УДК 621. 05

БЕЗОПАСНОСТЬ СЕТЕЙ В СТАНДАРТЕ IEEE 802.11

М.В. Ковалевская, магистрант,
Д.А. Довгяло, канд. техн. наук, доц.
Полоцкий государственный университет имени Евфросинии Полоцкой, Новополоцк, Беларусь

Рассматриваются вопросы безопасности в беспроводных локальных сетях стандарта IEEE 802.11. Описаны технологии защиты и некоторые способы взлома беспроводных сетей закрытого типа WEP, WPA, WPA2, WPA3.

Ключевые слова: *беспроводные сети, безопасность, фильтрация, технология защиты Wi-Fi, протоколы шифрования.*

С момента ратификации стандарта IEEE 802.11b в 1999 году беспроводные локальные вычислительные сети (ЛВС) получили широкое распространение. Сегодня их можно встретить во многих офисах, конференц-залах, на промышленных складах, в школьных классах. Беспроводные ЛВС стандарта IEEE 802.11b представляют собой ряд новых проблем для администраторов сетей и систем безопасности.

В отличие от проводных сетей Ethernet, беспроводные ЛВС стандарта IEEE 802.11b используют общедоступный радиоканал для связи с абонентами. Этот факт лежит в основе целого ряда новых сложных проблем, решение которых потребовало дополнений к стандарту IEEE 802.11.

На данный момент большинство фирм и предприятий все больше внимания уделяют использованию непосредственно Wi-Fi-сетей. Обусловлено это удобством, мобильностью и относительной дешевизной при связи отдельных офисов и возможностью их перемещения в пределах действия оборудования. В Wi-Fi-сетях применяются сложные алгоритмические математические модели аутентификации, шифрования данных, контроля целостности их передачи, что позволяет быть относительно спокойным за сохранность данных при использовании данной технологии.

Несмотря на положительные характеристики беспроводных ЛВС, существует и негативный аспект их применения, к которому можно отнести высокую незащищенность от помех, создаваемых как искусственно, так и в результате естественных причин, возможность перехвата нарушителем информативного сигнала, либо управления, навязывание ложных данных.

Безопасность функционирования и защита информации, передаваемой в беспроводных сетях, является достаточно серьезной задачей и проблемой, решение которой должно обеспечиваться на высоком техническом уровне. Для обеспечения безопасности сети согласно ГОСТ Р 59162-2020 необходимо чтобы обеспечивались:

– конфиденциальность: передаваемая информация не должна разглашаться (злоумышленник не должен прослушивать сеть);

– целостность: передаваемая информация не должна изменяться при передаче (злоумышленник не должен изменять или подменять передаваемые данные);

– доступность: услуги сети должны быть доступны (злоумышленник не должен мешать функционированию сети);

– аутентификация: подлинность пользователей или объектов, запрашивающих доступ к сети, должна быть подтверждена (злоумышленник не должен выдавать себя за санкционированного пользователя);

– контроль доступа: доступ к сетям и AP (англ. Access Point) должен контролироваться (злоумышленник не должен подменять сеть и AP);

– подконтрольность: любое нарушение политики должно быть прослежено до конкретного пользователя или субъекта (злоумышленник не должен иметь возможность скрывать свою активность в сети) [1].

В настоящее время существуют и применяются различные способы защиты беспроводных сетей стандарта IEEE 802.11, которые можно разделить на защиту:

– техническими способами:

1) WEP (Wired Equivalent Privacy) – протокол шифрования, основанный на алгоритме шифрования RC4 с 40, 104, 128 и 256-битными ключами, который складывается со сгенерированным вектором инициализации (24 бит) [2];

2) WPA (Wi-Fi Protected Access) – протокол шифрования, применяющий ключ 256-бит и паролей длиной от 8 до 63 байт, добавлена проверка целостности сообщений и протокол целостности временного ключа – TKIP (Temporal Key Integrity Protocol), позже замененный на AES (Advanced Encryption Standard);

3) WPA2 – протокол шифрования, использующий криптографический алгоритм AES совместно с режимом счетчика с протоколом кода аутентификации сообщений с алгоритмом блочного шифрования;

4) WPA3 – является новейшим протоколом шифрования, дополняющим и улучшающим перечисленные выше технологии, использует метод аутентификации устройства, применяющий криптографию для предотвращения получения пароля пользователя SEA (Simultaneous Authentication of Equals), поддерживает PMF (Protected Management Frames) для контроля целостности трафика [3];

5) фильтрация по MAC-адресу (на маршрутизаторе выключается возможность подключения устройств, которых нет в списке разрешенных адресов либо администратор запрещает сопряжение беспроводного устройства, которое ранее уже имело доступ к сети, указанная технология не предусматривается стандартами;

6) скрытие SSID (Service Set Identifier) – является техническим адресом устройства или идентификатором набора базовых услуг для защиты сети осуществляется отключение передачи в открытый радиоэфир SSID, после этого подключиться к сети возможно, только если знать название данного SSID;

7) WIDS (Wireless Intrusion Detection Systems) – система беспроводного обнаружения вторжений, путем мониторинга радиоэфира обнаруживают несанкционированные AP, анализируют полученные данные и на основе этой информации осуществляют предупреждение администратора о наличии подозрительной AP, о блокировании ее активности или действий неавторизованного пользователя;

8) WIPS (Wireless Intrusion Prevention System) – система предотвращения вторжений, позволяет определять и реагировать на различные сетевые атаки (DoS, Honeypot, MITM и др.), подмену MAC-адресов, неправильно настроенные или несанкционированные AP);

– организационную: физическое ограничение доступа посторонних лиц к AP, контроль выданных паролей для доступа пользователей к беспроводной сети (в больших организациях), обучение пользователей основам безопасного и защищенного использования AP.

Обозначим наиболее типичные из существующих уязвимостей и угроз безопасности стандарта IEEE 802.11. Угрозы безопасности информации беспроводных сетей в той или иной степени реализуются применением следующих способов:

– поддельная точка доступа;
– неправильно настроенная точка доступа;
– анализ пакетов;
– несанкционированный доступ (НСД);
– мошенничество;
– атака «отказ в обслуживании»;
– угрозы в сетях Ad-Hoc;
– прослушивание сети;
– создание помех или глушение сигнала;
– атаки на протоколы защиты сетей Wi-Fi;
– критическая уязвимость KRACK в протоколе защиты WPA2.

Аутентификация в беспроводных сетях подразумевает то, что точка доступа является той, которой себя называет. Как правило, она основывается на знании общей конфиденциальной информации, такой как, пара – имя пользователя и пароль, в более сложных системах данной общей информацией может являться проверка сертификатов или ключей.

RADIUS (Remote Authentication in Dial-In User Service) – протокол для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах. RADIUS-сервер интегрирован с абонентской базой данных зарегистрированных пользователей и является частью биллинговой политики сети. Механизм WPA2-PSK использует упрощенный алгоритм аутентификации (по паролю) без использования RADIUS-сервера.

Обобщенный процесс аутентификации с использованием RADIUS-сервера отображен на рисунке 1.

Клиент инициирует процесс аутентификации с помощью сообщения EAPOL-start. Аутентификатор запрашивает идентификатор клиента, который затем передает серверу. В запросе аутентификатора содержится информация о выбранном методе EAP.

Затем сервер запрашивает через аутентификатор единовременный пароль OTP (One-Time Password) клиента, который представляет собой 64-битовое сообщение MD5. После проверки OTP сервер разрешает или запрещает доступ устройству к сети.

Для перехода в неавторизованное состояние клиент посылает сообщение EAPOL-logoff.

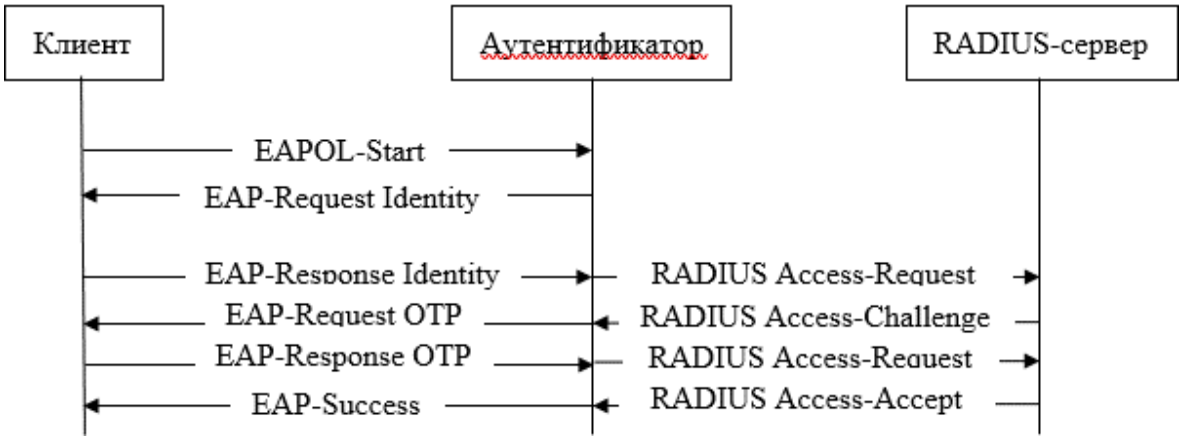

Рисунок 1. – Аутентификация абонента с использованием RADIUS-сервера

ЛИТЕРАТУРА

1. Атаки на сеть WI-FI вида WEP/WPA/WPA2 и методы борьбы с ними/Ахметова Б.А. [и др.] // Вес. современных исследований. –2020. – № 8-1(38). – С. 4–7.
2. Белетова, Д.У. Использование стандарта IEEE 802.1x для защиты от НСД/ Д.У. Белетова // Электронный журнал: наука, техника и образование. –2017. – № 1(10). –С. 6–15.
3. Кухта, А. И. Анализ методов защиты беспроводной сети Wi-Fi. / А.И. Кухта // Молодой исследователь Дона.– 2020. –№ 2(23). –С. 41–48.
4. Ковалев, Д. Механизмы аутентификации и управления ключами стандарта IEEE 802.11-2012 / Д. Ковалев // Первая миля. – 2014. –№ 3 (42). – С. 72–77.