УДК 004.732
DOI 10.21685/2587-7704-2019-4-1-4

Open Access | RESEARCH ARTICLE

Анализ основных угроз, уязвимостей и методов защиты беспроводных сетей

И. А. Костров
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

А. П. Иванов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. В статье рассматриваются основные угрозы и уязвимости локальных беспроводных сетей в организациях, а также методы защиты информации от утечек по этим сетям. Предложен перечень мер, обеспечивающий необходимый уровень защищенности информации в большинстве современных организаций.

Ключевые слова: беспроводные сети, информация, защита информации, угроза, уязвимость.

Analysis of main threats, vulnerabilities and methods to protect wireless networks

I. A. Kostrov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

A. P. Ivanov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The article considers main threats and vulnerabilities of local wireless networks in organizations, as well as methods to protect information against leaks via these networks. A list of measures providing the necessary level of information security in most modern organizations is proposed.

Keywords: wireless networks, information, information protection, threat, vulnerability.

В современном мире локальные беспроводные сети, такие как Wi-Fi, Bluetooth и т.п., а также сети сотовой связи имеют огромное распространение. Практически любая современная организация использует данные сети для передачи различной информации. Несмотря на свое постоянное развитие, данные сети имеют множество пробелов в системе безопасности, что позволяет злоумышленникам осуществлять перехват информации. Соответственно, организациям необходимо обеспечивать защиту информации от утечек как по локальным беспроводным сетям, так и по сетям сотовой связи.

Для того чтобы обеспечивать требуемый уровень защищенности информации, необходимо знать существующие угрозы и уязвимости беспроводных сетей. К основным угрозам, которым подвергаются беспроводные сети, можно отнести:

– прослушивание сети;
– отказ в обслуживании;
– кражу ресурсов;
– перехват и изменение передаваемых данных;
– глушение клиентской или базовой станции.

Прослушивание незащищенных каналов передачи информации в беспроводных сетях обычно используется злоумышленником для сбора информации о сети, на которую планируется дальнейшая атака. Оборудование для реализации прослушивания обычно не отличается от того, которое исполь-

зуется для обычного санкционированного доступа к данной беспроводной сети. Если канал беспроводной сети не является защищенным, то атаку посредством пассивного прослушивания обнаружить крайне сложно.

Кроме сбора информации о беспроводной сети, с помощью прослушивания также возможно получить какие-либо конфиденциальные сведения, утрата которых способна нанести ущерб организации.

Угроза типа «отказ в обслуживании» в результате своей реализации создает помехи при попытках доступа пользователей к беспроводной сети и ее ресурсам. Беспроводные сети являются крайне восприимчивыми к атакам, приводящим к отказам в обслуживании, так как для создания таких отказов достаточно лишь создать с помощью каких-либо устройств помехи на рабочей частоте беспроводной сети. Факт проведения атаки такого типа на беспроводную сеть доказать крайне трудно.

Кража ресурсов предполагает, что злоумышленник не имеет прямой цели получить конфиденциальную информацию организации, передающуюся в беспроводных сетях, а использует ресурсы беспроводной сети в личных целях, например для бесплатного доступа в Интернет. Как уже сказано, данные действия не несут прямой угрозы для информации, но они значительно снижают уровень защищенности сети от других атак, а также отнимают ресурсы сети у санкционированных пользователей.

Угроза перехвата и изменения передаваемых данных обычно реализуется с использованием атаки «человек посередине». Провести данную атаку на беспроводную сеть значительно проще, чем на проводную, так как в случае проводной сети необходим физический доступ к ней. Атаки данного типа используются как для нарушения целостности сеанса связи, так и для получения конфиденциальных сведений, передаются по данному каналу связи. Для проведения такой атаки злоумышленник должен обладать подробной информацией о беспроводной сети.

Глушение клиентской или базовой станции предоставляет злоумышленнику возможность либо представить себя на месте «заглушенного» клиента и получать предназначавшийся ему трафик, либо подменить «заглушенную» базовую станцию атакующей станцией злоумышленника. Глушение станций также может быть случайным, например, из-за помех на рабочей частоте, что приводит к отказу в обслуживании.

Данный перечень не является исчерпывающим, но он демонстрирует общую направленность угроз беспроводным сетям.

К возможности реализации угроз безопасности беспроводных сетей приводит наличие большого количества уязвимостей этих сетей, причем во многих организациях не применяются необходимые защитные меры по их устранению. Таким образом, к основным уязвимостям беспроводных сетей можно отнести:

– использование широковещательного радиомаяка;
– простоту обнаружение сети;
– простые протоколы криптозащиты;
– возможность создания ложной точки доступа к сети;
– простоту физического доступа;
– анонимность атак.

Использование широковещательного радиомаяка. Для того чтобы сообщить окрестным беспроводным узлам о своем присутствии, беспроводная точка доступа использует широковещательный радиомаяк, работающий на определенной частоте. Сигнал этого маяка содержит основную информацию о точке доступа и приглашает беспроводные узлы в зоне охвата подключиться к этой точке. В рассылаемом сигнале содержится SSID (идентификатор SSID представляет собой уникальный 32-значный буквенно-цифровой код, используемый для идентификации беспроводной локальной сети [1]), соответственно, устройство, получившее значение данного идентификатора, может беспрепятственно подключиться к беспроводной сети.

Простота обнаружения сети. С помощью простых утилит, таких как, например, NetStumber (NetStumber – это маленькая бесплатная утилита для поиска и настройки беспроводных сетей [2]), можно обнаруживать локальные беспроводные сети, а также определять некоторые их внутренние параметры. К таким параметрам относятся идентификатор SSID сети, а также информация об используемом методе шифрования в беспроводной сети.

Простые протоколы криптозащиты. В большинстве беспроводных сетей в качестве алгоритма шифрования используется достаточно простой алгоритм WEP. У данного алгоритма при исследованиях были выявлены уязвимости, которые позволяются восстановить используемый ключ шифро-

вания при перехвате незначительного количества трафика. Следовательно, использование данного алгоритма шифрования не обеспечивает защиты от атак опытных злоумышленников.

Возможность создания ложной точки доступа. Злоумышленник может осуществить полную имитацию сетевых ресурсов оригинальной точки доступа, при этом абоненты сети не будут ничего подозревать, подключаясь к данной точке. Таким образом злоумышленник может получить важную для него информацию.

Простота физического доступа. Злоумышленник для проведения различных атак на беспроводную локальную сеть может осуществить непосредственное физическое подключение к точке доступа, так как часто сами точки беспроводного доступа не защищены от такого подключения.

Анонимность атак. Для проведения атаки злоумышленник может находиться в любой точке действия беспроводной сети, и без соответствующего оборудования определить его местоположение, а значит, и установить личность не представляется возможным.

Для обеспечения необходимого уровня безопасности беспроводных сетей в организации необходимо избавиться от указанных уязвимостей путем использования различных защитных мер. Рассмотрим необходимые для принятия защитные меры с привязкой к конкретным, указанным ранее уязвимостям.

У каждой беспроводной точки доступа есть возможность отключения широковещательной передачи идентификатора SSID. В этом случае SSID будет скрыт, и каждому пользователю необходимо будет вручную прописывать этот идентификатор для подключения к данной локальной сети. Соответственно, этот идентификатор должны знать только санкционированные пользователи беспроводной сети.

Отключение широковещательной рассылки идентификатора SSID также усложнит обнаружение беспроводной сети. Усложнить его можно и с помощью снижения мощности передачи у точки беспроводного доступа, если ее функционал это позволяет.

Для обеспечения большой криптостойкости шифрованного трафика необходимо использовать более стойкие алгоритмы шифрования, такие как WPA и WPA2. WPA2 отличается от WPA поддержкой более стойкого шифрования AES, поэтому все же более предпочтительным со стороны обеспечения безопасности является использование алгоритма WPA2.

Чтобы защититься от создания ложной точки доступа к сети, можно использовать цифровые сертификаты и аутентификацию по методу EAP-TLS. При использовании цифровых сертификатов узел беспроводной сети и сервер аутентификации проверяют по ним подлинность друг друга. В таком случае созданная ложная точка доступа не сможет пройти проверку подлинности и будет вычислена.

Защиту от физического подключения к точке беспроводного доступа организовать несложно. Достаточно поместить ее в контролируемую зону и ограничить к ней доступ всех лиц, за исключением администраторов беспроводной сети.

Подводя итог, можно сказать, что для обеспечения безопасности беспроводной сети организации необходимо:

– использовать современные методы шифрования, аутентификации и фильтрации MAC-адресов;

– обеспечивать физическую защиту беспроводных точек доступа;

– не пренебрегать классическими мерами безопасности – осуществлять своевременную установку обновлений, использовать антивирусные программы, проводить мониторинг сети.

Некоторые организации в целях обеспечения безопасности вовсе отказываются от использования локальных беспроводных сетей. Но даже в этом случае нельзя говорить о полной защищенности организации от утечек по беспроводным сетям. Если использование мобильных телефонов на территории организации не регламентировано, то это создает канал утечки, так как практически все современные телефоны могут работать в качестве беспроводной точки доступа. Поэтому на сегодняшний день организациям необходимо дополнительно разрабатывать комплекс организационно-режимных и технических мер, предотвращающих утечки по такому каналу.

Библиографический список

1. Информационный портал «Лайфхакер». NetStumbler – бесплатная ищейка беспроводных сетей. – URL: https://lifehacker.ru/netstumbler-besplatnaya-ischeyka-besprovodnyih-setey/, свободный. (дата обращения: 14.10.2018).
2. Официальный сайт компании «Netgear». Что такое SSID беспроводной сети. – URL: https://kb.netgear.com /ru/22374/Что-такое-SSID-беспроводной-сети-1479991184049, свободный. (дата обращения: 14.10.2018).

Образец цитирования:

Костров, И. А. Анализ основных угроз, уязвимостей и методов защиты беспроводных сетей / И. А. Костров, А. П. Иванов // Инжиниринг и технологии. – 2019. – Vol. 4(1). – С. 1–4. – DOI 10.21685/2587-7704-2019-4-1-4.