITM-атаки, WLAN.*

Любой, у кого есть ПК и доступ к общедоступной сети, может захватывать сетевой трафик, что может поставить под угрозу конфиденциальность и надежность приложений. Следовательно, для беспроводных приложений обязательно гарантировать аутентификацию, конфиденциальность и целостность данных. В данной статье было рассмотрено основные уязвимости открытой беспроводной сети, перехвата трафика, утечки данных и т.д. Также в статье описывается способы защиты

В течение последнего десятилетия поддержка эффективной и надежной передачи данных по беспроводным сетям была предметом постоянных исследований. Основные проблемы были в области безопасности. Данные сталкиваются с угрозой безопасности во время передачи по беспроводной сети. Действительно, относительно легко подслушивать видео / аудио разговоры или перехватывать и изменять пакеты данных [1].

Взрывной рост беспроводных сетей за последние несколько лет напоминает быстрый рост Интернета в последнее десятилетие.

С появлением технологии беспроводной локальной сети (WLAN), компьютерные сети могут достичь подключения с приемлемым количеством полосы пропускания без подключения к сети через розетку.

Есть несколько основных концепции безопасности: аутентификация, конфиденциальность, целостность информации.

Аутентификация – это процесс подтверждения своей личности другому лицу или компоненту системы. Чем надежнее метод аутентификации, тем больше вы можете быть уверены, что люди, взаимодействующие с системой, являются теми, за кого они себя выдают. Распространенным методом аутентификации является вызов имени пользователя / пароля.

Конфиденциальность достигается путем шифрования. Шифрование-это процесс защиты информации от нежелательных получателей. Поэтому он обеспечивает конфиденциальность и часто используется в сочетании с аутентификацией, чтобы скрыть идентификационную информацию пользователя (например, имя пользователя и пароль) [2].

Целостность информации – это любая аутентификация и конфиденциальность, когда бит так же важен, как и безопасная передача информации между двумя сторонами. Целостность данных сохраняется с помощью цифровых подписей. Это механизм, используемый для проверки того, что часть информации поступила из источника, признанного системой, и не была изменена непризнанной стороной с авторизацией [3].

Рассмотрим вариант атаки *MITM*-атаки (*Man-in-the-Middle*)

Концепция MITM-нападения (Man-in-the-Middle) на удивление проста, и она не ограничивается безопасностью компьютера или онлайн-ресурса. В самом простом случае злоумышленнику надо всего лишь поставить себя в цепь между двумя общающимися сторонами, чтобы перехватывать их сообщения друг другу. При этом злоумышленник всегда должен выдавать себя за каждую из противоположных сторон.

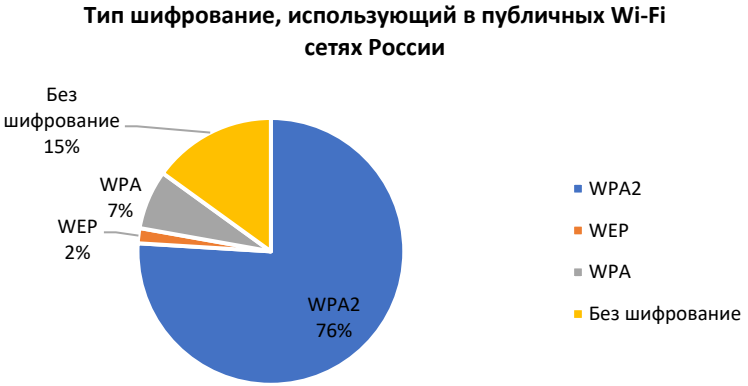
Больше всего распространены MITM-атаки, когда злоумышленник использует Wi-Fi-маршрутизатор в качестве инструмента перехвата сообщений. В данном случае создается подмена используемого роутера и подмена самой сети. Либо используются ошибки в настройке и защите сети, позволяющие вполне легально перехватывать сессии.

Например, злоумышленник настраивает в своем ноутбуке точку беспроводного доступа, давая ей то же имя, что и используемое в общественном месте с доступным Wi-Fi. Когда пользователи подключаются к этой псевдосети, то при попытке совершить какое-либо действие с коммерческими сайтами, банковскими или прочими финансовыми

ресурсами, их информация перехватывается, после чего злоумышленник уже может пользоваться ей по своему усмотрению.

Есть много вариантов, которые организации могут сделать сегодня, чтобы поставить надлежащую защиту безопасности вокруг своей беспроводной стратегии и технологии.

Согласно данным Kaspersky Security Network, что доля точек, в которых применяется довольно надежный протокол WPA2, в целом по России составляет чуть менее 76%:



Существует несколько эффективных средств защиты от MITM-атак, но почти все они используются либо в самом маршрутизаторе, либо на серверах, к которым обращается потенциальная жертва. При этом самой жертве непонятно, на настоящем она сервере либо это подделка, подставленная злоумышленником. Одним из способов защиты от такой атаки является использование стойкого шифрования между клиентом и сервером [4].

В таком случае сервер может идентифицировать себя посредством предоставления цифрового сертификата, после чего между пользователем и сервером устанавливается шифрованный канал для обмена конфиденциальными данными. Но в этом случае возникает зависимость от самого сервера и выбора им метода шифрования.

Безопасность беспроводной сети постоянно дорабатывается, протоколы развиваются для удовлетворения потребностей пользователей.

Библиографический список:

1. Kasperskiy daily [Электронный ресурс]. - Режим доступа: https://www.kaspersky.ru

2. Callegati, F., Cerroni, W., Ramilli, M.: Man-in-the-middle attack to the HTTPS protocol. IEEE Security Privacy **7**, 78-81 (2009)

3. Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A., Shrawne, S.: Vulnerabilities of wireless security protocols (WEP and WPA2). Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **1**(2), 34–38 (2012)

4. MITM-атака [Электронный ресурс]. - Режим доступа: http://ru.wikipedia.org

SECURITY OF DATA TRANSFER BY SOFTWAREWIRELESS NETWORK

Pichugina E.U.

Keywords: *information security, traffic interception, MITM attacks, WLAN.*

Anyone with a PC and access to a public network can hijack network traffic, which can compromise the privacy and reliability of applications. Therefore, it is imperative for wireless applications to guarantee authentication, confidentiality and data integrity. This article examined the main vulnerabilities of an open wireless network, traffic interception, data leakage, etc. The article also describes the methods of protection.